The Protection of banking customers from the risks of mobile payments in Saudi Arabia

Mohammed Ibrahim Alhamzi

A Thesis Submitted in Partial Fulfilment of the

Requirement for the Degree of Doctor of Philosophy

School of Law

University of Kent

May 2018

ABSTRACT

ABSTRACT

Demand for mobile payment (m-payment) services is transforming the banking payment system in unprecedented ways[1] and at a growing rate.[2] These developments raise unique concerns and risks[3] which must be managed by the adoption of an appropriate regulatory framework if this 'Fintech'[4] innovation is to offer a net social and economic benefit.[5]

This work will draw on Western and Islamic consumer protection literature to analyse how Saudi Arabian law at present protects consumers when it comes to m-payments, particularly unauthorised mobile payment transactions and consumer data in order to maintain privacy and protect them against breaches of their privacy. In so doing, the research seeks to make an original contribution to the Saudi Arabian legal system in the presently under-researched areas of both consumer protection and m-payment services. It will be demonstrated that the Saudi Arabian legal provisions are inadequate and fall

[1] A.A. Shaikh and H. Karjaluoto, 'Mobile banking adoption: A literature review' (2015) *Telematics and Informatics 32* (1), 129-142.
[2] P.A. Salz, *The Netsize Guide 2009: Mobile Society & Me, when worlds combine* (Netsize 2009) 102; S. Romero, 'The unstoppable growth of digital banking: 3 billion users by 2021', BBVA, 22 February 2017 <https://www.bbva.com/en/unstoppable-growth-digital-banking-3-billion-users-2021/> 19th November 2017.
[3] A. Zercan, *New Technologies, New Risks?: Innovation and Countering the Financing of Terrorism* (World Bank 2010) 11.
[4] The Oxford Dictionary defines Fintech as "[c]omputer programs and other technology used to support or enable banking and financial services." Oxford Dictionary, 'Fintech', 2017 <https://en.oxforddictionaries.com/definition/fintech> accessed 20th May 2017.
[5] G.G. Kaufman et al, *Achieving Financial Stability: Challenges To Prudential Regulation* (World Scientific 2017) 270.

short of the requirements of Sharia law in many respects: Consumer protection is insufficient and is not appropriately targeted to address the specific, unique risks raised by m-payment services.[6] At the same time, restrictive legislation designed in the context of traditional banking has created a hostile regulatory environment which has failed to stimulate innovation and growth within this potentially promising sector.

With a view to proposing a model for reform of Saudi regulation, the United Kingdom ('UK') legal system will be scrutinised to assess whether lessons can be learnt in providing greater protection to customers in a Saudi Arabian context while remaining Sharia compliant. The UK is a valuable selection as a comparator as it has succeeded in balancing these objectives to a significant extent, achieving greater consumer protection than is currently available in Saudi Arabia ('SA') without compromising the strength and freedom of the market. There are also strong parallels between the two societies particularly in respect of openness to Fintech innovation.[7] It will be proposed that the UK law provides a positive example of how this systematic defect in the regulation of m-payments can be remedied, in addition to more specific illustrations of provisions and policies which can aid in balancing the demands of consumer protection and market development. Recommendations are made as to how these can be usefully incorporated into a broader reform of the Saudi regulatory regime.

---

[6] A.S. Albaqme, 'Consumer Protection under Saudi Arabia Law' (2014) *Arab Law Quarterly* 28(2), 158-175.

[7] Saudi Arabian Monetary Authority, 'Saudi Arabian Monetary Authority Launches FintechSaudi with the Objective to Make the Kingdom a Pioneer in the Financial Technology Sector', 1 May 2018 <http://www.sama.gov.sa/en-US/News/Pages/news30042018.aspx> accessed 6 March 2019; Sir Mark Walport, *FinTech Futures: The UK as a World Leader in Financial Technologies*, Report of the UK Government Chief Scientific Adviser, March 2015, 1-68, 5.

ACKNOWLEDGEMENTS

ACKOWLEDGEMENTS

I would like to express my sincere gratitude to several people whose wonderful and continuous encouragement and support have been very important in enabling me to finish this thesis.

First and for most I owe deep sincere gratitude to my supervisors, Dr Simone Wong, Dr Asta Zokaityte and Professor Robin Mackenzie. You not only set an aspirational standard of excellence through your own work, but provided invaluable guidance, encouragement, patience, motivation, constructive feedback and tireless efforts throughout my studies. You led by example and inspired me to work my hardest.

I would also like to express my gratitude to Lynn Osborne, the postgraduate officer at the school of law. Without your limitless help the past years would doubtlessly have been much harder.

Finally, I would like to express sincere gratitude to my parents, my beloved wife, my wonderful children. You have been very supportive and very patient. I cannot thank you enough.

CONTENTS

TABLE OF CONTENTS

LIST OF ABBREVIATIONS

LIST OF ABBREVIATIONS

AIS	Account Information Services
AML	Anti-Money Laundering
AML Law 2003	Anti-Money Laundering Law 2003
API	Application Programming Interface
ATM	Automated Teller Machine
BBA	British Bankers Association
BCOBS	Banking Conduct of Business Sourcebook
CCR 2006	Consumer Credit Regulations 2006
CIL 2008	Credit Information Law 2008
CMA	Competition and Markets Authority
CRA 2015	Consumer Rights Act 2015
CTF	Counter-Terrorist Finance Initiative
DPA 1998	Data Protection Act 1998
EBA	European Banking Association

e-banking	Electronic Banking Model
EEA	European Economic Area
e-money	Electronic Money
EMR 2011	Electronic Money Regulations 2011
EMV	Europay, Mastercard, and Visa
ETL 2007	Electronic Transaction Law 2007
EU	European Union
FATF	Finance Action Task Force
FCA	Financial Conduct Authority
Fintech	Finance Technology
FSMA	Financial Services and Markets Act 2011
FTR 2015	EU Funds Transfer Regulation 2015
FUI	Financial Intelligence Unit
GPS	Global Positioning System
GSM	Global System for Mobile Communication
HCE	Host Card Emulation
ICO	Information Commissioner's Office
ICT	Information Communication Technologies

ID	Identity Card
IMEI	International Mobile Subscriber Identity
IT	Information Technology
KYC	Know Your Customer
m-banking	Mobile Banking
Mobile	Mobile Phone
m-payment	Mobile Payment
NFC	Near-Field Communications
OFCOM	Office of Communications
P2P	Peer to Peer
PC	Personal Computer
PI	Payment Institution
PIN	Personal Identification Number
PIS	Payment Initiation Services
PISP	Payment Initiation Service Provider
POS	Point of Sale
PRA	Prudential Regulation Authority
PRA	Prudential Regulation Authority

PSD	Payment Services Directive
PSR 2017	Payment Services Regulations 2017
PSR	Payment Systems Regulator
RFID	Radio-Frequency Identification
RRPPS 2012	Regulatory Rules for Prepaid Payment Services 2012
SA	Saudi Arabia
SAMA	Saudi Arabian Monetary Authority
SAR	Suspicious Activity Report
SIMAH	Saudi Arabia Credit Bureau
SLP	Standards of Lending Practice 2016
SPAN	Saudi Arabian Payments Networks
SMS	Short Message Service
SSL	Secure Sockets Layer
TPP	Third-Party Payment Provider
UCTA	Unfair Contract Terms Act 1977
UK	United Kingdom
UNGCP	United Nations Guidelines for Consumer Protection
URL	Uniform Resource Locator

UTCCR	Unfair Terms in Consumer Contracts Regulations 1999
WAP	Wireless Application Protocol
Wi-Fi	Wireless Fidelity

TABLE OF LEGISLATION

TABLE OF LEGISLATION

1. EU Legislation

Communications Act 2003

Directive (EU) 2015/849 of the European Parliament and of the Council of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, amending Regulation (EU) No 648/2012 of the European Parliament and of the Council, and repealing Directive 2005/60/EC of the European Parliament and of the Council and Commission Directive 2006/70/EC

Directive 2000/46/EC of the European Parliament and the Council on the taking up and prudential supervision of the business of electronic money institutions

Directive 2002/19/EC of the European Parliament and of the Council of 7 March 2002 on access to, and interconnection of, electronic communications networks and associated facilities

Directive 2002/21/EC of the European Parliament and of the Council of 7 March 2002 on a common regulatory framework for electronic communications networks and services

Directive 2006/48/EC of the European Parliament and of the Council of 14 June 2006 relating to the taking up and pursuit of the business of credit institutions

Directive 2007/64/EC on payment services in the internal market amending Directives 97/7/EC, 2002/65/EC, 2005/60/EC and 2006/48/EC and repealing Directive 97/5/EC, OJ L 319/1

Directive 2009/110/EC on the taking-up, pursuit and prudential regulation of the business of electronic money institutions amending Directives 2005/6-/EC and 2006/48/EC and repealing Directive 2000/46/EC

Directive 2009/140/EC of the European Parliament and of the Council of 25 November 2009 amending Directives 2002/21/EC on a common regulatory framework for electronic communications networks and services, 2002/19/EC on access to, and interconnection of, electronic communications networks and associated facilities, and 2002/20/EC on the authorisation of electronic communications networks and services, which amended both the Access and Framework Directive

Directive 2014/17/EU of the European Parliament and of the Council of 4 February 2014 on credit agreements for consumers relating to residential immovable property and amending Directives 2008/48/EC and 2013/36/EU and Regulation (EU) No 1093/2010

Directive 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU)

No 1093/2010, and repealing Directive 2007/64/EC (Text with EEA relevance)

Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data

European Union Funds Transfer Regulation 2015/847

General Data Protection Regulation (Regulation (EU) 2016/679)

Treaty on the Functioning of the European

Communications Act 2003

Directive 2013/36/EC of the European Parliament and of the Council of 26 June 2013 on access to the activity of credit institutions and the prudential supervision of credit institutions and investment firms, amending Directive 2002/87/EC and repealing Directives 2006/48/EC and 2006/49/EC

Directive 2015/849 of the European Parliament and of the Council of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, amending Regulation (EU) No 648/2012 of the European Parliament and of the Council, and repealing Directive 2005/60/EC of the European Parliament and of the Council and Commission Directive 2006/70/EC

Directive 2000/46/EC of the European Parliament and the Council on the taking up and prudential supervision of the business of electronic money

institutions

Directive 2002/19/EC of the European Parliament and of the Council of 7 March 2002 on access to, and interconnection of, electronic communications networks and associated facilities

Directive 2002/21/EC of the European Parliament and of the Council of 7 March 2002 on a common regulatory framework for electronic communications networks and services

Directive 2006/48/EC of the European Parliament and of the Council of 14 June 2006 relating to the taking up and pursuit of the business of credit institutions

Directive 2007/64/EC on payment services in the internal market amending Directives 97/7/EC, 2002/65/EC, 2005/60/EC and 2006/48/EC and repealing Directive 97/5/EC, OJ L 319/1

Directive 2009/110/EC on the taking-up, pursuit and prudential regulation of the business of electronic money institutions amending Directives 2005/6-/EC and 2006/48/EC and repealing Directive 2000/46/EC

Directive 2009/140/EC of the European Parliament and of the Council of 25 November 2009 amending Directives 2002/21/EC on a common regulatory framework for electronic communications networks and services, 2002/19/EC on access to, and interconnection of, electronic communications networks and associated facilities, and 2002/20/EC on the authorisation of electronic communications networks and services, which amended both the

Access and Framework Directive

Directive 2014/17/EU of the European Parliament and of the Council of 4 February 2014 on credit agreements for consumers relating to residential immovable property and amending Directives 2008/48/EC and 2013/36/EU and Regulation (EU) No 1093/2010

Directive 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC (Text with EEA relevance)

Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data

European Union Funds Transfer Regulation 2015/847

General Data Protection Regulation (Regulation (EU) 2016/679)

Treaty on the Functioning of the European

2. Saudi Arabian Legislation

Anti-Money Laundering Law 2003

Banking Control Law 1966

Basic Law of Governance of 1992

Charter of the Saudi Arabian Monetary Agency 1957

Consumer Credit Regulations 2006

Credit Information Law 2008

Electronic Transaction Law 2007

Financial Services (Banking Reform) Act 2013

Regulations for Consumer Financing 2014

Saudi Credit Information Law 2008

3. UK Legislation

Banking Act 2009

Communications Act 2003

Consumer Rights Act 2015

Data Protection Act 1984

Data Protection Act 1998

Electronic Money (Miscellaneous Amendments) Regulations 2002

Electronic Money Regulations 2011

Financial Services (Banking Reform) Act 2013

Financial Services (Banking Reform) Act 2013

Financial Services and Markets Act (Regulated Activities) Order 2001

(Statutory Instrument 2001/544) (Statutory Instrument 2001/544)

Financial Services and Markets Act 2000

Financial Services and Markets Act 2000 (Carrying on Regulated Activities by Way of Business) Order 2000 (Statutory Instrument 2001/1177)

Financial Services and Markets Act 2000 (Carrying on Regulated Activities by Way of Business)(Amendment) Order 2014 (Statutory Instrument 2014/3340)

Financial Services and Markets Act 2000 (Prescribed Financial Institutions) Order 2013

Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017

Payment Services Regulations 2009

Privacy and Electronic Communications (EC Directive) Regulations 2003

Sale of Goods Act 1979

Supply of Goods and Services Act 1982

Unfair Contract Terms Act 1977

Unfair Terms in Consumer Contracts Regulations 1999

Wireless Telegraphy Act 2006

Communications Act 2003

Consumer Rights Act 2015

Data Protection Act 1984

Data Protection Act 1998

Electronic Money (Miscellaneous Amendments) Regulations 2002

Electronic Money Regulations 2011

Financial Services (Banking Reform) Act 2013

Financial Services (Banking Reform) Act 2013

Financial Services and Markets Act (Regulated Activities) Order 2001 (Statutory Instrument 2001/544) (Statutory Instrument 2001/544)

Financial Services and Markets Act 2000

Financial Services and Markets Act 2000 (Carrying on Regulated Activities by Way of Business) Order 2000 (Statutory Instrument 2001/1177)

Financial Services and Markets Act 2000 (Carrying on Regulated Activities by Way of Business) (Amendment) Order 2014 (Statutory Instrument 2014/3340)

Financial Services and Markets Act 2000 (Prescribed Financial Institutions) Order 2013

Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017

Payment Services Regulations 2009

Privacy and Electronic Communications (EC Directive) Regulations 2003

Supply of Goods and Services Act 1982

Unfair Contract Terms Act 1977

Unfair Terms in Consumer Contracts Regulations 1999

Wireless Telegraphy Act 2006

4. South Korea Legislation

Electronic Financial Transaction Act No. 11087

5. Kenyan Legislation

National Payment Systems Act 2011

TABLE OF CASES

TABLE OF CASES

1. Saudi Arabian Cases

Abdullah Girgi Beserani v Ismale Fawzi Abu Khadra (1996) Board of Grievance, Case No. 2195

2. EU Case Law

Case C-362/14 *Maximillian Schrems v Data Protection Commissioner*

3. UK Cases

Agip (Africa) Ltd v Jackson (1989) 3 WLR 1367

Baden v Societe Generale (1983) BCLC 325

Bairstow Eves London Central Ltd v Smith (2008) EWHC 263

Bankers Insurance Co Ltd v South (2003) EWHC 380

Belmont Finance Corp Ltd v Williams Furniture Ltd (No 2) (1980) 1 All ER 393

Bond v British Telecommunications plc, Unreported, 28 March 2008, Walsall CC

Broadwater Manor School v Davis, unreported 8 January 1999, Worthing CC

Cavendish Square Holding BV v Makdessi; ParkingEye Ltd v Beavis (2015)

UKSC 67, (2015) 3 WLR 1383

Director General of Fair Trading v First National Bank (2001) UKHL 52

Director General of Fair Trading v First National Bank plc (2000) 1 All ER 240

Domsalla (t/a Domsalla Building Services) v Dyason (2007) EWHC 1174 (TCC), (2007) BLR 348

Durant v Financial Services Authority (2003) EWCA Civ 1746

Falco Finance Ltd v Gough (1999) CCLR 16

Falco Finance Ltd v Michael Gough Unreported 28 October 1998, Macclesfield CC

Greenwoods v Martins Bank (1933) AC 51

Heifer International Inc v Helge Christiansen (2007) EWHC 3015

Joachimson v Swiss Bank Corporation (1921) 3 KB 110

Libyan Arab Foreign Bank v Bankers Trust & Pharaon v BCCI (1989) AC 80

Lipkin Gorman v Karpnale Ltd (1992) 2 AC 548

London Joint Stock Bank v Macmillan and Arthur (1918) AC 777

Michael Douglas v Hello! Ltd (No. 2) (2003) EWCA Civ 139

Mid Essex Hospital Services NHS Trust v Compass Group UK and Ireland Ltd

(t/a Medirest) (2013) EWCA Civ 200

Midland Bank Ltd v Hett, Stubbs, Kemp & Co (A Firm) (1979) Ch 384

Oceano Grupo Editorial SA v Murciano Quintero C-244/98 to C/244/98

Office of Fair Trading v Abbey National plc and Others (2009) UKSC 6

Overy v *Paypal* (*Europe*) *Ltd* [*2012*] EWHC 2659 (QB), [2013] Bus LRD1

Royal Products v Midland Bank (1981) 2 Lloyds Rep 194

Scammel and Nephew Ltd v HC & JG Ouston (1941) AC 251

Sivagnanam v Barclays Bank Plc (2015) EWHC 3985 (Comm)

Smith v Lloyds TSB Bank (2000) 2 All ER (Comm) 693

Tai Hing Cotton Mill Ltd v Liu Chong Hing Bank (1986) AC 80

Tai Hing Cotton Mill v Liu Chong Hing Bank Ltd (1985) 2 All ER 947

TSG Building Services plc v South Anglia Housing Ltd (2013) EWHC 1151 (TCC)

Vidal-Hall v Google Inc (2015) EWCA Civ 311

West v Ian Finlay & Associates (2014) EWCA Civ 316, (2014) BLR 324

INTRODUCTION

INTRODUCTION

Research Aim and Objectives

Demand for mobile payment (m-payment) services through hand-held, portable devices is transforming the banking payment system in unprecedented ways as customers can now use their smartphones to conduct financial transactions and access financial information.[8] With the advent of the internet, online or e-banking has been made possible.[9] E-banking consists of making available traditional and new banking services and products through the internet from an electronic device, such as a personal computer ('PC').[10] Accordingly, certain banking services are delivered through the medium of the internet and not traditional bank branches.[11] E-banking enables bank customers to log into their bank accounts on the webpage of their bank in order to check their bank account and manage online payments.

With the arrival of the smartphone, customers can also access their bank account online. M-banking can be defined as using mobile devices to conduct banking business.[12] As mobile phones are small, it is not very practical

[8] Shaikh and Karjaluoto n 1.
[9] UNCTAD, *Information Economy Report 2007-2008: Science and Technology for Development: The new paradigm of ICT* (United Nations 2007) 213.
[10] V.C. Joshi, *E-Finance: The Future is Here* (2nd ed, Sage 2010) 37.
[11] UNCTAD n 9, 213.
[12] M. Khosrow-Pour, *E-Commerce for Organizational Development and Competitive Advantage* (IGI Global 2013) 227.

to log into the webpage online. M-banking apps have thus been made available which are more convenient and quicker to use, and which bank customers can download onto their smartphone.[13] These m-banking apps enable customers to check balances, send money to other accounts and make payments.[14]

Increasingly, bank customers have also been offered to use m-payment services which can be used for online and proximity payments, as further explored in chapter 1, section 1.2.[15] It is this latter m-payment innovation with which this research is concerned in the specific context of protecting consumers against unauthorised m-payment transactions, safeguarding consumers' data and their privacy, including against breaches of their privacy. The main focus of the thesis is thus on the use of mobiles for effecting payment transactions.

A m-payment consists of funds being transferred in return for a service or goods and the mobile phone is employed to initiate and confirm the payment.[16] The payer can be at the point of sale ('POS') or mobile.[17] In other words, a m-payment is a noncash kind of payment service conducted through a mobile.[18]

---

[13] M. Cerna et al, 'Quality in Mobile Payment Service in India' in A. K. Kar et al (eds), *Digital Nations – Smart Cities, Innovation, and Sustainability: 16th IFIP WG 6.11 Conference on e-Business, e-Services, and e-Society, i3E 2017, Delhi, India, November 21-23, 2017, Proceedings* (Springer 2017) 191.
[14] BBVA, 'Mobile Banking, New Experience in the Post PC Era', Innovation Edge, April 2012, 1-67, 23.
[15] OECD, 'Report on Consumer Protection in Online and Mobile Payments', 17 August 2012, 1-45, 8; BBVA, 'Mobile Payments, Paying with a mobile device', Innovation Edge, November 2012, 10.
[16] H. Nahari and R.L. Krutz, *Web Commerce Security: Design and Development* (Wiley Publishing Inc 2011) 1.6.
[17] Ibid.
[18] F.J. Mtenzi et al, *Mobile Technologies and Socio-Economic Development in Emerging Nations* (IGI Global 2018) 50.

The thesis is looking at how the laws in the UK and SA compare in terms of providing protection to consumers when they move increasingly to the use of their mobiles to effect payment transactions. In this context, it is essential to further distinguish online or electronic (e-) banking and m-banking services from m-payment services.

Online payments, including through e-banking or m-banking apps, can be made, for instance, via debit cards, credit cards, through an account based systems (such as a bank account), online payment banking whereby a consumer is redirected to his/her own bank from a merchant's website or mediating services (e.g. PayPal), prepaid payment services or electronic currency systems, automated bill payment mechanisms, escrow services or an online wallet registered with a payment provider to which money can be uploaded with a credit or debit card.[19]

In contrast, m-payments are made through smartphones in two main ways, namely through contactless, mobile, POS payments or mobile remote payments.[20] A contactless, mobile, POS payment takes place when the seller and buyer are there to execute a contactless payment through radio technologies, such as Bluetooth and NFC, as discussed in chapter 1, section 1.2.[21] A mobile remote (i.e. non-location specific) payment is made with the smartphone over a telecommunication network, e.g. the internet or the global system for mobile communication ('GSM').[22] The remote m-payment can be

[19] OECD n 15, 7-8.
[20] Ibid, 8-9.
[21] Ibid, 8.
[22] Ibid, 9.

conducted through a short message service ('SMS'):[23] A mobile payment service provider ('MPSP') allows the consumer to create an account.[24] The account is linked to a pre-paid, credit or debit card or bank account.[25] A SMS is sent by the consumer which contains the payee's phone number.[26] The consumer enters a personal identification number ('PIN') for authentication purposes.[27] The MPSP then submits the payment.[28] The remote m-payment can also be made through a wireless application protocol ('WAP'): The smartphone's browser is used to go to a web merchant where purchases are made, just like an online purchase.[29]

While traditional banking laws apply to online payments, they appear ill-suited for m-payments for a number of reasons, particularly the new risks they pose for customers, as detailed in chapter 2, as well as the innovation stifling impact they would have on Fintech[30] innovation.[31] Also, a different treatment in law appears essential since unlike credit institutions[32], payment institutions cannot accept funds in order to deposit them.[33]

Furthermore, it may be difficult to apply or adapt and adequately develop existing financial, telecommunications and consumer protection

[23] Ibid.
[24] Ibid.
[25] Ibid.
[26] Ibid.
[27] Ibid.
[28] Ibid.
[29] Ibid.
[30] Oxford Dictionary n 4.
[31] OECD n 15, 16; G. Gimigliano, *Bitcoin and Mobile Payments: Constructing a European Union Framework* (Palgrave Macmillan 2016) 124.
[32] See Financial Services and Markets Act 2000, Part IV.
[33] A.R. Lodder and A.D. Murray, *EU Regulation of E-Commerce: A Commentary* (Edward Elgar Publishing 2017) 158.

regulation to address emerging problems within this emerging field.[34] Countries, such as the UK[35], Kenya[36] and South Korea[37], have therefore promulgated new statutory regimes for payment services.[38] For instance, the UK has created two separate authorisation frameworks to permit non-banks, namely payment and e-money institutions, to make available m-payment services and to address the unique risk and protect customers, as discussed in chapter 4, sections 4.3.4 and 4.3.3.

A payment institution includes those which provide, for instance, account information services, provide and maintain payment accounts for payers, execute payment transactions or initiate payment services.[39] In contrast to payment institutions, an electronic money ('e-money') institution issues "means of payment in the form of electronic money"[40], though credit institutions can also issue electronic money ('e-money').[41] E-money is monetary value which is issued when funds are received and stored on a remote server or an electronic payment device by a money holder who has an

[34] Ibid (OECD) 17.
[35] The Payment Services Regulations 2009, the Electronic Money Regulations 2011 and the Payment Services Regulations 2017.
[36] The Kenyan National Payment Systems Act 2011.
[37] South Korea's Electronic Financial Transaction Act No. 11087.
[38] OECD n 15, 17.
[39] Regulation 2, Regulation 4(1)(a), Regulation 6 of the PSR 2017 and see esp. Part 1 of Schedule 1 (payment services).
[40] Directive 2000/46/EC on the Taking Up, Pursuit and Prudential Supervision of the Business of Electronic Money Institutions, Article 1(3)(a).
[41] Point 15 of Annex of Directive 2013/36/EC; Lodder and Murray n 33, 158; European Payment Institutions Federation, 'What is a Payment Institution?', 2019 <https://paymentinstitutions.eu/the-payment-institutions-sector/about/> accessed 1 March 2019.

e-money account.[42] Hence, e-money is monetary value which is stored electronically on a device to make payments.[43]

The statutory impetus in the evolving Fintech field is vital to safeguard m-payment customers, particularly against unauthorised m-payment transactions. Legislative steps must also be taken to protect m-payment customers' data and privacy, including against breaches, as m-payments enable companies to obtain a precise picture about consumers, to gather detailed information about consumers and to exchange data about their purchases with other businesses.[44] The making available of m-payment services by companies, such as Facebook, with extensive digitalised customer data further highlights the need for legislators to debate how best to protect customers' data, their privacy and protect them against breaches of their privacy.[45]

Also, an up to date legislative framework is essential to promote innovation in an area, which is witnessing massive growth; in 2016 the global m-payment market was valued an estimated $601 billion and by 2023 it is expected to grow to $4,574 billion.[46] Hence, legislators must address how m-payments are regulated in light of the popularisation of m-payments which is

[42] OECD n 15, 18; see Electronic Money Regulations 2011 ('EMR 2011'), Regulation 2(1); Electronic Money Directive 2009/110/EC, Article 2(2).
[43] M. Arnone and L. Bandiera, 'Monetary Policy, Monetary Areas, and Financial Development with Electronic Money', IMF Working Paper WP/04/122, July 2004, 4.
[44] C.J. Hoofnagle et al, 'Mobile Payments: Consumer Benefits & New Privacy Concerns' (2012) University of California, 1-19, 2 <https://ssrn.com/abstract=2045580> accessed 5 March 2019.
[45] D.A. Zetsche et al, 'From Fintech to TechFin: The Regulatory Challenges of Data-Driven Finance' (2017) European Banking Institute Working Paper Series 3, No.6, 1-36, 14.
[46] K. Sonawane, 'Mobile Payment Market Expected to Reach $ 4,574 Billion by 2023', Allied Market Research, February 2018 <https://www.alliedmarketresearch.com/press-release/mobile-payment-market.html> accessed 5 March 2019.

incrementally replacing cash.[47] Unlike traditional banking services, consumer protection for customers who use Fintech raises unique concerns due to some of the associated technological risks and dangers that these services pose in relation to the securing of financial assets and safeguarding of confidential, private personal online data against cybercriminal activity and failures in system functionality, as discussed in chapter 2.[48] Without consumer protection customers may be exploited by m-payment providers which unfairly hold them responsible for their own security breaches and system failings. If customers are inadequately protected, they could incur large financial losses and have their personal data and privacy breached e.g. through misuse of personal transaction data and transaction information.[49] Therefore, an appropriate legal framework must be adopted for Fintech innovation to be genuinely socially beneficial.[50] This framework would incorporate laws that allocated liability by carefully delineating the circumstances in which customers, m-payment providers or third parties are to be held accountable.

The research aim is thus to analyse how Saudi Arabian law protects m-payment customers, particularly against unauthorised m-payment transactions and protects consumers' data and their privacy, including against untoward privacy intrusions and thereby seeks to make an original contribution to the Saudi Arabian legal system in the presently under-researched areas of both consumer protection and m-payment services. The legislative analysis deals

[47] L. Lu, 'Decoding Alipay: mobile payments, a cashless society and regulatory challenges' (2018) *Butterworths Journal of International Banking and Financial Law*, 40-43, 40.
[48] Zercan n 3.
[49] P.-L. Chatain et al, *Integrity in Mobile Phone Financial Services: Measures for Mitigating Risks* (World Bank 2008) 40; S.-H. Chun, 'E-Commerce Liability and Security Breaches in Mobile Payment for e-Business Sustainability' (2019) *Sustainability*, 11, 715-733, 718.
[50] Kaufman et al n 5.

with m-payment services provided by banks and companies, such as Apple Pay or PayPal. For example, PayPal is available in the UK and SA.[51] PayPal provides a cloud-based remote mobile wallet through a closed loop system which makes it possible to use money held in the PayPal account for payments through a digital wallet.[52] ApplePay is a digital wallet through which m-payments can be made remotely and which can be used by the majority of bank customers with an iPhone in the UK.[53] While ApplePay had not been launched by the end of 2017 in SA, six banks of the neighbouring UAE announced its use in October 2017.[54] Procrastination in adopting a law by SA may mean that financial benefits for the economy are foregone. As citizen's property is being handled through the discussed technologies, the requisite legal consumer safeguards must also be debated by policy and lawmakers.

The predominant focus of this work is the consumer protection legal literature, in order to present the various arguments/rationales formulated to advocate for, or caution against, providing consumer protection through legal means. In chapter 3, the literature is synthesised in order to establish what is known and, by extension, the gaps in existing knowledge which may be addressed by this research. The review seeks to identify whether there are any

[51] PayPal Holdings Inc is a United States (US) based business which provides global online payments: PayPal <https://www.paypal.com/uk/home> accessed July 2015; PayPal, 'We get where you're coming from.' 2017 <https://www.paypal.com/en/webapps/mpp/country-worldwide> accessed 25 November 2017.
[52] C. Scardovi, *Restructuring and Innovation in Banking* (Springer 2016) 33-34.
[53] R. LeRoy Miller, *Business Law Today, Comprehensive Edition, Text & Cases* (11th ed, Cengage Learning 2017) 552; J. Russell, 'Apple is 'working rapidly' to launch Apple Pay in more countries in Asia and Europe', TechCrunch, 26 May 2016 <https://techcrunch.com/2016/05/26/apple-is-working-rapidly-to-launch-apple-pay-in-more-countries-in-asia-and-europe/> accessed 10 November 2016; Apple UK, 'Find it all in Wallet.' 2017 <https://www.apple.com/uk/apple-pay/> accessed 23rd November 2017.
[54] A.R. Cabrai, 'ApplePay launches in UAE and 3 other countries today', Khaleej Times, 24 October 2017 <https://www.khaleejtimes.com/technology/apple-pay-is-now-in-the-uae> accessed 16 November 2017.

gaps in the literature which the thesis intends to fill in and respond to in subsequent chapters. The review of the consumer protection literature also provides direction. It acts as a framework for the analysis of UK and Saudi laws in chapters 4 and 5 in order to ascertain the consumer protection approach being taken by each jurisdiction respectively in the context of m-payment services and helps with the recommendations which are derived from this research.

From this understanding in chapter 3, it emerges that a vulnerable customer should still be able to seek compensation from the m-payment provider, even in circumstances where s/he is partly to blame. In contrast, a reasonably circumspect customer will find it more difficult to pursue his/her m-payment provider for omissions on his/her behalf. The adoption of a vulnerable consumer approach within consumer protection law may promote naivety and does not encourage learning. However, it also arguably incentivises m-payment providers to adopt stronger security measures and to engage in heightened risk management, thereby helping to comply with the Islamic *halal* doctrine.[55] Such an approach may help to promote social unity because a wider safety net is created for consumers.[56] It should arguably always be the case when customers have discharged their basic obligations.

Accordingly, the thesis analyses how the laws in the UK and SA compare in terms of protecting consumers against unauthorised m-payment

[55] M.K. Hassan and M. Rashid, *Management of Islamic Finance: Principle, Practice, and Performance* (Emerald Publishing Limited 2019) 45.
[56] J.M. Paterson and G. Brody, '"Safety Net" Consumer Protection: Using Prohibitions on Unfair and Unconscionable Conduct to Respond to Predatory Business Models' (2015) *Journal of Consumer Policy* 38, 331-355, 340.

transactions and consumers data and their privacy, including against breaches of their privacy, when they move increasingly to the use of their mobiles to effect payment transactions. In addressing the research aim the following five objectives will be clearly defined and will be used to help direct the discussion:

1. What are the key technologies currently used to facilitate m-payment services? The answer to this will include showing the considerable impact that Fintech[57] has had upon the banking and financial sector. This question is a valuable starting point as it sheds light on the benefits which these technologies offer to consumers, which are to be weighed against the harm caused.
2. What risks do m-payment services pose in comparison to traditional, non-technological banking practices? This question is important as it provides the counterpoint to the benefits identified in answering the first question above; taken together these are the two sides of the debate which must be weighed and balanced by the law. Overall, the objective is to foreground what exactly it is that m-payment consumers need to be protected against since the law must respond to these practical issues as and when disputes arise. In short, legislation should demarcate the boundaries of acceptable business conduct for m-payment providers which offer m-payment services and the customers who utilise them, particularly in relation to unauthorised m-payment transactions and safeguarding consumers data and privacy.

[57] Oxford Dictionary n 4.

3. What does the existing legal consumer protection literature in the West and the Sharia reveal about the different consumer protection frameworks? What evidence is there that these frameworks are influenced by either the neo-liberal and 'consumer economic interest' or the social welfare and 'consumer protection interest approaches?"[58] And, where is Sharia law positioned in relation to these paradigms? Central to this objective is an evaluation of the Islamic stance towards business dealings, consumers, consumer rights and protection since all of these aspects are very influential in shaping the policy stance of the legislator. It is explored how the Sharia principle of good faith might be one way of to help developing a more pro-consumer set up of legislation or legislative provisions when it comes to m-payments. Answering these questions provides crucial background to the regulatory environments in the UK and SA, in the context of which regulation of Fintech can be appraised.
4. How does UK law frame, provide for and regulate the rights and obligations of the m-payment provider and customer, including in relation to unauthorised m-payment transactions and the protection of consumers' data and their privacy? And, what does this reveal about the policy orientation undergirding its legislation of the complex m-payment ecosystem?
5. How does Saudi Arabian law currently provide for and regulate the rights and obligations of the bank and the customer in payment

[58] J.Q. Whitman, 'Consumerism Versus Producerism: A Study in Comparative Law' (2007) *Yale Law Journal* 117, 340-406, 356.

transactions? And does this extend to m-payment services? The question of whether Saudi Arabian law adequately protects m-payment customers against the risks of unauthorised m-payment transactions and safeguards consumers' data and their privacy in a manner that is compliant with Sharia law, and if there are lessons that can be learnt from the UK requires critical appraisal.

Research Background and Focus

Consumer protection policies and laws are designed to mitigate business negligence and prevent the exploitation of consumers and enhance consumer wellbeing.[59] The rapid technological evolvement of Fintech and the globalised arena in which it functions has meant that customers are continuously offered a wide variety of diverse services, most recently m-payment services.[60] However, it is concerning that these complex technological developments have not been accompanied by the necessary financial consumer protection in countries, such as SA, as discussed in chapter 5.[61] This is a situation that leaves consumers exposed to the concomitant risks of regulatory weaknesses, including business and system failures, fraud or exploitation, as further discussed in chapter 2. In these circumstances, the state is the only authority

[59] P. Cartwright, *Consumer Protection and the Criminal Law: Law, Theory, and Policy in the UK* (CUP 2004) 194; J.J. Xiao, *Consumer Economic Wellbeing* (Springer 2015) 73; F. Kessler, 'The Protection of the Consumer under Modern Sales Law, Part 1, A Comparative Study' (1964-1965) *Yale Law Journal* 74, 262-285, 262.
[60] Ibid.
[61] I. Lukonga, 'Fintech, Inclusive Growth and Cyber Risks: Focus on the MENAP and CCA Regions', IMF Working Paper, WP/18/201, 2018, 19.

with any meaningful power to act to protect consumers,[62] particularly against unauthorised mobile payment transactions, as well as their data and privacy.

When considering how to draft and implement consumer protection laws within a m-payment context, a number of key aspects come into play and shall be the subject of in-depth analysis in the thesis; central to this is the question of fair allocation of liability between m-payment service providers and consumers. This requires delineating the rights and responsibilities of each party. Typically, m-payment risks arise from customer errors, security problems and third parties, as discussed in chapter 2. Consumer protection laws could incorporate the imposition of legal duties, such as, the tortious law of negligence and duty of care, general contract law, including statutes which limit unfair exclusion clauses, as well as regulations which promote fairness and justice, as identified through the analysis of the UK approach in chapter 4. They would demarcate statutory and regulatory obligations relating to mandated disclosure and the operation of effective risk management systems and oversight, to name but a few. Equally, the consumer also has rights and duties. The right to seek redress for unauthorised transactions and data breaches is essential, as identified in chapter 4. Customer duties could include keeping the identity authentication information safe, installing security, anti-virus and updating software, and exercising a level of discernment and vigilance when conducting m-payment transactions through public Wi-Fi networks, as observed in chapter 2.

[62] B. Schuller, 'Social peace via pragmatic civil rights -the Scandinavian model of consumer law'. In H.W. Micklitz (eds), *The Many Concepts of Social Justice in European Private Law* (Edward Elgar 2011) 384.

However, these considerations of the impact on m-payment providers and consumers are not the only forces which shape consumer protection policies; perhaps even more significantly, these reflect the policy orientation of a region, country or framework, as is explored in chapter 3. This becomes apparent when examining the G20 Financial Consumer Protection and the EU Consumer Protection. The former reflects a neo-liberal and consumer economic interest approach initiated in response to the financial crisis of 2008, rather than offering comprehensive consumer protection.[63] The latter, while more of a rights-based approach, neglects to take into account vulnerable people and their limited access to legal rights.[64] Should the law make special dispensation for specific demographics? If so, what does it mean for objectivity and equality in judicial proceedings? These questions demonstrate that how 'the consumer' is conceptualised in law is integral to the formulation of consumer protection legislation for it determines the extent of protection that the consumer both requires and can obtain.

The legal scope for consumer protection appears to be premised on an understanding of the consumer as either rational or vulnerable.[65] This is a highly contested area in the context of m-payment services, and it has been examined by academics who have referenced work from the fields of rational choice theory[66] and behavioural economics and cognitive psychology[67], as

[63] T. Williams, 'Continuity, not Rupture: The Persistence of Neoliberalism in the Internationalization of Consumer Finance Regulation'. In T. Wilson (eds), *International Responses to Issues of Credit and Over-indebtedness in the Wake of Crisis* (Routledge 2013) 3.
[64] H.-W. Micklitz, 'European Consumer Law'. In E. Jones et al (eds), *The Oxford Handbook of the European Union*, Oxford Handbooks Online, 2013, 1-20, 1.
[65] I. Ramsay, 'Regulation and the Constitution of the EU Single Market: The Contribution of Consumer Law' (2010) *Canadian Business Law Journal* 50, 322-346, 343.
[66] E.g. see R.A. Posner, 'Rational choice, behavioural economics, and the law' (1998) *Stanford Law Review* 50, 1551–1575, 1551.

discussed in chapter 3. Some areas under discussion have been: Are m-payment consumers able to reach adequate analytical economic decisions or do they require proactive protection? What about the role of IT consumer literacy? Who bears responsibility for it? Should legislation positively incentivise m-payment providers to educate their customers? In a rapidly changing technological field, even skilful users of smart devices can be deemed vulnerable to sophisticated cybercriminal activity and techniques. These are just some of the areas that shall require further critical attention in the research.

Consumer protection and the concept of rights are not clearly articulated and defined in Islamic law and literature.[68] Sharia law contains a wealth of information about how business obligations are to be met and business affairs are to be conducted.[69] It advocates for high business standards that incorporate good faith, honesty, transparency, delivering quality products and adhering to contractual business agreements.[70] Most assuredly, business discharged by these Islamic holy duties forgoes the need for consumer rights.[71] However, this business remit raises some pressing questions regarding certain neglected aspects of compliance and enforcement, namely: what about those instances where businesses fail to discharge their Islamic holy duties? Are consumers within their rights to bring a legal claim against those businesses which do not meet their obligations? Also, how would they do so? Should

---

[67] E.g. see R. Incardona and C. Poncibo, 'The Average Consumer, The Unfair Commercial Practices Directive, and the Cognitive Revolution' (2007) *Journal of Consumer Policy Issue* 30(1), 21-38, 21.
[68] M.A. Khan, 'Consumer Protection in Islamic Law (Shariah): An Overview' (undated) 45(31), 77-100, 77-78 <http://pu.edu.pk/images/journal/szic/PDF/English/6-%20Muhammad%20Akbar%20Khan%20Final%20Draft%20of%20Research%20Paper.pdf> accessed 10 February 2019.
[69] Albaqme n 6, 170.
[70] Ibid.
[71] Ibid.

there be state bodies or institutions charged with monitoring compliance with Islamic business values? Legal uncertainties such as these do not wholly take into account the role of the consumer and renders questionable the area of consumer rights and consumer protection in Islamic countries.

It is vital that Saudi legislation keeps apace with Fintech innovation. In the current digital age, it must be explored which legal measures are required to protect Saudi Arabian m-payment customers against harms arising from technological risk. The Quran commands that the state guarantees security.[72] Prophet Mohammed emphasised that "there should be neither harming (*dara*) nor reciprocating harm (*dirar*).[73] The challenges are how to apply these holy duties to commercial transactions and keep the Sharia up to date with the latest developments in business, since the precise scope of consumer protection within Islamic law has not been explored and has received very little attention in Muslim countries.[74] Some have suggested taking a progressive approach towards Quranic verses, but it is thought that this might be met by some resistance from the Hanbali School which is the foundation of Sharia principles in SA.[75] Another option to clarify Islamic law is to promulgate an Islamic consumer protection jurisprudence through the concept of *qiyas* (analogical reasoning).[76] Quranic business, religious and ethical principles, particularly the good faith principle, *haram* and *halal* and the profit and loss sharing principle,

[72] O.R. Al-Jayyousi, *Islam and Sustainable Development: New Worldviews* (Routledge 2016) 129.
[73] 40 Hadith Nawawi 32.
[74] D. Morris and M. Al Dabbagh, 'The development of consumer protection in Saudi Arabia' (2003) *International Journal of Consumer Studies* 28(1), 2-13, 2.
[75] J.-P. Platteau, *Islam Instrumentalized, Religion and Politics in Historical Perspective* (CUP 2017) 93.
[76] H.M. Ramadan, *Understanding Islamic Law: From Classical to Contemporary* (AltaMira Press 2006) 18.

could be used as a base to develop welfare-oriented consumer protection policies and laws. At present, there is a lack of Islamic consumer protection jurisprudence and government bodies do not ensure that consumer rights are upheld.[77] The topic of consumer protection therefore requires urgent attention by Islamic scholars.

The research aim is to analyse how Saudi Arabian law protects m-payment customers from the specific consumer welfare problems raised by m-payments: Unauthorised payments and data and privacy protection. There is a dearth of research related to consumer protection in SA,[78] and even less that is focused on m-payment services. This research analyses the Saudi legal system, using Western and Islamic consumer protection literature. Additionally, the UK legal system is scrutinised to assess whether lessons can be learnt in providing greater protection to customers in a Saudi Arabian context while remaining Sharia compliant. In so doing, the research seeks to make an original contribution to the Saudi Arabian legal system in the presently under-researched areas of both consumer protection and m-payment services. The overall aim is to supply recommendations that will result in greater consumer protection rights for Saudi Arabian people.

[77] A. Alqarni, 'Saudi Consumers' Experience toward the Role of the Government Agencies as Service Providers in Ensuring their Consumer Rights' (2016) *International Journal of Business and Social Sciences* 7(9), 72-76, 72.
[78] Albaqme n 6, 170.

Research Questions

The research examines Sharia-compliant consumer protection of Saudi Arabian customers who use m-payment services; it seeks to answer the following question:

- How does Saudi Arabian law protect customers who use m-payment services in SA, particularly against unauthorised m-payment transactions and protects consumers' data in order to maintain privacy, including against breaches of their privacy?

In attempting to answer this research question the following sub-questions will also need to be examined:

- What are the primary technologies which facilitate m-payment services? How do they benefit m-payment customers?

  This is essential to understanding the features of this innovation which any policy intervention should seek to preserve as far as possible.

- What are the main sources of risk involved in m-payment services? What problems can arise to disadvantage m-payment customers?

  These questions help to provide essential context for the consideration of policy issues through which risks and benefits must be balanced and managed.

- What are the paradigms of the Western and Islamic legal consumer protection literature? In what ways are the legal consumer protection measures in these demographics characteristic of these different approaches?

The answer to these questions provides essential context for the analysis of consumer protection in relation to m-payments services and is also critical in informing the recommendations at the end of the work.

- What legal framework has the UK adopted in respect of m-payment services? Which policy orientation underpins its laws?

This provides a point of comparison for Saudi Arabian legislation, from which inspiration for recommendations can also be drawn.

- What legal framework has SA adopted in respect of m-payment services? To what extent does its laws safeguard m-payment customers against unauthorised m-payment transactions and protects consumers' data in order to maintain privacy, including against breaches of their privacy, in a Sharia compliant manner?

This analysis forms the basis of a critical assessment later in the work.

- Can SA draw any lessons from the UK model of consumer protection legislation?

Answering this question is critical to the work as this draws together the doctrinal and theoretical analysis of UK and Saudi Arabian law to propose recommendations for improvement.

Scope of the Research

The thesis has narrowed its focus to the issues of consumer protection in the context of unauthorised payment transactions and protection against data/privacy breaches. The reason is that those are two areas which are likely to

be of primary concern to consumers making m-payment transactions in light of technological and operational risks involved as well as the potential for vast amounts of data to be collected in m-payment transactions. The technologies underlying m-payments heighten security risks, as discussed in Chapter 2, and consumer confidence and trust in m-payments and the evolving digital ecosystem would be undermined if consumers had to unfairly shoulder losses for unauthorised payment transactions.[79] The benefits for consumers, discussed in Chapter 1, as well as the wider economic benefits for society from this innovation, may be lost,[80] without financial consumers being protected against the new risks. In other words, security concerns constitute a significant barrier which is likely to adversely affect the take-up of m-payments and undermine the growth of the growing Fintech sector.[81] M-payment innovation can only be promoted if trust is built and this necessitates that potential security issues are addressed in such a way that consumers retain confidence.[82] Consumer protection in the context of unauthorised transaction is likely to lower consumer risk and promote consumer confidence.[83]

Moreover, the collection of payment data (i.e. personal data, namely the payer's and payee's names and bank details, as well as non-personal data, such

[79] International Financial Consumer Protection Organisation, 'Online and mobile payments, An overview of supervisory practices to mitigate security risks', January 2018, 1-79, 9 <http://www.finconet.org/FinCoNet_SC3_Report_Online_Mobile_Payments_Supervisory_Practices_Security_Risks.pdf> accessed 6 July 2019.
[80] The Wall Street Journal, 'How Mobile Money Drives Economic Growth', 2017 <http://www.wsj.com/ad/article/mlf-how-mobile-money-drives-economic-growth> accessed 16 December 2017.
[81] International Financial Consumer Protection Organisation n 79, 21.
[82] Ibid, 29.
[83] Ibid, 65.

as the time, date, amount and parties involved in the transactions[84]) plays an increasingly important role in the evolving payment sector[85] and data-driven economy.[86] It can be utilised to enhance services or "valuecreate commercial products."[87] This data can be sold to other organisations, analysed in order to gain insights and then applied.[88] For instance, Google Pay uses transaction data for advertising purposes.[89] However, these "data-related opportunities" may not be realised if consumers fear that their data is unsafe or is used inappropriately.[90] Also, data security and privacy concerns must be addressed in order to avoid that consumers are harmed.[91] Consumer protection through data privacy law is thus essential to balance protection with growth objectives.[92]

It is for these reasons that the focus of this research is on unauthorised m-payments and data/privacy breaches and not on other areas, such as cryptocurrencies, which also facilitate m-payments.[93] Also, as this thesis focuses on two specific consumer protection issues - unauthorised m-payments and data/privacy breaches, it does not deal with broader issues, such as risk management theory and risk management models or regulatory frameworks for m-payments in general. This is despite the fact that these are also areas which

[84] Payment Systems Regulator, 'Discussion paper: Data in the payments industry', June 2018, 1-66, 24, and 4.31 <https://www.psr.org.uk/sites/default/files/media/PDF/PSR-Discussion-paper-Data-in-the-payments-industry-June-2018.pdf> accessed 5 July 2019.
[85] Ibid, 11, para 3.
[86] Ibid, 60, para.2.17.
[87] Ibid, 6, para.1.12.
[88] Ibid, 6, para.1.10.
[89] Ibid, 13, para.3.9.
[90] Ibid, 7, para.1.13.
[91] M. N. Helveston, 'Consumer Protection in the Age of Big Data' (2016) *Washington University Law Review* 93(4), 859-917, 872.
[92] McKinsey&Company, 'McKinsey on Payments', Number 16, March 2013, 1-46, 38.
[93] S. Muruganand et al, *Proceedings of the International Conference on Interdisciplinary Research in Electronics and Instrumentation Engineering, 11-12 August 2015* (ICIREIE 2015) 73.

impact consumer protection. The work also does not address whether competition law can be evoked when companies, such as Facebook, abuse their position and require users to agree to untoward privacy terms and conditions.[94] Also, the many other issues which face electronic consumers of financial services, such as choice of law, are beyond the scope of this work;[95] nevertheless, literature exploring approaches to these issues may be valuable for illustrative purposes for the study of consumer protection.

The research is primarily a law-focused work informed by the technological context for which a legal answer is sought. The focus of the thesis is on customer protection, that is to say, m-payment provider conduct vis-à-vis customers.

Furthermore, the Saudi Arabian and UK legal systems are analysed. Other jurisdictions are only mentioned to highlight the importance for the Saudi legislator to take legislative action, including by taking into account new legislative impetus all over the world. Also, due to the UK's membership of the European Union ('EU') at the time of writing this research, it has transposed a number of EU laws. Recourse is therefore made to EU legislation when appropriate. Finally, as the research specifically deals with developing Sharia-compliant legal recommendations, Islamic verses are cited and arguments by Islamic scholars are presented. No other religious texts are referenced in the

[94] M.N. Volmar and K.I. Helmdach, 'Protecting consumers and their data through competition law? Rethinking abuse of dominance in light of the Federal Cartel Office's Facebook investigation' (2018) *European Competition Journal* 14(2-3), 195-215, 195.
[95] Y. Farah, 'Allocation of jurisdiction and the internet in EU law' (2008) *European Law Review* 33(2), 257-270.

research. It should be noted that this work analyses the law as at 1 May 2018; changes after this date are not generally considered.

Research Methodology

Since laws are identifiable facts, the thesis adopts the positivist stance.[96] A positivist ontology views reality as objective and external.[97] Thus, a doctrinal approach (also known as black letter law approach) was chosen.[98] Legal doctrine was studied, including its development and application.[99] Laws were systematically analysed, cases were cited, and accepted legal principles were discussed in the research.[100] Hence, recourse was made to primary, as well as secondary sources.[101] Academic arguments by scholars were being put forward, examined, interpreted and responded to by the researcher.[102] However, the focus was not only on what the law is, but it was also critically analysed.[103] Relevant legislation and cases were conceptually analysed to

[96] W.E. Conklin, *The Invisible Origins of Legal Positivism: A Re-Reading of a Tradition* (Kluwer Academic Publishers 2001) 9.
[97] L. Cohen et al, *Research Methods in Education* (7th ed, Routledge 2011) 27.
[98] M. McConville and W. Hong Chui, *Research Methods for Law* (Edinburgh University Press 2007) 4.
[99] V.M. Gawas, 'Doctrinal legal research method a guiding principle in reforming the law and legal system towards the research development' (2017) *International Journal of Law* 3(5), 128-130, 128-129.
[100] K.L. Bhatia, *Textbook on Legal Language and Legal Writing* (Universal Law Publishing Co Pvt Ltd 2010) 140.
[101] McConville and Hong Chui n 98, 4.
[102] Gawas n 99, 129.
[103] F. Cownie, *Legal Academics: Cultures and Identities* (Hart Publishing 2004) 69.

identify the law governing m-payment, particularly in relation to unauthorised payment transactions and protection of customers' data and their privacy.[104]

Moreover, the research had a small interdisciplinary component in order to take into account advances in information communication technologies ('ICT'). Technological developments and risks were described in chapters 1 and 2 in order to explain the context against which the legislator must develop its legislative framework. However, it is important to emphasise that the interdisciplinary part was only included in order to answer the legal questions which this research raises.[105] Hence, ICT developments and related technological risks which affect the law were considered.

Additionally, the policy considerations, including the wider ethical framework spelled out by the Sharia in SA and which may underpin the law were explored in chapter 3. These policy considerations were used to analyse the statutory frameworks in the UK and SA in chapters 4 and 5.

Furthermore, the comparative legal research method was chosen to identify solutions to a similar problem, namely unauthorised m-payments and data protection.[106] At present in SA, m-payment customers bear the full cost of any loss that follows from an unauthorised transaction. This approach to loss allocation presents a significant problem. The protection of customers' data and their privacy is also especially problematic under Saudi law, as no comprehensive data protection legislation has been enacted, leaving customers'

[104] T. Hutchinson, 'Valé Bunny Watson? Law Librarians, Law Libraries and Legal Research in the Post-Internet Era' (2014) *Law Library Journal* 106(4), 579-592, 584.
[105] M. Van Hoecke, *Methodologies of Legal Research: Which Kind of Method for What Kind of Discipline?* (Hart Publishing 2011) 253.
[106] P.G. Monateri, *Methods of Comparative Law* (Edward Elgar 2012) 151.

data unprotected.[107] The Sharia which is primarily concerned with promoting welfare is thereby contravened.[108] Such an approach is not unsurprising, given that the *fiqh* (the philosophy of Islamic law) literature does not deal specifically with the content of consumer law, including data and privacy protection.[109]

In other words, the rich Sharia base which stipulates principles of fairness and social justice, as discussed in chapter 3, section 3.6, has been insufficiently developed by Islamic scholars to protect consumers. The failure to develop a comprehensive Islamic consumer protection discourse results in consumers being inadequately protected in the context of unauthorised m-payments and data/privacy breaches. However, the Sharia could serve as a wider ethical framework which could be utilised to think about consumer protection in the Kingdom. The comparison with the UK assisted with developing recommendations on how the Saudi consumer protection rationale can be developed in line with its religious-based legal system.

The Sharia principle of good faith was identified as a crucial tool to promulgate more pro-consumer m-payment primary and secondary legislation, especially if it was utilised as a base for a principle of fairness. According to Article 1 of the Saudi Arabian constitutional law, the Basic Law of Governance of 1992, requires such an approach since it mandates that the Sharia is supreme over civil law.

---

[107] N. Kshetri et al, *Big Data and Cloud Computing for Development: Lessons from Key Industries and Economies in the Global South* (Routledge 2017) 67.
[108] B. Kettell, *Introduction to Islamic Banking and Finance* (John Wiley & Sons 2011) 14.
[109] Khan n 68, 77-78.

Furthermore, the legislative framework in SA which deals with m-payments is outdated. It focuses on e-banking and omits to address the consumer issues which arise from m-payment services. It is therefore only suitable for a Web 1.0 version of banking services (i.e. e-banking and m-payments), but not Web 2.0, let alone Web 3.0 Fintech innovation.[110] While Regulatory Rules for Prepaid Payment Services were adopted in 2012, they curtail m-payment innovation. Trade is thus undermined which is contrary to the Sharia.[111] The experience of another jurisdiction was therefore drawn upon[112] in order to gain insight how consumer protection values can co-exist and even support, strong competition within the market. It helped with identifying legislative responses to developments in the sector and policies which improve the rights of consumers without stifling the market. The comparison with another jurisdiction made it possible to recommend new legislative solutions on how consumer protection provisions can be enhanced, and laws can be updated to reflect advances in technology and the maturing of the Fintech sector, whilst maintaining or strengthening compliance with Sharia principles.

This was considered to aid SA develop its fintech market and become "a pioneer in the financial technology sector",[113] which is an important objective and forms part of the Saudi Arabian Monetary Authority's ('SAMA')

[110] K. Nath et al, 'Web 1.0 to Web 3.0 - Evolution of the Web and its various challenges' (2014) *ICROIT 2014 - Proceedings of the 2014 International Conference on Reliability, Optimization and Information Technology*, 86-89, 86.
[111] R. Bhala, *Understanding Islamic Law* (LexisNexis 2011) Chapter 17, section 17.01.
[112] C. Hunter and D. Cowan, *Integrating Socio-Legal Studies Into the Law Curriculum* (Palgrave MacMillan 2012) 39.
[113] SAMA, 'Saudi Arabian Monetary Authority Launches Fintech Saudi with the Objective to Make the Kingdom a Pioneer in the Financial Technology Sector', 1 May 2018 <http://www.sama.gov.sa/en-US/News/Pages/news30042018.aspx> accessed 5 July 2019.

Fintech Saudi initiative.[114] This initiative aims to promote the use of digital transactions and aid with the creation of a fintech hub in SA.[115]

It was worthwhile and meaningful to compare the UK approach towards consumer protection approach in respect of unauthorised m-payments and data/privacy breaches with that of SA for a number of reasons: The UK was chosen for the comparative method since it has statutorily responded to the problems of protecting consumers against unauthorised payments and data and privacy protection, as discussed in chapter 4. It has a long-standing history of protecting consumers against unfair business conduct, ever since the publication of the Molony Report in 1959.[116] It has consolidated its consumer protection legislation through the enactment of the Consumer Rights Act 2015, and which also protects m-payment customers against unfair terms and conditions. Consumer data has been protected by third-generation legislation - the General Data Protection Regulation ('GDPR') (Regulation (EU) 2016/679), which replaced the Data Protection Act 1998, and which was prior to the 1998 Act protected by the Data Protection Act 1984, as discussed in Chapter 4, section 4.5. The UK has also adopted legislation for payments, namely the Payment Services Regulations 2009, as well as second-generation legislation - the Payment Services Regulations 2017. It has also created an authorisation regime for e-money and e-money institutions by virtue of the Electronic

[114] Fintechnews Middle East, 'A Glimpse into Fintech in Saudi Arabia', 25 March 2019 <https://fintechnews.ae/3734/saudiarabia/fintech-saudi-arabia-overview/> accessed 5 July 2019.
[115] Ibid.
[116] Board of Trade, Final Report of the Committee on Consumer Protection (Molony Committee) Cmnd 1781/1962; P. Cartwright, *Consumer Protection in Financial Services* (Kluwer Law International 1999) 4-5.

Money Regulations 2011. UK legislators have thus made efforts to keep pace with technological progress in the m-banking sector.

Also, the UK has one of the largest financial centres in the world, coming second only after the United States.[117] It is a global financial power center and has the biggest capital market within Europe[118] and according to Groenfeldt, the City of London's success is particularly the result of its ability to adapt to changes within the business environment.[119] The UK Government's aim is for the UK to be a 'World Leader in Financial Technologies'.[120] KPMG reports that the UK was a 'global leader for fintech investment' in the first six months of 2018.[121] It attracted more investments than other countries around the world.[122] Hence, it is one of the fastest growing and developing Fintech markets in the world.

The UK has thus been chosen as a comparator to SA for a number of reasons and ultimately because of its carefully developed regime which finely balances market interests with those of the consumer.

It is considered that the comparative method provides worthwhile and meaningful insights not only about the law in the UK, but also Saudi law. By

---

[117] K. Allen, 'UK finance industry dominates European scene', Financial Times, 5 September 2018 <https://www.ft.com/content/88cdec40-b03c-11e8-8d14-6f049d06439c> accessed 10 February 2019.
[118] P. Asimakopoulos, 'Report: the size, depth & growth opportunity in UK capital markets', New Financial, May 2018 <https://newfinancial.org/report-the-size-depth-growth-opportunity-in-uk-capital-markets/> accessed 5 July 2019.
[119] P. Asimakopoulos, 'Report: the size, depth & growth opportunity in UK capital markets', New Financial, May 2018 <https://newfinancial.org/report-the-size-depth-growth-opportunity-in-uk-capital-markets/> accessed 5 July 2019.
[120] Sir Mark Walport n 7, 5.
[121] KPMG, 'UK global leader for fintech investment in H1 2018', 31 July 2018 <https://home.kpmg/uk/en/home/media/press-releases/2018/07/uk-global-leader-for-fintech-investment-in-h1-2018-.html> accessed 10 February 2019.
[122] Ibid.

comparing the two legal systems, it is possible for the researcher to reflect on the underlying thinking which has shaped the different approaches.[123] It helps to identify commonalities and differences.[124]

The findings are used to generate new solutions to the shared problem of how to protect m-payment customers, particularly against unauthorised m-payment transactions and protect consumers' data and maintain their privacy and safeguard against breaches of their privacy.[125] Essentially, this ensures that more knowledge is generated about a unique research area which requires new legislative impetus all over the world.[126] However, it is acknowledged that SA assigns supremacy to the Sharia and thus religious law.[127] In contrast, the UK adheres to a common law system which follows a system of precedent and which excludes religion from the legal arena.[128] As a result, the legal tradition of each state is very different. This has an impact on the knowledge and insight gained from the UK approach which cannot simply be transposed to a Sharia legal system.[129] In other words, 'cultural comparative law' must be undertaken i.e. it must be taken into account that the law is influenced and driven by the specific culture in each country.[130]

---

[123] E.J. Eberle, 'The Method and Role of Comparative Law' (2009) *Washington University Global Studies Law Review* 8(3), 451-486, 455.
[124] Ibid, 456.
[125] E. Örücü, *The Enigma of Comparative Law: Variations on a Theme for the Twenty-First Century* (Springer & Business Media 2004) 38.
[126] M. Andenas and D. Fairgrieve, *Courts and Comparative Law* (OUP 2015) 52.
[127] A. Roberts et al, *Comparative International Law* (OUP 2018) 587.
[128] Ibid.
[129] P. Legrand, 'The Impossibility of 'Legal Transplants' (1997) *Maastricht Journal of European and Comparative Law* 4(2), 111-124, 111.
[130] J. Husa, 'Farewell to Functionalism or Methodological Tolerance?' (2009) University of Helsinki, 1-25, 13 <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1488669> accessed 10 February 2019; Eberle n 123, 452.

Advocates of functionalism therefore observe that "the legal system of every society faces essentially the same problems, and solves these problems by quite different means though very often with similar results." [131] The concept of functionalism, especially 'equivalence functionalism', denotes that a similar problem, such as unauthorised m-payment transactions and data and privacy protection, may require different solutions and that it is not necessary to look for the best or similar solution.[132] Such an approach recognises that an issue in one society has a unique background, whereas this background is different in another society.[133] The functional approach was chosen to underpin this thesis for pragmatic reasons, as the focus was on getting results[134] by identifying a solution to a problem.[135] A problem was identified, namely providing protection to consumers when they move increasingly to the use of their mobiles to effect payment transactions, and for which the research then searched for a solution, by making recourse to the Saudi and UK legal regimes.

The functionalist method also helped informing the research design i.e. the different stages of the thesis.[136] During the first stage of the research, this method highlighted the importance of focusing on those issues which exist in both SA and the UK[137], namely that consumers who make m-payment

[131] K. Zweigert and H. Kotz, *An introduction to comparative law* (OUP 1998) 34.
[132] B. Wernaart, *The Enforceability of the Human Right to Adequate Food: A Comparative Study* (Wageningen Academic Publishers 2013) 40.
[133] Ibid.
[134] R. Michaels, 'The Functional Method of Comparative Law'. In K. Zimmermann and M. Reimann (eds), *The Oxford Handbook of Comparative Law* (OUP 2006) 340; J. Gordley, 'The functional method.' In P. G. Monateri (eds), *Methods of Comparative Law* (Edward Elgar 2012) 107.
[135] O. Brand, 'Conceptual Comparisons: Towards a Coherent Methodology of Comparative Legal Studies' (2007) *Brooklyn Journal of International Law* 32, 405-466, 409.
[136] F. Bignami and D. Zaring, *Comparative Law and Regulation: Understanding the Global Regulatory Process* (Edward Elgar 2016) 32.
[137] Brand n 135, 409.

transactions are at risk of unauthorised payments due to the heightened technological and operational risk and data/privacy breaches in light of the vast amounts of data being collected from m-payment transactions. The first two chapters, therefore, focused on understanding m-payment technologies and the particular risks they pose. During the second stage, it was analysed and presented how two very distinct legal systems, namely the UK and SA, respond to the issues of unauthorised payments and data/privacy breaches.[138] Similar structural laws were identified in both jurisdictions i.e. those which deal with unauthorised payments and data/privacy breaches and it was investigated what functions they play in addressing the two central research issues.[139] Such a structural comparison made it possible to scrutinise differences and similarities.[140] While critics of functionalism point out that it is hardly a theory,[141] it was nonetheless considered helpful to single out dissimilarities and resemblances.[142] During the last step, the analyses of the UK and Saudi responses and solutions were compared and evaluated.[143] The core objective was thus to identify the 'better law'[144] by focusing on comparing, understanding and critiquing the different laws which exist in the UK and SA.[145] It allowed for the law to be determined, particularly the flaws in respect of consumer protection. It provided a window of novel solutions and impetus for legal

[138] Ibid.
[139] J. Husa, 'Research Designs of Comparative Law - Methodology or Heuristics?' In M. Adams, D. Heirbaut (eds) *The Method and Culture of Comparative Law: Essays in Honour of Mark Van Hoecke* (Hart Publishing 2014) 61-62.
[140] Ibid, 62.
[141] G. Frankenberg, 'Critical Compromises: Rethinking Comparative Law' (1985) *Harvard International Law Journal* 26(2), 411-456, 416.
[142] Gordley n 134.
[143] Brand n 135, 409.
[144] R. Michaels, 'The Functional Method of Comparative Law'. In M. Reimann and R. Zimmermann (eds), *The Oxford Handbook of Comparative Law* (OUP 2006) 373.
[145] Ibid, 339.

change for very real problems for m-payment customers in SA.[146] These new solutions are designed to enrich the debate about consumer protection in SA and may play a positive role in influencing legal reform which better protect Saudi m-payment customers.[147]

The functionalist approach revealed that the UK has regularly updated and reviewed its laws to ensure that they evolve alongside the changing risks of the Fintech sector, in contrast to SA which has failed to modernise its legislation in order to accommodate technological advance. In the UK, the consumer protection rationale has been firmly embedded in the Payment Services Regulations 2009, the Electronic Money Regulations 2011, the Payment Services Regulations 2017, the Data Protection Act 1998, the GDPR and the Consumer Rights Act 2015 and in various codes of conduct. As a result, consumers are well protected against unauthorised m-payments and data/privacy breaches. This is in marked contrast to SA which has not ensured that the 2012 Regulatory Rules for Prepaid Payment Services adequately protect consumers against unauthorised m-payment transactions, but only against a much narrower operational risk which causes billing errors. Other laws and regulations, such as the e-Banking Rules 2010 and 2013 Banking Consumer Protection Principles and Banking Consumers' Guide, also fail to adequately address the risk of unauthorised payments. The topic of data/privacy breaches is particularly underdeveloped, as no data protection law has been enacted.

---

[146] A. Watson, 'Legal Transplants and Law Reform' (1976) *Law Quarterly Review* 92, 79-84, 79; Eberle n 123, 485.
[147] I. Calboli, 'A Call for Strengthening the Role of Comparative Legal Analysis in the United States' (2017) *Saint Johns Law Review* 90(3), 609-638, 613.

Motivation and Originality

The legislative analysis deals with m-payment services provided by banks and companies, such as Facebook, ApplePay and PayPal. As citizens' property is being handled through these new technologies, the requisite legal consumer safeguards must be addressed by policy and lawmakers. In SA where the primary source is the Sharia, and as discussed in chapter 3, the main objective is to realise welfare and the conceptualisation of welfare includes the protection of property.[148] As emphasised in chapter 5, the Saudi Arabian Monetary Authority's ('SAMA') regulatory efforts have focused predominantly on a reloadable gift card or stored-value system, but not on facilitating wider m-payment innovation. However, it is unlikely that economic growth within the FinTech sector is going to come from companies having their own reloadable gift card or stored-value system, as discussed in chapter 1.

Moreover, it is normal for states to enact consumer protection laws and policy for important services.[149] As a large part of consumers' daily lives involve making payments, these services are arguably 'services of general economic interest'.[150] It is for this reason essential to close this legislative lacuna in SA in order to protect m-payment customers and the future financial system.

---

[148] A.A. Elias, 'Sharia, Fiqh, and Islamic Law explained', 18 April 2013 <https://abuaminaelias.com/is-the-sharia-a-single-code-of-law-an-explanation-of-sharia-fiqh-and-islamic-law/> accessed 19th November 2017.
[149] Ibid.
[150] M. Durovic and H.W. Micklitz, *Internationalization of Consumer Law: A Game Changer* (Springer 2016) 51.

Without legislative reform, risks which come with these technologies may be unfairly distributed. Consumer property may not be adequately protected because of the practical technical issues which may arise, and which are discussed in chapter 2.

Structure of the Thesis

The thesis is divided into six chapters. Chapter 1 describes the m-payment innovation which is taking place globally and how this is simultaneously transforming the banking sector and the way that customers conduct their financial activity. It provides a brief overview of the predominant technologies which can be employed for m-payments; these include Near-Field Communications ('NFC'),[151] Bluetooth, mobile apps and digital wallets, cloud computing, algorithms, and encryption techniques. The chapter details the many financial transactions and financial information-based advantages that each of these technologies offers to m-payment customers. In other words, it is explained how benefits are created through Fintech innovation. The chapter explains how these interactive technologies benefit customers by facilitating the creation of a quick, convenient and dynamic payment channel, in any location and at any time.

Chapter 2 discusses how the many freedoms brought about by m-payment services have not come without risk. It examines a variety of practical issues and risks associated with the m-payment technologies in order

[151] Near Field Communication Forum, 2013 <http://www.nfc-forum.org/home/> accessed 28 October 2013.

to determine why consumers who use m-payment services need legal protection, what they need protection against and as a result of this, how these customers might be conceptualised in law. To this end, the chapter is divided into three core areas: (1) Customer errors; (2) technology problems and risks; and (3) risks and issues caused by third parties. The reason why these practical issues and risks are discussed is that it is imperative that the law is able to ascertain who is at fault when things go wrong, in order to protect m-payment customers in a highly complex technological ecosystem, particularly against unauthorised m-payment transactions and their data, including against breaches of their privacy.

Chapter 3 explores the Western and Islamic legal consumer protection literature. It covers consumer law, international consumer law, consumer protection laws and embeds the academic contractual literature on unauthorised transactions and the question of loss allocation in the m-payment provider/customer context. The chapter provides an overview of the types of laws that could be rallied to protect m-payment customers, such as, the tortious law of negligence and duty of care. It draws on rational choice theory and behavioural economics and cognitive psychology literature to assess whether the duties and obligations of the m-payment customer should be based on a construction of them as circumspect, rational or vulnerable, and what this, in turn, might mean for the legal threshold available to them. The chapter analyses different policy orientations comprised of the consumer protection interest, consumer economic interest, social welfare or neo-liberal approach that can be adopted when formulating consumer protection legislation in respect of m-payment transactions and m-payment consumers' data. A central

focus of the chapter is Sharia law and its perspective on consumer rights and protection. The chapter provides a general overview of a number of business, religious and ethical principles that can be applied to this area. It is argued that the Sharia requires a social welfare approach and, as Prophet Mohammed was a businessman, it is imperative that innovation must also be promoted. It is argued that the Islamic principle of good faith, alongside other Islamic principles, could be utilised to develop more pro-consumer legislation or legislative provisions when it comes to m-payments in SA.

Chapter 4 analyses the legal framework which the UK has adopted in respect of m-payment services and identifies which policy orientation underpins these laws. The chapter argues that the UK has opted for a policy that reflects a combination of the social welfare and neo-liberal approaches. The UK legal consumer protection measures are comprehensive. As a result, a protective safety net has been created for vulnerable customers who make use of innovative m-payment technologies. The chapter commences with discussing how the UK has facilitated a m-payment third-party collaboration environment, including by pursuing a consumerist policy orientation to facilitate entry and access by third parties and addressing the risk which arise from third-party collaboration. For instance, this has been achieved through the adoption of the Privacy and Electronic Communications (EC Directive) Regulations 2003, the Wireless Telegraphy Act 2006, the Electronic Money Regulations 2011 and the regulation of e-money institutions and voluntary codes of conduct.

Subsequently, the legal sources which govern the rights and obligations of banks including payment institutions and electronic money institutions and customers are discussed, particularly in respect of unauthorised m-payment transactions. Recourse is made to contract and tort law and legislation, such as: the previous Payment Services Regulations 2009 and the new Payment Services Regulations 2017; the FCA's Banking Conduct of Business Sourcebook and the voluntary Standards of Lending Practice 2016.

Thereafter, it is explored how contract performance and unfair terms are dealt with by the Consumer Rights Act 2015 and are likely to impact consumer understanding in respect of unauthorised m-payment transactions.

Finally, the chapter deals with the question of how English law protects consumners' data in order to maintain privacy, as well as how it protects against breaches of consumers' privacy. The mainly repealed Data Protection Act 1998 and the General Data Protection Regulation; the Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017; and the EU Funds Transfer Regulation 2015 are referred to.

Like chapter 4, chapter 5 asks what are the different sources of Saudi law that deal with unauthorised m-payment transactions and the protection of consumers' data in order to maintain their privacy. Chapter 5 firstly scrutinises whether SA facilitates a m-payment third-party collaboration environment, including by drawing a legal distinction between bank status and m-payment providers and highlights the problem with the Banking Control Law 1966 in relation to this. It also discusses the shortcomings of the Electronic Transaction Law 2007.

Thereafter, the Saudi sources of law which govern the rights and obligations of m-payment providers and their customers, particularly in respect of unauthorised m-payment transactions are discussed. The 2012 Regulatory Rules for Prepaid Payment Services and the failure to address the thorny issue of unauthorised m-payment transactions are highlighted. The e-Banking Rules 2010 and the Manual of Combating Embezzlement & Financial Fraud & Control Guidelines 2008 are analysed in order to identify shortcomings.

It is then assessed how contract performance and unfair terms are addressed by the 2013 Banking Consumer Protection Principles and Banking Consumers' Guide. The failure to utilise the principles and guide to seek compensation for unauthorised m-payment transactions is emphasised.

The final section deals with the question of how Saudi law protects consumers' data in order to maintain privacy, as well as how it protects against breaches of consumers' privacy. It considers: The Credit Information Law 2008; the Consumer Credit Regulations 2006, and the Anti-Money Laundering Law 2003 and related rules and regulations and their application to data and privacy protection of m-payment customers' data.

It is argued that Saudi Arabian laws do not mirror UK laws as they are more web 1.0 laws than web 2.0 (as in the UK) and hence outdated. The failure to keep pace with innovation has resulted in Saudi m-payment customers being inadequately protected against unauthorised m-payment transactions. M-payment consumers' data and their privacy are also not safeguarded. This is particularly apparent from the UK legal analysis in chapter 4 which is drawn

upon as a comparator. Hence, Saudi Arabian law is deficient in several aspects and customers who use m-payment services are inadequately protected.

The Conclusion assesses the lessons that SA can learn from the UK in providing greater protection to customers while remaining compliant to Sharia law. Recommendations and suggestions are made therein for the Saudi legislators. The Conclusion also considers how the preceding chapters have met the research aim and questions. The core research findings are presented, including the view that UK laws are comprehensive and far-reaching, and that they protect customers who use m-payment services to a greater degree.

CHAPTER 1

A PRACTICAL OVERVIEW OF M-PAYMENTS

1.1 Introduction

The objective of this chapter is to point out how Fintech innovates the banking sector. The predominant technologies are identified, as well as how they benefit m-payment customers. This is an essential starting point for the thesis as a whole, as it identifies the key challenges which need to be addressed and the benefits of these technologies which regulation should seek to preserve. On the basis of such understanding, we can ensure that the law protects m-payment customers adequately. Awareness of the different technologies also makes it possible to identify the main advantages for m-payment customers. In other words, the chapter depicts the context against which the subsequent legal discussions must be viewed.

However, the chapter is not intended to be an in-depth examination of the technologies. Instead, it gives, by way of background, a brief overview of the particular technology trends and developments, and the advantages which these technologies bring for m-payment customers. For this purpose, the dominant and preferred technologies which are being used or considered for m-payment services are identified. The chapter concludes by summarising the latest trends and stressing the main advantages which arise from the new financial technologies.

ICT have created a significant change from the traditional banking model of face-to-face interaction towards an increasingly depersonalised system.[1] This allows banks to market their services to customers at reduced costs and enables customers to conduct their daily banking transactions in a much more convenient and flexible manner.[2] For example, customers can check their bank accounts, statements and bank account activity through an app on their mobile device. Hence, the fusion of banking with technology creates a new and more self-service oriented m-payment infrastructure.[3] This new infrastructure was initially driven by the increasing adoption of the World Wide Web in the late 1990s and the 2000s, which allowed the retail consumer to enact financial transactions from a personal computer through a web browser.[4] Such innovation gave rise to m-banking services and has allowed customers to enact financial transactions on a convenient '24/7' basis,[5] free from geographical restraint. However, with the rise of mobile smartphones, one of the most profound innovations within this development has been m-payments.

In addition, customers can now install mobile apps, namely device-based or cloud-based digital wallets,[6] to perform the function of e-wallets

[1] Y. Baghdadi, *ICT for a Better Life and a Better World: The Impact of Information and Communication Technologies and Organizations and Society* (Springer 2019) 154.
[2] Ibid.
[3] B. Nicoletti, *The Future of FinTech: Integrating Finance and Technology in Financial Services* (Palgrave Macmillan) 284.
[4] It should be noted, however, that electronic banking on personal computers dates back to the pre World Wide Web days of the early 1980s, with systems such as Minitel in France, and Prestel's Homelink service in the UK: R.K. Miryala and M.V. Ramana Reddy, *Trends, Challenges & Innovations in Management - Volume III* (Zenon Academic Publishing 2015) 112.
[5] R.H. Weber and A. Darbellay, 'Legal Issues in Mobile Banking' (2010) *Journal of Banking Regulation* 11, 129-145, 130.
[6] D. Morley and C.S. Parker, *Understanding Computers: Today and Tomorrow* (15th ed, Cengage Learning 2015) 445.

carrying e-money. Through cryptographic techniques, mobiles thereby become money repositories.[7] Customers can also use their mobiles to make certain types of payments via apps, i.e., they can make m-payments. This type of technology provides customers with direct access to their bank accounts at no additional charge.[8] A connection can be established by a third-party payment provider ('TPP') between the customer's bank and the merchant's bank.[9]

Indeed, since the arrival of e-banking in 1999, demand for m-banking has grown considerably from an estimated 300 million customers globally in 2011 to an estimated one billion by 2019.[10] Increasingly m-payments are becoming popular, with 27% of all card purchases in the UK having been made with contactless cards in 2016.[11] Over £10 billion had been transferred through m-payment apps, such as, Pingit.[12]

Demand for m-payments through smartphones is transforming the payment system as currently known, also since m-payments with digital money

---

[7] A. Hnaif and M.A. Alia, 'Mobile Payment Method Based on Public-Key Cryptography' (2015) *International Journal of Computer Networks and Communications Security* 7(2), 81-92, 81.

[8] D. Hinds, 'Micropayments: A technology with a promising but uncertain future'. In N. Mallat et al (eds), 'Mobile Banking Services' (2004) 47(5) *Communications of the ACM*, 42–46, 44; A. Boden, 'Explaining PSD2 without TLAs is tough!' Starling Bank, 9 October 2015 <https://www.starlingbank.com/explaining-psd2-without-tlas-tough/> accessed 10th September 2016.

[9] R. Wandhofer, 'European Payments: A Path Towards the Single Market for Payments'. In B. Batiz-Lazo and L. Efthymiou (eds), *The Book of Payments: Historical and Contemporary Views on the Cashless Society* (Palgrave Macmillan 2016) 346.

[10] P.A. Salz, *The Netsize Guide 2009: Mobile Society & Me, when worlds combine* (London, Netsize 2009) 102; D. McMillin, 'Massive mobile banking growth', Bankrate, year? <http://www.bankrate.com/financing/banking/massive-mobile-banking-growth/> accessed 13 October 2013; S. Romero, 'The unstoppable growth of digital banking: 3 billion users by 2021', BBVA, 22 February 2017 <https://www.bbva.com/en/unstoppable-growth-digital-banking-3-billion-users-2021/> 19th November 2017.

[11] UK Cards Association, 'UK Card Payments Summary 2017', 2017, 1-4, 1 <http://www.theukcardsassociation.org.uk/wm_documents/UK%20Card%20Payments%202017%20-%20Summary%20FINAL.pdf> accessed 1st September 2017.

[12] D. Worth, 'Mobile banking services pose major security risks, warns financial watchdog', V3.co.uk, 2013 <http://www.v3.co.uk/v3-uk/news/2291042/mobile-banking-services-pose-major-security-risks-warns-financial-watchdog> accessed 28 October 2013.

is increasingly replacing cash.[13] In the future, it may be possible that users will be able to conduct all purchases without cash.[14] As a result, traditional debit and credit cards, as well as cash machines may eventually become replaced.[15] Even cashiers may no longer be required since goods can be scanned and purchased while walking through a shop and users can store their travel cards, gift vouchers, tickets and even their identity cards ('IDs') and driving licences on their mobiles phones, thereby opening the door to myriad new possibilities.[16] Equally, merchants can gather useful data about consumers which can be utilised for marketing and advertising purposes.[17] This raises profound data protection and privacy implications, especially since it enables banks, e-money and payment institutions to hold much more precise transactional, financial, behavioural and other kind of data which profiles customers.[18] This data is certainly valuable from a commercial perspective, but it is important that an appropriate balance is struck between commercial and consumer interests.[19]

[13] V. Marria, 'What A Cashless Society Could Mean For The Future', Forbes, 21 December 2018 <https://www.forbes.com/sites/vishalmarria/2018/12/21/what-a-cashless-society-could-mean-for-the-future/#e40fc1332638> accessed 10 February 2019.
[14] Ibid.
[15] Ibid.
[16] A. Tabakovic, 'The prepaid mobile wallet: A powerful product for an impatient ecosystem' (2014) *Journal of Payments Strategy & Systems* 8(3), 254-263, 254.
[17] C.J. Hoofnagle et al, 'Mobile Payments: Consumer Benefits & New Privacy Concerns' (2012) University of California, 1-19, 6 <https://ssrn.com/abstract=2045580> accessed 5 March 2019
6 <http://ssrn.com/abstract=2045580> accessed 19 December 2013.
[18] Payment Systems Regulator, 'Discussion paper: Data in the payments industry', June 2018, 1-65, 6.
[19] Ibid 5-6.

Micro-business is also encouraged in places where individuals frequently only own a mobile phone and not a computer and often do not have a bank account.[20] M-payments can thus bridge the poverty gap.

All of these innovations are made possible through FinTech, which provides a fusion of financial services with technology. [21] Different technologies fall within the scope of FinTech, and this chapter provides a brief overview of the predominant technologies which can be employed for m-payments.

1.2 The m-payment technologies

A Wireless Application Protocol ('WAP') - i.e. a set of technical protocols - can be used for mobile phones to access the internet.[22] A WAP gives a similar user experience as e-banking, but the problem is that many clicks are necessary.[23] As mobile phone screens are tiny, this is impractical for banking customers.[24] Most banks instead offer m-banking and most recently m-payment apps as they are more user-friendly and convenient to use.[25] These m-payment

[20] G. Demombynes and A. Thegeya, 'Kenya's Mobile Revolution and the Promise of Mobile Savings' (2012) *World Bank Policy Research Working Paper* No.5988, 1-32, 6 <http://ssrn.com/abstract=2017401> accessed 5 January 2014.
[21] Nicoletti n 3, 12.
[22] M. Rouse, 'WAP (Wireless Application Protocol)', TechTarget.com, 2017 <http://searchmobilecomputing.techtarget.com/definition/WAP> accessed 15th November 2017.
[23] Ibid.
[24] T. Lerner, *Mobile payment* (Springer 2013) 45; A. Kaikkonen and V. Roto, 'Navigating in a mobile XHTML application', *Proceeding CHI '03 Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* 2003, 329-336; S. Singhal, *WAP-the Wireless Application Protocol: Writing Applications for the Mobile Internet* (Addison-Wesley 2001) 11.
[25] See, e.g., Barclays, 'Barclays Mobile Banking app', 2013 <http://www.barclays.co.uk/BarclaysMobileBanking/BarclaysMobileBankingapp/P1242609123821> accessed 28 October 2013; Pingit, 2019 <https://www.pingit.com/> accessed 1 February 2019.

apps are also offered by non-banks, e.g. companies such as Facebook.[26] These apps have several functionalities which pave the way for transaction-based, as well as informational services.[27] Mobile phones can be turned into a mobile brokerage through which transactions and payments, including financial trades, can be conducted.[28] For example, one can easily find out one's account balance and mobile accounting software ensures that new balances are instantaneously displayed.[29] M-payments apps permit users to make electronic transfers of funds from their accounts. Additionally, m-payment apps can turn phones into money repositories by performing the function of e-wallets.[30] Phones can be swiped or scanned to settle payments in shops and stores, just like debit or credit cards, but much faster.[31] Hence, customers can now use a convenient, fast and easy channel.[32] M-payment customers do not have to use cash. They do not have to take out their debit or credit card and sign or enter their personal identification number ('PIN').[33] Waiting time is thereby reduced, as a simple tap or scan with their mobile phone is sufficient to execute the payment.[34]

[26] M. Muchmore, 'The Best Mobile Payment Apps', PC Mag, 2 April 2018 <https://www.pcmag.com/roundup/358553/the-best-mobile-payment-apps> accessed 20 April 2019.
[27] Essvale Corporation Ltd, *Business Knowledge in IT in Global Retail Banking, the Complete Handbook for IT Professionals* (Essvale Corporations Ltd 2011) 16.
[28] Alpari, 'Mobile trading', 2013 <http://www.alpari.co.uk/trading-platforms/mobile-trading> accessed 29 October 2013.
[29] Essvale Corporation Ltd n 27, 16.
[30] D. Neef, *Digital Exhaust: What Everyone Should Know About Big Data, Digitization, and Digitally Driven Innovation* (Pearson Education 2015) 60.
[31] B. King, *Bank 3.0, Why Banking Is No Longer Somewhere You Go, But Something You Do* (Marshall Cavendish Business 2013) 191.
[32] Ibid.
[33] Neef n 30, 60.
[34] Ibid.

The latter function is facilitated, for instance, with the help of Near-Field Communications ('NFC').[35] NFC refers to a set of standards that allow electronic devices to communicate with computer networks through radio communication in close proximity.[36] It covers both network protocols (i.e. clearly defined procedures, rules and formats for network devices to communicate[37]) and data exchange formats (i.e. conversion of source data by a program into an exchange format for further conversion into a target format),[38] and is defined under a range of international standards[39] as set by the NFC Forum, a consortium established by some of the major mobile technology providers.[40] The benefits of NFC are that it is more stable, secure and faster than, for example, Wifi, Bluetooth, Sound Wave and Infra-red.[41]

Bluetooth is a low energy frequency, which establishes a connection with the internet through a 'low energy sensor device' and is particularly utilised by mobile phones; Wireless-Fidelity ('Wi-Fi') is a 'networking standard' particularly employed to quickly transfer big data.[42] Sound waves

---

[35] Near Field Communication Forum, 2013 <http://www.nfc-forum.org/home/> accessed 28 October 2013.
[36] Ibid.
[37] Ibid.
[38] A. Hernich, *Foundations of Query Answering in Relational Data Exchange* (Logos Verlag GmbH 2010) iii.
[39] For instance, ISO 15693, ISO 18000, ISO 18092/NFCIP-1, ISO 21481/NFCIP-2, ISO 14443: A. Attard, 'A Novel Card-Present Payment Scheme using NFC Technology', Royall Holloway, University of London, 2010-2011, 1-98, 12 <http://www.ma.rhul.ac.uk/static/techrep/2012/MA-2012-07.pdf> accessed 27 December 2013.
[40] NFC Forum, 'Our Members NFC', 2019 <https://nfc-forum.org/about-us/our-members/> accessed 5 March 2019.
[41] SPD Bank, 'NFC and Mobile Bank 2.0', GSMA (2013), 1-20, 4 <http://www.gsma.com/mobilecommerce/wp-content/uploads/2013/07/3.-XUE-JIANHUA-Pudong-Dev-Bank.pdf> accessed 29 October 2013.
[42] P. Smith, 'Comparisons between Low Power Wireless Technologies, Bluetooth low energy, ANT, ANT+, RF4CE, ZigBee, Wi-fi, Nike+, IrDA and NFC, CSR Whitepaper' (2013), 1-29, 5-6 <http://www.csr.com/sites/default/files/white-

and infra-red are other electromagnetic spectra, which are utilised by communication technologies.[43]

These technologies have different capabilities of carrying data and use different means, i.e., electromagnetic waves are carried through metallic wires, radio waves through radio masts or 'lightwaves through optical cables'.[44] NFC requires radio-frequency electromagnetic fields through which data can be transmitted wirelessly and contactless and allows electronically tagged objects, which store information, to be identified and tracked; this then renders them into 'contactless smart cards' due to the communication dialogue, which has been created.[45] NFC is therefore an extension of Radio-Frequency Identification ('RFID'), i.e., the NFC protocol and interface are added to the RFID infrastructure.[46] RFID is normally used to link two devices which are in close contact and the NFC protocol ensures that the configuration data is integrated within a peer-to-peer ('P2P') network[47] when the device is in Active Mode.[48] However, communication can continue even when the device is in Passive Mode, using longer range technology, such as Bluetooth, thereby

papers/comparisons_between_low_power_wireless_technologies.pdf> accessed 29 December 2013.

[43] S. Boydell and R. Braidwood, *Preliminary Physics, Cambridge Checkpoints 2012* (CUP 2011) 70-72.

[44] A. Valdar, *Understanding Telecommunications Networks* (Institution of Engineering and Technology 2006) 16.

[45] A. Rida et al, *RFID-Enabled Sensor Design and Applications* (Artech House 2010) 18.

[46] S. Ahson and M. Ilyas, *RFID Handbook, Applications, Technology, Security, and Privacy* (CRC Press 2008) 376.

[47] A Peer-to-Peer (P2P) network is an architecture which links tasks amongst the peers and these peers gain equal privileges through the nodes which connects all peers with each other: L.T. Yang et al, *Handbook on Mobile and Ubiquitous Computing: Status and Perspective* (CRC Press 2012) 40.

[48] The active mode or 'forward active mode' means that the device can be operated through a bipolar junction transistor through which the current can flow. The current does not flow through the bipolar junction transistor since this is in reverse: M.B Patil, *Basic Electronics Devices and Circuits* (PHI Learning 2013) 197.

optimising battery use due to lower energy consumption.[49] Hence, only one device has to be powered, whereas the other is powered by the transmission of radio waves.[50] This makes it possible for NFC card readers to accept payments through contactless credit cards, so long as both devices are brought into close contact.[51]

The RFID infrastructure coupled with NFC can be used for three different types of operation: Firstly, through NFC, mobile devices can read information contained on 'passive RFID tags' which are stored publicly and respond to information on a 'Uniform Resource Locator' ('URL') (for instance, by allowing information from a web address to be decoded). In addition, data can be added to tags, including on other devices. Hence, NFC has a 'writing and reading' mode.[52] Secondly, NFC allows mobile device owners to undertake business transactions without any contact through payment identification and access control management as it has a 'card emulation' mode.[53] Thirdly, NFC allows for increased interaction with others since data is transferred 'peer-to-peer',[54] for instance via Bluetooth.[55] NFC is ideal for mobile device owners who can enter their PIN or other identification each time they make a payment.[56]

---

[49] Ibid.
[50] Ahson and Ilyas n 46, 12.
[51] Ibid.
[52] A. Cavoukian, 'Mobile Near Field Communications (NFC) "Tap 'n Go" Keep it Secure & Private, Information and Privacy Commissioner Ontaria', Canada, 2013, 1-22, 5 <http://www.ipc.on.ca/images/Resources/mobile-nfc.pdf> accessed 29 December 2013.
[53] Ibid.
[54] Ibid.
[55] E. Haselsteiner and K. Breitfuss, 'Security in Near Field Communication (NFC), Strengths and Weaknesses', undated, 1-11, 4 <http://ece.wpi.edu/~dchasaki/papers/Security%20in%20NFC.pdf> accessed 27 December 2013.
[56] M. Hendry, *Near Field Communications Technology and Applications* (CUP 2014) 185.

Yet NFC is not the only technology which allows greater m-payment functionality. Apple recently replaced NFC with iBeacon, a low energy Bluetooth which has wireless sensors to detect transmitted data in a particular location, such as, customised coupons upon entering a shop, and allows payments to be made via mobile phones.[57] Equally, PayPal has adopted the 'PayPal Beacon' which is simply connected to a power outlet in a store and when those who have downloaded the PayPal app then enter the shop, a dialogue, which is facilitated through Bluetooth, is created.[58] As a result, customers are immediately checked in upon entering a shop and can pay hands-free.[59] Other competitors to NFC are, for example, QR Codes/2D Barcodes, which can be used on most devices and are inexpensive to adopt and maintain.[60] Barcodes are commonly found in supermarkets on products and are normally scanned at the till by the cashier.[61] However, barcodes do not possess strong security features and can also easily be obscured.[62] This method has thus not become widely accepted.[63] Otherwise, traditional plastic cards, such as, Europay, MasterCard and Visa ('EMV') which use chip-and-PIN or magnetic stripes, compete with NFC and clouds.[64] Yet these technologies do not allow

[57] G. Gilchrist, *Learning iBeacon* (Packt Publishing 2014) Chapter 1.
[58] J. Xu, *Digital Payment Systems, Managing Digital Enterprise* 2014, 159-175; R. Borison, 'PayPal challenges NFC with bluetooth-enabled mobile payments', Mobile Commerce Daily, 2013 <http://www.mobilecommercedaily.com/paypal-gives-nfc-a-run-for-its-money-with-new-bluetooth-mcommerce-option> accessed 30 December 2013.
[59] Borison (ibid).
[60] F. Stertz et al, 'NFC-Based Task Enactment for Automatic Documentation of Treatment Processes'. In I. Reinhartz-Berger et al (eds.), *Enterprise, Business-Process and Information Systems Modeling* (Springer 2017) 42.
[61] Ibid.
[62] Ibid.
[63] J.T.J. Penttinen, *The Telecommunications Handbook: Engineering Guidelines for Fixed, Mobile and Satellite Systems* (John Wiley & Sons 2015) 123
[64] Ibid.

customers to undertake anything else apart from the transaction and are therefore not suitable for m-payments.[65]

Irrespective of the particular enabling technology (e.g. NFC, QR Codes or Bluetooth), the advantage is that customers are enabled to store e-money like in a conventional bank account in a digital wallet, which they can use to settle transactions and make payments by either tapping a screen or swiping their phone.[66] Contactless cards, such as London Oyster Card, the Japanese Rail Suica Card, South Korean T-money or the Mumbai's transport system bus card, can already be used for transport or to pay in convenience stores.[67] Contactless pay and touch terminals have also been set up, for example, by Starbucks, Barclays, GooglePay and ApplePay.[68] This, coupled with the increasing use of smartphones, has further paved the way for NFC or similar technologies to become integrated within mobile phones.[69]

Apart from close-proximity m-payments facilitated through apps and, e.g. NFC or Bluetooth, remote m-payments can be made via mobile apps which are linked to the payer's credit and/or debit cards, or the customer's account to pre-set payees.[70] The advantage for m-payment customers is that

---

[65] Ibid; M. Liard and R. Gupta, 'NFC vs Current Mobile Payment Alternatives, Transaction World Magazine', 2013 <http://www.transactionworld.net/articles/2013/may/global-nfc.html> accessed 20 December 2013.

[66] J. Xu, *Managing Digital Enterprise: Ten Essential Topics* (Atlantis Press 2014) 184.

[67] Rida et al n 73, 18.

[68] R. Boden, 'Barclays and Starbucks promote contactless in UK', NFC World, 18 June 2015 <https://www.nfcworld.com/2015/06/18/336077/barclays-and-starbucks-promote-contactless-in-uk/> accessed 1 March 2019; F. Campbell, 'Contactless payments continue to grow in the UK', Mobile Transaction, 2 January 2019 <https://www.mobiletransaction.org/contactless-payments-uk/> accessed 1 March 2019.

[69] B. Leighton, 'NFC mobile payments: overcoming the barriers for banks', Banking Technology, 2013 <http://www.bankingtech.com/151452/nfc-mobile-payments-overcoming-the-barriers-for-banks/> accessed 29 October 2013.

[70] N. Ozatac and K.K. Gökmenoglu, *Emerging Trends in Banking and Finance: 3rd International Conference on Banking and Finance Perspectives* (Springer 2018) 207.

they do not have to enter their details each time.[71] Instead this is stored and can be easily confirmed by entering the username and password.[72] These apps make use of either server-side[73] or client-side wallets,[74] both of which can be used with all types of merchants or only particular vendors.[75] Server-side wallets store all data with a third party, whereas client-side wallets store all data on the device of the owner.[76] Server-side wallets have particularly become facilitated due to the arrival of cloud-based solutions.[77] Cloud computing involves various computers which all use the same application and are being connected through a network, most frequently the internet.[78] Yet there are not that many cloud-based service providers so possible trust issues can arise.[79] This is because the few providers would have an oligopoly and could easily dominate the market and consumers may not want to entrust important data to just a few corporations.[80] Nonetheless, in 2014, Visa launched the first cloud-based system for m-payments.[81] The cloud may become the favoured technology since banks and m-payment providers do not have to commit a lot of resources to develop the software and hardware.[82]

---

[71] Ibid.
[72] Ibid.
[73] The digital wallet can be stored on the server of the business.
[74] The digital wallet can be stored on the electronic device by the customer.
[75] Tabakovic n 16.
[76] Ibid.
[77] Ibid.
[78] Y. Feng et al, 'Price Competition in an Oligopoly Market with Multiple IaaS Cloud Providers' (2014) *IEEE Transactions on Computers* 63(1), 59-73, 59; A.S. Horvath and R. Agrawal, 'Trust in cloud computing', *South East Conference*, 9-12 April 2015, 1-8, 1.
[79] Ibid (Feng et al).
[80] Ibid.
[81] VISA, 'BBVA and Visa launch first commercial solution for cloud-based mobile payments', 2015 <http://www.visaeurope.com/newsroom/news/bbva-and-visa-launch-first-commercial-solution-for-cloud-based-mobile-payments> accessed 18 July 2015.
[82] N. Daidj, *Developing Strategic Business Models and Competitive Advantage in the Digital Sector* (IGI Global 2015) 2011; B. Nicoletti, *Cloud Computing in Financial Services* (Palgrave Macmillan 2013) 80.

Another advantage for m-payment customers is that device security, application security and network security are ensured.[83] For this purpose, cryptographic techniques have been integrated within mobile devices, the apps and the network in order to facilitate their use as money repositories and to make m-payments via apps.[84] Indeed, mobile phones offer password protection and apps, including for cloud-based systems, and integrate further security features.[85] Tokenisation has become particularly popular to achieve security in respect of m-payment services via apps.[86] A higher value account number is being replaced by a lower value token which is only issued for one transaction, thereby screening the account number against unlawful use.[87] Hence, the static credentials are being replaced with different credentials.[88] Tokenisation reduces the amount of sensitive data that is being kept on mobile devices and sent over the network when a m-payment is made, which reduces the risk of security breaches.[89] In addition, security is facilitated through Host Card Emulation ('HCE') which can be installed through an app, which verifies the data from the operating system of the phone against the data of the HCE app.[90] All these technological developments have made m-payments possible since security risks have been curtailed.

---

[83] T. Nguyen et al, *IBM Redbooks, IBM MobileFirst in Action for mGovernment and Citizen Mobile Services* (International Business Machines Corporation 2015) 26-27.
[84] Ibid.
[85] Ibid.
[86] J. Stapleton and R.S. Poore, 'Tokenization and Other Methods of Security for Cardholder Data' (2011) *Information Security Journal: A Global Perspective* 20(2), 91-99, 91-92.
[87] Ibid.
[88] Ibid.
[89] Ibid.
[90] T. Khiaonarong, 'Oversight Issues in Mobile Payments' (2014) IMF Working Paper, 1-35, 19.

1.3 Conclusion

The provision of m-payment services through digital devices is undoubtedly a very important future market with the potential to transform the payment system, the banking system and the retail sector.[91] These developments may pave the way for a future cashless society.[92] The leading technologies, e.g., m-payment apps, digital wallets carrying e-money, NFC or Bluetooth (i.e., contactless or tap and go technology), realise the 'jump' from the traditional (physical) credit/debit card to a sophisticated m-payment system embedded within the various functionalities of today's smartphones.[93] As a result, m-payment customers can easily access many different functionalities and services, the checkout becomes faster and simpler and the m-shopping customer experience becomes enhanced.[94]

The life of consumers becomes simplified. Also, the accessibility of financial services to consumers is enhanced.[95] Consumers are empowered to conduct financial transactions extremely easily. For instance, proximity payments through card swiper technology enables them to authorise transactions simply by tapping the device on the POS terminal.[96] M-payment customers may also be able to scan products which they intend to purchase and

[91] C.J.F. Li et al, 'Exploring Mobile Peer-to-Peer Payment Adoption: The Effects of SNS and Native Mobile Banking Apps Usage' (2018) *PACIS 2018 Proceedings*, 109-118, 109.
[92] Marria n 13.
[93] M.Y. Zhang and M. Dodgson, *High-tech Entrepreneurship in Asia: Innovation, Industry and Institutional Dynamics in Mobile Payments* (Edward Elgar 2007) 144.
[94] E. Taylor, 'Mobile payment technologies in retail: a review of potential benefits and risks' (2016) *International Journal of Retail and Distribution Management* 44(2), 159-177, 164.
[95] X. Zhu, *Emerging Champions in the Digital Economy: New Theories and Cases on Evolving Technologies and Business Models* (Springer 2019) 40.
[96] J.T.J. Penttinen, *Wireless Communications Security: Solutions for the Internet of Things* (John Wiley & Sons 2017) 18.

to automatically pay for them when they visit stores.[97] Consequently, m-payment technology enables them to avoid waiting in any queues and they thus can save time.[98] The available software also ensures that customers have a more seamless payment experience.[99]

As a self-service technology, m-payments can increase efficiency and result in cost savings.[100] Much more dynamic economic engagement is being facilitated between consumers and businesses.[101] Such progression goes hand in hand with the evolution of the internet from web 1.0 to the more interactive and dynamic web 2.0 version and in the future web 3.0.[102] A study about the US economy found that increased use of self-service technology could boost the US economy by US$130 billion annually.[103] The potential boost to the US economy is likely to be replicated in the UK and SA where self-service technology is also being increasingly adopted. In the UK, many of the major banks[104], as well as companies, such as Facebook Messenger[105] and PayPal, offer m-payment services.[106] However, it will still take time to create the

[97] L. Tugby, 'Sainsbury's to launch scan-and-go smartphone shopping app', RetailWeek, 15 April 2015 <https://www.retail-week.com/sectors/grocery/sainsburys-to-launch-scan-and-go-smartphone-shopping-app/5073990.article> accessed 15th September 2017.
[98] Taylor n 94, 164.
[99] Ibid.
[100] Ibid 165-166.
[101] Ibid 165.
[102] P. Kommers et al, *The Evolution of the Internet in the Business Sector: Web 1.0 to Web 3.0* (IGI Global 2015) 336.
[103] Financial Action Task Force, 'Guidance for a Risk-Based Approach, Prepaid Cards, Mobile Payments and Internet-Based Payment Services', June 2013, 1-47, 3 <http://www.fatf-gafi.org/media/fatf/documents/recommendations/guidance-rba-npps.pdf> accessed 1 March 2015.
[104] E.g. see Paym, 'The UK's Mobile Payment System', 2019 <https://paym.co.uk/> accessed 2 March 2019.
[105] N. Lanxon, 'Facebook to Make Mobile Payments Service Available Outside U.S.', Bloomberg, 6 November 2017 <https://www.bloomberg.com/news/articles/2017-11-06/facebook-to-make-mobile-payments-service-available-outside-u-s> accessed 1 March 2019.
[106] Finder, 'Mobile payment apps make it easy to pay (and collect) money between friends', 7 March 2019 <https://www.finder.com/uk/peer-to-peer-payment-apps?country_from=GBR&country_to=USA&amount=5000> accessed 12 March 2019.

infrastructure for proximity m-payments facilitated through NFC or Bluetooth because payment of sale terminals have to be further rolled out, e.g., for Apple Pay or other third-party payment specialists.[107] Consequently, the m-payment infrastructure has to mature.

Consumers must also become more accustomed to making use of their phones for payments, instead of traditional visa and debit cards or cash.[108] In light of these emerging trends, the thesis focuses on remote m-payments. The reason is that the m-payment transformation is at present being facilitated through remote m-payments, which are provided by companies, such as PayPal and Facebook Messenger.[109] It also discusses proximity m-payments transactions.

The changes within the finance sector due to the use of these technologies necessitate that SA urgently updates its laws, as stressed in chapters five and the conclusion. Accordingly, the legislative analysis deals with m-payment services provided by banks and companies, such as Facebook Messenger, Apple Pay or PayPal. It is for this reason essential to close this legislative lacuna in SA in order to protect not only m-payment customers, but also the future financial system.

Without legislative reform measures, the problem is that the risks which come with these technologies may be unfairly distributed. Consumer property,

---

[107] J.A. Martin, '7 reasons mobile payments still aren't mainstream', CIO Insider, 7 June 2016 <http://www.cio.com/article/3080045/payment-processing/7-reasons-mobile-payments-still-arent-mainstream.html> accessed 10th November 2016.

[108] H. Qasim and E. Abu-Shanab, 'Drivers of mobile payment acceptance: The impact of network externalities' (2016) *Information Systems Frontiers* 18(5), 1021-1034, 1021.

[109] Information Resources Management Association, *Banking, Finance, and Accounting: Concepts, Methodologies, Tools, and Applications* (Business Science Reference 2015) 183; Finder n 106.

as well as personal data, may not be adequately protected because of the practical technical issues which may arise, and which are discussed in the next chapter.

CHAPTER 2

FINTECH INNOVATION AND RISKS FOR CONSUMERS

2.1 Introduction

Whilst FinTech innovation has various advantages for m-payment customers, it also gives rise to a host of disadvantages and risks.[1] This chapter therefore identifies the main sources of risk of m-payment services - 1. customer errors; 2. technology problems and risks; and 3. risks and issues caused by third parties. The practical problems which can arise and cause disadvantages for m-payment customers are explained. Any m-payment law must ideally mitigate the risk and practical issues and allocate responsibilities for the different sources of risk. Together with Chapter 1, this chapter thus provides the context for the discussions, especially in the later discussion of the legal position in the UK and SA and of potential reforms which might be introduced in the latter. Hence, this chapter highlights the most pressing matters which a legislator must consider when devising laws for m-payments designed to protect m-payment customers. It particularly stresses the need to protect m-payment customers against unauthorised m-payment transactions and to protect consumers' data in order to maintain privacy. The reason is that security and data/privacy breaches are arguably the most serious concerns within the m-

[1] Y.-C. Pan et al, 'Extending Technology Acceptance Model for Proximity Mobile Payment via Organisational Semiotics'. In K. Liu et al (eds), *Digitalisation, Innovation, and Transformation* (Springer 2018) 48.

payment space.[2] Cyber attacks which are perpetrated to commit fraud, disrupt or harm the payment system and/or collect data are on the increase and cause substantial losses.[3] It is, therefore, essential to understand the potential sources of new security risks within the complex m-payment ecosystem which brings together different stakeholders, most notably banks, telecom operators, card issuers, software developers, security experts, cloud storage providers, mobile device operators, retailers and loyalty scheme providers.[4]

Hence, the implementation of any of the m-payment technologies (discussed in chapter 1) requires banks to make investments to integrate instant payment features made available through NFC, iBeacon or other similar technologies.[5] Banks must thus develop the technological capacity to create and maintain an integrated m-payment infrastructure.[6] Alternatively, they must enter into new partnerships as already seen, for instance, by the Google Wallet adoption or development of applications, such as Orange, Barclays' Quick Tap or Paym.[7] New alliances must be formed which may be bank-led, i.e., the bank can remain responsible for 'the customer account relationship', but enter into, for instance, a joint venture with a non-bank or various partnerships and

[2] EY, 'The heightened threat of cyber attacks is fueling payment losses - how should your business respond? April 2018, 1-4, 2 <https://www.ey.com/Publication/vwLUAssets/EY-convergence-of-payments-and-cybersecurity/$File/EY-convergence-of-payments-and-cybersecurity.pdf> accessed 10 July 2019.
[3] Ibid.
[4] DM Wallet Summit, 'Digital Wallet Opportunity', 2013 <http://www.dmwsummit.com/digital-wallet-opportunity/> accessed 13th October 2013.
[5] Essvale Corporation Ltd, *Business Knowledge in IT in Global Retail Banking, the Complete Handbook for IT Professionals* (Essvale Corporations 2011) 16.
[6] Ibid.
[7] M. Warman, 'Orange and Barclaycard launch 'Quick Tap' mobile phone payments', The Telegraph, 20 May 2011 <https://www.telegraph.co.uk/technology/news/8525031/Orange-and-Barclaycard-launch-Quick-Tap-mobile-phone-payments.html> accessed 10 February 2019.

alliances.[8] Alternatively, it may be bank-focused or non-bank led where the bank is responsible for safeguarding the funds but not account management on a daily basis.[9] Whilst a non-bank led model may emerge in the future, this appears to be most likely based on collaboration.[10] For example, many of the biggest US banks have teamed up with Google Wallet, ISIS, iPhone or Master Card/Visa.[11] ISIS allows users to purchase goods through NFC at particular terminals.[12] Google Wallet allows users to shop in stores, which allow contactless payments, to buy goods and services online and send money, including from users' debit and credit cards.[13]

However, one disadvantage for m-payment customers is that some stores only accept a particular m-payment mechanism.[14] For instance, whilst Apple Pay may work in most stores, it is not accepted by Walmart in the US.[15] This is because Walmart has its own m-payment app which it wants its customers to use.[16] Consequently, m-payment customers may have to install several m-payment apps on their phones if they do not wish to use cash or credit and debit cards.[17] They may find this frustrating as the use of multiple apps does not make their lives easier. The advantage of the otherwise more convenient m-payment channel may thus be lost. Non-acceptance of certain m-

[8] Essvale Corporation Ltd n 5.
[9] Ibid.
[10] Ibid.
[11] B. King, *Bank 3.0, Why Banking Is No Longer Somewhere You Go, But Something You Do* (Marshall Cavendish Business 2013) 191.
[12] B. Nicoletti, *Mobile Banking: Evolution Or Revolution?* (Palgrave Macmillan 2014) 128.
[13] Google Wallet, 'Shop, Save. Pay. With your phone', 2013 <http://www.google.co.uk/wallet/index.html> accessed 29 December 2013.
[14] S. Epstein, 'Is the fintech industry killing mobile payments?' Finextra, 16 August 2016 <https://www.finextra.com/blogposting/12976/is-the-fintech-industry-killing-mobile-payments> accessed 1st September 2017.
[15] Ibid.
[16] Ibid.
[17] Ibid.

payment apps by merchants also constitutes an entry barrier for new market participants.[18] Similarly, the fact that there exist various different technologies which can be employed for m-payments may result in the market becoming more fragmented.[19] However, the most significant risk and thus disadvantage for m-payment customers is that the complex technology and complicated relationships between different stakeholders give rise to new security risks. These risks may particularly impact payment transactions and payment data. For that reason, the next section discusses how m-payments heighten technological risks.

2.2 M-payments and the magnified technological risks

In any legal system, the law must find answers to the different practical problems which may arise when technological risk occurs in order to protect m-payment customers. Fundamentally, m-payments magnify technological risks as two extra elements are added – the mobile handset or electronic device and the mobile network.[20] This is because the chain across which services are rendered is considerably extended.[21] As a result, m-payments pose various new risks, specifically operational, credit and regulatory risk.[22] Basel II defines

[18] Ibid.
[19] S. Pandy and M. Crowe, 'What's New with Regulation in the Mobile Payment and Fintech Space?' Federal Reserve Bank of Boston, MPIW Meeting with Regulators Report, 25 May 2017, 1-7, 3 <http://www.asbasupervision.com/es/bibl/x-lecturas-recomendadas/1507-lr229/file> accessed 2nd September 2017.
[20] J. Téllez and S. Zeadally, *Mobile Payment Systems: Secure Network Architectures and Protocols* (Springer 2017) 26.
[21] Essvale Corporation Ltd n 5.
[22] Financial Conduct Authority, 'Mobile banking and payments -supporting an innovative and secure market', Thematic Review TR13/6, August 2013, 1-12, 6-7 <http://www.fca.org.uk/your-fca/documents/thematic-reviews/tr13-6> accessed 12 October 2013.

operational risk as damage due to failed or inadequate systems, people or processes, which can be caused by external or internal circumstances.[23] Credit risk is occasioned when there is a default, i.e. when a credit obligation is not paid, including on time.[24] Credit risk is a loss as a result of a 'credit event' which can be occasioned through fraud and theft; the risk of fraud may be elevated due to high operational risk.[25] Strictly speaking, credit risk is best considered as part of operational risk.[26] There is thus a certain degree of overlap since operational and credit risks particularly emanate from various security[27] and technology risks.[28] The newly emerging m-payment market also raises regulatory questions which impact customer protection. For instance, a pressing regulatory matter is e-wallet regulation.[29] The reason for this is that e-wallets are often provided by third parties, which thereby effectively assume a vital payment role.[30] Hence, when banks collaborate with third-party digital wallet providers, it must be ensured that these third parties protect customer funds, including their data and privacy.[31] Customers must also be empowered

[23] Bank for International Settlements, 'Basel Committee on Banking Supervision, Consultative Document, Operational Risk', Supporting Document to the New Basel Capital Accord, 2001, 1-30, 2 <http://www.bis.org/publ/bcbsca07.pdf> accessed 28 October 2013; P. Curwen and J. Whalley, *Mobile Telecommunications in a High-Speed World, Industry Structure, Strategic Behaviour and Socio-Economic Impact* (Gower Publishing 2010) 218.
[24] M. Anolli et al, *Retail Credit Risk Management* (Palgrave MacMillan 2013) 34.
[25] M. Choudhry, *The Principles of Banking* (John Wiley & Sons Singapore Pte Ltd 2012) 143; I. Matthaus-Maier and J.D. von Pischke, *New Partnerships for Innovation in Microfinance* (Springer-Verlag 2009) 161.
[26] P. Goldmann, *Financial Services, Anti-Fraud Risk and Control Workbook* (John Wiley & Sons Inc 2010) 39-40.
[27] P. Suresh and J. Paul, *Management of Banking and Financial Services* (2nd ed, Dorling Kindersley (India) Pvt Ltd 2010) 500.
[28] J.L. Bayuk et al, *Cyber Security Policy Guidebook* (John Wiley & Sons Inc 2012) 192.
[29] G. Dorfleitner et al, *FinTech in Germany* (Springer 2017) 82.
[30] S. Pandy and M. Crowe, 'What's New with Regulation in the Mobile Payment and Fintech Space?' Federal Reserve Bank of Boston, MPIW Meeting with Regulators Report, 25 May 2017, 1-7, 3 <http://www.asbasupervision.com/es/bibl/x-lecturas-recomendadas/1507-lr229/file> accessed 2nd September 2017.
[31] Ibid.

to resolve disputes which arise because of e-wallet providers.[32] Another important legal reform could be to establish digital identities with the help of banks.[33] Both areas go to the core of customer protection. This is because fraud prevention ultimately protects the m-payment customer.

In the context of m-payments, consumer protection especially requires that the magnified technological and thus operational risks are combated. Customers must be assured that payment transactions can be safely sent through the m-payment system and that the related data, including their privacy, is also safeguarded. The negative impacts which arise from security failures, including in respect of payment data, must be understood. Legislators must try and minimise the primary problems which arise from m-payments by addressing how liability should be allocated when customer funds are lost because technological and operational risks materialise and/or the vast amount of collected consumer data is not adequately protected.

In other words, a purely contractual position and thus neo liberal position[34] in the context of unauthorised transactions and the protection of customers' data is unlikely to guarantee fairness for customers.[35] For instance, research, which investigated whether bank terms and conditions in respect of accepting liability for unauthorised transactions was fair, found that banks

[32] Ibid.
[33] World Economic Forum, 'A Blueprint for Digital Identity, The Role of Financial Institutions in Building Digital Identity', August 2016, 1-108, 1 <http://www3.weforum.org/docs/WEF_A_Blueprint_for_Digital_Identity.pdf> accessed 1st May 2017.
[34] K. Birch, *A Research Agenda for Neoliberalism* (Edward Elgar 2018) 156.
[35] I. Becker et al, 'International comparison of bank fraud reimbursement: customer perceptions and contractual terms' (2017) *Journal of Cybersecurity* 3(2), 109-125, 109-110.

unfairly imposed liability on customers.[36] Another study identified that bank terms and conditions lacked adequate information for customers to know how to comply with their contractual duties.[37] It has also been observed that bank practices in respect of allowing personal identification numbers (PINs) changes sometimes facilitate that customers breach the terms and conditions.[38]

It is for this reason important to discuss the different sources of risk to understand the various circumstances which can arise, so that legal liability can be correctly allocated.[39] Otherwise, m-payment providers will act carelessly when it comes to guaranteeing security if customers were too easily held accountable for unauthorised m-payment transactions.[40] Also economic efficiency will most likely be realised if the risks were allocated to the party who is most able to minimise the occurrence of the unauthorised transaction and who is able to adopt a clear process for retrieving funds.[41]

Risk can be caused by m-payment customers, security issues, as well as third parties which provide the m-payment infrastructure together with banks, as discussed in the next sections: M-payment customers may not be refunded missing, lost, stolen or wrongly sent funds. They may fall victim to fraud,

---

[36] N. Bohm et al, 'Electronic commerce: Who carries the risk of fraud' (2000) *The Journal of Information, Law and Technology*, 3 <https://warwick.ac.uk/fac/soc/law/elj/jilt/2000_3/bohm/> accessed 10 April 2019.
[37] S.J. Murdoch et al, 'Are payment card contracts unfair?' In: J. Grossklags and B. Preneel (eds), *Financial Cryptography and Data Security* (Springer 2016) 600-608, 600.
[38] Becker et al n 35, 110-111.
[39] Ibid, 111.
[40] Ibid.
[41] A.C.B. Hache and N. Ryder, 'Tis the season to (be jolly?) wise-up to online fraudsters. Criminals on the Web lurking to scam shoppers this Christmas: A critical analysis of the United Kingdom's legislative provisions and policies to tackle online fraud' (2011) *Information & Communications Technology Law* 20, 35-56, 35; ibid.

including identity theft. Their personal data may be used without authorisation, may be compromised, and their privacy invaded.

Consequently, m-payments have various disadvantages because of technology-related practical problems. These issues must be understood in order to analyse in subsequent chapters how greater protection can be achieved for m-payment customers. Put differently, any legal system must consider the different sources of risk, i.e. whether a risk was caused by a m-payment customer, as opposed to security issues or third parties. The next sections therefore provide an overview of the practical technological problems which cause disadvantages for m-payment customers. For this purpose, it is firstly discussed which problems may be caused by m-payment customers. Thereafter, common security issues are highlighted, as well as which problems may arise because of third parties which help to create the m-payment infrastructure.

2.2.1 Technological risks and consumer understanding

One disadvantage of m-payment services is that customers may make mistakes and as a result lose money.[42] The question of how the law should treat such customers depends on whether customers are conceptualised as reasonably circumspect or vulnerable, as briefly outlined in this section and discussed in

[42] M. Solin and A. Zerzan, 'Mobile Money: Methodology for Assessing Money Laundering and Terrorist Financing Risks' (2010) GSMA Discussion Paper, 1-35, 6-7 <http://www.gsma.com/mobilefordevelopment/wp-content/uploads/2012/03/amlfinal35.pdf> accessed 1st September 2016; Basel Committee, 'Risk management for electronic banking and electronic money activities', March 1998, 1-25, 20-21 <https://www.bis.org/publ/bcbsc215.pdf> accessed 1st September 2016.

greater detail in chapter 3. Also, many different case scenarios may arise to which the law must find answers. M-payment customers may act negligently, follow bad customer security procedures, and have poor levels of information technology ('IT') literacy.[43] Customers may enter incorrect details due to smaller mobile phone screens, so that there are more data-entry mistakes.[44] This may result, for example, in the wrong amount being paid or the wrong recipient receiving a payment. The instantaneous nature of m-payments can also result in hasty decisions and this tends to cause more mistakes.[45] Mobiles are also generally prone to data loss because of decommissioned, lost or stolen devices.[46] This is because users may make poor PIN selections, choose no password at all or fail to use encryption.[47] Stolen phones on which customer data is stored thus heighten the risk of misuse.[48]

The personal information of the customer is also at risk, as data can be seamlessly transferred to another device if security has been compromised, for example, as a result of a virus.[49] Low technological literacy amongst consumers can equally result in wrong or incomplete transactions and careless safekeeping of personal data.[50] Even 'fat fingers' can cause errors.[51] Practical

---

[43] Ibid.
[44] A. Scupola, *Developing Technologies in E-Services, Self-Services, and Mobile Communication: New Concepts* (Information Science Reference 2011) 202.
[45] Curwen and Whalley n 23, 218.
[46] Cloud Security Alliance, 'Security Guidance for Critical Areas of Mobile Computing', November 2012, 1-60, 16 <https://downloads.cloudsecurityalliance.org/initiatives/mobile/Mobile_Guidance_v1.pdf> accessed 1st September 2016.
[47] Ibid.
[48] Ibid.
[49] R. Baldoni and G. Chockler, *Collaborative Financial Infrastructure Protection, Tools, Abstractions, and Middleware* (Springer-Verlag 2012) 222.
[50] Mobile Financial Services Working Group, 'Mobile Financial Services, Consumer Protection in Mobile Financial Services' (2014) Guideline Note No.13, 1-15, 3 <http://www.afi-global.org/sites/default/files/publications/mfswg_guideline_note_7_consumer_protection_in_mfs.pdf> accessed 1st September 2016.

factors, such as, an insufficiently charged mobile phone, may also cause uncertainty for the customer as to whether or not the transaction has been completed, or may result in duplicate transactions.[52] Similarly, unstable internet connections may cause uncertainty for customers. All of these scenarios may result in customers losing funds and possibly not being refunded and may cause disputes in respect of unauthorised m-payment transactions. While customers may be responsible for losing funds or falling prey to cybercriminals in certain cases, this is not always the case and can also be attributable to security issues, which are discussed next.

2.2.2 Technological risks and security

The disadvantage for m-payment customers to lose money or have their personal data compromised is primarily present because operational risk is heightened when security is weak, and it is easy to gain illegal and unauthorised access.[53] Any legal system must mandate risk management, prevent m-payment customers from being unfairly blamed for security failures outside their control and protect their data and privacy in a data-driven world. Security weaknesses can arise because of more seamless applications favoured by customers and enhanced functionalities, but which increase the risk of fraud.[54] Smartphones are already equipped with different functionalities, for

[51] R. Jones, 'Regulator warns of dangers of mobile banking', The Guardian, 27 August 2013 <https://www.theguardian.com/money/2013/aug/27/dangers-mobile-banking-regulator> accessed 1st September 2016.
[52] Curwen and Whalley n 23.
[53] Solin and Zerzan n 42.
[54] I. Schneider, '5 Critical Strategies for Mobile Banking Security', BankTech, 2012 <http://www.banktech.com/risk-management/5-critical-strategies-for-mobile-banking/240003902> accessed 28 October 2013.

instance, Global Positioning System ('GPS'), high-resolution cameras, storage of personal information, diary commitments and contacts, etc. As more data is available, security threats are likely to increase, especially since the data network is constantly connected to the internet.[55] The security of mobile devices is thus threatened because of vulnerabilities of third-party applications, the devices, their operating systems and the design.[56] This makes it easier to intercept transaction data at the service terminal when NFC is being used, thereby heightening the risk of fraud and theft.[57] The risk of financial identity theft and fraud is also elevated since other parties may replicate the identity of the customer in order to carry out transactions.[58] Theft and fraud are particularly facilitated since hacking programs are commercially available, including for mobiles.[59]

Hacking denotes gaining unauthorised access over a remote mobile device.[60] These malicious software programs are used to appropriate transaction details from customers when they access their digital wallets on

---

[55] J.J. Park et al, *IT Convergence and Services, ITCS 2011 & IRoA 2011* (London, Springer 2012) 158.
[56] Cloud Security Alliance n 46, 16.
[57] Ibid 3.
[58] N.S. van der Meulen, *Financial Identity Theft: Context, Challenges and Countermeasures* (TMC Asser Press 2011) 208.
[59] R. Sidel, 'Mobile Bank Heist: Hackers Target Your Phone', The Wall Street Journal, 26 August 2016 <http://www.wsj.com/articles/mobile-bank-heist-hackers-target-your-phone-1472119200> accessed 1st September 2016.
[60] A hacking team which researched the security of the Samsung Galaxy S3 mobile phone sent a malicious file (a Trojan horse) via NFC and this was routinely opened by the document viewer and an attack could be launched. The hackers had then access to all the data on the phone. Whilst Android 4.0.4 has adopted anti-exploit mitigations in its code, these were found to be easy to circumvent: R. Naraine, 'Exploit beamed via NFC to hack Samsung Galaxy S3 (Android 4.0.4)', Zero Day, 19 September 2012 <http://www.zdnet.com/article/exploit-beamed-via-nfc-to-hack-samsung-galaxy-s3-android-4-0-4/> accessed 1 September 2016; R. Samani et al, *CSA Guide to Cloud Computing: Implementing Cloud Privacy and Security* (Elsevier 2015) 83; House of Commons, *Committee on Standards and Privileges, Privilege: Hacking of Members' mobile phones, Fourteenth Report of Session 2010-11* (TSO Shop 2011) 5.

their mobile phones or other digital devices.[61] Moreover, SIM cards are particularly vulnerable to hacking, as they contain the identity of the customer and payment credentials of mobile wallets in NFC-enabled mobiles, which can then be remotely cloned.[62] For instance, Zeus, a malicious Trojan horse, attacks personal computers ('PCs') and a new version has been developed to harm mobile operating systems, such as, Apple, Android, Blackberry, Windows 6.5, Palm OF and others.[63] A malicious trojan horse tries to gain access by the user wrongly installing it, which then enables the malicious code to access the secure zone and to obtain control or send denial-of-service attacks.[64] New hacking strategies are also continuously developed. For instance, in 2016, it was reported that there was a new 'Android Stagefright Exploit', which left millions of Android users vulnerable.[65] It enabled the Android devices of all those who visited a webpage with a malicious multimedia file to be remotely hacked in under ten seconds.[66]

As social media users and news outlets publish links increasingly to multimedia files, which are particularly popular, it is very difficult to screen against these types of security threats.[67]

---

[61] Ibid.
[62] S. Sposito, 'Mobile Bank Accounts May Be Vulnerable from SIM Card Hack', American Banker, 2013 <http://www.americanbanker.com/issues/178_141/mobile-bank-accounts-may-be-vulnerable-from-sim-card-hack-1060802-1.html> accessed 28th October 2013.
[63] Scupola n 44, 202; E.P. Doherty, *Digital Forensics for Handheld Devices* (CRC Press 2013) 4.
[64] See J.M. Stewart, *Comp TA Security + Review Guide* (2nd ed, Wiley & Sons 2011) Chapter 3.
[65] H. Be'er, Metaphor, 'A (real) real-life Stagefright exploit', Exploit, 1-38, 1 <https://www.exploit-db.com/docs/39527.pdf> accessed 1st September 2016 (Be'er); S. Khandelwal, 'New Exploit to 'Hack Android Phones Remotely' threatens Millions of Devices', The Hacker News, 16 March 2016 <http://thehackernews.com/2016/03/exploit-to-hack-android.html> accessed 1st September 2016.
[66] Be'er (ibid).
[67] Ibid.

Security is also compromised when the handset is used in Wi-Fi hotspots in public spaces.[68] This is because mobiles can be more easily accessed illegally.[69] Smart-devices are also vulnerable since hackers may steal information, money, listen to voice mails, send viruses and spy by exploiting the distinct vulnerabilities of mobiles.[70] The risk posed by hacking is further compounded by the ever-changing *modus operandi* of hackers.[71] Hackers are often at the forefront of technological innovation and make use of the latest criminal toolkits available online.[72] Target banks, which are attacked by professional hackers, may therefore struggle with continuously maintaining and improving their systems in order to sufficiently protect the m-payment market.[73] For example, in 2016, NatWest conceded that its online banking system was defective since cyberthieves could hack accounts through stolen smartphones and by pretending to be the victims in order to receive SMS sent

[68] P. Collinson, 'Don't bank on your phone - it could be hacked by Zeus 'trojan horse'', The Guardian, 2011 <http://www.theguardian.com/money/2011/jul/22/smartphones-hacked-zeus-malware> accessed 28 October 2013.
[69] Ibid.
[70] Certified Ethical Hacker, 'Ethical Hacking and Countermeasures Version 6, Module XXXVI, Hacking Mobile Phones, PDA and Handheld Devices', 2008, 1-90, 9-10 <http://blurredlogic.net/data/tut/Ethical_HackingV6/CEH-v6_Instructor_slides/CEHv6%20Module%2036%20Hacking%20Mobile%20Phones,%20PDA%20and%20Handheld%20Devices.pdf> accessed 30 December 2013.
[71] State of New Hampshire Department of Information Technology (2012), *Monthly Security Tips Newsletter* 7(1), 1-2, 1 <http://www.nh.gov/doit/cybersecurity/resources/documents/nl1201-emerging-trends.pdf> accessed 27 December 2013; Sophos, 'Security Threat Report 2012, Seeing the Threats Through the Hype', 2012, 11-31 <http://www.sophos.com/medialibrary/PDFs/other/SophosSecurityThreatReport2012.pdf> accessed 1st September 2017; Press Trust of India, 'Hackers come up with new tricks to attack bank accounts', 2013 <http://ibnlive.in.com/news/hackers-come-up-with-new-tricks-to-attack-bank-accounts/422343-11.html> accessed 28 October 2013.
[72] R. O'Harrow, 'Hacking tool kits, available free online, fuel growing cyberspace arms race', Washington Post, 2013 <http://www.washingtonpost.com/investigations/hacking-tool-kits-available-free-online-fuel-growing-cyberspace-arms-race/2012/11/12/1add77a4-21e6-11e2-ac85-e669876c6a24_story.html> accessed 8 January 2014; S.-P. Oriyano and M. Gregg, *Hacker Techniques, Tools, and Incident Handling* (Jones & Bartlett Learning 2011) Chapter 1.
[73] J. Rouse et al, *Hacking Exposed Mobile: Security Secrets & Solutions* (McGraw Hill Professional 2013) 74.

to other SIM cards.[74] This latter hacking strategy is also known as 'blagging' where someone is impersonating another by using, for instance, a personal identification number ('PIN').[75]

As mobile phones have similar applications as PCs, they are also prone to viruses. In 2011, over 200 specific viruses targeted mobiles, such as, SpyEye,[76] with this number being on the increase.[77] Vulnerabilities caused through viruses are further elevated for m-payment services since anti-virus programmes for mobiles are not as effective as for PCs.[78] Malware, i.e., malicious software to spy, invade or harm a mobile, can be accidentally downloaded when a m-payment product is loaded.[79] In 2012, there were over 350,000 malicious malware available for Android apps.[80] This information-stealing malware is mainly found on third-party app stores, i.e., those that are not on Google's Play Store.[81] Kaspersky, a security company, explains that, whilst most mobile malware is designed for Android devices, the iPhone which

---

[74] M.-A. Russon, 'NatWest online banking flaw enables hackers to drain bank accounts by stealing your smartphone', IB Times, 7 March 2016 <http://www.ibtimes.co.uk/natwest-online-banking-flaw-enables-hackers-drain-bank-accounts-by-stealing-your-smartphone-1548002> accessed 1st September 2016.

[75] House of Commons, *Committee on Standards and Privileges, Privilege: Hacking of Members' mobile phones, Fourteenth Report of Session 2010-11* (TSO Shop 2011) 5.

[76] SpyEye is a toolkit for criminals, which functions like a Trojan and for instance, makes 'keylogging' possible, 'autofills credit cards modules' and carries out daily backups: Symantec, 'SpyEye Bot versus Zeus Bot', 2010 <http://www.symantec.com/connect/blogs/spyeye-bot-versus-zeus-bot> accessed 23 December 2013; Baldoni and Chockler (n 30).

[77] C. Wild et al, *Electronic Mobile Commerce Law, An analysis of trade, finance, media and cybercrime in the digital age* (University of Hertfordshire Press 2011) 281.

[78] T. Beck and S.M. Maimbo, *Financial Sector Development in Africa, Opportunities and Challenges* (The World Bank 2011) 59; P. Lambert, 'How effective is antivirus software on smartphones?' IT Security, 2012 <http://www.techrepublic.com/blog/it-security/how-effective-is-antivirus-software-on-smartphones/7629/> accessed 28th October 2013.

[79] N. Chesworth, 'Be smart, stay safe: security and mobile banking', The Telegraph, 2013 <http://www.telegraph.co.uk/sponsored/finance/natwest-mobile-banking/10292506/smartphone-security-mobile-banking.html> accessed 28 October 2013.

[80] G. McIlraith, 'How to Ensure Mobile Banking App Security', BankTech, 2013 <http://www.banktech.com/risk-management/how-to-ensure-mobile-banking-app-securit/240163093> accessed 28 October 2013.

[81] Cloud Security Alliance n 44, 16.

uses iOS, namely, a closed system, is also at risk.[82] According to Kaspersky, all systems have vulnerabilities and the risk of iPhones being infected by malware attacks may eventuate. This can lead to many iPhones being infected as there is no antivirus currently available since companies are not permitted at present to design such end-point security for Apple.[83] Unofficial stores thus expose users to possible viruses, malware, Trojans and adware[84] which they may accidentally download.[85]

When customers unlock their smartphones and install apps from third parties,[86] they also heighten the risk of spoofing attacks, which are strikes whereby a malicious application replicates the way another one looks; a popular spoofing attack is phishing.[87] Phishing attacks result in users disclosing their password to an unauthorised application in order to obtain banking data.[88] McAfee, an online security firm, also points out the threats for mobiles, particularly from malware shopping sprees facilitated by the sale of apps with

[82] P. Sonne, 'Data-Security Expert Kaspersky: There Is No More Privacy', *The Wall Street Journal*, 3 September 2013 <http://www.wsj.com/articles/SB10001424127887324432404579053091175949708> accessed 1st September 2016; M. Asay, 'Why Your iPhone Will Inevitably Catch a Virus', Hack, 5 September 2013 <http://readwrite.com/2013/09/05/kaspersky-the-ios-malware-dam-will-break/> accessed 1st September 2016; Samani et al n 58, 83.
[83] Ibid (Sonne).
[84] Adware in the mobile context is called 'malware', but is not illegal, but opens advertisements, but often spyware is concealed in adware: M.E. Vermaat et al, *Discovering Computers 2014, Technology in a World of Computers, Mobile Devices, and the Internet* (CengageBrain 2013) 231.
[85] S. Peng et al, 'Smartphone Malware and Its Propagation Modeling: A Survey' (2013), 16(2), *IEEE Communications Surveys & Tutorials*, 925-941, 925; M. Khosrow-Pour, *Encyclopedia of Information Science and Technology* (3rd ed, Information Resources Management Association 2014) 5681.
[86] D. Chell et al, *The Mobile Application Hacker's Handbook* (Indianapolis, John Wiley & Sons Inc 2015) 491.
[87] L. Malisa et al, 'Detecting Mobile Application Spoofing Attacks by Leveraging User Visual Similarity Perception' (2015) International Association for Cryptologic Research, 1-17, 1 <https://eprint.iacr.org/2015/709.pdf> accessed 1st September 2016.
[88] M. Dawson and M. Omar, *New Threats and Countermeasures in Digital Crime and Cyber Terrorism* (IGI Global 2015) 55.

worms by malware authors.[89] The availability of NFC means that digital wallets have the potential to be common, particularly in densely populated places.[90] This may result in mobile worm attacks which bump into the connection and then infect the phone to appropriate e-money.[91] However, mobiles which have not been unlocked can be automatically updated to protect against recognised threats, though malware can prevent these updates.[92]

Furthermore, mobile numbers store the International Mobile Subscriber Identity ('IMEI') of the consumer, but this can be stolen when a phone is infected.[93] With this IMEI number, malware writers then inform mobile phone companies that the handset is stolen in order to obtain a new SIM card which they use to gain fraudulent access to the person's bank account.[94] Consequently, the mobile is taken over in order to sidestep the security checks of banks.[95]

The adoption of technology like Bluetooth or NFC within m-payments can also lead to additional security breaches as Bluetooth and NFC are like radio communications which can be intercepted and even enhanced through an antenna.[96] Even if encryption is used, a traffic analysis can nevertheless be

---

[89] McAfee Labs, '2013 Threats Predictions', Report, 2013, 1-16, 4 <http://www.mcafee.com/uk/resources/reports/rp-threat-predictions-2013.pdf> accessed 20 December 2013.
[90] Ibid.
[91] Ibid 4.
[92] Ibid.
[93] A. Klein, 'SIM-ple: Mobile Handsets Are Weak Link in Latest Online Banking Fraud Scheme', Security Intelligence, 13 March 2012 <https://securityintelligence.com/sim-ple-mobile-handsets-are-weak-link-in-latest-online-banking-fraud-scheme/> accessed 1st September 2016.
[94] Ibid.
[95] Ibid.
[96] A. Dubey and A. Misra, *Android Security, Attacks and Defenses* (Taylor & Francis Group LLC 2013) 222.

carried out.[97] For instance, NFC is prone to eavesdropping; an attacker can corrupt, change or insert data and there can be a 'man-in-the-middle attack' when two parties try to communicate.[98] While eavesdropping is minimised when the device is in Passive Mode, it cannot be entirely prevented.[99] Apple's iBeacon is equally vulnerable.[100] As Ozguc explains, the 'iBeacon's fundamentally open design means that any mobile app could be designed to pick up a retailer's location broadcast, including apps developed by competitors or unscrupulous third-party developers'.[101] Gonsalves further warns that '[t]hese apps could use that broadcast information to locate and track a user, possibly without their permission.'[102] Some experts therefore warn that m-payments can result in 'fraudsters' heaven'.[103]

Research published in 2014 also found that 40 out of 60 apps from leading banks had serious security flaws which could possibly compromise financial data.[104] Only under 20% of apps were designed to protect against

---

[97] Ibid.

[98] E. Haselsteiner and K. Breitfuss, 'Security in Near Field Communication (NFC), Strengths and Weaknesses', undated, 1-11, 4 <http://ece.wpi.edu/~dchasaki/papers/Security%20in%20NFC.pdf> accessed 27 December 2013, 4-6.

[99] Ibid 7-8.

[100] iBeacon is a technology standard which was developed by Apple. When apps are installed on Android and iOS devices, signals can be received from the beacons. iBeacon employs Bluetooth, a low energy, which can sense in close proximity in order to send an identifier standard, which is read by a compatible operating system or app: iBeaconInsider, 'What is iBeacon? What are iBeacons?' 2016 <http://www.ibeacon.com/what-is-ibeacon-a-guide-to-beacons/> accessed 10th November 2016.

[101] Cited from A. Gonsalves, 'What Apple's iBeacon rollout doesn't say', ComputerWorld, 2013 <http://blogs.computerworld.com/mobile-security/23256/what-apples-ibeacon-rollout-doesnt-say> accessed 20 December 2013.

[102] Ibid.

[103] Scupola n 44, 203; also see L. Bachelor, 'Contactless card fraud is too easy, says Which?', Guardian, 23 July 2015 <http://www.theguardian.com/money/2015/jul/23/contactless-card-is-too-easy-says-which> accessed 17 July 2015.

[104] A. Sanchez, 'Personal banking apps leak info through phone', 8 January 2014, IOActive <http://blog.ioactive.com/2014/01/personal-banking-apps-leak-info-through.html> accessed 1st September 2016; Z. Epstein, 'Major security holes found in 90% of top mobile banking apps',

memory corruption attacks, i.e., no Stack Smashing Protection and Position Independent Executable were enabled.[105] Additionally, 40% of tested apps failed to verify whether the Secure Sockets Layer ('SSL') certificates where authentic, thereby allowing 'man-in-the-middle' attacks.[106] Half of the tested apps permitted emails and SMS to be sent from the consumer's device because the UIWebView was insecure and JavaScripts could be injected.[107] Furthermore, 90% of the tested apps had various non-SSL links which made interception possible and allowed HTML and JavaScript codes to be injected with a view to generating false login signals.[108] Accordingly, one of the significant risks is that flaws within the m-payment technology may be exploited by cybercriminals, including employees of the stakeholders within the m-payment ecosystem, who may commit theft or fraud.[109] Hence, security weaknesses may result in unauthorised m-payment transactions and/or data/privacy breaches. However, customers should not be responsible for security issues and should be refunded when they become victims of fraud without being at fault themselves. Otherwise, the convenience of using m-payments apps is outweighed by the great disadvantage of cyber fraud. Certainly, security issues are not just caused by m-payment providers. Instead, issues can arise because of the inadequate performance by one or several players within the chain, which the next section discusses. It is also

---

BGR, 14 January 2014 <http://bgr.com/2014/01/14/mobile-banking-apps-security-vulnerabilities/> accessed 1st September 2016.

[105] Ibid.

[106] Ibid.

[107] Ibid.

[108] Ibid.

[109] Mobile Financial Services Working Group n 50, 4.

acknowledged that there exists an overlap between security issues and performance by third parties within the m-payment ecosystem.

2.2.3 Technological risks and third-party collaboration

Collaboration is required to fuse banking services with technological advances.[110] Different stakeholders rely on the performance of other stakeholders.[111] An interdependent relationship is thus created.[112] In other words, supply chain risk is heightened due to the unique operational set-up required to facilitate m-payments.[113] Technical problems, particularly the complex technical set up to deliver services, can cause service disruptions.[114] For example, customers may not be able to make transactions due to system outages.[115] System outages may occur, for instance, because of a failure to properly organise the ecosystem between the various parties within the m-payment infrastructure, i.e., the relationship between the mobile network operator, the issuer or bank, the mobile service provider, the trusted service manager(s)[116] ('TPPs') and any other parties.[117] Delays may happen anywhere

[110] DM Wallet Summit, 'Digital Wallet Opportunity', 2013 <http://www.dmwsummit.com/digital-wallet-opportunity/> accessed 13th October 2013.
[111] Ibid.
[112] Ibid.
[113] T. Hinkel, 'Banks Beware: Operational Risk Increasing', Bank Systems & Technology, 2012 <http://www.banktech.com/risk-management/banks-beware-operational-risk-increasing/240005678> accessed 28 October 2013.
[114] Ibid.
[115] Responsible Digital Payments Guidelines. July 2016, 1-28, 6 <http://www.cashlearning.org/downloads/btca-responsibledigitalpaymentsguidelinesandbackground-(1).pdf> accessed 1st September 2016.
[116] A trusted service manager is a function which arises when near field communication is used. The role consists of establishing technical connections, as well as entering into agreements with device manufacturers, mobile network operators and other parties which are responsible for the security on mobile devices. A trusted service manager thus provides a contactless service management platform and thereby connects the service provider, the application owner, the mobile station holder, the card issuer and the SIM card manufacturer: F.

within the m-payment infrastructure and resultantly, it can be unclear whether a transaction has to be made again or not.[118] Delays may also result in incorrect balances being shown, so that either transactions are declined or customers incur overdrafts.[119] Another practical problem which can arise is that not all the changes to the value stored within the m-payment system are accurately identified on a daily basis.[120]

Other issues can also arise. Banks' agents may, for instance: charge unauthorised fees; tie customers in, e.g., by requiring that services or goods are bought to make use of their service; lose customer records or assets; incorrectly enter data; manage cash wrongly, so that the funds of customers are unavailable; or fail to address customer complaints and/or to pass them onto the bank.[121] Agents may also be targets of third-party theft and fraud.[122] Moreover, criminals may try and steal funds from those agents which accept cash.[123] Unauthorised agents may try to defraud customers. There further exists the risk that agents may accept counterfeit money when they load electronic

---

Resatch, *Ubiquitous Computing: Developing and Evaluating Near Field Communication Applications* (Springer 2010) 30.

[117] S. Allums, *Designing Mobile Payment Experiences: Principles and Best Practices for Mobile Commerce* (O'Reilly Media 2014) 36.

[118] B. Ayari et al, 'Delay-Aware Mobile Transactions'. In U. Brinkschulte et al (eds), *Software Technologies for Embedded and Ubiquitous Systems: 6th IFIP WG 10.2 International Workshop, SEUS 2008, Anacarpi, Capri Island, Italy, October 2008, Proceedings* (Springer 2008) 280-291, 280

[119] NatWest, 'NatWest App not Updating Balances Over Weekends', Communities Natwest, 31 August 2015 <http://www.communities.natwest.com/t5/Ways-to-Bank/NatWest-App-Not-Updating-Balances-Over-Weekends/td-p/41285> accessed 1st September 2016.

[120] A.J. Lake, 'Risk management in Mobile Money: Observed Risks and Proposed Mitigants for Mobile Money Operators', International Finance Corporation/World Bank Group, November 2013, 1-22, 15.

[121] K. Lauer et al, 'Bank Agents: Risk Management, Mitigation, and Supervision' (2011) CGAP Focus Note 75, 1-24, 4.

[122] Ibid.

[123] Ibid.

funds onto a mobile device.[124] The risk of fraud may be elevated by the partnerships, especially when poor processes, product designs, compliance and monitoring practices are adopted.[125] Due to the complex ecosystem, it may be difficult to establish which party is responsible for holding funds within the m-payment infrastructure.[126] It may also be difficult to identify which party failed to discharge its respective duty. As a result, customers may experience problems when they complain about violations of their consumer rights.[127]

Another fundamental disadvantage for m-payment customers is the misuse of their sensitive personal data by those within the m-payment ecosystem.[128] For instance, Facebook has made m-payment available via its Messenger app.[129] However, it has also been found to have shared data from its users illegitimately with over 60 companies with which it entered into data partnerships.[130] A drawback for m-payment customers may therefore be that their m-payment transaction history is shared with various companies which sell the data for commercial gain.[131] Nonetheless, the trend is towards predictive hyper personalisation.[132] In other words, the personal data of m-payment customers is likely to be utilised to create a personalised shopping

---

[124] J. Luminzu Mudiri, 'Fraud in Mobile Financial Services', MicroSave, 2014, 1-48, 6 <http://www.microsave.net/files/pdf/RP151_Fraud_in_Mobile_Financial_Services_JMudiri.pdf> accessed 1st September 2016.
[125] Mobile Financial Services Working Group n 50, 4.
[126] Ibid 3.
[127] Ibid 3.
[128] M.P. Malloy, *Banking Law and Regulation* (2nd ed, Wolters Kluwer 2016) 3.02.
[129] N. Lanxon, 'Facebook to Make Mobile Payments Service Available Outside U.S.', Bloomberg, 6 November 2017 <https://www.bloomberg.com/news/articles/2017-11-06/facebook-to-make-mobile-payments-service-available-outside-u-s> accessed 1 March 2019.
[130] C. Kurtz et al, 'The Unlikely Siblings in the GDPR Family: A Techno-Legal Analysis of Major Platforms in the Diffusion of Personal Data in Service Ecosystems' (2019) *Proceedings of the 52nd Hawaii International Conference on System Sciences*, 5059-5068, 5059.
[131] Ibid.
[132] S. Consolvo et al, *Mobile User Research: A Practical Guide* (Morgan & Claypool 2017) 161.

experience.[133] Rhoen also notes that automated processes, including m-payments, result in datafication and the Internet of Things ('IoT') (i.e. connected objects and devices) will further heighten data generation.[134] The thereby generated big data will be tantamount to permanent consumer surveillance.[135] This raises the question how the law should strike a balance between protecting the personal data of m-payment users and allowing companies to utilise such data.

Moreover, cloud providers are entrusted with sensitive personal data which they may commercially utilise on the basis of broadly drafted privacy agreements or the cloud may be targeted by cybercriminals.[136] As a result, data may be lost by the cloud provider or misutilised.[137] Hence, m-payments raise consumer privacy issues as providers, including their agents and cloud providers, gather and retain sensitive data.[138] Agents may also store insufficient e-funds to settle transactions, so that liquidity problems can arise.[139] Equally, stored customer funds can be at risk, e.g. when the m-payment provider which holds the funds is insolvent.[140] A related issue is that

---

[133] Ibid.
[134] M. Rhoen, 'Beyond consent: improving data protection through consumer protection law' (2016) *Internet Policy Review*, 5(1) <https://policyreview.info/articles/analysis/beyond-consent-improving-data-protection-through-consumer-protection-law> accessed 15 April 2019.
[135] Ibid.
[136] K.A. Ahmat, 'Emerging Cloud Computing Security Threats' (2015) City University of New York, 1-4, 2 <https://arxiv.org/ftp/arxiv/papers/1512/1512.01701.pdf> accessed 5 March 2019.
[137] Ibid.
[138] C.J. Hoofnagle et al, 'Mobile Payments: Consumer Benefits & New Privacy Concerns' (2012) University of California, 1-19, 1 <https://ssrn.com/abstract=2045580> accessed 5 March 2019.
[139] M. Flaming et al, 'Agent Management Toolkit, 'Building a Viable Network of Branchless Banking Agents, Technical Guide' (2011) Consultative Group to Assist the Poor (CGAP)/The World Bank, 1-171, 5 <http://www.cgap.org/sites/default/files/CGAP-Technical-Guide-Agent-Management-Toolkit-Building-a-Viable-Network-of-Branchless-Banking-Agents-Feb-2011.pdf> accessed 1 September 2016.
[140] T. Khiaonarong, 'Oversight Issues in Mobile Payments' (2014) IMF Working Paper, 1-35, 19.

deposit insurance may not be taken out. A deposit insurance protects customers in case a bank or payment institution or e-money institution goes insolvent.[141] For instance, the Nigerian Deposit Insurance Corporation offers pass-through deposit insurance, so that the funds which customers deposit are insured and the m-payment provider and its agents become custodians for their customers.[142] A premium is payable by the bank or m-payment operator for having the funds insured up to a certain maximum limit.[143] Yet even when this has been done, the insurance may not cover the entire amount when accounts are pooled, thus exposing customers and issuers.[144] Customer claims may also not rank above creditor claims when funds are held by the issuer.[145]

Anti-Money Laundering ('AML') checks may be less stringent for small values and criminals may exploit this by dividing transactions in order to circumvent AML checks.[146] Moreover, when the 'Know Your Customer' ('KYC') rules are weak, criminals may use false identities to bring in funds.[147] Equally, merchants, intermediaries, banks' agents and retail partners can undermine the integrity of the m-payment system when they allow criminals to use the payment system, particularly for cross-border transfers.[148]

---

[141] GSMA, 'Safeguarding Mobile Money: How providers and regulators can ensure that customer funds are protected', January 2-16, 1-31, 20 <http://www.gsma.com/mobilefordevelopment/wp-content/uploads/2016/01/2016_GSMA_Safeguarding-Mobile-Money_How-providers-and-regulators-can-ensure-that-customer-funds-are-protected.pdf> accessed 10 November 2016.
[142] B. Konolafe, 'NDIC issues deposit insurance guidelines for mobile money', Vanguard, 18 January 2016 <http://www.vanguardngr.com/2016/01/ndic-issues-deposit-insurance-guidelines-for-mobile-money/> accessed 10th November 2016.
[143] Ibid.
[144] C. Batista et al, International Experiences of Mobile Banking Regulation, International Growth Centre Policy Brief 36012, January 2012, 1-15, 1 <http://www.theigc.org/wp-content/uploads/2015/03/Batista-Et-Al-2012-Policy-Brief.pdf> accessed 1st September 2016.
[145] Ibid.
[146] Solin and Zerzan n 42, 16.
[147] Ibid.
[148] Ibid 17.

Consequently, when bank's agents use inadequate verification procedures for KYC purposes, it becomes more difficult to monitor whether accounts are used for criminal purposes.[149] This may result in m-payment customers being wrongly accused of money laundering. Yet the traceable and digital nature of m- payments means that money laundering and terrorist financing risks are lower than for cash.[150]

2.3 Conclusion

M-payment services give rise to many new forms of risk and particularly heighten technological and operational risks. As the technology becomes increasingly popular, the potential for m-payment customers to become victims of financial crimes, especially fraud, theft, money laundering, unauthorised access and data security and data protection breaches, is significantly increased.[151] The occurrence of financial crime is further exacerbated in a more globalised world in which people conduct m-payment services across borders. There thus exist various problems within the emerging m-payment market which require legislative impetus. For instance, the creation of digital identities with the help of banks,[152] e-wallet regulation or even the question whether customers funds should be insured in case a m-payment provider becomes insolvent are areas which are important within the context of consumer protection. However, as the m-payment space matures, these other areas are

[149] Ibid.
[150] McAfee n 89.
[151] D. Benyon, 'Banks fear in increase in financial crime', Risk.Net, 2008 <http://www.risk.net/operational-risk-and-regulation/news/1499571/banks-fear-increase-financial-crime> accessed 28 October 2013.
[152] World Economic Forum n 33, 1.

likely to receive attention and at present, the most pressing threat for consumers is the risk that they must shoulder the losses from unauthorised transactions and have little or no recourse when their data is misappropriated.

The core reason why customers use m-payment services is that they want to make payments. An unauthorised m-payment transaction goes to the root of the agreement which a customer enters into with a m-payment provider. Loss of funds due to cyber fraud is also most concerning to the nascent m-payment market which depends on customer trust. Also, as discussed, payment data is extremely valuable in our data-driven digital economy and it must, therefore, be equally protected. Rules must be developed which spell out the rights, duties and liabilities in respect of the different circumstances which can arise, as discussed above. Accordingly, the law must protect m-payment customers against the risks of unauthorised m-payment transactions and inadequately protected consumers' data, which in turn necessitates a determination of the parameters of protection available for m-payment customers.

As discussed in the next chapter, the scope of protection depends on whether a given policymaker favours the neo-liberal or social welfare approach to consumer protection. Yet irrespective of the chosen policy direction, laws are necessary; this work offers detailed recommendations as to the scope and content of these laws, encompassing both changes to the content or interpretation of existing Saudi regulation, and suggestions as to new laws which might be introduced. The market entrants which facilitate m-payments must be regulated and adopt prudent business processes and engage in risk

management. Laws must address the topic of customer negligence and mistakes, security incidents in relation to unauthorised m-payment transactions, as well as the topic of protecting customers' data in order to maintain privacy and to protect against breaches of privacy. It is essential for the law to describe in which cases m-payment providers are responsible to refund customers who have been defrauded and had their funds stolen. Equally, it must be identified when customers cannot seek a refund. For instance, a neo-liberal stance may be taken, so that no refund can be sought in cases where m-payment customers do not display sufficient technological literacy. Yet clearly, it would be unfair if m-payment customers could not seek refunds in instances where the provided services are not secure. Similarly, in instances where third-parties are directly or indirectly responsible for financial losses and data and privacy breaches, m-payment customers should not shoulder the losses. When m-payment services are interrupted, the compensation of customers may be warranted in certain cases. However, customers may also be made to bear some responsibility for the loss of funds. The question of how best to balance customer economic interests against customer welfare interests depends on the priorities which any consumer protection law sets. The next chapter therefore reviews the literature about legal consumer protection measures in order to further identify the underlying policy orientations which Saudi legislators may adopt.

CHAPTER 3

A LITERATURE REVIEW ABOUT THE CONSUMER PROTECTION LEGAL LITERATURE

3.1 Introduction

This chapter identifies the paradigms of the Western and Islamic legal consumer protection literature and the legal consumer protection measures characteristic of the different approaches. This literature review helps to reflect on the UK and Saudi laws in chapters four and five and identifies the underlying policy orientation which underpin the different laws. While this chapter deals with consumers, it is relevant to customers/bank users of m-payment services, including businesses which make use of m-payment services. However, a consumer is often considered an individual[1], whereas a customer/bank user is not just an individual but can also be a business. Nevertheless, making such a distinction is less important in this specific content since individuals and businesses can both be 'final users' of m-payment services.[2]

Consumer law can be premised on a pre-interventionist and liberal approach or on interventionist regulation which seeks to promote welfare considerations.[3] Accordingly,

[1] E.g. see the Consumer Rights Act 2015, s2(3).
[2] Also see Directive 2007/64/EC, Article 4(10)&(11); D. Parry et al, *The Yearbook of Consumer Law 2009* (Routledge 2008) 73.
[3] L. Nottage, 'Product safety regulation.' In G. Howells et al (eds) *Handbook of International Consumer Law and Policy* (Edward Elgar 2010) 257.

governments have different options when it comes to adopting consumer protection regimes.[4] They can adopt a non-interventionist approach rooted in neo-liberalism by adopting market-based legal measures to protect consumers.[5] In this context it is important to emphasise that contract law, including contracts, have played an important role to further neoliberalism.[6] Boilerplate i.e. standardised contracts empower companies to dominate at the expense of the consumer and undermine the idea that a consumer can give informed consent.[7] Consumers are unable to act rationally to protect their own interests because the necessary legal framework and public institutions have not been created, including to challenge unfair contract terms.[8] It is therefore difficult for consumers to pursue legal action or to employ dispute settlement procedures.[9] As a result, consumers must themselves try to solve issues they may encounter.[10]

Without interventionist regulation, consumers will most likely find it difficult to seek redress, whether for unauthorised m-payment transactions or data breaches, in circumstances where boilerplate contracts and fragmentary contracts are used and the consumer encounters readability issues and there exists no choice apart from not using the service.[11] For instance, lengthy privacy agreements are typically used which consumers mostly do not read prior to clicking that they agree.[12] Even if they read the agreement, they may struggle to comprehend it and the provided consent may lack voluntariness.[13] As a result, access to a huge amount of

[4] UK Department of Trade and Industry, *Comparative report on consumer policy regimes*, 2003; L.M. Delgadillo, 'An Assessment of Consumer Protection and Consumer Empowerment in Costa Rica' (2013) *Journal of Consumer Policy* 36, 59-86,63.
[5] Ibid (Delgadillo).
[6] K. Birch, *A Research Agenda for Neoliberalism* (Edward Elgar 2018) 156.
[7] R.J. Mann, 'Contracting' for Credit' (2006) *Michigan Law Review* 104, 899-932, 901.
[8] Delgadillo n 4.
[9] Ibid.
[10] Ibid.
[11] Mann n 7, 902-904.
[12] M. Bashir et al, 'Online privacy and informed consent: The dilemma of information asymmetry' (2016) *Proceedings of the Association for Information Science and Technology* 52(1), 1-10, 1 <https://onlinelibrary.wiley.com/doi/full/10.1002/pra2.2015.145052010043> accessed 20 April 2019.
[13] Ibid.

personal information is given to companies, resulting in consumers' data being inadequately protected.[14]

At present and as discussed in more detail in chapter 5, a non-interventionist approach seems to have been adopted in SA which may in part be due to the lack of attention given to consumer protection by Islamic scholars and policymakers.[15] As discussed in section 3.6, the Islamic consumer protection literature has been insufficiently developed and a central tenet of the Sharia which requires individuals to be given adequate legal protection to realise a fair society[16] may, therefore, be undermined. Consequently, it is of utmost importance that a discourse ensues to promulgate the necessary Islamic consumer protection jurisprudence. The grant of consumer rights in line with the Islamic good faith principle is a particularly pressing issue, alongside the creation of relevant consumer rights institutions. Put differently; the existing Islamic business restrictions must be supplemented by a legal consumer rights discourse.[17] This can safeguard m-payment customers against the heightened technological and related operational and credit risk discussed in Chapter 2 which can significantly disadvantage m-payment customers and override any of the advantages described in Chapter 1.

The OECD points out that consumers are increasingly offered more complicated services due to technological advances, new services, globalised markets and regulatory changes.[18] One such new complex financial service is m-payment transactions. The question therefore arises whether legal consumer protection measures are required to safeguard m-

[14] Ibid.
[15] D. Morris and M. Al Dabbagh, 'The development of consumer protection in Saudi Arabia' (2003) *International Journal of Consumer Studies* 28(1), 2-13, 2.
[16] H. Abdalati, *Islam in Focus* (2nd ed, Dar Al-Elm Printing and Publishing Co 1985) 10.
[17] A.S. Albaqme, 'Consumer Protection under Saudi Arabia Law' (2014) *Arab Law Quarterly* 28(2), 158-175, 170.
[18] OECD, *Consumer Policy Toolkit* (OECD 2010) 2.

payment customers particularly against unauthorised m-payment transactions and to protect consumers' data and their privacy.

Without legal consumer protection measures the risk is that consumers have to shoulder liability and are unable to seek compensation due to carefully drafted contractual terms and conditions.[19] For instance, when automated teller machines ('ATMs') and Chip and Pin were introduced in the UK, banks were allowed to argue that customers were colluding or negligent in using their card and PIN.[20] However, the shift of liability to UK bank customers led to banks acting carelessly in respect of security and significantly increased the occurrence of fraud.[21] Without legal intervention, m-payment providers will use unfair contract terms to shift liability and will render the consumer liable for unauthorised m-payment transactions and prevent redress for data and privacy breaches in line with neo-liberal thought.[22]

The lack of consumer protection in this field is also attributable to the insufficient international consumer protection measures for m-payments, as discussed in section 3.2 below. It is therefore important to explore the two main policy options available to legislators: To intervene, including by curtailing unfair contractual terms and conditions[23], in order to promote the social welfare 'consumer protection interest' objective or to opt for the "contract-modeled" neo-liberal[24] 'consumer economic interest' objective.[25] Depending on the choice, consumer law can be underpinned by either one of these objectives or a mixture.

[19] I. Becker et al, 'International comparison of bank fraud reimbursement: customer perceptions and contractual terms' (2017) *Journal of Cybersecurity* 3(2), 109-125, 109.
[20] Ibid, 111.
[21] R. Anderson and T. Moore, '*The economics of information security'* (2006) *Science* 314, 610-613, 610; ibid.
[22] Becker et al n 19, 124.
[23] R.J. Mann, 'Contracting' for Credit' (2006) *Michigan Law Review* 104, 899-932, 922.
[24] D. Singh Grewal and J. Purdy, 'Introduction: Law and Neoliberalism' (2015) *Law and Contemporary Problems*, 1-23, 6 <https://scholarship.law.duke.edu/lcp/vol77/iss4/1/> accessed 15 April 2019.
[25] J.Q. Whitman, 'Consumerism Versus Producerism: A Study in Comparative Law' (2007) *Yale Law Journal* 117, 340-406, 356.

3.1.1 The nature and purpose of consumer law

Consumer law is a form of private law which fulfils a coordinative role.[26] Put differently, consumer law honours the principle of party autonomy, so that parties can freely determine the main contractual matters.[27] Consumer law thus interferes with the fundamental concept of freedom of contract, which is one of the cornerstones of market economies around the world.[28] Freedom of contract is thought to efficiently allocate resources and to enhance community and individual welfare.[29] However, unrestrained freedom of contract disregards that parties do not possess equal skill, knowledge and bargaining power.[30] The law therefore steps in to create the public system which facilitates private ordering.[31] The underlying rationale for the law to intervene is to reduce unequal bargaining power.[32] In other words, consumer law tames the unfair excesses of freedom of contract.[33] "Consumer-welfarism" requires fairness and reasonableness when contracting.[34]

Consumer law can consist of rules, principles and specific illustrations of proscribed activities.[35] Whilst freedom of contract is maintained, certain limits are imposed in the name of public policy and justice.[36] It seeks to ensure that social ideas, including notions of fairness, are integrated into the market place.[37] Whitman explains that "consumerism" means

---

[26] G.-P. Calliess, 'Transnational Consumer Law: Co-Regulation of B2C-E-Commerce' (2007) Law Research Institute Research Paper Series 3(3), 1-54, 1.
[27] Ibid.
[28] C. Edwards, 'Freedom of Contract and Fundamental Fairness for Individual Parties: The Tug of War Continues' (2009) *UMKC Law Review* 77(3), 647-696, 647.
[29] Ibid.
[30] Ibid.
[31] Ibid.
[32] I. Ramsay, 'Consumer Law, Regulatory Capitalism and the 'New Learning' in Regulation' (2006) *Sydney Law Review* 28(9), 9-35, 9.
[33] L. Mulcahy and J. Tillotson, *Contract Law in Perspective* (4th ed, Cavendish Publishing Ltd 2004) 41.
[34] Ibid.
[35] H. Collins, 'Harmonisation by Example: European Laws against Unfair Commercial Practices' (2010) *The Modern Law Review* 73(1), 89-118, 89.
[36] Calliess n 26, 1.
[37] I. Ramsay, 'Regulation and the Constitution of the EU Single Market: The Contribution of Consumer Law' (2010) *Canadian Business Law Journal* 50, 322-346, 346.

that the law protects the economic interests and rights of consumers.[38] Hence, it is the opposite of "producerism" where the law prioritises the interests and rights of suppliers.[39]

Consumer protection through legal means in the West is not something new. For instance, usury laws existed a very long time in the West and in the UK until the mid-19th century.[40] These laws protected customers against excessive interest rates charged by moneylenders.[41] However, these were abolished since they contravened free market ideas.[42] Hence, it was thought that such consumer protection measure contravened neoclassical economic ideology which argues that the market is the best means to regulate affairs.[43] As a result, in the early twentieth century, a producerist legal order became primarily adopted in Europe.[44] For instance, it was thought that guilds were beneficial for society, despite their having an anti-competitive effect.[45]

In contrast, the Anglo-American legal system started to increasingly embrace the idea of consumerism since the 19th century.[46] For instance, in 1912, Weyl stated that the new economic driver underlying America is that the interests of consumers have become united.[47] This change in the political attitude was primarily caused by increasing prices which stemmed from producers having monopolies.[48] Consumerism therefore particularly gave rise to the law trying to prevent certain groups of competitors from coming together in order to

[38] Whitman n 25, 356.
[39] Ibid.
[40] I. Ramsay, '"A very intrusive proposition"? - the long and winding road to payday loan price controls', Credit Debt and Insolvency, October 2013 <https://creditdebtandinsolvency.wordpress.com/2014/07/22/a-very-intrusive-proposition-the-long-and-winding-road-to-payday-loan-price-controls/> accessed 1 July 2017.
[41] Ibid.
[42] Ibid.
[43] Ibid.
[44] Whitman n 25, 359.
[45] Ibid 360.
[46] Ibid.
[47] W.E. Weyl, *The New Democracy: An Essay on Certain Political and Economic Tendencies in the United States* (Harper & Row 1912, 1964) 250.
[48] Ibid 250-251.

protect themselves against new competitors.[49] The prime change in the policy approach was therefore that it was no longer accepted that groups of producers could protect themselves since it was considered that consumers should enjoy low prices.[50] Accordingly, promoting competition became an important strand of protecting the economic interests of consumers. In the context of m-payments, such a consumerist policy orientation would mean encouraging other market-entrants to enter the market and not to keep it solely restricted to banks.

However, the economic interests of consumers, e.g., to receive services and goods at very low prices, to be able to have access to finance or to purchase goods and services around the clock, do not constitute legal consumer protection measures.[51] Legal consumer protection measures refer to safety and protection laws which outlaw unfair commercial practices, such as exclusion clauses and defective services.[52] Rigid legal provisions are thus enacted which impose specific requirements.[53] Additionally, broader legal provisions are enacted to foster substantive fairness, for instance, through the law governing unfair contract terms.[54] This is, therefore, a more welfare-oriented approach since specific rules, and general standards are adopted to firmly embed the broader values of conscience and fairness.[55] However, as noted by Whitman, such an approach is paternalistic and does not promote consumer choice.[56] The reason is that these legal requirements make it more difficult for new market participants to enter the market.

[49] Whitman n 25, 362.
[50] Ibid 363.
[51] Ibid 366.
[52] Ibid 367.
[53] J.M. Paterson and G. Brody, '"Safety Net" Consumer Protection: Using Prohibitions on Unfair and Unconscionable Conduct to Respond to Predatory Business Models' (2015) *Journal of Consumer Policy* 38, 331-355.
[54] Ibid.
[55] Ibid.
[56] Whitman n 25, 367.

Nonetheless, the adoption of legal consumer protection measures has become an increasingly common occurrence in what some, e.g., Ramsay, describe as 'regulatory capitalism'.[57] Regulatory capitalism considers that neo-liberalism has not resulted in the state retreating ,[58] but rather that the form of regulation has shifted.[59] It is being delegated through self-regulation and, correspondingly, government is regulated more tightly to prevent corruption.[60] The adoption of new regulatory measures requires corporations to engage in internal monitoring.[61] It means that international technical standards are increasingly imposed.[62] The term also denotes the global communication of regulatory concepts through regulatory organisations.[63] Heightened regulation takes place due to international competition in reaching certain thresholds.[64] New regulatory bodies have been set up to deal with pressing public matters.[65] However, even when a mixture of the neo-liberal and social welfare approach has been adopted, it is possible to determine whether a country leans more towards the neo-liberal or the social welfare paradigm of consumer protection. It is therefore important to understand the different aims and objectives of these two distinct approaches. It must also be identified which approach is supported by the Sharia and has been adopted by the UK and SA at present. Otherwise, the risk is that the findings from the analysis of the UK legal framework in chapter 4 and the analysis of the Saudi Arabian legal framework in chapter 5 result in recommendations which are not Sharia compliant. In this context, it is argued that a Sharia-compliant approach requires social welfare considerations to be firmly embedded in what otherwise can be a free market place. The reason for this is that the Sharia

[57] Ramsay n 32, 11.
[58] Ibid.
[59] D. Levi-Four, 'The Global Diffusion of Regulatory Capitalism' (2005) *Annals of the American Academy of Political and Social Science* 598, 12-32, 12.
[60] Ibid.
[61] Ibid.
[62] Ibid.
[63] Ibid.
[64] Ibid.
[65] Ramsay n 32, 12.

emphasises the importance of protecting the weak in order to create social cohesion within society.[66]

It is against this background that this chapter builds on chapter 2 and looks predominantly at the consumer protection legal literature and links it to the academic contractual literature on unauthorised transactions. This is done to present the various arguments/rationales formulated to advocate for, or caution against, providing consumer protection through legal means. Hence, this chapter focuses on evaluating the consumer protection literature in order to determine what arguments have been made in the academic literature about the following: The aims/objectives of consumer protection measures; the problems or advantages of formulating consumer protection policies; and the use of the law to achieve those objectives, including in respect of unauthorised transactions. It seeks to identify what aims and objectives ought to be prioritised to protect m-payment customers as well as the pitfalls, if any, of seeking to provide adequate protection to consumers. In order to achieve these objects, the literature is synthesised in order to establish what is known and, by extension, the gaps in existing knowledge which may be addressed by this research. The review seeks to identify whether there are any gaps in the literature which the thesis intends to fill in and respond to in subsequent chapters. The review of the consumer protection literature also serves as a framework for the analysis of UK and Saudi laws in subsequent chapters in order to ascertain the consumer protection approach being taken by each jurisdiction respectively in the context of m-payment services and helps with the recommendations which are derived from this research. There are therefore two purposes of this chapter: Firstly, to evaluate the arguments for consumer protection, including in the context of unauthorised transactions and the protection of consumer data and their privacy,

[66] K.B. Jedidia, 'How can Islamic banks achieve social justice? A discourse'. In T. Azid and L. Sunar (eds), *Social Justice and Islamic Economics: Theory, Issues and Practice* (Routledge 2019) Chapter 5.

and how these arguments may inform and influence the various theoretical approaches; and secondly, to identify gaps in the literature which may fall to be addressed in this work. This duality is reflected in the chapter structure set out below.

In terms of structure, the chapter firstly commences by studying international guidelines, such as the United Nations Guidelines for Consumer Protection ('UNGCP') in section 3.2. This section examines whether substantive guidance exists at the international level to afford protection to customers, which include the protection of m-payment customers or which pre-date the recent shift to m-payments and therefore did not originally envisage protection for such customers but may nevertheless have been drafted in a way which is amenable to extension to this context. The analysis in section 3.2 will show that there is a lack of international consumer protection instruments for m-payment customers. Section 3.3 then analyses the potential aims/objectives which consumer protection policies and laws governing m-payment services should have. In other words, the two main policy options available for legislators are introduced, namely to promote either the 'consumer protection interest' objective or the 'consumer economic interest' objective.

Section 3.4 builds on this by discussing how liability can be allocated in respect of unauthorised transactions in a manner representative of the social welfare or neoliberal approach. It is also explored how the conceptualisation of a consumer in law can practically reflect these different aims/objectives. The way in which a consumer can be conceptualised is particularly important for the analysis of the UK and Saudi legal frameworks in chapters four and five, as well as the recommendations in the conclusion. Subsequently, section 3.5 presents the arguments made in academic materials. However, most of the literature is written mainly by Western academics, who are writing about consumer protection in relation to Western legal systems. They therefore tend to focus on identifying problems or advantages of

formulating consumer protection policies, and in trying to use the law to achieve the objectives identified in section 3.3 from the perspective of Western legal systems. It is evaluated whether legal consumer protection measures are necessary to protect consumers against unauthorised m-payment transactions and their data in order to maintain privacy or whether other options are available to legislators. Accordingly, it is further probed whether the neo-liberal approach can sufficiently protect m-payment customers. For this purpose, recourse is made to the scholarly work of academics, such as, Iain Ramsay, Geraint Howells and Thomas Wilhelmsson.

Furthermore, relevant materials written by Islamic scholars relating to consumer protection more generally and also on m-payment are presented in section 3.6. The purpose of analysing how Sharia law protects consumers, including m-payment customers, is to compare and assess the approach with that in the West. Additionally, it is identified what underlying policy considerations the Sharia advocates in order to protect consumers, as well as how this is currently achieved. Such an analysis is important to ensure that the evaluation of the Saudi legal framework and the recommendations comply with the overarching direction which the Sharia gives. Islamic business law principles which safeguard consumers are discussed, including the principle of good faith and the concepts of *halal* and *haram*. Thus, part of the aim of this literature review is to identify the extent to which there is available literature on consumer protection that could be used to develop a more pro-consumer set up of legislation that includes consideration of other legal systems, particularly, a Sharia legal system. The literature review also helps to identify whether there is a gap within the Sharia legal literature and is intended to provide a timely addition to the state of the art.

The chapter concludes with a summary of how the law can ensure consumer protection objectives are embedded within the law. The discussion in subsequent chapters then draws on the legal literature and relevant Sharia tenets relating to consumer protection in order to evaluate how, why and when the law should (or should not) intervene in order to provide protection to consumers against unauthorised m-payment transactions and to protect their data in order to maintain privacy. It is argued that providing consumer protection through legal means is no easy task in the context of m-payments. Consumers can greatly contribute to occasioning losses and have to therefore act with heightened due diligence when using their smart-devices. Yet m-payment service providers must ensure that the platforms which they make available to their customers are operated properly, including by third parties. They must therefore ensure that the infrastructure which they make available to m-payment customers is safe and secure and functions properly.

3.2 International consumer law

Durovic and Micklitz explain that Article 10bis of the Paris Convention for the Protection of Industrial Property of 1883 was the first international instrument which required some degree of consumer protection by proscribing unfair commercial practices.[67] In 1985, the United Nations then published Guidelines on Consumer Protection, which were amended in 1999 and 2016 respectively. These guidelines particularly focus on ensuring fair advertising practices so that consumers can reach decisions on an informed basis, as well as independently.[68] The 2016 version further extended the rules in order to prevent fraudulent, deceptive, and misleading online advertisements.[69] Accordingly, these guidelines focus on

[67] M. Durovic and H.W. Micklitz, *Internationalization of Consumer Law: A Game Changer* (Springer 2016) 29.
[68] UN Guidelines on Consumer Protection, Articles 17 and 22-26.
[69] Durovic and Micklitz n 67.

disclosure, i.e., providing correct information to consumers, so that they can reach informed decisions about goods and services in line with autonomy theory.[70] Hence, the right of consumers to receive information is advocated. The guidelines are not a strong instrument for consumer rights because their scope is limited to advertising. Also, an international instrument could have been adopted which incorporates broader consumer rights, e.g., not to be treated unfairly or to have one's economic rights protected.

Apart from the UN Guidelines on Consumer Protection which call for consumer protection, the OECD also published the Guidelines for Protecting Consumers from Fraudulent and Deceptive Commercial Practices Across Borders in 2003. Like the UN Guidelines, these Guidelines focus on deceptive and fraudulent commercial practices. They are therefore an expression of a market-based approach towards consumer protection. The same can be said of the International Chamber of Commerce's Code on Advertising and Marketing Communication Practices 2011.[71] As observed by Calliess, a co-regulatory approach has been adopted and no multilateral treaty has been enacted.[72] The absence of a multilateral treaty arguably leaves consumers unprotected against corporate interests, including customers who make use of the new technologies which facilitate m-payment transactions.

The international legal framework for consumer protection is therefore explored too narrowly from a neoliberal perspective which allows too little room for contemplation of a social welfare approach.[73] It also does not address the main problem which arises in the context of m-payment transactions. The issue when making m-payments is not necessarily

[70] M.J. Radin, *Boilerplate: The Fine Print, Vanishing Rights, and the Rule of Law* (Princeton University Press 2013) 271.
[71] Durovic and Micklitz n 67, 35.
[72] Calliess n 26, 2.
[73] C. Lima Marques and D. Wei, *Consumer Law and Socioeconomic Development: National and International Dimensions* (Springer 2017) 8.

that m-payment service providers publish misleading information. Instead, the fundamental question is how to allocate liability fairly for unauthorised payment transactions between m-payment service providers and consumers and when data is not adequately protected. Put another way, the instances in which consumers should be able to seek redress from m-payment service providers because they have failed to manage risk properly should be spelt out. Equally, it should be addressed whether more leverage should be conferred on consumers when it comes to companies using consumer data. Yet a determination of this question depends on the aims/objectives of consumer protection measures which law makers may choose to pursue. This in turn depends on the policy orientation which a country may pursue. As pointed out by Dagan and Heller, consumer protection policies and laws diminish autonomy.[74] They therefore undermine the neoliberal ideal of individual freedom, including in respect of contracting.[75] The extent to which autonomy should be diminished in relation to this emerging market must therefore be analysed. This is arguably also important in order to promote m-payment innovation which may benefit consumers as discussed in chapter 1.

However, as emphasised by the OECD's G20 High-Level Principles on Financial Consumer Protection, a market can only properly function if there exists consumer trust and confidence.[76] This in turn requires that steps are taken to protect consumers and to promote financial stability.[77] The G20 principles therefore call on governments to create financial consumer protection frameworks.[78] Yet, the principles acknowledge that a balance must be struck between allocating responsibility.[79] Customers therefore also have certain

[74] H. Dagan and M. Heller, *The Choice Theory of Contracts* (CUP 2017) 82.
[75] A.M. Kelly and A. Beaumont, 'Freedom After Neoliberalism' (2018) *Open Library of Humanities*, 1-26, 7&10.
[76] OECD, G20 High-Level Principles on Financial Consumer Protection, Paris, OECD, October 2011, 1-7, 4.
[77] Ibid.
[78] Ibid.
[79] Ibid.

obligations.[80] The principles emphasise the need for a supervisory, legal and regulatory framework.[81] Specific oversight bodies must be created to ensure financial consumer protection,[82] such as, an ombudsman service or the UK Competition and Markets Authority.[83]

The principles further provide that consumers must be treated in a fair and equitable manner.[84] However, what this precisely means in the context of m-payment transactions is unclear. Moreover, like the other international instruments, emphasis is placed on providing consumers with important information, i.e., through transparency and disclosure.[85] Consumers must be educated and awareness must be raised about their responsibilities and consumer rights,[86] including how to resolve complaints and seek redress.[87] However, the neoliberal approach of providing information may be problematic in respect of unauthorised m-payment transactions. The reason is that research suggests that even knowledgeable and skilled customers are vulnerable to digital banking fraud.[88]

The principles further stipulate that competition should be encouraged.[89] It is mandated that financial services providers as well as their agents, must adopt responsible business practices, especially to ensure that consumer assets are protected against misuse and fraud and their data and privacy rights are safeguarded.[90] The OECD principles are a reflection of a neo-liberal approach which emphasises individual autonomy and that might cause the principles to have more limited effect for consumer protection purposes. Williams

[80] Ibid.
[81] Ibid 5.
[82] Ibid.
[83] Ramsay n 32, 11.
[84] OECD n 76, 5.
[85] Ibid 6.
[86] Ibid.
[87] Ibid 7.
[88] J. Jansen and R. Leukfeldt, 'Phishing and Malware Attacks on Online Banking Customers in the Netherlands: A Qualitative Analysis of Factors Leading to Victimization' (2016) *International Journal of Cyber Criminology* 10(1), 79–91, 79.
[89] Ibid.
[90] Ibid.

also states that the framework which the principles spell out is a neoliberal variant.[91] This model was primarily devised as a tool to address financial instability following the global financial crisis which started in 2008.[92] Hence, it was not necessarily conceived as a policy tool to ensure comprehensive consumer rights.

The G20 principles are therefore not necessarily prescriptive since governments can still determine which policy model they want to adopt. Put differently, countries can choose whether to opt for more public and thus statutory and other more stringent regulatory measures, or for more private measures to protect consumers, e.g., through disclosure and voluntary industry codes. Ramsay comments that the protection of consumer interests in the context of finance is still rather weak.[93] Similarly, Calliess points out that consumer protection is not a topic which has received much attention at the international level.[94] As a result, it is difficult to enforce domestic consumer protection frameworks due to insufficient international cooperation.[95] The lack of international guidance on substantive consumer rights constitutes an issue which may disadvantage m-payment customers. In light of the inadequacy of the international consumer protection instruments to provide clarity on how to protect customers who use m-payments services, it is particularly important for all legislators and policy makers to be clear on which aims and objectives they choose to promote. This is discussed in the next section.

[91] T. Williams, 'Continuity, not Rupture: The Persistence of Neoliberalism in the Internationalization of Consumer Finance Regulation'. In T. Wilson (eds), *International Responses to Issues of Credit and Over-indebtedness in the Wake of Crisis* (Routledge 2013) 3.
[92] Ibid.
[93] I. Ramsay, 'Consumer credit regulation after the fall: international dimensions' (2012) *Zeitschrift für Europäisches Unternehmens- und Verbraucherrecht Journal of European Consumer and Market Law* 1, 24–34, 24.
[94] Calliess n 26, 1.
[95] Ibid.

3.3 Consumer policy and legal protection measures: Aims and objectives

At the outset, it is essential to understand the 'menu' of underlying policy aims and objectives which can be reflected in m-payment laws. Whitman observes that there exist two competing policy objectives which legislators may want to pursue when they enact consumer protection laws:[96] The first is the objective of upholding the "consumer economic interest", i.e., to promote consumer choice and low prices.[97] The other objective can be the "consumer protection interest", i.e., to protect consumers against low-quality and unsafe goods and services.[98] As these latter goods and services are typically cheap, it may be difficult to align these two consumer policy objectives.[99] Like Whitman, Ramsay states that policymakers and legislators can focus on social welfare by enacting robust consumer rights and creating the institutions to enforce the "consumer protection interest".[100] In the alternative, they can prioritise economic interests by promoting increased competition and innovation.[101] Accordingly, when the consumer economic interest is prioritised less concern is raised about consumer protection. When dealing with the broader question of the research, namely how the law protects m-payment customers against unauthorised m-payment transactions and safeguards customers' data and their privacy, the question of whether the consumer economic interest trumps the consumer protection interest is very relevant.

Whilst those favouring the consumer protection interest objective require bureaucratic regulation, those advocating the consumer economic interest leave more to the market in line with neo-liberal thought.[102] The latter is a soft approach characterised by promoting best practices and requiring information disclosure, but does not overly focus on minimising the

[96] Whitman n 25, 367.
[97] Ibid.
[98] Ibid.
[99] Ibid.
[100] Ibid.
[101] Ramsay n 37, 347.
[102] Whitman n 25, 367.

social costs to consumers.[103] This is because consumer law is primarily viewed as a tool to promote business interests.[104] The objective of consumer law and policy is therefore to simply facilitate consumer confidence without granting substantive rights.[105] In this context, Whitman points out that policymakers who opt for promoting the consumer economic interest often tend to encourage consumer spending, whereas this is not the underlying aim of safeguarding the consumer protection interest.[106]

Micklitz explains that, in the EU, consumer policy and law have been primarily employed to develop the internal market.[107] As a result, social justice has not been promoted as much.[108] The EU approach to devising consumer protection rules is therefore not an example of the 'consumer economic interest' approach. Winn and Jondet share this opinion and point out that the EU has adopted a "co-regulation" approach, so that standard developers and legislators work together.[109] The co-regulation approach is only used to cut down technical barriers with a view to facilitating trade.[110] The law has thus been driven by market considerations, mainly to realise economic efficiencies.[111] This is not to say that consumers have not been granted rights. As explained by Valant, initially consumer protection was based on five core rights in the EU: Health and safety rights for consumers; the consumer's right to receive education; the right of consumers to be heard; and to have their economic interests protected.[112] This later became expanded to equipping consumers with easy

[103] Ramsay n 37, 349.
[104] Ibid.
[105] Ibid 352.
[106] Whitman n 25, 367.
[107] H.-W. Micklitz, 'European Consumer Law'. In E. Jones et al (eds), *The Oxford Handbook of the European Union*, Oxford Handbooks Online, 2013, 1-20, 1.
[108] Ibid.
[109] J. Winn and N. Jondet, 'A "New Approach" to Standards and Consumer Protection' (2008) *Journal of Consumer Policy* 31, 459-472, 459.
[110] Ibid.
[111] Micklitz n 107, 1.
[112] J. Valant, 'Consumer protection in the EU, Policy overview', European Parliamentary Research Service, September 2015, 1-24, 4.

enforcement measures, including for the settlement of disputes.[113] Nonetheless, such a rights-based approach poses a risk to consumers who do not have the requisite abilities to make use of their legal rights.[114] Micklitz states that, as a result, more vulnerable individuals are at risk of being disadvantaged.[115] Soederberg also cautions against perceiving consumer protection as a tool to strengthen market mechanisms.[116] It reinforces market-based citizenship by allowing risky practices, as long as rudimentary standards are met.[117] To this extent, the EU approach represents a compromise between the two approaches which offers the 'best' (or perhaps from a more critical perspective, the 'worst') of both options.

A consumer protection framework for m-payment customers engages a wide range of core rights, which reflects the fact that there are a variety of ways in which Fintech may damage consumer interests and wellbeing, as discussed in chapter 2. As pointed out by the Financial Stability Board in the UK, the protection of financial consumers forms an aspect of a public policy regime and can, therefore, be found in most prudential, regulatory or legislation structures.[118] For instance, in the context of consumer lending, the UK Consumer Credit Act 2006 focuses on creating a competitive, more transparent and fairer credit market.[119] A mix of consumerist and producerist policy objectives are thus pursued. The consumer credit literature is useful and relevant since it highlights the importance of giving

[113] Ibid 14.
[114] Micklitz n 107, 1.
[115] Ibid.
[116] S. Soederberg, 'The US Debtfare State and the Credit Card Industry: Forging Spaces of Dispossession' (2013) *Antipode* 45(2), 493-512, 500.
[117] Ibid.
[118] Financial Stability Board, Consumer Finance Protection with particular focus on credit, 26 October 2011, 1-53, 4.
[119] T. Edmonds, 'High Cost Consumer Credit', House of Commons Briefing Paper, Number 05849, 15 July 2014, 1-48, 1.

rights to consumers so that they can challenge unfair agreements and can resolve disputes easily, including in respect of unauthorised transactions.[120]

In the m-payment context, unfair practices must also be combated through specific action, such as, ensuring that consumers are furnished with information. Hence, like in the consumer credit context, steps should be taken to support welfare and social objectives. Regulation should also be adopted to enhance the licensing system, which indirectly protects consumers.[121] However, Ramsay argues that, despite consumer rights having been granted, the policy orientation in jurisdictions like the UK, has been to prioritise consumer choice.[122] As a result, the objective of protecting consumers from market risks has been marginalised.[123]

Certainly, there is always the risk that a legal consumer protection regime is not entirely balanced so that both business and consumer interests are not entirely equally promoted. Nonetheless, it is argued that a policy mix as found in, for instance, the UK Consumer Credit Act 2006 appears most advantageous for the newly emerging m-payment market. Yet, as observed by Poncibò, this can be difficult, though not impossible, since both are to a certain extent complementary.[124] Accordingly, one aim should be to promote competition so that consumer choice is increased.[125] Care must be taken when legal duties are imposed on m-payment service providers so that new market entrants are not deterred by stringent regulatory requirements and legal obligations.[126] Otherwise, the risk is that

[120] Ibid.
[121] J. Macleod, *Consumer Sales Law, The Law Relating to Consumer Sales and Financing of Goods* (Cavendish Publishing Ltd 2002) 203.
[122] I. Ramsay, 'To Heap Distress Upon Distress?' Comparative Reflections on Interest-Rate Ceilings' (2010) *University of Toronto Law Journal* 60, 707-730, 730.
[123] Ibid.
[124] C. Poncibò, 'Networks to Enforce European Law: The Case of the Consumer Protection Cooperation Network' (2012) *Journal of Consumer Policy* 35, 175-195, 185.
[125] Whitman n 25, 365.
[126] Poncibò n 124, 185.

competition, and thus consumer choice, will be adversely affected.[127] Nonetheless, it is crucial that consumer law ensures honest and fair market practices so that consumers can have faith in m-payment services.[128] Trzaskowski states that this means that businesses must exercise professional diligence.[129]

Professional diligence in the m-payment context particularly requires that specific attention is paid to the governance of information and communication technology ('ICT'). Winn and Jondet explicate that ICT standards are a very important means to heighten consumer protection.[130] They argue that effective consumer protection requires that the objectives of consumer protection laws are embedded by standards organisations.[131] However, ICT standards are normally promulgated by informal standards organisations and not the legislator.[132] Yet in the context of m-payments, it may be useful for domestic authorities to spell out ICT standards, especially in respect of consumer protection.[133]

As discussed in the previous chapter, in the context of m-payments, the issue is how to ensure that the heightened technological and thus operational risk is adequately addressed, particularly the issue of unauthorised m-payment transactions and that consumer data is protected in order to maintain privacy. The conditions must be analysed which must be created through the legal framework for this new market to operate in order to contribute to economic growth. Large scale cyber-attacks of increasingly digital outlets of banks are likely

[127] Ibid.
[128] J. Trzaskowski, 'Behavioural Economics, Neuroscience, and the Unfair Commercial Practises Directive' (2011) *Journal of Consumer Policy* 34, 377-392, 381.
[129] Ibid.
[130] Winn and Jondet n 109, 459.
[131] Ibid.
[132] Ibid.
[133] Ibid 470.

to become more commonplace.[134] More importantly, consumer funds must be protected, as well as their data. Whilst the aim of the law ought to be to promote consumer choice and allow a more market-oriented policy approach, it must nonetheless ensure that consumers are adequately protected against financial losses and privacy breaches.

The adoption of legal means to heighten security for m-payment customers, particularly in respect of unauthorised payment transactions, the utilisation of consumer data by m-payment providers, as well as data breaches, should, therefore, be on the policy agenda of all legislators.[135] As identified in chapter 4, consumer protection laws should impose legal duties (e.g., through tort law, especially the negligence and duty of care concept, general contract law in the form of the law governing unfair exclusion clauses and terms to promote fairness and justice), as well as specific statutory and regulatory obligations (e.g., mandated disclosure,[136] and to operate effective risk management systems and adhere to certain ICT standards). As one of the main issues is the allocation of liability when consumer funds go missing, the law must address how liability should be allocated and this depends on how one conceptualises a consumer, as discussed next.

3.4 Allocating liability: A neo-liberal or social welfare consumer construct

Whitman defines a consumer as any person who consumes services or goods.[137] Valant also favours a broad construction of the term consumer.[138] She even suggests the adoption of the

[134] E. Glazer and M. Farrell, 'Big U.S. Banks Face Increase in Attempted Cyberattacks', 30 September 2018 <https://www.wsj.com/articles/big-u-s-banks-face-increase-in-attempted-cyberattacks-1538317920> accessed 5 March 2019.
[135] T. Khiaonarong, 'Oversight Issues in Mobile Payments', International Monetary Fund Working Paper No. 14/123, July 2014, 1-36, 5.
[136] T. Baker and P. Siegelman, 'Protecting Consumers from Add-On Insurance Products: New Lessons for Insurance Regulation from Behavioral Economics' (2013) University of Pennsylvania Law School Research Paper No. 13-1, 1-61, 7.
[137] Whitman n 25, 366.

notion of "prosumers", i.e., a hybrid of a professional, a producer and a consumer.[139] This is because, in an increasingly collaborative economy, also known as 'sharing economy', it is more difficult to distinguish between professionals, freelancers and hobbyists.[140] Durovic and Micklitz also caution that, without a broad construction of what constitutes a consumer, the danger is that material inequalities arise between natural and legal persons.[141] Whilst traders have arguably more leverage to negotiate terms than individual consumers, in the context of banking, standardised terms are provided.[142] It is for this reason that it is argued that all those making m-payment transactions should be classified as consumers. Accordingly, anyone making use of m-payment services should be considered a consumer (even if the m-payment is enacted on behalf of a company, as a company like a natural person would not enjoy any power to negotiate the terms of use of the service with a provider, such as Facebook).

The more complicated legal question is whether the consumer should be conceptualised as vulnerable, credulous, average or rational and therefore reasonably circumspect.[143] Such a question is important when assessing whether a consumer has been negligent and thus the question of loss allocation. Abbamonte explains that the way in which a consumer is conceptualised serves as a legal threshold.[144] Against this threshold, it is evaluated whether there exists unfairness against which a consumer should be protected.[145] Quirk and Rothchild observe that consumer protection systems normally benchmark their

---

[138] Valant n 112, 16.
[139] Ibid.
[140] Ibid.
[141] Durovic and Micklitz n 67, 39.
[142] M. Andenas and I. H.-Y. Chiu, *The Foundations and Future of Financial Regulation: Governance for Responsibility* (Routledge 2014) 92.
[143] Ramsay n 37, 343.
[144] G.B. Abbamonte, 'The Unfair Commercial Practices Directive: An Example of the New European Consumer Protection Approach' (2006) *Columbia Journal of European Law* 12(3), 695-712, 707.
[145] Ibid.

legal safeguards on the "average" or "reasonable" consumer.[146] Ramsay explains that those subscribing to the neo-liberal paradigm favour such a depiction of the consumer. [147]

Such a threshold is laxer and, by extension, fewer legal consumer protection measures and interventions are required. Faure and Luth explain that the rational/average consumer standard is rooted in rational choice theory.[148] Rational choice theory posits that individuals opt for the choice which increases their welfare most when faced with decisions.[149] However, they criticise rational choice theory which is based on the neo-liberal paradigm on the grounds that it is an oversimplification to assume that human beings always act rationally.[150] History also proves that human beings do not always act rationally.[151] Faure and Luth do not consider that there exists one general theory and therefore favour the behavioural economics and law approach.[152]

Those endorsing a behavioural economics and cognitive psychology approach and who argue in favour of a vulnerable/credulous consumer standard challenge the rational choice theory on the grounds that individuals are inherently irrational.[153] In other words, the notion of the rational or average consumer bears no resemblance to real life.[154] For instance, a study by Gidlöf et al found that consumers did not reach adequate economic decisions when choosing products in store, despite not receiving misleading information.[155] Hence, it is

[146] P. Quirk and J.A. Rothchild, 'Consumer Protection and the Internet'. In G. Howells et al, *Handbook of Research on International Consumer Law* (Edward Elgar 2010) 338.
[147] Ramsay n 37, 343.
[148] R.A. Posner, 'Rational choice, behavioural economics, and the law' (1998) *Stanford Law Review* 50, 1551–1575, 1551.
[149] Ibid.
[150] M.G. Faure and H.A. Luth, 'Behavioural Economics in Unfair Contract Terms' (2011) *Journal of Consumer Policy* 34, 337-358, 337.
[151] G.M. Hodgson, 'On the Limits of Rational Choice Theory' (2012) *Economic Thought* 1, 94-108, 94.
[152] Ibid.
[153] Ramsay n 37, 343&345; R. Incardona and C. Poncibo, 'The Average Consumer, The Unfair Commercial Practices Directive, and the Cognitive Revolution' (2007) *Journal of Consumer Policy Issue* 30(1), 21-38, 21.
[154] Ibid (Incardona and Poncibo).
[155] K. Gidlöf et al, 'Material Distortion of Economic Behaviour and Everyday Decision Quality' (2013) *Journal of Consumer Policy* 36, 389-402, 400.

wrong to assume that consumers reach rational decisions and possess the cognitive abilities to do so.[156] They may not have unlimited time to analyse information and read lengthy terms and conditions and privacy agreements.[157]

Esposito argues that effective information disclosure is an inadequate consumer policy which disregards the findings of the behavioural science literature.[158] Equally, Incardona and Poncibo question the workability of the average consumer standard.[159] They argue that providing information and trusting that consumers are rational is insufficient to protect consumers.[160] Faure and Luth also stress that it is not enough to provide consumers with standard form contracts and to assume that such information disclosure rectifies market failures.[161] Consumers often sign/agree to standard contract terms without reading what is actually written.[162] Similarly, Van Boom argues that furnishing more information to consumers does not enhance their ability to reach decisions, especially since this often results in a cognitive overload.[163] Weatherill further points out that there is no one homogenous class of consumers and whilst some may be circumspect and informed, others may lack such attributes.[164] Even opponents of behavioural economics, such as Epstein, concede that consumers frequently make fundamental errors.[165]

The problem of choosing a rational/average consumer threshold for the m-payment context is thus that it imposes a very high threshold for consumers to meet. Trzaskowski

[156] Ibid 389.
[157] Ibid.
[158] F. Esposito, 'A Dismal Reality: Behavioural Analysis and Consumer Policy' (2017) *Journal of Consumer Policy* 40, 193-216.
[159] Incardona and Poncibo n 153, 21.
[160] Ibid.
[161] Faure and Luth n 150, 337.
[162] Ibid.
[163] W.H. van Boom, 'Price Intransparency, Consumer Decision Making and European Consumer Law' (2011) *Journal of Consumer Policy* 34, 359-376, 361.
[164] S. Weatherill, 'Who is the "average consumer?' In S. Weatherill and I. Bernits (eds), *The regulation of unfair commercial practices under EC Directive 2005/29: New rules and new techniques* (Hart Publishing 2007) 1.
[165] R.A. Epstein, 'Behavioral Economics: Human Errors and Market Corrections' (2006) *University of Chicago Law Review* 73, 111-132, 111.

therefore labels this test unrealistic.[166] This is supported by a study by Daly and Scardamaglia.[167] The research investigated whether the average internet user in Australia has a general understanding of how Google's search engine operates.[168] It was found that there was a significant imbalance which disadvantaged consumers in the online context.[169] The behavioural economics approach is arguably very relevant to the m-payment context. Consumers may not be sufficiently knowledgeable to adequately protect their funds against cybercrime and illegal privacy intrusions.[170] It is for this reason that it is arguably important that consumer interests are proactively protected.[171] A conceptualisation of the m-payment customer as credulous and vulnerable will heighten the level of protection for consumers.[172] It will also incentivise the system operator to adopt precautionary measures.[173]

A vulnerable consumer test is less rigid than the average consumer test.[174] Yet Incardona and Poncibo argue that such a test is too paternalistic, unnecessary and devoid of any coherent base.[175] The vulnerable consumer test contravenes the notion of 'the literate consumer' who is empowered by knowledge.[176] Such a consumer should have responsibilities[177] and it appears justified to judge him/her according to the rational/average consumer test. A compromise is to adopt a rational/average consumer test, but to lower the threshold for specific consumer groups, e.g., those who are more vulnerable, such as, the

[166] Trzaskowski n 128, 383.
[167] A. Daly and A. Scardamaglia, 'Profiling the Australian Google Consumer: Implications of Search Engine Practices for Consumer Law and Policy' (2017) *Journal of Consumer Policy*, 1-22, 4.
[168] Ibid.
[169] Ibid.
[170] Ibid.
[171] Ibid.
[172] I. Ramsay, *Advertising Culture and the Law: Beyond Lies, Ignorance and Manipulation* (Sweet & Maxwell 1997) 70-98.
[173] R.J. Mann, 'Making Sense of Payments Policy in the Information Age' (2005) *Georgetown Law Journal* 93, 633-673, 638.
[174] Trzaskowski n 128, 385.
[175] Incardona and Poncibò n 153, 21.
[176] T. Williams, 'Empowerment of Whom and for What? Financial Literacy Education and the New Regulation of Consumer Financial Services' (2007) *Law & Policy* 29(2), 226-256, 227.
[177] Ibid.

elderly.[178] Certainly younger people may be more accustomed to using mobile apps and may therefore be more circumspect. This is because they may know more about how to secure their smart devices against cyber-attacks. However, this is a generalisation and it would contravene the principle of equality to protect one group of consumers less than others.

Durovic and Micklitz state that precisely such an approach has been integrated by Article 5(3) of EU Directive 2005/29/EC on unfair commercial practices which provides that the "mental or physical infirmity, age, or credulity" are to be considered when assessing whether commercial practices are fair.[179] A European Commission Report on the application of this Directive points to evidence that suggests that more steps should be taken to protect citizens who are in a weak position, especially children, elderly persons and others who are particularly vulnerable.[180] However, such an approach may be problematic in the context of m-payments. If a m-payment customer has competence in law (that is, is *compus mentus* and over the legally prescribed age limit for the activity in question) and can in practice install and use a m-payment app, it should arguably not be an excuse to plead, e.g., old age, when that person fails to keep his/her PIN code safe. It may also introduce a subjective assessment into legal proceedings which is difficult for judges to decide objectively. A m-payment customer should be expected to owe certain basic obligations. A customer ought not to be able to seek redress or only to a limited extent from their m-payment provider in certain circumstances, as discussed in chapter 2, section 2.2.1. For instance, the right to have an unauthorised payment refunded could be curtailed in circumstances, e.g. where a customer failed to keep the PIN securely stored; or did not install security software or run anti-virus and malware scans; failed to install updates; or conducted transactions in a more high-risk

[178] Durovic and Micklitz n 67, 38.
[179] Ibid.
[180] European Commission, 'Report from the Commission to the European Parliament, the Council and the European Economic and Social Committee, First Report on the application of Directive 2005/29/EC of the Unfair Commercial Practices Directive, Brussels, COM(2013) 139 final, 14 March 2013, 1-31, 13.

environment through a more unsecure public Wi-Fi network. These are very different situations to the scenarios, discussed in chapter 2, sections 2.2.2 and 2.2.3, where a m-payment provider fails to ensure that it has an adequate risk management system, or it is the fault of a third-party provider and where it is unfair to allocate responsibility for financial losses to m-payment customers.

Yet if m-payment customers are uneducated, e.g., because technology is very fast moving, including in respect of new cybercrime, a consumer protection model premised on a vulnerable consumer may be more appropriate initially. However, as time passes and consumers increasingly become accustomed to using their mobile phones to conduct m-payment services, it may be possible for the law to move towards a conceptualisation of a reasonable consumer approach. Nonetheless, this necessitates that the technological and operational risks discussed in chapter 2 for which m-payment providers and third parties are responsible become reduced. For instance, this may happen in the future because the digital identity of customers is more easily verifiable through, e.g., the creation of a new legal digital identity.[181] The researcher would argue that a vulnerable consumer conceptualisation appears best suited since m-payment technology is still in its infancy. More steps must be taken to promote IT consumer literacy further and to reduce risk. Arguably, the legal test should only be changed to the more onerous rational/average consumer test once more public awareness is raised, and consumers possess the requisite skills and m-payment technology has become safer.

[181] World Economic Forum, 'A Blueprint for Digital Identity, The Role of Financial Institutions in Building Digital Identity', August 2016, 1-108, 10.

Accordingly, it may be better to conceptualise consumers as regulatory subjects, who must be taken to act responsibly.[182] Hence, consumers not only have rights, but also duties.[183] Such an approach recognises that in the specific context of unauthorised transactions, losses can be most effectively minimised by allocating them with the party which is most able to prevent or decrease them, as observed by Geva.[184] It is argued that such an approach is particularly useful for the m-payment context since it helps to overcome the tension which exists between the neo-liberal and the social welfare approach[185] which underlie the average/rational and credulous/vulnerable consumer tests. Put differently, this means that it becomes unnecessary to opt for "soft paternalism" in line with a more liberal approach or hard paternalism in line with the behavioural and more socialist approach.[186]

Instead, a middle path can be chosen, so long as consumer education is made a priority by policymakers and m-payment providers alike. Geva also states that the overarching framework to implement or maintain consumer fairness in the specific context of allocating losses from unauthorised funds transfers should be market-oriented.[187] Geva further illustrates how such an approach works by citing UK consumer legislation governing credit accounts as an example.[188] Under s.83 of the Consumer Credit Act 1974, a debtor cannot be held liable by the creditor in circumstances where another person uses the credit facility and causes any loss, except for up to £35 from when the authorised person has no longer possession of the credit-token.[189] However, the no-liability provision does not apply if

[182] Ramsay n 32, 9&13.
[183] Ibid.
[184] B. Geva, 'Consumer Liability in Unauthorised Electronic Funds Transfers' (2003) *Canadian Business Law Journal*, 207-281, 211.
[185] R.S. Turner, *Neo-Liberal Ideology, History, Concepts and Policies* (Edinburgh University Press 2008) 5.
[186] Epstein n 165, 132.
[187] Geva n 184, 211.
[188] Ibid 248-249.
[189] Consumer Credit Act 1974, s84(1).

the debtor has consented to another person using the credit token.[190] However, liability for up to £35 or for any loss[191] ceases from the point when the creditor has been notified that the credit-token has been stolen, lost or is being misused.[192] The onus of proof rests with the creditor to demonstrate authorised use, including that the use occurred prior to it receiving notice.[193] Geva observes that there are ultimately three scenarios:[194] Under the first scenario, it is proven that the use was unauthorised, but the user did not contribute to the loss and is fully exonerated. In the second case, it is shown that there was an unauthorised use and the user contributed to the loss and must shoulder significant liability. In the third instance, there is an unauthorised use, though it is not evidenced that the user contributed to any loss and liability is thus limited. In other words, according to Geva, the best approach to consumer liability in respect of unauthorised transfers is to hold the creditor accountable, except where the debtor is to blame and in unclear cases to partly hold the debtor liable but at a capped amount. This reflects a market-oriented approach and incentivises both parties to try their best to minimise losses.

An Anglo-Saxon market-oriented approach must adhere to the "principles of economic efficiency" which require "loss spreading, loss reduction, and loss imposition", according to Cooter and Rubin.[195] These principles highlight the importance of supplementing private payment service agreements, including m-payment service agreements, in order to address market failures, particularly the issues of asymmetrical information and high negotiation costs,[196] which also exist in respect of unauthorised m-payment transactions. Under the loss spreading principle, it is thought that financial

[190] Consumer Credit Act 1974, s84(2).
[191] Consumer Credit Act 1974, s84(1)-(2).
[192] Consumer Credit Act 1974, s84(3).
[193] Consumer Credit Act 1974, s171(4)(a)-(b).
[194] Geva n 184, 277.
[195] R.D. Cooter and E.L. Rubin, 'A Theory of Loss Allocation for Consumer Payments' (1987) *Texas Law Review* 66(3), 63-130, 63.
[196] Ibid 68&70.

institutions should be liable for losses, as they can spread the costs which are caused by unauthorised transactions among its customers.[197] The loss reduction principle commands that rules are created which incentivise the party with the ability to lower the losses by imposing liability on the party for whom it is the easiest to prevent the loss.[198] Negligence rules which also include a defence of contributory negligence arguably incentivise each party more than a simple strict liability or no liability rule.[199] The loss imposition principle requires that efficiency is promoted by considering what is the cheapest enforcement process.[200] However, this does not mean imposing liability on the creditor.[201] Instead, it requires that legal mechanisms are developed which enhance consumers' readiness to evoke their legal rights.[202]

When rules are devised to allocate liability in line with the "principles of economic efficiency"[203], it must be also considered who can avert the unauthorised transaction prior to it arising and also subsequently after the first one has occurred.[204] In a case where it is only the financial institution which can minimise the loss, strict liability should be imposed on it.[205] When each party can reduce the unauthorised transaction, liability for losses should fall on both parties, though the consumer should only be held responsible for a small amount.[206] Hence, the consumer's liability should be capped.[207] The reason is that a technology-driven system, such as m-payments, is most likely best placed to reduce losses.[208] Facciolo also

[197] Ibid 71.
[198] Ibid 73.
[199] Ibid 74.
[200] Ibid 78.
[201] Ibid.
[202] Ibid 81.
[203] Ibid 63.
[204] F.J. Facciolo, 'Unauthorized Payment Transactions and Who Should Bear the Losses' (2008) *Chicago-Kent Law Review* 83(2), 605-631, 605.
[205] Cooter and Rubin n 195, 124.
[206] Ibid.
[207] Ibid 63.
[208] Mann n 173, 638.

stresses that the increasing complexity within payment transactions arguably requires that financial institutions are best placed to police payment systems and to avert unauthorised transactions.[209] However, account holders should shoulder liability when they can prevent unauthorised transactions by exercising due diligence.[210] Hence, losses should not just be allocated to the financial institution, but to both the financial institution and the consumers in accordance with negligence principles,[211] and as also mandated by the economic and efficiency promoting loss reduction principle, discussed above.[212]

However, a social welfare centric consumer approach would ignore negligence by the consumer prior to the first transaction taking place.[213] In contrast, a mixed social welfare and neo-liberal approach would consider whether a consumer was negligent or a neo-liberal stance would permit strict liability, so that the consumer is responsible so long as the security procedure by the provider was reasonable.[214] Once an unauthorised transaction takes place, it is normal to request the consumer to notify the unauthorised transaction.[215] If this is done promptly, no liability may be imposed for the first and other unauthorised transactions.[216] In contrast, a lengthy delay typically bars a consumer from recovering any losses.[217] However, as pointed out by Facciolo, in light of account holders making numerous transactions, it may be challenging for them to monitor whether transactions are unauthorised.[218]

As private agreements vary and address the issue of loss allocation differently, UK law has adopted a flexible and general fairness concept in respect of unfair terms found in

[209] Facciolo n 204, 630.
[210] Ibid 608.
[211] Cooter and Rubin n 195, 85.
[212] Ibid 74.
[213] Facciolo n 204, 606.
[214] Ibid.
[215] Ibid 607.
[216] Ibid.
[217] Ibid.
[218] Ibid 630.

consumer contracts[219], including in respect of m-payment service agreements. Fairness has been linked to the concepts of reasonableness and good faith,[220] though good faith is more of a civil law concept.[221] Hence, norms such as good faith and reasonableness in the earlier legislation, such as the Unfair Terms in Consumer Contracts Regulations (UTCCR) 1999[222] and Unfair Contract Terms Act (UCTA) 1977[223], have found their way into consumer protection literature and legislation and case law.[224] The Consumer Rights Act 2015[225] also integrates a fairness concept, as further discussed in Chapter 4, section 4.4.1. The use of these concepts has allowed the law to respond to various circumstances[226] and which consumers can utilise to challenge unfair terms which govern unauthorised m-payment transactions. The adoption of such a broad and flexible fairness concept avoids that courts have to construe exemption clauses in an extreme manner in order to prevent them from operating.[227] A statutory fairness concept is thus "a powerful weapon against unfair terms"[228] which payment institutions impose to escape liability in respect of unauthorised m-payment transactions. The English approach tempers classical contract theory which upholds a bargain between parties.[229] It makes it possible to safeguard the consumer who has less power and as a result agrees to prejudicial terms.[230] It is thus a way to overcome the problems which arise from a purely contractual approach which relies on boilerplate contracts, lengthy terms and unfair exclusion clauses.

---

[219] A. Giordano Ciancio, 'Fairness in Consumer Law: A Vague, Flexible Notion' in V.K. Bhatia et al (eds) *Vagueness in Normative Texts* (Oxford, Peter Lang 2005) 413.
[220] Ibid.
[221] E. McKendrick, *Contract Law: Text, Cases, and Materials* (8th ed, OUP 2018) 483.
[222] UTCCR 1999, Reg.5(1).
[223] UCTA, s11 and Sched.2.
[224] C. Willett, *Fairness in Consumer Contracts: The Case of Unfair Terms* (2nd ed, Abingdon, Routledge 2016) Chapter 3.
[225] Consumer Rights Act 2015, s71.
[226] Giordano Ciancio n 219, 413.
[227] D. Rowland and E. Macdonald, *Information Technology Law* (3rd ed, Cavendish Publishing 2005) 184.
[228] E. Macdonald, 'Unifying Unfair Terms Legislation' (2004) *The Modern Law Review* 67(1), 69-93, 69.
[229] M.S. Hussain, 'The Reasonableness of the UCTA 1977's Test of Reasonableness' (2017) SSRN Electronic Journal, 1-4, 1 <10.2139/ssrn.3058489> accessed 1 March 2019.
[230] Ibid.

However, English contract law does not require that the contract performance and interpretation is governed by a good faith principle, as the common law adopts a piecemeal approach.[231] Such an approach is more reflective of a neo-liberal, as opposed to a paternalistic consumer protection approach.[232] The reason is that it is not a "general fairness model" under which the state does not permit agreements which are significantly unfair.[233] Instead, it represents a "consumer protection model" which focuses on an imbalance and the bargaining power between the consumer and the business.[234] Hence, it is a consumer protection calibrated neoliberal approach which values private autonomy, rationality and market forces[235] and only indirectly regulates fairness.[236]

Accordingly, there exist various ways to allocate liability and it depends on whether one opts for a neo-liberal or social welfare consumer construct. The adoption of either the credulous/vulnerable or average/rational consumer test in law, specific loss allocation rules and general fairness and reasonableness standards, presuppose that legal consumer protection measures are adopted. However, the literature highlights that consumer protection policies and law have advantages and disadvantages. The next section, therefore, explores the arguments made by Western scholars for and against the adoption of legal consumer protection measures.

---

[231] *Interfoto Picture Library Ltd v Stiletto Visual Programmes Ltd* [1989] QB 433, 439 per Bingham LJ; A.D.M. Forte, *Good Faith in Contract and Property* (Oxford, Hart Publishing 1999) 7.
[232] R.S. Dorfman, 'The Regulation of Fairness and Duty of Good Faith in English Contract Law: A Relational Contract Theory Assessment', The New Jurist, 13 October 2015 <http://newjurist.com/fairness-in-english-contract-law.html> accessed 7 July 2019.
[233] T. Wilhelmsson, 'Various Approaches to Unfair Terms and Their Background Philosophies' (2008) *Juridica International* XIV, 51-57, 54.
[234] Ibid, 55.
[235] Ibid.
[236] R.S. Dorfman, 'The Regulation of Fairness and Duty of Good Faith in English Contract Law: A Relational Contract Theory Assessment' (2013) *Leeds Journal of Law & Criminology* 1(1), 91-116, 92.

3.5 Advantages and problems with legal consumer protection measures and policies

According to the OECD, the main reason for formulating consumer protection policies and in trying to use the law is that this helps to remedy market failures.[237] Circumstances can arise where markets do not create optimal outcomes.[238] Baker and Siegelman emphasise the danger of an unregulated and therefore free capitalistic market, as advocated by neo-liberals.[239] They cite as example of such a danger the insurance market where consumers are offered add-on insurance cover when they purchase services or products. The cover is only for low-value losses. However, an application of utility theory shows that it does not make economic sense to purchase such insurance. A neo-liberal paradigm nonetheless allows insurance companies to charge amounts which are far in excess of the actual cost of insuring against these low-value losses. Similarly, Delgadillo explains that markets are not perfect.[240] There exists insufficient competition, negative externalities and information asymmetries.[241] Soederberg further argues that we live in an era of "cannibalistic capitalism" where social protections from the state have been increasingly eroded.[242] Instead, individual responsibility has been advocated.[243]

One advantage of consumer protection law is that it addresses the tension which has been created by diminishing the exploitation of consumers.[244] Trentman cites as example welfare systems in Scandinavia which have adopted extensive social protections to lessen the impact of social and economic issues.[245] Similarly, Soederberg argues that consumer policy

[237] OECD n 18, 2.
[238] Ibid 3.
[239] Baker and Siegelman n 136, 1.
[240] Delgadillo n 4, 60.
[241] Ibid.
[242] Soederberg n 116. 495&499.
[243] Ibid 499.
[244] Ibid.
[245] F. Trentman, *'Empire of Things: How We Became a World of Consumers, from the Fifteenth Century to the Twenty-First* (Harper 2016) 433.

and consumer protection law help to address the unequal relationship which exists between consumers and businesses.[246] The unequal relationship is particularly apparent when standardised contracts are used, which most likely prejudice the weaker party, namely the consumer, deprive the consumer of the possibility to revise the contractual bargain and allow the professional party to exploit superior information.[247]

The extent to which a level playing field is being created between businesses and consumers depends on whether one subscribes to the social welfare or the neo-liberal paradigm. The researcher would argue that the Sharia requires that the social welfare approach is firmly embedded within the law for the reasons discussed in more detail below. Legal consumer protection measures are needed to supplement the contractual agreement between m-payment providers and customer. Most fundamentally, Saudi law must clearly define the circumstances when m-payment customers should not shoulder financial losses and/or are entitled to compensation or refunds. Saudi law must also ensure that the data of m-payment customers is protected. Consequently, specific statutory provisions and substantive law must be enacted which ensure that overall fairness is being promoted, including through the Islamic good faith principle. The law must prevent that m-payment providers use their stronger bargaining power to exploit customers. The rights and responsibilities of both m-payment providers and customers must be detailed. Additionally, legal procedures must be spelled out for customers to enforce the substantive law.

Ramsay states that the financial crisis in 2008 highlights that the standard policy assumptions about neo-liberal approaches are not necessarily correct.[248] Individuals do not

[246] Soederberg n 116, 494.
[247] P. Nebbia, *Unfair Contract Terms in European Law: A Study in Comparative and EC Law* (Hart Publishing 2007) 34.
[248] I. Ramsay, 'Changing Policy Paradigms of EU Consumer Credit and Debit Regulation.' In D. Leczykiewicz and S. Weatherill (eds), *The Image of the Consumer in EU Law* (Hart 2016) 1.

reach logical decisions when they are provided with adequate information, markets do not correct themselves, and the distribution channels also require oversight.[249] Financial consumer protection policies and law help to increase risk management, promote financial stability and also competitive markets.[250] More oversight is being created and regulatory weaknesses and gaps which may otherwise pose risks to consumers are closed.[251] More accountability is realised as more monitoring is required. Ramsay states that, in the UK, this is particularly visible since the focus has been on realising transparency, formality and accountability, including through codes of conduct.[252] One fundamental advantage of consumer protection policies and laws is that irresponsible market behaviour is combated.[253] In the context of m-payments, legal consumer protection measures can ensure that m-payment providers do not offer high-risk services to consumers.[254] As discussed further below, the Sharia particularly requires adherence to the principle of good faith which further highlights the need for legal consumer protection measures.

In addition, learning and self-reflection by consumers can be encouraged.[255] In the context of m-payments, this means that certain minimum legal obligations should be imposed on consumers. For instance, they may be required to store passwords safely and to install up to date security software. However, this can arguably be achieved through the terms and conditions of m-payment providers and does not necessarily require the law to intervene. Epstein also reasons that the fact that consumers hear about the mistakes from others and also learn from errors means that consumer protection through legal means is superfluous.[256] Such

[249] Ibid.
[250] Financial Stability Board n 118, 3.
[251] Ibid 5.
[252] Ramsay n 32, 32.
[253] Ibid.
[254] Financial Stability Board n 118, 5.
[255] Epstein n 165, 111.
[256] Ibid.

a view is challenged by Bar-Grill, who argues that all depends on the context.[257] Also, there exist certain limits to learning.[258] Certainly, when consumers first use m-payment apps, they may not be familiar with ensuring that their smart devices are adequately secured. Even when they are apt users, they may fall prey to the latest trends in cybercrimes. Legal intervention, therefore, closes possible gaps which may leave customers unprotected. Also, the terms and conditions of companies are likely to contain broad exclusion and limitation clauses. For example, an analysis of Facebook's terms and conditions found that it contained various provisions which contravened consumer protection law in Europe.[259] Facebook's privacy settings also did not meet European requirements concerning consent by data subjects.[260]

Ben-Shahar and Schneider point out that learning and self-reflection by consumers may also be promoted by mandated disclosure.[261] M-payment providers can be required by law to provide information, so that it becomes easier for customers to reach decisions.[262] Even Epstein, who favours a more liberal and market-based approach, acknowledges that information is crucial for consumers to reach informed decisions.[263] Hence, even those who caution against providing consumer protection through legal means concede that some degree of legal prescription is necessary in order to create a level playing field between businesses and consumers.

---

[257] O. Bar-Grill, 'The Behavioral Economics of Consumer Contracts' (2008) *Minnesota Law Review* 92, 749-802, 755.
[258] H. Latin, '"Good" Warnings, Bad Products and Cognitive Limitations (1994) *University of California Law Review* 41, 1193-1295, 1252-1253.
[259] B. Van Alsenoy et al 'From social media service to advertising network, A critical analysis of Facebook's Revised Policies and Terms', 23 February 2015, 1-61, 7 <https://www.law.kuleuven.be/citip/en/news/item/facebooks-revised-policies-and-terms-v1-1.pdf> accessed 10 March 2019.
[260] Ibid.
[261] O. Ben-Shahar and C.E. Schneider, 'The Failure of Mandated Disclosure' (2011), 159(3) *University of Pennsylvania Law Review*, 101-204, 104.
[262] Ibid.
[263] R.A. Epstein, 'The Neoclassical Economics of Consumer Contracts' (2008) *Minnesota Law Review* 92, 803-835, 803.

Put differently, even a reasonably circumspect m-payment customer, as opposed to a vulnerable one, may require at least some degree of legal consumer protection measures in the form of mandated disclosure or the requirement to obtain consent in respect of the collection of consumer data.[264] In the context of m-payments, the average consumer may know about the importance of securing his/her smart device. The standardised terms and conditions provided by m-payment providers must spell out the scope of the mandate, including the instances in which liability rests with the provider or the consumer. However, as pointed out by Ben-Shahar and Schneider, mandated disclosure is often not an effective regulatory technique.[265] Not all information may be provided or consumers may not be able to fully take into account the information.[266] For instance, m-payment customers may be too busy to properly read the terms and conditions.[267] They may not understand the information due to innumeracy and illiteracy or may not be able to fully evaluate or remember it.[268] Accordingly, they may find the information simply too complex.[269]

There will also exist a great information asymmetry in the context of m-payments. It is virtually impossible for m-payment customers to pinpoint and evidence where fault exactly lay when a transaction is not properly executed or funds go missing. Also, mandatory disclosure does not protect m-payment customers adequately against the new technological risks discussed in chapter 2. The main advantage of using more interventionist legal consumer protection measures is therefore that responsibility and risk are not placed unfairly

[264] Bashir et al n 12.
[265] Ben-Shahar and Schneider n 261, 159.
[266] Ibid.
[267] Ibid.
[268] Ibid 164-174.
[269] Ibid 175.

on m-payment customers. It also ensures that sufficiently knowledgeable customers, who are confronted with a difficult and new situation, are better safeguarded.[270]

It is for these reasons advantageous to require m-payment providers to additionally provide assistance to customers, e.g., the necessary security updates in order to help customers safeguard their m-payment apps. Risk management may also be heightened through regulatory oversight and supervision. [271] The threat of punishment in the form of fines by oversight bodies and/or compensation awards or refunds to customers help to create a level playing field between m-payment providers and customers. [272]

Bar-Grill acknowledges that it matters whether there is standardisation.[273] Clearly, in respect of m-payment apps, a standardised service is being provided, and most available information about m-payment apps is relevant for other consumers.[274] However, each m-payment provider may opt for a slightly different interface of the m-payment app. Bar-Grill further calls for consumer protection through legal means since the use patterns vary from consumer to consumer.[275] For instance, one customer may use the m-payment app only for a limited amount of payments, whereas another may frequently use the service. Consumers, Epstein argues, can seek advice[276] (e.g., on how to protect their smartphone from cyber-attacks, including their digital wallets, through the installation of a particular software or cryptographic techniques) but others may solely rely on m-payment providers to provide a secure infrastructure.[277] Imposing legal measures on m-payment providers to protect

[270] Ibid 200-201.
[271] Epstein n 165, 111.
[272] Ibid.
[273] Bar-Grill n 257, 756.
[274] Ibid.
[275] Ibid 757.
[276] Epstein n 263, 813.
[277] Bar-Grill n 257, 757.

customers may incentivise them to educate them.[278] In other words, m-payment providers would have to ensure that their customers do not underestimate the technical and operational risks inherent when using their m-payment services.[279] However, Epstein considers it unrealistic to expect businesses to be responsible for correcting customers' mistakes.[280] Even aside from the impracticalities of such an approach, the cost associated with this additional responsibility would ultimately either deter providers from entering the market or would be passed on to more careful customers.[281]

An advantage of formulating consumer protection policies and laws is that "systematic misperception(s)" by customers can be addressed and that m-payment providers cannot design services which exploit these misperceptions.[282] Put differently, m-payment customers are optimistic about the new services which are being made available to them[283] and may fail to fully appreciate the higher technological and operational risks, discussed in chapter 2. For instance, a study by Gross and Souleles lends support to the claim that consumers display irrational behaviour.[284] Legal consumer protection measures may, therefore, safeguard consumers against otherwise irrational behaviour. Without legal consumer protection measures, m-payment providers may strategically abuse failures by customers (e.g., to secure their mobile devices adequately) in order to escape legal liability for financial losses or other harm (e.g. data protection breaches).[285] In some scenarios, it may be warranted for the law not to hold m-payment providers liable for unauthorised payment transactions, as further explored in chapter 4, section 4.3.3. The advantage of consumer

[278] Ibid 759.
[279] Ibid 760.
[280] Epstein n 165, 120.
[281] Ibid.
[282] Bar-Grill n 257, 761.
[283] Ibid 763.
[284] D.B. Gross and N.S. Souleles, 'Do Liquidity Constraints and Interest Rates Matter for Consumer Behavior? Evidence from Credit Card Data' (2002) *Quarterly Journal of Economics* 117(1), 149-185, 149.
[285] Bar-Grill n 257, 766.

protection through legal means is that risks which arise from the new technologies are not borne unequally only by customers.

Moreover, Warren emphasises that innovative financial products are far more unsafe than tangible goods.[286] The same can be said of m-payment services since the technological and operational risks are much higher than with traditional banking services, as discussed in chapter 2. Warren is therefore in favour of strong consumer protection and advocates that a new regulatory organisation ought to be created for this purpose.[287] Such a body should be entrusted in ensuring that financial products and services are safe.[288] She justifies such a paternalistic approach by stressing that companies devise many different strategies, such as lengthy terms and conditions, in order to avoid being held liable for misconduct.[289] She also points out that there exists insufficient consumer-friendly regulation.[290]

Furthermore, Ramsay states that the finance industry is rather well-organised and can, therefore, exert influence.[291] The risk that consumer interests are not properly protected is heightened.[292] Consequently, an advantage of consumer protection law is that the influence which financial institutions have exercised over time in respect of lawmaking becomes eroded and more balance is achieved.[293] Ramsay notes that this was one of the reasons for the creation of the UK Financial Ombudsman Service.[294] The Financial Ombudsman Service may evoke notions of fairness to determine disputes which individuals have with financial institutions.[295] Another advantage is that consumer protection law can help with building

[286] E. Warren, 'Unsafe at Any Rate' (2007) *Democracy Journal* 5, 1-15, 2.
[287] Ibid.
[288] Ibid 11.
[289] Ibid 5.
[290] Ibid 13.
[291] Ramsay n 32, 8-9.
[292] Ibid.
[293] Ibid 9.
[294] Ibid.
[295] Ibid.

public realisation of the creation of value and positive welfare for people.[296] Economic growth may be promoted since a market must also ensure that consumers are served well.[297]

More importantly, consumer protection law confers rights on m-payment customers. M-payment customers are enabled to seek remedies, e.g., by pursuing court proceedings or through dispute resolution procedures.[298] The decisions by judges can be incorporated in the standardised terms and conditions and can also shape business processes.[299] Yet no consumer protection framework can close all gaps which may leave consumers exposed.[300] The adoption of legal rules can to some extent assist in shielding companies which are already regulated against new competitors.[301] Nonetheless, in the context of m-payment, it is important to licence service providers, even if this creates market barriers for new joiners.[302]

While there are clear advantages, some of the literature also cautions against providing consumer protection through legal means. Proponents of anti-regulation are advocates of free markets and freedom of contract and neo-liberalism.[303] They reject legal consumer protection measures since they interfere with the ideal of freedom of contract and go against liberal market ideas.[304] Hence, it is assumed that issues which may arise can be resolved through market mechanisms. For instance, Durovic and Micklitz argue that consumers do not necessarily have to be protected through legal means since it is possible to self-regulate.[305] Equally, Delgadillo argues that consumer protection can be promoted

[296] Ramsay n 32, 32-33.
[297] Valant n 112, 1.
[298] Delgadillo n 4, 61.
[299] Ramsay n 32, 33.
[300] Paterson and Brody n 53, 340.
[301] Edmonds n 119, 7.
[302] Ibid 8.
[303] Esposito n 158, 211.
[304] Ramsay n 32, 34.
[305] Durovic and Micklitz n 67, 34.

through the adoption of non-binding industry codes.[306] Callies also favours codes of conduct and considers that these can be effective tools to protect consumers.[307] Private regulation by industry sectors can extend beyond regional or national borders.[308] It appears particularly attractive for the increasingly fluid m-payment transactions which can be executed in one corner of the world and reach another almost instantaneously. Durovic and Micklitz stress that private regulation is more flexible because stakeholders can incrementally develop their own codes.[309]

The adoption of voluntary codes of conduct also saves public money since governments do not have to ensure that the law is being complied with.[310] Governments can endorse a code instead of adopting a law.[311] Additionally, consumer advocacy groups can be consulted on those codes and can highlight particular issues.[312] Codes of conduct are certainly a less intrusive form of intervention than compulsory legal provisions.[313] Abbamonte notes that it is easier to change codes of conduct.[314] This makes it possible to quickly react to market developments, whereas lawmaking often takes more time.[315] Self-regulatory bodies may also come to decisions more quickly than courts.[316] Yet, as voluntary codes only apply to members, this can leave consumers exposed.[317] There is also the issue of whether the industry sector would adopt principles and codes of conduct which adequately protect consumer interests.[318] Policymakers must, therefore, assess whether there exist consumer

[306] Delgadillo n 4, 60.
[307] Calliess n 26, 6.
[308] Durovic and Micklitz n 67, 34.
[309] Ibid.
[310] Delgadillo n 4, 60.
[311] Ibid 61.
[312] Ibid.
[313] Ibid.
[314] Abbamonte n 144, 710.
[315] Ibid.
[316] Ibid.
[317] Ibid.
[318] Ibid.

issues which pose a significant detriment to consumers and require government intervention.[319] Protection can be further bolstered through trustmarks.[320] Trustmarks are granted by an independent party for meeting certain technical standards.[321] For instance, m-payment providers can get ISO 31000 risk management certified. Responsible norms of business behaviour can thus be established.[322]

Another reason why some caution against the adoption of social welfare based legal consumer protection measures (i.e. far-reaching consumer rights) is that market pressures can help ensure that consumers receive what they ask.[323] For example, negative publicity in the media about m-payment providers attributing liability to customers for a cyber attack can result in customers switching to competitors. Online reputation can thus perform an important mechanism to prevent unfair behaviour.[324] The internet makes it possible to communicate to a very broad mass through leaving feedback.[325] However, it is doubtful that reputational loss is sufficient in the absence of substantive consumer protection laws which consumers can evoke in their favour.[326] In other words, the leverage of consumers must be strengthened by granting certain legal rights. It is also not necessary to resolve disputes through the courts, which often takes a long time, as a Financial Ombudsman Scheme can be created, as the UK has done.[327] Such a Financial Ombudsman Scheme negates the risk of links to industry (as

[319] OECD n 18, 3.
[320] Calliess n 26, 6.
[321] Ibid.
[322] Ibid 9.
[323] Ramsay n 37, 351-352.
[324] Calliess n 26, 6.
[325] Ibid 4-5.
[326] S. Estreicher and D. Sherwyn, *Alternative Dispute Resolution in the Employment Arena: Proceedings of the New York University 53rd Annual Conference on Labor* (Kluwer Law International 2004) 112.
[327] P. Cartwright, *Banks, Consumers and Regulation* (Hart Publishing 2004) 175.

the state guarantees the impartiality of the Ombudsman) while preserving the benefits of efficiency.[328]

As the m-payment industry is still developing, policymakers should seriously consider whether they want to opt for comprehensive legal consumer protection measures in line with the social welfare approach. A light-touch approach through government-approved codes of conduct, certification standards, statutory and regulatory requirements, technical standards, together with certain basic default rights for consumers may prove to be a more flexible approach.[329] It may help to encourage Fintech innovation[330] which in turn is likely to increase consumer choice. However, the trade-off is that overall fairness may not be prioritised as much as business interests. It is argued that as consumer's finances are concerned, great care must be taken. A robust legal framework must be enacted to safeguard m-payment customers. The question arises whether Sharia law would also require far-reaching legal consumer protection measures. The next section, therefore, explores the aims/objectives of consumer protection as advocated by Islamic law, including Islamic banking law. Problems or advantages of formulating consumer protection policies based on the Sharia and in trying to use Sharia law to achieve those objectives are identified. Gaps within the Sharia legal literature are highlighted.

[328] G. Howells and I. Ramsay, *Handbook of Research on International Consumer Law* (2nd ed, Edward Elgar 2018) 431.
[329] E. Stokes, 'Double Movements in the Regulation of New Technologies: The Case of Nanotechnology'. In B. Lange et al (eds), *Regulatory Transformations: Rethinking Economy-Society Interactions* (Hart Publishing 2015) 213.
[330] Ibid.

3.6 Safeguarding customers through Sharia law

All major religions spell out moral and ethical values and, in the past, the law was also interwoven with religious principles.[331] In the case of Islam, this is still the case to this present day. [332] Islam is based on the Quran, as well as the *Sunnah*.[333] While the Quran is the primary source, the *Sunnah* is essential because it is 'a set of rules deduced from the pronouncement and conduct of the Prophet'.[334] Where the Quran deals with a particular situation, it takes precedence over the *Sunnah*.[335] There are also the following secondary sources: Firstly, *Ijtihad,* which can be translated as logically reaching one's own opinion by interpreting the Quran, i.e., "progressive reasoning by analogy". Secondly, *Ijma,* which denotes the generally agreed opinion of learned persons, i.e., "consensus". Thirdly, *Qijas,* which means a comparison when things are similar, i.e., "analogy".[336] These diverse sources validate different eclectic interpretations but result in Sharia concepts not being universally ascertainable.[337] This issue is further heightened by the fact that different schools of thought advocate for the implementation of different equivocal Sharia standards.[338] In SA, Sharia principles are based on the Hanbali School.[339]

---

[331] Morris and Al Dabbagh n 15, 2.
[332] Ibid.
[333] B. Kettell, *Introduction to Islamic Banking and Finance* (John Wiley & Sons 2011) 20.
[334] D.J. Karl, 'Islamic Law in Saudi Arabia: What Foreign Attorneys Should Know' (1991) *The George Washington Journal of International Law and Economics* 25(1), 131-170, 138; A.K. Aldohni, *The Legal and Regulatory Aspects of Islamic Banking: A Comparative Look at the United Kingdom and Malaysia* (Routledge 2011) 30.
[335] H.M. Ramadan, *Understanding Islamic Law: From Classical to Contemporary* (Rowman & Littlefield Publishers Inc 2006) 28.
[336] Kettell n 333, 20-21; cited from D. Jonsson, *Islamic Economics and the Final Jihad, The Muslim Brotherhood to the Leftist/Marxist - Islamist Alliance* (Xulon Press 2006) 559.
[337] M.S. Malik and W. Mustafa, 'Controversies that make Islamic banking controversial: An analysis of issues and challenges' (2011) *American Journal of Social and Management Issues* 2(1), 41-46, 42.
[338] R. Wilson, *Legal, Regulatory and Governance Issues in Islamic Finance* (Edinburgh University Press Ltd 2012) 1996; S. Tahir, 'Current Issues in the Practice of Islamic Banking, International Institute of Islamic Economics of the International Islamic University', Islamabad, 2003, 1-8, 2. <http://www.sbp.org.pk/departments/ibd/Lecture_8_Related_Reading_1.pdf> accessed 5 October 2014.
[339] S. Zuhur, *Saudi Arabia* (ABC-CLIO LLC 2011) 176.

The Hanbali School values doctrinal purity by interpreting the Quran literally, resulting in it being the strictest of the four main Sunni Schools.[340] More weight is given to firstly the Quran and after that the Sunnah, *Ijma* of the companions of the Prophet, individual opinions by companions of the Prophet, weak *Hadiths,* i.e. actions, words and unspoken approval by the Prophet and *Qiyas*, i.e. deductive analogy.[341] It is essential for Islamic jurists to recognise that consumer protection constitutes an area where *Qiyas* must be liberally used. One way is to view consumer protection as falling within the commercial sphere and an extension of Islamic business values. Such an approach would ensure that consumer protection is interpreted liberally. The reason is that the Hanbali School is only "strict in …personal morality and criminal law" but is otherwise "liberal on economic and business issues."[342] However, as discussed above, a purely liberal policy orientation may not necessarily adequately protect m-payment customers.

Put differently, an overly liberal approach towards commercial matters appears to fundamentally contravene the primary objective of Islamic law, namely that wealth creation promotes unity within society through high business standards.[343] Islam also commands that every person considers how his/her behaviour impacts others, including when wealth is created.[344] Accordingly, the welfare of society is more important than individual welfare.[345] In the context of m-payment, this should mean that m-payment providers cannot prioritise their welfare over those of their customers and must, therefore, safeguard customers against unauthorised payment transactions and protect customers' data. As explained by Albaqme, the prime aim of the Sharia is to guarantee the rights of individuals and to ensure that society

[340] R. Wilson, *Legal, Regulatory and Governance Issues in Islamic Finance* (Edinburgh University Press 2012) 31.
[341] Ramadan n 335.
[342] A. Al Rajhi et al, *Economic Development in Saudi Arabia* (Routledge Curzon 2004) 14.
[343] Abdalati n 16, 10.
[344] H. Ayob, 'Consumer Protection in Islam: An Overview' (2014) *Malaysian Journal of Consumer and Family Economics*, 1-10, 2.
[345] Ibid.

is united.[346] Consumer protection is and should, therefore, be a central and indispensable element of any Islamic legal system. As the Sharia governs all aspects of life[347], it must also extend to consumer protection.

However, at present Islamic consumer protection is primarily achieved through morals and values which apply to commerce.[348] Mannan opines that those parts of the Quran which deal with economics emphasise that social aspects must be incorporated.[349] Honesty, transparency, being considerate, offering high-quality products and discharging the respective obligations under an agreement, including any specific rules which apply to it, constitute some of these important business values.[350] Various Quranic verses stress that Allah requires adherence to the duties to transact fairly and honestly.[351] For instance, Surah Al-Rahman 55:9 provides that "And establish weight in justice and do not make deficient the balance."[352] Surah Al-lsra' 17:35 states "And give full measure when you measure, and weigh with an even balance. That is the best [way] and best in result."[353]

These ethical commands are very similar to the Western social welfare consumer construct discussed above. Social justice thus plays a prime role within Islam, as made clear by the Quran which states that the objective is 'establishing what is right and forbidding what is wrong'.[354] However, one notable distinction to the Western social welfare approach is that Islam achieves this not through the grant of rights, but through the imposition of duties, as

[346] Albaqme n 17, 170.
[347] B. Warner, *Sharia Law for Non-Muslims* (Center for the Study of Political Islam 2010) 6.
[348] Albaqme n 17, 170.
[349] M.A. Mannan, *Islamic Economics: Theory and Practice* (Hodder and Stoughton 1986) 15.
[350] Ibid.
[351] E. Abu Bakar and N. Amin, 'Consumer Protection under Islamic Law in the Service Industry' (2011) *International Journal of Social Policy and Society* 8, 37-49, 38.
[352] Sahih International <https://quran.com/55/9> accessed 10 February 2019.
[353] Sahih International <https://quran.com/17/35> accessed 10 February 2019.
[354] Quran 3:103, 109, 113; 9:71, 22:41; 31:17; cited from M. A. Khan, 'The Role of Islamic State in Consumer Protection' (2011) *Pakistan Journal of Islamic Research* 8, 31-44, 31.

observed by Rice.[355] In contrast, in the UK various legal rights have been granted through the imposition of contractual liability for breach of a term of contract, tortious liability, implied terms (such as a statutory duty of reasonable care and skill[356]), legislation regulating unfair contract terms, as well as sector-specific legislation, such as the PSR 2009 and PSR 2017, which thereby comprehensively embed the consumer protection rationale, and as explored in chapter 4, sections 4.3 and 4.4.

In contrast, as explicated by Ayob, Islamic consumer needs are addressed through the *aqad* (the legal relationship) relating to a transaction and trading. [357] In other words, consumer needs can be made part of the contractual obligations which the parties determine, as the "The Contract is the Law of the Parties."[358] However, it also permits companies to utilise exclusion and limitation clauses by making them part of the legal relationship, subject to the caveat that they are clearly defined, do not contravene the *good faith* principle and the matter can also not be *haram* as discussed below.[359] Additionally, consumer needs are addressed through ethical and moral principles and spiritual matters.[360] Spiritual matters concern the relationship between Allah and consumers, whereas ethical and moral matters concern the relationship between the trader and the consumer. It is assumed that this ensures that rights are automatically guaranteed.[361]

Nonetheless, one issue with such an approach premised on ethical and moral principles and spiritual matters is that it creates vagueness and legal uncertainty. Countries,

[355] G. Rice, 'Islamic ethics and the implications for business' (1999) *Journal of Business Ethics* 18, 345-358, 345.
[356] See Consumer Rights Act 2015, s49.
[357] Ayob n 344, 1.
[358] Saudilegal, '2. Islamic Contract Law', 2018 <http://www.saudilegal.com/saudilaw/02_law.html> accessed 15 February 2019.
[359] Ibid.
[360] Ayob n 344, 1.
[361] Rice n 355, 345.

such as SA have recognised this issue and have started to "codify Sharia 'for clarity."[362] However, such reform has only progressed slowly and has not extended to consumer law.[363] The failure to take legal steps to protect consumers is also reflective of the fact that the topic of consumer protection has not received much attention in Islamic societies.[364] By default, neo-liberal contractual primacy has thus been permitted due to the failure to clearly and comprehensively specify and develop the ethical, moral and spiritual principles on which consumers can rely.

One serious issue with such an approach is that it causes problems in respect of the enforcement of consumer rights. In the absence of clearly formulated consumer rights, as opposed to broad and vague principle containing social justice concepts, it arguably falls on the state to ensure that businesses discharge their Islamic holy duties. By corollary, this necessitates that the necessary state bodies and institutions are created to monitor compliance with Islamic business morals and values. Nonetheless, this alone is insufficient to ensure that individual cases are properly dealt with. Without knowledge of wrongdoing in a particular case, e.g., through the consumer's right to complain, it is difficult to see how an Islamic duty can be enforced in specific cases. In this context, Radwan states that Sharia law is insufficient without consumers being sufficiently aware.[365] It is thus imperative for Islamic scholars to develop the concept of consumer rights in order to rein in contractual primacy.

[362] C. Murphy, 'Saudi to codify Sharia 'for clarity', The National, 21 July 2010 <https://www.thenational.ae/world/mena/saudi-to-codify-sharia-for-clarity-1.518063> accessed 10 February 2019.
[363] Ibid.
[364] Morris and Al Dabbagh n 15, 2.
[365] S. Radwan, 'Islamic Banking: Why Transparency Matters', International Sharia Research Academy for Islamic Finance, Wahed, 14 June 2017 <https://journal.wahedinvest.com/islamic-banking-why-transparency-matters/> accessed 1 September 2017.

Duties create rights and rights create duties[366], and there is a gap within the Islamic literature on consumer rights, as such rights are not being clearly articulated within Islamic law at present. As a result, companies are given more leeway on how to draft their terms and conditions. They do not have to ensure that specific consumer rights are upheld, as is, for example, the case in the UK, as discussed in chapter 4, sections 4.3 and 4.4. A more liberal market approach is thereby facilitated, but this appears to contravene the social welfare approach which Islam otherwise commands. It is thus more appropriate to speak of Islamic consumer protection through business regulation. As explained by Mancuso, Prophet Mohammed was a merchant, and he, therefore, spelt out specific prescriptions.[367] Islamic scholars should nevertheless deliberate what the consequences are when these specific prescriptions are not met towards consumers. Put differently; it must be addressed whether a failure to meet a specific Islamic business obligation entitles a customer to bring a legal claim.

Yet one obstacle may be that conservative Hanbali scholars view these as holy duties which can only be interpreted narrowly.[368] For this reason, it may be difficult to apply them to particular commercial transactions, including m-payment services.[369] As suggested above, this problem may be overcome by considering consumer protection a commercial matter and treating it in a liberal and not doctrinally pure manner. That is to say, the concept of *qiyas* could be utilised to overcome such an issue, particularly in light of the rich Islamic jurisprudence on social justice, as, e.g. found in the aforementioned Quranic verses, Surah Al-Rahman 55:9 and Surah Al-lsra' 17:35. Arguably any other approach fundamentally

[366] W. Newcomb Hohfeld, 'Some Fundamental Legal Conceptions as Applied in Judicial Reasoning' (1913) *Yale Law Journal* 23(1), 16-59.
[367] S. Mancuso, 'Consumer Protection in E-Commerce Transactions: A First Comparison between European Law and Islamic Law' (2007) *Journal of International Commercial Law and Technology* 2(1), 1-8, 4.
[368] Ibid.
[369] Ibid.

contravenes the equity, fairness and justice commands of the Sharia and thereby frustrates the primary goal of Islam.[370]

Such a progressive approach is also necessary since contemporary society is very different from the times when Prophet Mohammed lived. Consequently, it is important that Islamic scholars apply these holy prescriptions liberally. They must also not uphold pre-Islamic Arab tribal customs at the expense of the holy commands of the Sharia.[371] They should, therefore, abandon rigidity, focus on core values and the essence contained in the holy text.[372] Undoubtedly, the Islamic social justice principles can serve as an immensely helpful ethical base from which a jurisprudential discourse about consumer rights can be developed. Mancuso further states that there are many Quranic verses which emphasise that individuals must be protected, especially against undue interference. [373] Islamic scholars must thus focus on these verses in order to interpret them in relation to the consumer protection specific context, including m-payment transactions.

This particularly requires that important Islamic business principles are elaborated on in respect of the different consumer protection areas where they may be relevant:[374] One such principle is that sellers and buyers ought to be allowed to trade freely.[375] Another Islamic business principle imposes a duty on agents and brokers to offer assistance to sellers and buyers, so that a fair bargain can be reached.[376] Ignorance can also not be exploited by

---

[370] M.M. Keshavjee, *Islam, Sharia and Alternative Dispute Resolution: Mechanisms for Legal Redress in the Muslim Community* (I.B. Tauris & Co Ltd 2013) 78.
[371] H. Esmaeili, 'On a Slow Boat Towards the Rule of Law: The Nature of Law in the Saudi Arabian Legal System' (2009) *Arizona Journal of International & Comparative Law* 26(1), 1-47, 16.
[372] S. Akbarzadeh and B. MacQueen, 'Framing the debate on Islam and human rights', in Islam and Human Rights in *Practice: Perspectives across the Ummah* (Taylor & Francis 2008) 3.
[373] Mancuso n 367, 6.
[374] M. Akbar Khan, 'Consumer Protection and the Islamic Law of Contract' (2011) *Islamabad Law Review* 2(2), 62-73, 73; Morris and Al Dabbagh n 15, 4-5; A.H. Siddiqi, *Sahih Muslim, Volume III, Book IX* (Jeddah, undated) 799; M.M. Khan, *Sahih Al Bukhair* (Dar Al Arabi 1985) 191.
[375] Ibid (Akbar Khan).
[376] Ibid.

principals.[377] In the context of m-payments, this could be interpreted as requiring other stakeholders in the m-payment transaction network to support each other in such a way that customers are treated fairly. Hence, the operations must be managed effectively, so that customers are not left exposed to additional risks. The principle could thus be used as a base to impose a duty on the various stakeholders involved in m-payment services to be a good manager by facilitating that electronic financial transactions are safely processed, as, e.g. South Korea has done.[378] Additionally, the principle could be evoked to allow customers to notify any party within the m-payment ecosystem when they lose or have their mobile device stolen.[379] This would be a more helpful approach to customers.

Another Islamic business principle provides that a creditor who recovers money from a debtor must duly consider the debtor's financial circumstances.[380] However, when goods have not been paid for, the seller is entitled to them.[381] In the context of m-payment, this could be interpreted as the court having to determine whether the m-payment customer should shoulder responsibility for a specific cyber attack. The caveat that a seller is entitled to unpaid goods could be interpreted as meaning that a m-payment provider is entitled not to pay back its customer when the customer has not fulfilled his/her respective duties under the agreement.

Another Islamic principle is the requirement for goods not to harm individuals.[382] Goods should be extended to services by analogical reasoning in light of the overall aims of Islam, including m-payments. Another important Islamic duty in the context of consumer

[377] Ibid.
[378] South Korea's Electronic Financial Transaction Act No. 11087, Article 21(1).
[379] Also see, South Korea's Electronic Financial Transaction Act No. 11087. Articles 10(1) and 11(3).
[380] Akbar Khan n 374.
[381] Ibid.
[382] Morris and Al Dabbagh n 15, 5.

protection is the requirement to conduct business fairly and to protect consumers. [383] Moreover, when Islamic law is not adhered to, a transaction is unenforceable.[384] However, in the context of unauthorised payment transactions and customers' data breaches, a different remedial response must be developed than rendering a transaction unenforceable, e.g. they must be refunded the unauthorised amount and/or compensated for the data breach if sufficiently serious.

While some Islamic scholars may aver that Islamic principles cannot be changed, as pointed out by Albaqme, this does not appear necessary.[385] As suggested above, *qiyas* can be employed, so that the Islamic principles remain intact, but are just interpreted so that current issues can be solved.[386] Albaqme also does not consider that this constitutes a problem[387] and Islamic scholars ought to work on ensuring that the application of these Sharia principles are fully understood in respect of modern day consumer law affairs. One way to facilitate this is for SA to enact secular consumer laws, just like it has done in respect of commercial laws.[388]

The adoption of consumer laws would also resolve the issue that at present the precise scope of the protection of consumers within Islamic law has not been further explored. Albaqme stresses that Muslim customers are normally unaware of the Islamic verses which may relate and be applicable to customer protection.[389] Morris and Al Dabbagh confirm that this is because the topic of consumer protection has received very little attention in Muslim countries, including in SA.[390] However, consumer protection will remain inefficient, even if a

[383] R.A.K. Habib, 'Consumer Policy in Less Developed Countries: A Saudi Arabian Context, PhD Thesis, University of Glasgow, 1988, 232-234.
[384] Albaqme n 17, 171.
[385] Ibid, 170.
[386] Ibid.
[387] Ibid.
[388] Morris and Al Dabbagh n 15, 2.
[389] Albaqme n 17, 173.
[390] Morris and Al Dabbagh n 15, 2.

consumer law was enacted, without an academic discourse by Islamic scholars.[391] The main reason why consumer protection will not be effective without promulgating Islamic consumer protection jurisprudence is that the Sharia is supreme over civil law.[392] Put differently, even if a statute was enacted, its provisions could be overridden on the basis that there is a conflict with the Sharia. However, there exist Islamic principles which have received more attention, as the principles mentioned above and which can serve as important tools to the Islamic social justice command and from which an Islamic customer protection discourse can be developed. These principles are discussed next.

3.6.1 The Islamic principle of good faith

A particularly important Islamic business principle is that of good faith,[393] as it forms the base of Islamic contract law jurisprudence.[394] In Islam, the concept of good faith requires being sincere, straightforward, just, fair, truthful, transparent and requires each party to honour promises.[395] Islamic scholars have defined good faith in different ways, for instance, as decency, communal standards concerning fairness or reasonableness.[396] The good faith principle is important in respect of unauthorised payment transactions by m-payment providers to their customers since it can help to delineate the extent to which Sharia law will impose or permit the exclusion of liability. It also provides a point of comparison on

[391] Albaqme n 17, 175.
[392] Basic Law of Governance 1992, Article 7.
[393] N.H.D. Foster, 'Islamic Commercial Law: An Overview (II)' (2007) *InDret: revista per a analisi del dret* 1, 405-425, 428.
[394] A. Borroni and C. Tabor, 'Caveat Emptor's Current Role in Louisiana and Islamic Law: Worlds Apart yet Surprisingly Close' (2009) *Journal of Civil Law Studies* 2(1), 61-100, 71.
[395] S.B. Choi et al, 'Towards A Better Understanding of Good Faith Concept in Islamic Contract Law' (2018) *International Journal of Engineering & Technology* 7(4), 247-253, 247.
[396] A. Zahid et al, 'Good faith in international commercial contracts under un sale convention and Islamic law: A brief comparison' (2016) *International Journal of Applied Business and Economic Research* 14(13), 9075-9183, 9075.

unauthorised m-payments with English law, particularly with the CRA 2015 and the test of fairness and treatment of exclusion of liability, discussed in chapter 4, section 4.4.

The Islamic good faith principle requires both parties to a transaction to be honest and truthful i.e. corporate and private individuals must abide by the principle.[397] In the context of m-payment, the Islamic good faith principle could be utilised to impose a duty on the m-payment provider and third parties and the customer to act in good faith and to cooperate. For instance, m-payment customers must keep their PIN codes safe and must be honest when they have failed to keep them safe. Equally, m-payment service providers must admit when they have failed to provide a secure m-payment infrastructure or third-party collaborators are to blame.

The rule that transactions should be conducted justly and honestly is evident for instance from Surah Al-Bayyinah 98:5; Surah Al-Baqarah 2:188; Surah Al-Anam 6:152, Surah Al-Mutaffifin 83:1-5, Surah Al Baqarah 2:177; Surah Al-Isra' 17:35; Surah Al-Isra 17:34, Surah Al-Baqarah 2:190; Surah Al-Mu'minun 23:8 and Surah Al-Humazah 104:1-4.[398] The requirement that business transactions are fair[399], is also apparent from the following Quranic verse: 'Who to those who deal in fraud, those who, when they have to receive by measure from men, exact full measure, but when they have to give measure or weight to men give less than due. Do they not think that they will be called to account on a mighty day, a day when (all) mankind will stand before the Lord of the Worlds?'[400] Another Quranic verse which requires that transactions are fair is found in Surah An-Nisa 4:29 and which states "O

[397] Akbar Khan n 374, 62; Choi et al n 395.
[398] Abu Bakar and Amin n 351, 38; Choi et al n 395.
[399] Morris and Al Dabbagh n 15, 4.
[400] Quran, Surah al-Mutaffifin, 83: verses1-6; Al-Ali, *The Meaning of the Glorious Quran* (Jeddah, Islamic Books 1934) 42.

ye who believe! Eat not up your property among yourselves in vanities: But let there be amongst you Traffic and trade by mutual good will."[401]

There are many other Quranic verses which command fair and honest dealings, such as Surat Al-Baqarah 2:224-25, and Surat Al-Ma'idah 5:89.[402] It has been said that the Prophet declared that a trustworthy and truthful merchant will join the Prophets.[403] Fundamentally, Islam emphasises fairness and considers the contract divine in accordance with Surah Al-Ma'idah 5:1.[404] It thus strikes a balance between social welfare interests and neo-liberal tenets, similar to the position in the West discussed in section 3.4. The Islamic requirement for the deal to be fair appears different to the Western concept which permits freedom of contract. [405] However, as discussed in chapter 4, sections 4.3.1 and 4.4, fairness rules have also been developed in the West to protect consumers against oppressive and sharp practices which arise as a result of unequal bargaining power, most notably the CRA 2015.[406] Also, the Islamic dogma of the contract being divine means that in Islamic legal culture, the Western concept of *pacta sunt servanda* is firmly recognised.[407] It means that in Islam, contracts, including all contractual duties, are upheld so long as the Sharia or a Sharia public policy is not contravened.[408] In this context, Ibn Taymiya, a Hanbali jurist, observed that any contractual clauses are permitted if valid and not forbidden or deemed forbidden because of *qiyas* or a text.[409]

When determining what is a valid and forbidden exclusion of liability in the context of the good faith principle, it is important to understand that it relates to three areas: The

[401] The Holy Quran 4:29.
[402] Foster n 393, 429.
[403] Ibid.
[404] Borroni and Tabor n 394, 69.
[405] W. Fikentscher, *Modes of Thought: A Study in the Anthropology of Law and Religion* (2nd ed, Mohr Siebeck 2004) 42.
[406] J. Goldring et al, *Consumer Protection Law* (5th ed, The Federation Press 1998) 32.
[407] A. Atilgan, *Global Constitutionalism: A Socio-legal Perspective* (Springer 2018) 265.
[408] Borroni and Tabor n 394, 70.
[409] C. Mallat, 'Commercial Law in the Middle East: Between Classical Transactions and Modern Business' (2000) *American Journal of Comparative Law* 48(1), 81-141, 91.

contracting parties, the goods and the value of the goods.[410] By virtue of *qiyas,* this must also extent to services, particularly in an age where service technologies, such as NFC discussed in chapter 1, play an essential part within today's knowledge economy.[411]

For instance, in respect of the contracting parties, the principle requires that there is mutual consent which has been freely given.[412] The seller is not permitted to lie, should be kind, prioritise justice, not engage in speculation or interfere in another person's contract or resell goods before receipt.[413] Furthermore, Uqba bin Amir, a companion of the Prophet, noted that a thing can also not be sold which is defective or has issues, except if the buyer was informed of it.[414] Hence, the seller cannot hide any defects.[415] This highlights that the Western concept of mandated disclosure (i.e., providing intelligible information to consumers) can be said to exist in Islam. This is further supported by the Quran, verse 33:70 which states '...make your utterance straightforward'.

Accordingly, the principle of good faith extends to the pre-contractual stage where bargaining or talks take place.[416] In the m-payment context, it may be important to require that prospective customers are informed about the key security features, e.g. which in-app protection against unauthorised transactions and malware form part of the service. Such an initiative has been proposed by the Islamic Malaysian Central Bank, Bank Negara.[417] The way in which personal data is being dealt with should also be clearly stipulated. The rule not to sell a thing which is defective also arguably necessitates that m-payment providers only offer services to customers when, in all honesty and good faith, they know that customers'

[410] Choi et al n 395, 250.
[411] E. G. Popkova et al, *Industry 4.0: Industrial Revolution of the 21st Century* (Springer 2019) 61.
[412] Choi et al n 395; Surah An-Nisa 4:29.
[413] Ibid (Choi et al) 251-252.
[414] Foster n 393, 429.
[415] Choi et al n 395, 251-252.
[416] D. Elkarkouri, 'Pre-Contractual Liability in Islamic Construction Contracts' (1992) *International Construction Law Review* 4, 544-551, 545-546.
[417] J. Chin, 'Bank Negara plans minimum standards for mobile payments, more safeguards', The StarOnline, 12 April 2018 <https://www.thestar.com.my/business/business-news/2018/04/12/bank-negara-plans-minimum-standards-mobile-payments-more-safeguards/> accessed 13 February 2019.

funds and their personal details will be safe. This facet of the Islamic good faith principle, if properly developed, has the potential to encourage them to adopt the latest technology and operational processes and comply with their obligation to maintain secure systems.

In respect of goods, it is not allowed to trade in things which are deemed unlawful, e.g. pork.[418] Accordingly, it must be considered whether something is *halal* or *haram*, as discussed in the next section. Moreover, the quantity and any characteristics of the item must be clear.[419] In this context, uncertainty or excessive risk i.e. trickery must be avoided.[420] In relation to the value of the goods, the price must be clearly stated.[421] Payment must also not be delayed.[422]

A breach of the Islamic good faith principle entitles a buyer to return goods when s/he notices a defect (i.e. anything which decreases its value), though s/he can opt to keep the goods (though without seeking compensation).[423] Even when a buyer was not ignorant and knew about the defect, s/he can choose to rescind the contract or affirm it.[424] Sellers must thus give refunds for defective products.[425] Such a rule appears similar to the implied terms contained in the UK Sale of Goods Act 1979, the Supply of Goods and Services Act 1982 and the Consumer Rights Act 2015, mentioned in chapter 4, section 4.3. Through the application of *qiyas* (analogy), the same principle arguably also applies to defective services. Accordingly, when a defect is not revealed, the contract is unenforceable under Islamic

[418] Choi et al n 395, 252.
[419] Ibid.
[420] Ibid.
[421] Ibid.
[422] Ibid.
[423] Borroni and Tabor n 394, 75.
[424] Ibid.
[425] Ibid.

law.[426] The fact that an exemption clause has been inserted in the agreement does not change this, so long as the consumer establishes that the defect was known, but not disclosed.[427]

The consumer protection rationale clearly underlies this Islamic rule, and which has the potential to fulfil a similar protective role as, e.g. the tortious duty of care and the UK CRA 2015 do, as discussed in chapter 4, section 4.4. While at first sight it appears that there is a disconnect between Islamic and Western contract law, this is not necessarily the case.

Similarly, when there is dishonesty, the deceived party can revoke the contract and thereby bring it to an end.[428] Hence, the contract is unenforceable when either one of the parties engages in fraud or misstatements.[429] Accordingly, liability cannot be excluded for these matters. This fundamental rule not to deceive but to be honest governs all business transactions, as proclaimed by Prophet Mohammed (peace be upon him).[430] Yet deception can take many different forms and there are also different standards of honesty. A business may choose to disclose basic information about its services but may not detail everything. Important information may be provided but in such a form that most consumers will not read it. This is arguably the case when m-payment customers are provided with very lengthy terms and conditions. While some may consider that this is a weak form of deception, this has become a standard practice around the world.

The various aspects of the Islamic good faith principle highlight that it is a well-developed Islamic business principle which promotes fairness. It should ideally be utilised to address to what extent Sharia law will impose or permit the exclusion of liability of m-

[426] Akbar Khan n 374, 73.
[427] Ibid.
[428] Ibid.
[429] A. Husain, 'Contract in Islamic Commercial and Their Application in Modern Islamic Financial System', Global Islamic Finance, 30 September 2008 <http://www.global-islamic-finance.com/2008/09/contract-in-islamic-commercial-and.html> accessed 23 September 2017.
[430] Hadith 12 states: Whosoever deceives is not one of us.

payment providers in the context of unauthorised payment transactions and data utilisation and data

breaches. It would be desirable for Islamic jurists to promulgate a consumer protection discourse based on it, alongside the broader command for wealth to create social unity, as well as other relevant business principles, such as the *halal* and *haram* concepts discussed in the next section.

3.6.2 The *halal* and *haram* concepts

Consumer protection is also indirectly promoted through the Sharia outlawing sinful activities, such as, alcohol, gambling, and anything related to pornography.[431] The *halal* concept proscribes unethical business methods, such as, high risk activities, fraud and deception, as well as those which are considered socially harmful and thus sinful.[432] Such activities are examples of what is termed *haram*.[433] Hence, *haram* denotes unacceptable Islamic activities, whereas *halal* denotes acceptable practices.[434] In other words, goodness must govern business activity in the spirit of God and the legal framework must enact values which promote this.[435] Justice, honesty and public interest are such values, whereas malpractices must be prevented, e.g. greed, fraud and speculation.[436] Those economic activities which exemplify positive values are permitted i.e. *halal* and those which are negative are proscribed i.e. *haram*. The *halal* and *haram* concepts could be utilised as a legal

[431] M.F. Khan and M. Porzio, *Islamic Banking and Finance in the European Union: A Challenge* (Edward Elgar Publishing Ltd 2010) 136; Kettell n 333, 22.
[432] Ibid (Khan and Porzio).
[433] K. Hassan and M. Mahlknecht, *Islamic Capital Markets: Products and Strategies* (John Wiley & Sons Ltd 2011) 176.
[434] A.M. Venardos, *Islamic Banking and Finance in South-East Asia: Its Development and Future* (3rd edn, World Scientific Publishing Co Pte Ltd 2012) 157.
[435] M.K. Lewis et al, *Risk and Regulation of Islamic Banking* (Edward Elgar 2014) 67.
[436] Ibid.

balancing tool to determine situations where the acceptable Islamic ethical business values have become transgressed.

The concepts are particularly useful when determining whether a payment transaction is authorised or unauthorised. For instance, m-payment services can only be offered to customers if they are not high risk and fraud and deception are adequately combated. Hence, the risks detailed in Chapter 2 which contribute to unauthorised payment transactions and data breaches must be adequately mitigated for the service not to become *haram*. If a m-payment service is found to be too risky and exposes customers to fraud (e.g., because of inadequate risk management), liability should not rest with consumers. The concepts of *halal* and *haram* could also be used to declare unenforceable terms and conditions in m-payment service agreements, e.g. which leave too much risk to customers.[437] Such terms and conditions would then become *haram* and would no longer be deemed *halal*, despite the fact that *prima facie* m-payments should be deemed *halal*.

As mentioned above, Islam emphasises the importance of benefiting the wider society.[438] Aldohni therefore argues that, while parties can freely agree to their respective rights and obligations, this has to be done constructively within the parameters of Islamic law, including the good faith principle and the *halal* and *haram* concepts.[439] This also highlights that Islamic law requires that welfare considerations are upheld. It therefore resembles in some aspects the more paternalistic and interventionist approach advocated by some Western scholars, as discussed above. Hence, despite the different heritage of English and Sharia law, these principles share similar policy considerations. However, one gap within the Islamic consumer protection literature is to spell out whether a finding of *haram*, as well

[437] *Abdullah Girgi Beserani v Ismale Fawzi Abu Khadra* (1996) Board of Grievance, Case No. 2195.
[438] Aldohni n 334, 88-89.
[439] Ibid.

as any other contravention of the ethical and moral Islamic business rules, will prevent the operation of exclusion clauses. The remedial consequences which flow from a breach of the Islamic business rules have also not been sufficiently clarified, leaving customers exposed.

3.6.3 The Islamic profit and loss sharing principle

Another important Islamic banking principle is the profit and loss sharing principle.[440] Under the principle, profits can not be determined and are thus variable and vague and may even not eventuate.[441] The underlying requirement is to employ money productively and to share the rewards which come from wealth, as well as the risk.[442] It originates from the idea that the weak party needs to be protected.[443] In the context of m-payments, the weak party is the consumer. It is, therefore, a principle which promotes fairness. While it is normally applied in the context of sharing business risks and profits,[444] it could serve as a basis for an Islamic consumer protection jurisprudence. Quranic verse 2:275 from which this principle has been developed[445] states "Allah hath permitted business and forbidden usury." Under the principle, profits cannot be reaped from financial products and services without the beneficiary also facing potential loss.[446] The risks which stem from customers' activities should therefore not be separated from m-payment providers and third-party collaborators. In other words, the m-payment provider and third-party collaborators which benefit from m-payment services

[440] J.A. DiVanna, *Understanding Islamic Banking, The Value Proposition That Transcends Cultures* (Leonardo and Francis Press Ltd 2006) 2.
[441] Md. T. Islam, 'The Theological Foundations of Islamic Banking: A Critical Review'. In M. Zulkhibri and T. A.A. Manap (eds), *Islamic Finance, Risk-sharing and Macroeconomic Stability* (Springer 2019) 50.
[442] Ibid.
[443] C. Porzio, 'Islamic banking versus conventional banking'. In M.F. Khan and M. Porzio (eds), 'Islamic Banking and Finance in the European Union, A Challenge (Edward Elgar 2010) 91.
[444] A.H. Gait and A.C. Worthington, 'A Primer on Islamic Finance: Definitions, Sources, Principles and Methods' University of Wollongong, School of Accounting and Finance, Working Paper Series, No. 07/05, 1-27, 12.
[445] H.T. Ahsanullah, *Turning Point: Breaking the Shackles of Dependant Thinking a Personal Journey in Discovering God and Myself* (Authorhouse 2013) Chapter 7.
[446] Md. T. Islam, 'The Theological Foundations of Islamic Banking: A Critical Review'. In M. Zulkhibri and T.A.A. Manap (eds), *Islamic Finance, Risk-sharing and Macroeconomic Stability* (Springer 2019) 50.

should not be allowed to exclude all liability at the expense of the customer. The customer may also be held liable for losses. Consequently, each party to a m-payment transaction must share the risk under the profit and loss sharing principle[447], ideally the risk for which each party is responsible as discussed in chapter 2. Geva also argues that loss allocation is best done by holding those responsible who are most able to prevent or decrease the particular risk.[448] The profit and loss sharing principle therefore rules out the option that customers bear the full cost of any loss that follows from an unauthorised payment transaction. However, despite this Islamic principle, in SA customers currently bear the full cost of any loss that follows from an unauthorised transaction, as discussed in chapter 5. This approach to loss allocation presents a problem since it contravenes the underlying fairness commands inherent in the profit and loss sharing principle. The alternative of shifting the loss entirely to the m-payment provider equally violates the principle. Instead, the principle requires that there is balance.

The principle is justified on the grounds that the resources of the economy are thereby more efficiently allocated.[449] The extension of this principle to the m-payment context may ensure that m-payment providers are incentivised to educate customers about the importance of updating security and anti-virus programs; and exclusion and limitation clauses may not be used to the detriment of consumers. However, like with the other principles discussed above, the issue is that the profit and loss sharing principle has been left undefined and it remains unclear how it applies and can be enforced by customers against m-payment providers and third-party collaborators.

[447] Porzio n 443.
[448] Geva n 184, 211.
[449] N. Schoon, *Islamic Banking and Finance* (Spiramus Press 2009) 21.

3.7 Conclusion

The question in the case of unauthorised payment transactions and customers' data breaches is to identify against which types of business conduct consumers should be protected. Answering this question will invariably depend on the type of values and policy orientation which a country chooses to promote.[450] A very neo-liberal stance will permit a purely contractual position in the context of unauthorised transactions and data protection. The middle approach is to adopt public and private measures to protect consumers.[451] In other words, legal measures are adopted so that consumers can enforce their legal rights in the courts. However, self-regulation is also employed to protect consumers by virtue of market forces. When devising rules in relation to loss allocation, it may be taken into account that m-payments are a technology-driven system and that liability should be curtailed only in circumstances when consumers can prevent unauthorised transactions.[452] In respect of data protection, legal rules are created which safeguard personal data but they may be mainly concerned with providing information and obtaining consent.[453] Hence, the focus is on getting consumers to consent i.e. a neo liberal informational model is employed. The other model which can be adopted is one rooted in paternalism and therefore characterised by extensive state intervention.[454] Accordingly, more far-reaching legal consumer protection measures are adopted. For instance, rules may be adopted which attribute responsibility for losses predominantly with m-payment providers. Such an interventionist approach also necessitates that the state dedicates resources to create the necessary bureaucratic structures to monitor compliance.

[450] Paterson and Brody n 53, 337.
[451] Ibid.
[452] Mann n 173, 638.
[453] Bashir et al n 12.
[454] Paterson and Brody n 53, 337.

Paterson and Brody argue that an effective legal consumer protection framework employs a range of provisions, such as, bright-line rules, bans, and prohibitions which incorporate broader moral standards of unconscionable and unfair conduct.[455] Similarly, Abbamonte argues that self-regulation plays a useful role, but it is essential to create regulatory safeguards.[456] Nottage states that to date a post-interventionist approach has been preferred. [457] Such a stance ensures that neo-liberal ideas are maintained through deregulation while "re-regulation" takes place through a "neo-proceduralist" approach.[458] This thesis argues that a purely private approach towards consumer protection is difficult to align with the broader social welfare concerns stipulated by the Sharia. While the Saudi Arabian Hanbali school makes it possible to integrate neo-liberal ideas and therefore promote consumer choice, it must fundamentally ensure that customers' funds are safe and also that their privacy is protected.

Hence, the main aim and objective which ought to be prioritised are to protect the financial assets of m-payment customers, as well as their privacy. When this is not ensured, customers ought to be granted rights to hold their m-payment provider and third-party collaborators accountable. This arguably necessitates that, as consumers, customers have to discharge their respective duties to the m-payment provider. Yet, as discussed above, the legal threshold to establish this depends on whether one conceptualises them as vulnerable, average or reasonably circumspect. A vulnerable customer should still be able to seek compensation from his/her m-payment provider, even in circumstances where s/he is partly to blame, e.g., for having fallen prey to a new cybercrime trick.

[455] Ibid, 352-353.
[456] Abbamonte n 144, 707.
[457] Nottage n 3.
[458] Ibid.

In contrast, a reasonably circumspect customer will find it more difficult to pursue his/her m-payment provider for omissions on his/her part. The adoption of a vulnerable consumer approach within consumer protection law may promote naivety and moral hazard but does not encourage learning. However, it also arguably incentivises m-payment providers to adopt stronger security measures and to engage in heightened risk management. The Islamic *halal* and *haram* doctrines arguably mandate such an approach. It highlights one of the pitfalls of seeking to provide adequate protection to m-payment customers.

Nonetheless, such an approach may help to promote social unity because a more comprehensive safety net is created for customers.[459] Legislators must, in turn, identify the circumstances in which m-payment customers should be protected against unauthorised payment transactions and data breaches.[460] It should possibly always be the case when customers have discharged their basic obligations. In such instances, they should be granted the legal right to seek financial redress from their m-payment providers for unauthorised transactions and data breaches.

For Islamic m-payment customers, it is currently complicated due to the absence of consumer rights and the undeveloped Islamic jurisprudence and the resultant primacy of contract law. More steps must, therefore, be taken to ensure that the holy Islamic prescriptions are upheld. Islamic consumers must be granted rights. Enforcement channels must be created, especially for consumers, through private and public means. ICT standards which incorporate consumer protection objectives should be promulgated, as the m-payment infrastructure is created through ICT.

[459] Paterson and Brody n 53, 339.
[460] Ibid.

While the Islamic consumer protection discourse is still rather rudimentary, it has been shown that the basic tenets which underlie consumer protection policies and laws are very similar in both the West and Islam. In both systems, the ideas of social welfare and fairness are firmly established. However, without the topic of consumer protection being explored by Islamic scholars, including the question of the extent to which Sharia law will impose or permit the exclusion of liability, the problem is that Muslims are deprived of Islamic social justice. It undermines the positive transformative effect which the Sharia can have on Muslim societies. Additionally, it might make those countries less competitive in the global financial world stage. Muslim countries may otherwise become "cannibalistic" societies dominated by capital.[461] The overall objective to create wealth for society in a way which promotes solidarity will then also become more challenging to realise. In other words, the moral compass which Islamic law provides must not be lost. The good faith principle could be further developed to achieve fair outcomes for consumers, alongside the *halal* and *haram* and profit and loss sharing concepts, especially in the context of the problem of unauthorised transactions and data protection and to determine the extent to which Sharia law will impose or permit the exclusion of liability by m-payment providers. That way it will be prevented that SA customers bear the full cost of any loss that follows from an unauthorised m-payment transaction and are left without recourse when their data is misutilised.

It is against this background that the next chapter analyses the UK legal framework which has been created to regulate m-payment services. It is explored how these different strands of consumer protection policies and laws have been embedded in UK law.

[461] Soederberg n 116, 495&499.

CHAPTER 4

THE M-PAYMENT PROVIDER-CUSTOMER RELATIONSHIP IN THE M-PAYMENT ENVIRONMENT WITHIN THE UK

4.1 Introduction

The aim of this chapter is to conduct a doctrinal analysis of the UK legal framework concerning m-payment services and evaluate the policy orientation which underpins the UK law. The legal evaluation is significant to the overall thesis as it permits a comparative analysis with the Saudi legal framework and supports the exploration of this thesis' central research question concerning whether SA might be positively influenced by the UK model.

As discussed in chapter 2, the extension of finance into mobile information and communications technology ('ICT') creates a new complex environment in terms of the law and, subsequently, liability and this area is one of crucial importance in terms of mitigating consumer risk in this new financial market.[1] The use of technology particularly increases the risk of unauthorised m-payment transactions and renders it more difficult to protect customers' data in order to maintain privacy which raises particularly essential legal questions, such as, who should be held responsible for these issues, what happens when errors occur, when liability may be seen to be discharged and when transactions may be

[1] D.A. Zetsche et al, 'From Fintech to TechFin: The Regulatory Challenges of Data-Driven Finance' (2017) European Banking Institute Working Paper Series 3, No.6, 1-36, 1.

reversed.[2] Legal answers must be found to address the new technology's operational and security risks. The law must delineate responsibility, at least in relation to the main factual scenarios, i.e. when risks arise because of customers, security or third-party collaboration (as discussed in chapter 2) and which result in unauthorised payment transactions or cause privacy issues and data breaches. Otherwise, it is unlikely that consumers will reap the advantages identified in chapter 1 and trust in m-payment services may be eroded. Financial stability may also be undermined without laws which create accountability – whether vis-à-vis the customer, the m-payment provider or other third parties.

The literature review in chapter 3 highlighted how legislative responses depend on whether the legislator endorses a neoliberal or social welfare consumer protection framework. Chapter 3 argued that the preferred consumer protection approach for SA should be predominantly rooted in principles of social welfare due to Islamic ethics being culturally important, while, nonetheless, still promoting innovation and progress. The mode of social welfare better mitigates technological risks and, relatedly, the security and privacy perils faced by customers using m-payment services.

This chapter advances the argument that the UK's approach is neoliberal, with a firm emphasis on 'consumer economic interest', though equally embeds social welfare approaches, resulting in a mixed approach. The initially more permissive approach of the Payment Services Regulations 2009 ('PSR 2009') enabled the UK to promote Fintech innovation. As the market matured, however, second-generation legislation was adopted. Hence the Payment Services Regulations 2017 ('PSR 2017') signalled that social welfare objectives were being further developed and strengthened as this introduced regulations for new services – namely, payment initiation services ('PIS') and account information services

[2] A. Rosenberg, 'Better than cash? Global proliferation of payment cards and consumer protection policy' (2006) *Columbia Journal of Transnational Law* 44, 520-578, 563.

('AIS'), as well as new conditions for e-money issuers and payment services providers,[3] as discussed in section 4.3.3. The PSR 2017 has thus struck a balance between allowing competition within the financial services market and subjecting those offering m-payment and related services to legal consumer protection measures.

This distinctive legislative approach has been conducive to the development of the emerging m-payment market, and increasing economic growth.[4] Despite these laws being framed in a neoliberal manner, they are also influenced by the more paternalistic social welfare-based consumer protection model and this philosophy of regulation has been promoted across various interrelated forms of, legislation, as examined in this chapter. Comprehensive legal consumer protection measures have been enacted in order to equip UK m-payment customers with various rights. The policy objectives of social welfare have, therefore, not been ignored, despite the impact of neoliberal, free-market ideas on this legislation. A protective safety net has been created for vulnerable m-payment customers who make use of these innovative m-payment technologies which inherently pose greater risks. M-payment customers are, indeed, better protected against unauthorised m-payment transactions and personal data breaches in the UK than in SA, despite Sharia's social welfare commands, as discussed further in chapter 5.

4.1.1 The structure of this chapter

This chapter firstly discusses the background to m-payment regulation in the UK and how the emergence of technological innovation within the financial services sector has resulted in

[3] FCA, 'Implementation of the revised Payment Services Directive (PSD2): Approach Document and final Handbook changes', Policy Statement, PS17/19, September 2017, 1-279, 1.7.
[4] The Wall Street Journal, 'How Mobile Money Drives Economic Growth', 2017 <http://www.wsj.com/ad/article/mlf-how-mobile-money-drives-economic-growth> accessed 16 December 2017.

new authorisation regimes for what are effectively 'limited banks',[5] i.e., payment institutions and e-money institutions. It is explored how communications companies which act as 'limited banks' are prevented from undermining their competition and narrowing consumer choice within the emerging m-payment market. The section thus examines the tools which are employed to promote a pro-competition stance. The use of e-money via prepaid debit cards or apps which can be used to purchase goods at selected retailers is another potential growth area in the context of m-payments.[6] E-money and its associated authorisation regime and its regulation, particularly in terms of the Electronic Money Regulations 2011 ('EMR 2011'), as well as voluntary codes, are therefore analysed. It is considered whether the EMR 2011 is framed in a way which adequately protects customers in terms of the issues posed by the utilisation of the new electronic financial world.

The next section examines relevant sources of law which govern the rights and obligations of m-payment providers and customers in the UK: Contract and tort law; the mainly repealed PSR 2009 and the new PSR 2017; the FCA's Banking Conduct of Business Sourcebook ('BCOBS') and the voluntary Standards of Lending Practice 2016. It is identified how customers and, particularly their funds, are protected through these different sources of rights when using these new technological forms of fiscal transactions.

The penultimate section scrutinises the requirements imposed by contract law and the extent to which consumers can challenge m-payment terms and conditions. Issues with information disclosure and transparency are identified. Particular recourse is made to the CRA 2015 and relevant case law.

---

[5] A. Scupola, *Innovative Mobile Platform Developments for Electronic Services Design and Delivery* (Business Science Reference 2012) 181.
[6] B. Masters and E. Moore, 'E-money' challenge for high street banks', *The Financial Times*, 14 April 2013 <https://www.ft.com/content/88d9b378-a1fa-11e2-ad0c-00144feabdc0> accessed 13 December 2017.

The final section looks at the issues of data protection, and privacy, which are of particular importance as highly sensitive big data is collected during the provision of m-payment services. It provides a brief analysis of how the risk of money laundering is combated via the AML requirements (contained in the Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017 ('MLRs 2017')) and the impact that these provisions may have on the balance between the prevention of money laundering and consumers' rights, or offer potential legal loopholes which may allow data to be accessed without consent, giving rise to related data protection issues.

All of this material provides a basis for the discussion in chapter 5 and, particularly the conclusion, of, firstly, whether SA's approach to m-payments should rightly adopt a social welfare approach in order to be compliant with Sharia law and principles and, secondly, whether Saudi legislation could usefully mirror the UK approach of combining neoliberal and more paternalistic models of consumer protection.

4.2.1 Background to m-payment regulation in the UK

In 2007, the online bank, Virgin Money, launched a prepaid MasterCard with the e-money issuer PrePay.[7] Similarly, Vodafone was granted a licence to operate as a small issuer of e-money for its m-pay service.[8] Moneybookers have also obtained an e-money licence.[9] This

[7] Finextra, 'Virgin Money to launch pre-paid MasterCard', 18 November 2016 <https://www.finextra.com/newsarticle/17133/virgin-money-to-launch-pre-paid-mastercard> accessed 10 November 2016.
[8] S. Lelieveldt, 'Which future for electronic money in Europe', Lelieveldt Consultancy, 2015, 1-4, 2.
[9] Ibid.

type of service consists of issuing e-money which can be stored electronically and spent later.[10]

A distinction, however, should be drawn between the services provided by e-money institutions and m-payments made through apps.[11] Mobile apps offer different options, e.g., payments via credit and/or debit cards and payment transfers from one account to another.[12] The former do not involve direct access to the funds in the customer's bank account.[13]

The first UK bank to offer customers the possibility of making payments from their mobiles was Barclays with its 'Pingit' app, which was launched in 2012.[14] This app allows person-to-person mobile transfers, including the payment of bills.[15] The mobile network operator, O2, also launched a mobile wallet app, but closed this in 2014.[16] In 2014, 'Paym' was launched and this app resulted from a collaboration between the main UK banks, including Barclays.[17] Like Pingit, Paym can be used by customers to pay other businesses which also have the app.[18] In 2015, Barclays, together with First Direct, HSBC, Nationwide, Metro Bank and Santander entered into an agreement with Zapp, a digital payment service,

[10] Directive 2000/46/EC on the taking up, pursuit of and prudential supervision of the business of electronic money institutions, OJ L 275/39, paras 5-7.
[11] D. Hinds, 'Micropayments: A technology with a promising but uncertain future' in N. Mallat, M. Rossi and V. K. Tuunainen (eds), 'Mobile Banking Services' (2004), 47(5) *Communications of the ACM*, 42–46, 44; A. Boden, 'Explaining PSD2 without TLAs is tough!' Starling Bank, 9 October 2015 <https://www.starlingbank.com/explaining-psd2-without-tlas-tough/> accessed 10 September 2016.
[12] Ibid.
[13] Ibid.
[14] M. Brignall, 'Barclays launches Pingit money-sending service for smartphones', *The Guardian*, 16 February 2012 <https://www.theguardian.com/money/2012/feb/16/barclays-pingit-money-sending-smartphone> accessed 1 November 2016.
[15] Zapp, 'Barclays Pingit set to be first bank app live with Zapp', 7 July 2015 <http://www.zapp.co.uk/blog/2015/07/barclays-pingit-set-be-first-bank-app-live-zapp-2> accessed 10 November 2016.
[16] K. Rushton, 'O2 to launch mobile money transfer app to rival Barclays' Pingit', *The Telegraph*, 27 February 2012 <http://www.telegraph.co.uk/finance/newsbysector/mediatechnologyandtelecoms/telecoms/9109155/O2-to-launch-mobile-money-transfer-app-to-rival-Barclays-Pingit.html> accessed 10 November 2016; O2, O2 Momey <http://www.o2.co.uk/money> accessed 10 November 2016.
[17] S. Murrant, 'Pingit will be marginalized by Pam, Verdict Financial, 15 May 2014 <http://www.verdictfinancial.com/pingit-will-be-marginalized-by-paym/> accessed 10 November 2016.
[18] T. Green, 'Zapp and Paym - just what is the difference?' Mobile Money Revolution, 25 March 2014 <http://www.mobilemoneyrevolution.co.uk/zapp-and-paym-just-what-is-the-difference/> accessed 10 November 2016.

which enables customers to pay merchants online.[19] Corporate customers can, therefore, receive money and various retailers, such as, Shop Direct and Sainsbury's, have signed up to it, so that customers can use mobile phones to make payments in their shops.[20]

Banks also compete against card providers, e.g., Visa's 'V.me', and other digital payment providers, such as, Sage Pay, Worldpay, Optimal Payments and Eleavon.[21] Another important competitor is Apple, which launched 'Apple Pay' in the UK.[22] This service allows users to add a credit or debit card and, for additional security, it is linked to the person's registered fingerprint.[23] In the UK, over 250,000 shops now accept Apple Pay so that not only remote but also proximity payments can be carried out at stores like M&S and Waitrose.[24] Indeed, the introduction of biometric identification seems to be increasing with banks as well.[25] For example, Natwest and Royal Bank of Scotland are now using a fingerprint login.[26]

4.2.2 The m-payment third-party collaboration environment and the legal distinction concerning bank status

These new developments raised specific challenges for the banking industry from a legal perspective as new players had to be accommodated within the legal framework for financial services in order that customers were adequately protected in this new world of technology.

[19] E. Dunkley, 'UK banks seek to Zapp Apple with digital payment services', *Financial Times*, 7 July 2015 <https://www.ft.com/content/4bc7b682-23e0-11e5-9c4e-a775d2b173ca> accessed 10 November 2016.
[20] Ibid.
[21] Dunkley, 'UK banks seek to Zapp Apple with digital payment services' (n 19).
[22] R. Williams, 'How to set up Apple Pay', *The Telegraph*, 14 July 2015 <http://www.telegraph.co.uk/technology/apple/11737576/How-to-set-up-Apple-Pay.html> accessed 10 November 2016.
[23] Ibid.
[24] Ibid.
[25] D. Drinkwater, 'RBS and NatWest to let mobile customers sign-in with biometrics', *SC Magazine*, 18 February 2015 <https://www.scmagazineuk.com/rbs-and-natwest-to-let-mobile-customers-sign-in-with-biometrics/article/537599/> accessed 15 December 2017.
[26] Ibid.

However, the distinct nature of m-payment transactions meant that the authorisation regime that was in place which allowed banks to carry out regulated activities as credit institutions was unsuitable for these new types of services.[27] The stringent authorisation regime for banks would have stifled innovation in the m-payment market. A new authorisation regime was, therefore, developed by virtue of the PSR 2009 which transposed Directive 2007/64/EC, the first Payment Services Directive ('PSD'), so that m-payment services were regulated, but might also be offered by mobile operators as an additional feature.[28] Payment institutions ('PI's) have to adhere to those Regulations, which applied to banks, e-money issuers, building societies, money remitters, non-bank merchant acquirers and non-bank credit card issuers.[29] They are, therefore, regulated by the Financial Conduct Authority ('FCA').[30]

Consequently, the legislation promoted consumer choice through increased competition and innovation; such an approach was also thought to be more appropriate since, unlike credit institutions, payment institutions are not allowed to engage in a broad range of business activities,[31] such as, providing guarantees or taking deposits.[32] By contrast, credit institutions can also be payment institutions, but not all payment institutions will be credit institutions.[33]

---

[27] FSMA 2000, s22 and Schedule 2; also see the FSMA 2000 (Regulated Activities) Order (Statutory Instrument 2001/544), the FSMA 2000 (Carrying on Regulated Activities by Way of Business) Order 2000 (Statutory Instrument 2001/1177) and the FSMA 2000 (Carrying on Regulated Activities by Way of Business)(Amendment) Order 2014 (Statutory Instrument 2014/3340).
[28] Directive 2007/64/EC on payment services in the internal market amending Directives 97/7/EC, 2002/65/EC, 2005/60/EC and 2006/48/EC and repealing Directive 97/5/EC, OJ L 319/1, Article 5.
[29] FSA, Payment Services Regulations, 2013 <http://www.fsa.gov.uk/doing/regulated/banking/psd> accessed 1 April 2013.
[30] Ibid.
[31] FSA Handbook of the Electronic Money, paras 4.2.3, 4.3.2–4.3.7 and 6.9.1 <http://fsahandbook.info/FSA/html/handbook/ELM/4> accessed 29 March 2013.
[32] P. Makin, 'Regulatory Issues around Mobile Banking in Organisation for Economic Co-operation and Development'. In OECD (eds), *The Development Dimension ICTs for Development: Improving Policy Coherence* (OECD Publishing, 2010) 145.
[33] Directive 2007/64/EC, paras 8 and 11.

As further discussed in section 4.3.3 below, the less interventionist PSR 2009 was replaced by the more forceful PSR 2017, which came into force on 13 January 2018[34] and transposed the Second Payment Services Directive 2007/64/EC ('PSD2').[35] Both the PSR 2009 and the PSR 2017 adopted a unified liability approach between the companies and the customer, which is aimed at fostering consumer protection by providing clearer and more accessible avenues of recourse for consumers and accountability for service providers. Yet, the PSR 2017 heightens consumer protection since it clarifies how liability is allocated when unauthorised transactions occur and thus it appears to promote a social welfare-based legal policy too.

As noted in chapter 2, it is not only m-payment customers who may be responsible for unauthorised transactions as they may also occur because of common security issues for which m-payment providers are to blame, or even third parties who helped to create the m-payment infrastructure. Clarification of such liability sues by the PSR 2017 signifies a slight shift towards a more social welfare-oriented model of consumer protection. The PSR 2017 further extended the definition of payment institutions by including third party payment providers ('TPPs').[36] In doing so, producerist policy objectives have found their way into the PSR 2017 as more participants can enter the market, thus promoting business interests.

---

[34] Explanatory Memorandum to the Payment Services Regulations 2017, 1-6, 1 <http://www.legislation.gov.uk/uksi/2017/752/pdfs/uksiem_20170752_en.pdf> accessed 15 December 2017.

[35] Directive 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No. 1093/2010, and repealing Directive 2007/64/EC (Text with EEA relevance) ('PSD2') entered into force on 12th January 2016 and has to be implemented by Member States within two years: European Banking Authority, 'Consultation on the Guidelines on the criteria on how to stipulate the minimum monetary amount of the professional indemnity insurance under PSD2', 22 September 2009 <https://www.eba.europa.eu/news-press/calendar?p_p_id=8&_8_struts_action=%2Fcalendar%2Fview_event&_8_eventId=1586016> accessed 10 September 2016.

[36] TPPs fulfil either the role of a payment initiation services provider ('PISP') or an account information service provider ('AISP'). They thus create the Application Programming Interface ('API') which establishes the requisite connection to link merchants with banks. Hence, these TPPs deal with mobile payments and have direct access to customers' bank accounts: European Commission, 'Payment Services Directive: frequently asked questions.' Brussels, 8 October 2015, 1-8, 3.

A neoliberal, consumer choice stance can also be seen from the expansion of a regulatory regime for e-money institutions.[37] As discussed in chapter 1, mobiles can function as e-wallets in terms of carrying e-money. This facilitates the use of prepaid cards which can be stored on a phone. In the UK, businesses that provide this function have been empowered to enter the market by the authorisation system made possible by Art.8 of Directive 2000/46/EC concerning the taking up, pursuit of and prudential supervision of the business of e-money institutions ('the first Electronic Money Directive 2000'), which permitted a waiver in relation to some or all provisions of the Directive if certain conditions were met.[38] These were implemented in the UK by virtue of the Electronic Money (Miscellaneous Amendments) Regulations 2002, which made changes to the Financial Services and Markets Act 2000.[39]

The first Electronic Money Directive 2000 was, however, replaced by Directive 2009/110/EC on the taking up, pursuit and prudential supervision of the business of e-money institutions ('the second Electronic Money Directive'). The capital requirements were lowered[40] and laxer regulatory conditions were introduced for so-called small e-money issuers.[41] In the UK, these changes were given effect by the Electronic Money Regulations 2011 ('EMR 2011'), as further discussed in sections 4.2.4.1 and 4.2.4.2 below.[42] A less

[37] Electronic Money (Miscellaneous Amendments) Regulations 2002, Regulation 21(a); Payment Service Regulations 2009, Regulation 2(1); also see Directive 2006/48/EC relating to the taking up and pursuit of the business of credit institutions, Article 4 explains that a credit institution means '(a) an undertaking whose business is to receive deposits or other repayable funds from the public and to grant credits for its own account; or (b) an electronic money institution within the meaning of Directive 2000/46/EC'; also see Financial Services and Markets Act 2000 (Prescribed Financial Institutions) Order 2013, Regulation 1(2).
[38] First Electronic Money Directive 2000, Article 8(1)(a)-(c).
[39] I. Lloyd, *Information Technology Law* (7th ed, OUP 2014) 460.
[40] Directive 2009/110/EC on the taking up, pursuit and prudential supervision of the business of electronic money institutions (the second Electronic Money Directive), Regulation 19.
[41] HM Treasury, 'Laying of regulations to implement the new E-Money Directive, a consultation document.' October 2010, 1-112, 10 <https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/81328/emoney_directive_consultation.pdf> accessed 10 September 2016.
[42] (SI 2011/99); FCA n 3.

stringent authorisation regime has been adopted which favours a neoliberal vision of consumer protection.[43]

Until 12 July 2018, e-money institutions were permitted to issue e-money and also offer m-payment services[44], even if they were not registered or separately authorised under the PSR 2009.[45] Under the PSR 2009, authorisation by the FCA for e-money institutions did not require separate authorisation for payment service purposes. However, this is no longer possible under the PSR 2017.[46] Instead, the PSR 2017 requires compliance with the PSD2 in that e-money institutions must apply for re-authorisation.[47] Initially, the law was driven by a neoliberal emphasis on market considerations, mainly to realise economic efficiency and development. However, the adoption of the PSR 2017 signals a slightly more interventionist social welfare approach in terms of the regulation of the m-payment market, thus consumer protection interests are being increasingly given prominence as the technology and services available, and so too the inherent risks to customers, grows. As a result, mobile financial services providers now have to be granted authorisation.[48]

The EMR 2011, PSR 2009 and PSR 2017 recognise that m-payments are different in scope than the general payment services currently provided by banks via the use of mobiles, as discussed in the introduction.[49] The term 'mobile' deals with the medium of delivery and whether or not an institution is a bank will depend on the functions and services it provides.[50]

---

[43] FSMA 2000, ss40-41; see esp. FSMA (Regulated Activities) Order 2001 (Statutory Instrument 2001/544), s4; also see Directive 2000/46/EC on the taking up, pursuit of and prudential supervision of the business of electronic money institutions (the first Electronic Money Directive 2000), para.7 of the preamble; A. Murray, *Information Technology Law: The Law and Society* (3rd ed, OUP 2016) 530.

[44] FCA, 'Authorised electronic money institution (authorised EMI)', 22 September 2017 <https://www.fca.org.uk/authorised-electronic-money-institution-authorised-emi> accessed 15 December 2017.

[45] FCA n 3.

[46] FCA n 44.

[47] Ibid.

[48] Financial Services and Markets Act 2000, s19(1).

[49] OECD, 'Report on Consumer Protection in Online and Mobile Payments', 17 August 2012, 1-45, 8.

[50] FCA, 'Payment Services and Electronic Money - Our Approach, The FCA's role under the Payment Services Regulations 2017 and the Electronic Money Regulations 2011', September 2017, 1-237, 23.

The distinction between a bank, a payment institution and an e-money institution, therefore, depends on the range of regulated activities which the particular institution pursues.[51]

For example, if an institution provides deposit-taking, whether via a high street branch, mobile, internet or telephone, it is, arguably, a 'bank' for the purposes of Part IV of the FSMA 2002 and the Banking Act 2009, s2 (which is the relevant definition of 'bank' adopted for the purposes of this work).[52] It must therefore seek authorisation from the Prudential Regulation Authority ('PRA') for deposit-taking activity.[53] The fact that a payment is made via a mobile, rather than through conventional methods, does not mean that the service should fall outside the package of services one ordinarily associates with what banks do, i.e. making and collecting payments on behalf of their customers.

However, at present, an exception has been permitted for payment and e-money institutions which results in m-payments being afforded special status.[54] M-payments made through payment institutions or with e-money from e-money institutions are not deemed to constitute deposit taking; these institutions are thus not equivalent to banks.[55] Ordinarily, deposit-taking denotes paying money to a financial institution for it to hold and generate interest.[56] By contrast, m-payments do not earn interest for customers.[57]

---

[51] Ibid.
[52] E.P. Ellinger et al, *Ellinger's Modern Banking Law* (5th ed, OUP 2011) 79&90.
[53] A. Hill-Smith, *Consumer Credit: Law and Practice* (2nd ed, Routledge 2015) 38.
[54] P. Delimatsis and N. Herger, *Financial Regulation at the Crossroads: Implications for Supervision, Institutional Design and Trade* (Kluwer Law International 2011) 349.
[55] Ibid.
[56] A.K. Kashyap et al, 'Banks as liquidity providers: An explanation for the coexistence of lending and deposit-taking' (2002) *The Journal of Finance* 57(1), 33-73, 33.
[57] Delimatsis and Herger n 54, 349.

4.2.2 Communications companies and the furtherance of a consumerist policy orientation to facilitate entry by third parties

As noted above, UK legislation has been adopted which has paved the way for mobile phone operators to enter the payments market, so long as they obtain the necessary e-money institution or payment institution authorisation. Mobile service operators which enter the m-payment market may, therefore, compete with banks.[58] One of the key areas pertaining to m-payments is access and the interoperability between different electronic communications services.[59] Electronic communications services include those which consist wholly or mainly in the conveyance of signals on electronic communications networks.[60]

As m-payments depend on mobile phone services, including internet access, problems may arise when operators have undue market dominance.[61] In other words, consumer choice may suffer in the neoliberal sense as there will be decreased competition. Hence, the EU regulatory framework for electronic communications places the notion of significant market power (i.e., having a 25% market share)[62] at its heart within both the Access[63] and Framework Directives.[64] Access has been emphasised, i.e., 'the making available of facilities

[58] Communications Act 2003, s151; see also Eur-Lex, 'Access to electronic communications networks', 10 September 2015 <http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=URISERV%3Al24108i> accessed 10 November 2016.
[59] Ibid.
[60] Directive 2002/21/EC on a common regulatory framework for electronic communications networks and services ('Framework Directive'), Article 2(c).
[61] Eur-Lex n 58.
[62] Commission guidelines on market analysis and the assessment of significant market power under the Community regulatory framework for electronic communications networks and services, para. 3, Official Journal C 165, 11/07/2002 P. 0006 - 0031.
[63] Directive 2002/19/EC on access to, and interconnection of, electronic communications networks and associated facilities ('Access Directive'). Further amendments were made to the framework with the introduction of Directive 2009/140/EC amending Directives 2002/21/EC, Directive 2002/19/EC, and Directive 2002/20/EC, which amended both the Access and Framework Directive.
[64] The Framework Directive.

and/or services, to another undertaking, under defined conditions, on either an exclusive or non-exclusive basis, for the purpose of providing electronic communications services'.[65]

Access is defined very broadly and includes access to physical infrastructure, software and virtual network services as well as interconnectivity as a 'specific type of access implemented between public services operators'.[66] Interoperability is expressly recognised in order to enhance freedom of choice for end users.[67] Consequently, the neoliberal notion of 'consumerism' discussed in chapter 3 is powerfully promoted.

In the UK, the Framework and Access Directives were transposed through the Communications Act 2003, the Privacy and Electronic Communications (EC Directive) Regulations 2003 and the Wireless Telegraphy Act 2006.[68] An underlying policy objective is to promote an open and competitive market for electronic communications networks, services and associated facilities in line with the proposals of the 2000 Communications White Paper – A New Future for Communications (Cm 5010).[69]

This market-based approach is clearly illustrated by the Office of Communications ('OFCOM') being entrusted with ensuring adequate and fair competition between the communication entities within these various market sectors.[70] As the national regulatory body for the communication industries, including the telecommunications spectrum, OFCOM enhances the interests of the public, including consumers, by fostering competition in a

[65] Access Directive, Article 2(a).
[66] Access Directive, Article 2(b).
[67] Access Directive, Recital 9 of the Preamble.
[68] Department for Culture, Media and Sport, 'Implementing the revised EU Electronic Communications Framework, Impact Assessment', April 2011, 1-204, 8 <https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/77643/Implementing_revised_EU_ElectronicCommunicationsFramework_IA.pdf> accessed 10 November 2016.
[69] Framework Directive; Communications Act 2003, Article 7, Explanatory Notes, 4 <http://www.legislation.gov.uk/ukpga/2003/21/notes/division/2> accessed 10 November 2016.
[70] O. Boyd-Barrett, *Communications Media, Globalization, and Empire* (John Libbey Publishing Ltd 2016) 192.

neoliberal fashion.[71] It does so by regulating *ex ante*, whether market participants have significant market power.[72]

For this purpose, a non-discrimination obligation is contained in s. 87(6)(a) of the Communications Act 2003 which permits OFCOM to impose 'a condition requiring the dominant provider not to discriminate unduly against particular persons, or against a particular description of persons, in relation to matters connected with network access to the relevant network or with the availability of the relevant facilities'.[73] If OFCOM determines that a provider has significant market power jointly or singularly in a particular market segment, it can impose extra conditions on the entity in order to realise adequate and fair competition.[74] OFCOM also discharges its duties under the Competition Act 1998[75] by virtue of s371(1) of the Communications Act 2003. It may, therefore, be possible that, as mobile companies enter the payments market, competition law rules start to come into play that prevent market dominance and these laws may affect how m-payments operate in future. Consequently, active steps have been taken to remove market barriers for new entrants, thus promoting the neoliberal policy model and possibly heightening consumer risk, even as there is increased consumer choice.

[71] Competition and Markets Authority and the Office of Communications, 'Memorandum of understanding between the Competition and Markets Authority and the Office of Communications - concurrent competition powers', 2 February 2016, 1-21, 6 <https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/502645/Ofcom_MoU.pdf> accessed 10 November 2016.
[72] Communications Act 2003, ss79-93; M. Feintuck and M. Varney, *Media Regulation, Public Interest and the Law* (2nd ed, Edinburgh University Press 2006) 68.
[73] W. Lemstra and W.H. Melody, *The Dynamics of Broadband Markets in Europe: Realizing the 2020 Digital Agenda* (CUP 2015) 184.
[74] Boyd-Barrett n 70, 192.
[75] See also Treaty on the Functioning of the European Union, Articles 101-102.

4.2.4 Electronic money, m-payments and addressing the risk which arise from third-party collaboration

As noted above, transactions using electronic money ('e-money')[76] on mobiles are another potential growth area for m-payments which are becoming a salient feature of mobile financial services in the UK.[77] E-money need not be held on mobiles and can be kept on servers and prepaid cards, or transferred through web-based providers, e.g., PayPal.[78] That means that e-money can be stored in digital, electronic, mobile or virtual wallets.[79]

4.2.4.1 The Electronic Money Directive 2009: An authorisation framework to promote third-party collaboration within the emerging m-payment space

In light of global industry trends, the UK implemented the Electronic Money Directive 2009[80] through the EMR 2011. These Regulations create a new authorisation framework and rules of conduct for e-money institutions and issuers.[81] They are intended to foster the development of secure and innovative e-money services, as well as competition, by enabling other companies to access the market and they are, therefore, critical to the future of m-payments.[82] E-money institutions are allowed to issue and administer not only e-money and store data, but also provide different business activities.[83] The FCA further has to take into

[76] Directive 2007/64/EC on payment services in the internal market amending Directives 97/7/EC, 2002/65/EC, 2005/60/EC and 2006/48/EC and repealing Directive 97/5/EC, Article 4(5).
[77] Masters and Moore n 6.
[78] J. Firpo, 'E-Money - Mobile Money - Mobile Banking - What's the Difference?', The World Bank, 21 January 2009 <http://blogs.worldbank.org/psd/e-money-mobile-money-mobile-banking-what-s-the-difference> accessed 10 November 2016.
[79] Ibid.
[80] Directive 2009/110/EC on the taking-up, pursuit and prudential regulation of the business of electronic money institutions amending Directives 2005/6-/EC and 2006/48/EC and repealing Directive 2000/46/EC.
[81] Explanatory Memorandum to the Electronic Money Regulations 2011, No.99, 1.
[82] European Commission, 'E-money', 2013 <http://ec.europa.eu/internal_market/payments/emoney/> accessed 28 May 2013.
[83] HM Treasury n 41.

account 'the desirability of facilitating innovation in connection with the issuance of e-money and the provision of payment services.'[84] Hence, the neoliberal concept of consumer economic interest appears to be the underlying objective behind these Regulations.

A more updated definition was adopted for e-money, which includes value that is stored magnetically or on IT servers and plastic cards, for making payment transactions by legal and natural persons.[85] Consequently, e-money denotes cash stored on electronic devices, including mobile phones.[86] The 'electronic money institution' is regulated through a separate regulatory regime than a payment institution, discussed in section 4.3.3.[87] Regulation 6 of the EMR 2011 sets out the conditions which have to be satisfied in order for authorisation to be granted. Regulation 6(5)(a)-(c) recognises the risks inherent in the use of e-money, even in m-payments, in order to protect consumers by requiring applicants to demonstrate that they have:

a) robust governance arrangements for its electronic money issuance and payment service business, including a clear organisational structure with well-defined, transparent and consistent lines of responsibility;
b) effective procedures to identify, manage, monitor and report any risks to which it might be exposed; and
c) adequate internal control mechanisms, including sound administrative, risk management and accounting procedures.

These measures must be comprehensive and proportionate to the nature, scale and complexity of the e-money to be issued and the payment services to be provided. The risks include

[84] Electronic Money Regulations 2011 ('EMR 2011'), Article 47(2)(d).
[85] HM Treasury n 41, 6.
[86] European Commission n 82.
[87] HM Treasury n 41, 6.

settlement, operational, counterparty, liquidity and market risk, as well as financial crime risk, which are similar to the risks addressed by the PSR 2009.[88] Similar conditions in relation to governance and risk are imposed on small e-money institutions seeking registration.[89] However, as these rules are slightly more relaxed for smaller operators, one may conclude that the consumer protection interest was not considered as much a priority as the consumer economic interest.

This does not mean that more social welfare-based consumer interests have been completely disregarded. New conditions were imposed in relation to redeeming and protecting customer funds, replacing provisions that were unclear in the First Electronic Money Directive 2000.[90] For example, when funds are received, e-money had to be issued at par value without delay and the customer had to be able to redeem the e-money at any time at the par value.[91] The agreement had to clearly spell out the conditions in relation to redemption and fees and the customer had to be informed of these prior to entering into any contract.[92] In other words, a typical neoliberal approach of information disclosure is mandated which places an emphasis on enabling comprehension by a circumspect consumer.

However, the consumer is still protected as redemption fees can only be charged in certain narrow circumstances;[93] these have to be proportionate and commensurate to the actual costs.[94] No time limit or interest can be imposed in relation to the right of redemption,

[88] FSA, 'Tracked changes version of the FSA's role under the Electronic Money Regulations 2011: Our approach', April 2013, 24 <http://www.fsa.gov.uk/static/pubs/international/draft-approach-emoney.pdf> accessed 1 April 2013.
[89] EMR 2011, Regulation 13.
[90] Directive 2000/46/EC of the European Parliament and the Council on the taking up and prudential supervision of the business of electronic money institutions; HM Treasury n 41, 6.
[91] EMR 2011, Article 39.
[92] EMR 2011, Article 40.
[93] EMR 2011, Article 41(1)(a)-(c).
[94] EMR 2011, Article 41(2).

redemption has to take place for amounts below €10[95] and it is not possible to contract out of the provisions of the EMR 2011 (or the PSR 2017).[96] The provisions in the EMR 2011 (and the PSR 2017) governing unauthorised e-money payment transactions cannot be excluded when an e-money issuer and an e-money holder or a payment service user enter into an agreement.[97] Such social welfare requirements are essential in order to protect consumers against providers contracting out of statutory obligations, especially important rights, such as, redemption and refund.

4.2.4.2 The regulation of e-money institutions

Another indication of social welfare-based consumer protection interests being entrenched in the regulation of the e-money sector, despite the neoliberal objective to encourage new market entrants, is that prudential requirements will now apply to e-money institutions, whereas, in the past, all e-money institutions were exempted. However, the €150 storage limit for devices has been lifted.[98] Consumers' ability to store e-money on electronic devices is no longer curtailed despite the risk which comes with higher limits, a move that posits consumers as circumspect and responsible in a neoliberal sense. Not all prudential requirements are applied to small e-money institutions, i.e., those which have total liabilities of less than Euros 5 million within a six months period.[99] This reflects the prevalence of neoliberal policy considerations which may compromise and subordinate consumer protection to the commercial needs and realities of operators, particularly, small institutions.

[95] FSA n 165, 7; see also EMR 2011, Article 45.
[96] EMR 2011, Article 73.
[97] Ibid.
[98] HM Treasury n 41, 17; also see Electronic Money Directive 2000/46/EC, Article 8 where the previous limitation of €150 was established.
[99] HM Treasury n 41, 6; HM Revenue & Customs, 'Financial Services Authority to supervise small electronic money issuers' <http://www.hmrc.gov.uk/mlr/news/supervision-semi-fsa.htm> accessed 25 July 2013.

Banks and building societies have a separate authorisation regime from non-bank e-money issuers but all institutions issuing e-money have to adhere to the same provisions relating to e-money issuance, redeemability, interest and complaints.[100] This is based on the distinction drawn between issuance of e-money and deposit taking as regulated activities, with the former constituting a means of paying and not saving.[101] Consequently, a less stringent approach has been permitted in order to promote business interests and a neoliberal policy objective. This permissive stance is visible in the exemption offered in respect of limited networks for a narrow group of services or goods or in relation to e-money in online accounts which are held on an electronic device or card.[102] There is no definition for limited networks, but examples are single retailer cards, membership cards or vouchers.[103] This definition is likely to cover banks which decide to venture into the issuance of e-money as part of their m-payment services and other potential m-payment providers, e.g., mobile companies. The issue then is that, due to the expected growth within the m-payments sector, it will become difficult to distinguish limited networks, which are exempt, and general purpose networks, which are not, and this makes consumers vulnerable.[104]

4.2.4.3 Voluntary codes of conduct

It is important that voluntary codes of conduct and/or statutory measures are adopted in order to safeguard customers who use limited networks. The adoption of voluntary codes of practice, as opposed to statutory measures, may be better until this new sector becomes more consolidated, so that innovation is not stifled.

[100] Ibid 7.
[101] Ibid.
[102] Ibid 11.
[103] Ibid.
[104] Ibid 12.

However, with a code, there is a problem with voluntary subscription.[105] Those which do not subscribe to the code are not bound to follow it. For this reason, it is essential that statutory obligations are at least imposed on general purpose networks in order to protect customers, as well as financial stability. Hence, the OECD's G20 High-Level Principles on Financial Consumer Protection must be honoured, as discussed in chapter 3. One way to achieve this is through requiring e-money institutions to comply with capital requirements, i.e., to have at all times at least €350,000 in order to comply with the funds requirement of paragraph 13 of Schedule 2.[106] Customer funds are protected to a certain degree by such a requirement.

The EMR 2011 further imposes requirements for safeguarding funds received in exchange for e-money which may be discharged through either option 1 or option 2.[107] Under option 1, funds have to be segregated from other funds of the e-money institution. Under option 2, insurance cover or a guarantee from an authorised insurer or credit institution has to be obtained, so that the funds become payable in case of an insolvency event. A case in point is the HMV Rewards Scheme:[108] The administration of HMV illustrates the risk still faced by consumers. When HMV went into administration, it was initially announced that customers could not redeem their gift and prepaid cards because administrators normally were not obliged to honour these.[109] The HMV case illustrates the complexities and problems with the

[105] E. Stokes, 'Double Movements in the Regulation of New Technologies: The Case of Nanotechnology'. In B. Lange et al (eds), *Regulatory Transformations: Rethinking Economy-Society Interactions* (Hart Publishing 2015) 213.
[106] EMR 2011, Article 19.
[107] EMR 2011, Articles 20-22.
[108] J. Thompson, 'U-turn on HMV gift cards as its survival hopes improve', *The Independent*, 2013 <http://www.independent.co.uk/news/business/news/uturn-on-hmv-gift-cards-as-its-survival-hopes-improve-8460995.html> accessed 2 April 2013.
[109] Daily Record, 'HMV customers furious as collapsed music chain refuse to honour vouchers and gift cards', 2013 <http://www.dailyrecord.co.uk/news/uk-world-news/hmv-cutomers-angry-as-music-chain-1535990> accessed 28 May 2013.

use of e-money in the event of an issuer's insolvency, which may constrain the extent to which a social welfare approach to consumer protection might be effected.[110]

E-money issued by building societies and banks is not protected by the Financial Services Compensation Scheme (FSCS) as it does not constitute deposit taking.[111] Deposit taking denotes storing value, which is repayable as a debt, whereas e-money means buying a way to make payments.[112] The FSCS will only apply to e-money if Article 9J of the Financial Services and Markets Act 2000 (Regulated Activities) Order 2001 is amended.[113] An amendment would ensure that treatment of e-money in the UK is comparable to some European countries,[114] but it would place a burden, particularly for low value transactions, on businesses.[115]

This is likely to be of relevance for m-payments on two levels. Firstly, where new practices and systems are being developed, an overly strict regulatory regime may hinder innovation and limit the use of such practices. Secondly, where large sums of money are stored on a mobile, the risk of loss is high without statutory protection. Accordingly, the downside of this business-friendly approach is that customer protection is not maximised and consumers using these services are still at risk. Instead, the exclusion of e-money from the FSCS reflects a typical neoliberal approach which emphasises the disclosure of information by payment service providers to their customers so that they are informed of the risks involved. The provisions of the FCA's BCOBS, which provide mandatory rules for the

[110] Deloitte, 'HMV Administration-FAQ', 2013 <http://www.deloitte.com/view/en_GB/uk/services/corporate-finance/restructuring-services/updates-for-insolvencies/hmv/4d244ad0cd24c310VgnVCM2000003356f70aRCRD.htm> accessed 2 April 2013.
[111] HM Treasury n 41, 13.
[112] FCA, The Perimeter Guidance Manual, Chapter 3A, Guidance on the scope of the Electronic Money Regulations 2011, 1-14, 11 <https://www.handbook.fca.org.uk/handbook/PERG/3A.pdf> accessed 10 November 2016.
[113] Ibid; E. Todoroki et al, *Making Remittances Work: Balancing Financial Integrity and Inclusion* (The World Bank 2014) 185.
[114] Several European countries have extended the financial services compensation scheme to e-money.
[115] HM Treasury n 41, 14.

conduct of banking business, further do not apply to the issuance of e-money,[116] as BCOBS applies only to accepting deposits from banking customers.[117]

Consumer protection is, therefore, not provided to customers of e-money institutions which do not fall within the PSR 2017 discussed below in section 4.3.3. [118] This is unfortunate, as Chapter 5 of the BCOBS, especially rule 5.11R (which renders banks liable for unauthorised payments) and rule 5.1.12R (which provides the liability of banking customers for unauthorised payments), as well as rules 5.12R-5.1.19R, contain similar provisions as Part 7 of the PSR 2017.[119] The BCOBS, therefore, fails to address a lacuna within the law for e-money institutions and to mitigate against the risks which may arise, including the exclusion of e-money from the FSCS. It may, therefore, be concluded that a neoliberal vision still dominates and a more interventionist legal consumer protection measures should be enacted to regulate e-money.

4.3.1 The sources of law which govern the rights and obligations of m-payment providers and their customers, including in respect of unauthorised m-payment transactions:

The different sources of law which confer rights and obligations on m-payment providers and customers must be examined in order to explore the form of consumer protection framework that has been adopted for m-payment customers. Hence, the following sections analyse how various types of legislation have responded to the multiple risks involved, particularly

[116] A. Burrows, *Principles of English Commercial Law* (OUP 2015) 198.
[117] BCOBS 1.1.1R.
[118] Burrows n 116, 198.
[119] Ibid.

unauthorised m-payment transactions, ultimately developing consumer protection in the UK according to a combination of neoliberal and social welfare principles.

It is firstly discussed how contract and tort law apply to the m-payment context. Section 4.3.3 analyses the rights and obligations of payment service providers and customers, particularly in respect of unauthorised m-payment transactions, under the old PSR 2009 and the new PSR 2017, and how this has shaped the conceptualisation of consumers, i.e., either vulnerable or reasonably circumspect. Section 4.3.4 explores how the obligations contained in the PSR 2009 and PSR 2017 have been further supplemented by the Financial Conduct Authority's Banking Conduct of Business Sourcebook ('BCOBS') and the Standards of Lending Principles 2016.

4.3.2 Contractual and tortious rights and obligations relevant to consumer understanding

As with traditional banking, the relationship between m-payment providers and customers has been regulated by a mixture of contract law, implied terms[120], consumer protection law, and other forms of regulation.[121] Hence, while this relationship is largely based on contract, additional legal interventions bolster it. [122] Given that the new technologies involved in m-payments carry an increased risk for the consumer, as discussed in chapter 2, these legal interventions potentially allow for significant protections as explored further below.

[120] CRA 2015, s49.
[121] A. Gkoutzinis, *Internet Banking and the Law in Europe, Regulation, Financial Integration and Electronic Commerce* (CUP 2006) 29.
[122] Ibid.

Accordingly, the contractual agreements between the m-payment provider and customer do not overrule the pre-existing amalgam of tort law and contract law.[123] They also do not overrule legislation such as the Payment Services Regulations 2009 ('PSR 2009') and the Payment Services Regulations 2017 (PSR 2017), discussed in section 4.3.3 below. Instead, the PSR 2009 and the PSR 2017, in fact, further define the m-payment provider's duty of care and the customer's corresponding ones. Gkoutzinis observes that the financial institution's duty to exercise care and skill, including to maintain confidentiality and to protect data thus provide substantive bases for customer protection.[124] He further adds that financial institutions have to maintain their networks and the available functionality infrastructure through strong security measures. Hence, a failure to provide a generally available technology, including security measures, would be tantamount to a breach of their duty of care.

An important aspect of the duty of care is access control since this ensures data protection, banking confidentiality and prevents unauthorised transactions.[125] M-payment providers are exposed to new liabilities arising from negligently processed payments or systems failures, including in respect of cybercrime, when providing m-payment services.[126] S13 of the Supply of Goods and Services Act 1982 (SOGSA) implies a duty to 'carry out the service with reasonable care and skill'. Equally, s49 of the CRA 2015 (discussed in sections 4.4.1 to 4.4.3 below) states the need to 'perform the service with reasonable care and skill'.[127] Consequently, a customer can invoke this duty of reasonable care and skill based on the

[123] Contract and tort law, as well as equity and legislation, e.g., the CRA 2015, are equally applicable to the scope and application of the m-payment service agreement.
[124] Gkoutzinis n 121, 36-37.
[125] Ibid.
[126] J. O'Donovan, *Lender Liability* (Sweet & Maxwell 2005) 193.
[127] J. Poole, *Casebook on Contract Law* (13th ed, OUP 2016) Chapter 8.

contractual obligation derived from the agreement with the service provider (either under an express term or a term implied under s13 of SOGSA 1982 and s49 of the CRA 2015).

However, given the complexity of the underlying technology, as discussed in chapter 1, section 1.2, it is doubtful that contract law alone offers sufficient consumer protection. The PSR 2009 and the PSR 2017, as well as other legislation, such as, the Data Protection Act 1998 (which was replaced by the General Data Protection Regulation (GDPR) on 25 May 2018, discussed in section 4.5.5), have further helped to shape the duty of care in the m-payment context. These laws put forward a particular conceptualisation of the consumer, as discussed in chapter 3. The analysis of the different sources of law and regulations indicates that a social welfare-based notion of consumer protection has been consistently embedded in such legislation. Such an approach helps m-payment customers overcome otherwise insurmountable legal obstacles, e.g., providing evidence as to why an unauthorised transaction has occurred. The adoption of these statutes appears to be better for realising consumer protection than through contract law alone as the legislation fleshes out the contractual duty of care, particularly what is expected of m-payment providers in order to mitigate the risk to customers who use m-payments. It is harder for m-payment providers to circumvent their obligations through exemption clauses.[128]

The next section provides an overview of the old PSR 2009 and the new PSR 2017 in order to scrutinise the type of consumer protection frameworks that these laws stipulate and the way in which they conceptualise the consumer.

[128] R. Kidner, *Casebook on Torts* (12th ed, OUP 2012) 166.

4.3.3 The PSR 2009 and the PSR 2017: Liability frameworks to regulate unauthorised transactions and address security and technological risks, including from third-party collaboration

The extension of the payment services system to mobile ICT raises some difficult questions in relation to the allocation of liability arising from the inherently heightened technological and operational risks, particularly in relation to unauthorised m-payment transactions, as discussed in chapter 2. In this context, the old PSR 2009 and the new PSR 2017 are particularly pertinent since they spell out the initial and currently applicable statutory regime for m-payments. As mentioned above, the PSR 2017 transposes the PSD2 into UK law. Whilst it would exceed the scope of the thesis to scrutinise all of the provisions of the PSR 2017, a broad overview is given, with particular emphasis being placed on the evolution of the liability regime relevant to m-payments services.

Under the PSR 2017, a register of all institutions and agents is required to be kept.[129] Part 1 of Schedule 1 of the PSR 2017 delineates which activities constitute payment services and Part 2 details activities that do not. Paragraph 1(a) to (h) of Schedule 1 lists the following seven kinds of activities which are considered payment services if they are pursued as part of a regular occupation or business activity:

- Services enabling cash to be placed on a payment account.
- Services enabling cash withdrawals from a payment account.
- Direct debits, payment transactions through a payment card or similar device and credit transfers, including standing orders.

[129] PSR 2017, Regulation 4.

- Direct debits, payment transactions through a payment card or similar device and credit transfers where the funds are covered by a credit line.
- Issuing payment instruments or acquiring payment transactions.
- Money remittance.
- Execution of payment transactions where consent has been given through a telecommunication, digital or IT device.
- Account information services.

Hence, m-payments fall within the scope of the definition for payment services.

4.3.3.1 Technological risks and security and the role of risk management

Authorised institutions had to demonstrate under the PSR 2009 that risk was being properly managed through the adoption of internal control mechanisms[130] which, as noted in chapter 2, acknowledges that m-payments pose additional security risks.[131] This led to the PSR 2017 imposing more stringent payment security obligations than the PSR 2009. For example, payment service providers have to furnish a security policy, which consist of a comprehensive risk analysis, and they have to explain how fraud is being combated and personal and sensitive data kept secure.[132]

[130] PSR 2009, Regulation 6(5).
[131] S. Padmalatha and J. Paul, *Management of Banking & Financial Service* (2nd ed, Pearson 2010) 500.
[132] Payments UK, 'The Second Payment Services Directive (PSD2)', July 2016, 1-20, 12 <http://www.paymentsuk.org.uk/sites/default/files/PSD2%20report%20June%202016.pdf> accessed 10 September 2016: See, e.g., PSR 2017, Regulation 98.

In addition, incident management processes have to be implemented in order to detect and classify security and operational incidents.[133] Statistical data about fraud and details about mitigation measures, as well as up-to-date security and operational risk assessments have to be provided to regulatory authorities on an annual basis.[134] When a major security or operational security event takes place, regulators have to be promptly notified and when customers are affected, they have to be alerted.[135]

The PSD2 mandated that the European Banking Authority ('EBA') must publish regulatory technical standards on strong customer authentication and secure communications by the beginning of 2017 and UK payment service providers had to comply with the PSR 2017.[136] When payment service providers fall short of these regulatory technical standards, liability does not rest with the customers (subject to the exceptions in the case of fraud or gross negligence by the consumer).[137] Such an approach to loss allocation is reflective of an acknowledgement that m-payments are a technology-driven system and that losses are most likely best reduced by the respective operators, as discussed in chapter 3, section 3.4.[138]

Further, a party, e.g., a merchant who does not provide strong customer authentication,[139] will incur liability for any unauthorised payments.[140] Accordingly, the PSR 2017 renders payments more secure since payment service providers have to demonstrate that they have adopted adequate measures to protect their customers against the heightened risk of

[133] PSR 2017, Regulation 99.
[134] Ibid.
[135] Ibid.
[136] European Banking Authority, 'EBA seeks input on strong customer authentication and secure communication under PSD2', 8 December 2015 <https://www.eba.europa.eu/-/eba-seeks-input-on-strong-customer-authentication-and-secure-communication-under-psd2> accessed 10 September 2016.
[137] Payments UK n 132, 12.
[138] R.J. Mann, 'Making Sense of Payments Policy in the Information Age' (2005) *Georgetown Law Journal* 93, 633-673, 638.
[139] PSR 2017, Regulation 100.
[140] Payments UK n 132, 12.

these new technological advances, including providing strong customer authentication, and those measures are also scrutinised by the regulator.

These regulatory requirements, heightened by the PSR 2017, thus provide increased customer protection in this new technological milieu which seemingly adopts a social welfare policy model via regulatory technical standards that are more interventionist in nature than voluntary codes of conduct. Although it could be argued that the PSR 2017 continues to focus on the consumer economic interest, this interpretation fails to account for the enforced allocation of liability to service providers in the event of a failure to comply or the imposition of regulatory scrutiny and monitoring by the state. Many of the provisions serve dual purposes in that they strengthen the industry itself through building consumer trust and confidence as well as protect consumers from the worst risks of m-payment technology, such as, fraud.

Indeed, Chapter 3 has confirmed that ICT standards are an important means to heighten consumer protection.[141] The PSR 2009 was not as prescriptive in this regard and more neoliberal in that it was intended to develop the market. However, under the PSR 2017, social welfare considerations, such as, protection against fraud, are much more prevalent. This perhaps represents a shift based on the progress of technology and the growth in number of these types of transactions.[142] Whilst it is not possible to cover every single aspect of a payment service transaction, the subsequent sections focus on issues of information asymmetry, unauthorised payments, whether by the m-payment provider or a third party, and complaints/dispute resolution and the ways in which the regulations aim to protect consumers and/or develop the market in terms of these issues.

---

[141] J. Winn and N. Jondet, 'A "New Approach" to Standards and Consumer Protection' (2008) *Journal of Consumer Policy* 31, 459-472, 459.

[142] A. Ashta, 'Evolution of Mobile Banking Regulations: A Case Study on Legislator's Behavior' (2017) *Strategic Change: Briefings in Entrepreneurial Finance* 26(1), 3-20.

4.3.3.1 Issues of information asymmetry and consumer understanding

The problem of information asymmetry between payment service providers and customers has been legally addressed as customers must be provided with information before they enter into payment service contracts and framework contracts[143] and information must be communicated in easily understandable language.[144] Under the PSR 2009, it was up to the payment service provider to establish that a service user had not given his authority for a transaction, or to show that the payment transaction was incorrect or a payment was the result of technical problems.[145] PSR 2017 goes further by requiring the correction of the error and providing that consumers should be better informed of, and able to enforce, their rights.[146] Accordingly, the burden of proof fell on the payment service provider and not the customer. Consumer social welfare is thus being promoted since customers do not have to overcome insurmountable evidential issues when legally challenging payment service providers. Moreover, a recorded payment is not sufficient to establish the authenticity of the transaction or that the payer acted fraudulently or with gross negligence.[147] In other words, payment service providers cannot easily argue that their customers were to blame. Under the PSR 2017, customers also receive similar protection, giving consumers a greater sense of safety.[148]

[143] PSR 2017, Part 6.
[144] PSR 2017, Regulation 55.
[145] PSR 2017, Regulation 60.
[146] Ibid.
[147] PSR 2017, Regulation (3)(a)-(b).
[148] See, e.g., PSR 2017, Regulation 137.

4.3.3.2 Security and unauthorised payments, whether by the bank or a third party

Under the now repealed Regulation 61 of the PSR 2009, payment service providers had to refund the unauthorised amount or restore the debited amount. Furthermore, customers were required to pay no more than £50 where the payment instrument had been lost or stolen, or they had not kept their personalised security feature safe.[149] Such an approach protected vulnerable m-payment customers to a reasonable extent as payment service providers were responsible for refunding the customer the full amount,[150] so long as the claim was made within eight weeks.[151] This did not apply to cases of fraud, however, or where the customer, with intent or gross negligence, had not complied with Regulation 57. This Regulation required adherence to the terms and conditions and reporting of any loss, theft, appropriation or unauthorised use of the payment instrument without undue delay.[152] The meaning of 'undue delay' was not, however, defined by the PSR 2009, and Regulation 57 did not apply to payments relating to the use of a credit card.[153]

A balance was, therefore, struck under the PSR 2009. On the one hand, the customer was required to discharge certain duties and act at least in a reasonably circumspect fashion, thus a neoliberal attitude to the individual was adopted. On the other hand, they had a right to a refund in cases of theft, loss or the failure to keep security features safe. For example, an error on the customer's part in terms of safeguarding his/her personalised security feature and device did not bar them from seeking a refund from their bank,[154] with their liability being capped at £50. This appeared to promote a social welfare-based model of consumer protection. However, a failure to adhere to terms and conditions with gross negligence

[149] PSR 2009, Regulation 62.
[150] PSR 2009, Regulation 63.
[151] PSR 2009, Regulation 64(1).
[152] PSR 2009, Regulation 62(2).
[153] PSR 2009, Regulation 52.
[154] PSR 2009, Regulation 58(2).

operated as an exemption.[155] The customer's right to a refund was thus not unlimited. Otherwise, business interests would not be adequately protected and, as is often the case, UK law aims to create a balance between neoliberal and social welfare principles.

There is some material similarity between the PSR 2017 and the PSR 2009. For instance, the PSR 2017 retains the 'gross negligence' exemption in Regulation 77 (3) (b). The exclusion of the payment service provider's liability in situations of 'gross negligence' by the payment service user raises a definitional issue. It is the researcher's view that what may be considered a grossly negligent failure to adhere to terms and conditions has not been adequately explained. A lack of clarity in terms of the meaning of 'gross negligence' is problematic as it offers the potential for abuse, with m-payment providers reneging on their responsibilities.

The PSR 2017 also provides customers with a right to an automatic refund within eight weeks, starting on the date when the funds were taken, even in circumstances where the facts giving rise to the refund are disputed.[156] In addition, aside from cases of gross negligence or fraud, the PSR 2017 has reduced the liability of payers who are required to pay no more than £35.[157] Hence, consumers do not stand to lose a lot when unauthorised payment transactions are made and the risks posed by m-payments services are legally mitigated.

As with the PSR 2009, a customer is entitled under the PSR 2017 to bring legal action when s/he suffered losses due to a payment institution acting without their permission.[158] A customer can also pursue proceedings against a payment service provider for failing to

[155] PSR 2009, Regulation 60(3).
[156] PSR 2017, Regulation 79; Payments UK n 132, 9.
[157] PSR 2017, Regulation 77.
[158] PSR 2017, Regulation 21.

comply with safeguarding requirements.[159] They further have the right to bring action when a payment service provider fails to comply with requirements concerning single payment service contracts, framework contracts, common provisions or the authorisation or execution of payment transactions on their time and value date and this has caused them a loss.[160] For instance, they can argue that a payment provider's failure to credit the amount stated in a payment order by the end of the business day has been detrimental.[161] Such an approach is actually quite social welfare-centred and paternalistic in its conceptualisation of the consumer as someone needing state protection since it is premised on the assumption that the consumer is either unaware of where their interests lie or unable to act independently to protect them.

The overarching approach of the PSR 2017 nevertheless highlights a neoliberal pro-business policy orientation. It raises the possibility of a hybrid approach whereby neoliberal ideals of competition and efficiency of markets requiring minimal state intervention are retained subject to the demands of consumer welfare considerations. This 'mixed' approach offers the flexibility to accommodate and respond to the rapid technological changes and, relatedly, the risks that come with mobile ICT, detailed in chapter 2, sections 2.2.1 to 2.2.3.

The PSR 2009 did not fully shield vulnerable customers because it depended on the customer having to make a claim or to initiate legal proceedings which some may not be empowered to do. By contrast, the PSR 2017 furthers social welfare concerns more than the PSR 2009 since customers are granted the automatic right to a refund unless there is evidence of 'gross negligence' on the customers' part.[162] This greatly reduces the risk posed to customers using the new technology. Ashta welcomes the development as a natural development in the evolution of regulatory approach within the European Union, and regards

[159] PSR 2017, Regulation 23.
[160] PSR 2017, Part 6.
[161] PSR 2017, Regulation 86.
[162] PSR 2017, Regulation 79.

the new regulation as a first step rather than an end goal of regulation in this burgeoning area of technology.[163] The principal reason for this view is simply that the technology itself is still at a relatively young stage by comparison to its potential. It is inevitable that these regulations will in time reveal their flaws and weaknesses and give rise to demands for reform and become outdated and will thus require revision in order to respond to new, as yet unknown, risks and challenges. Consumer attitudes will similarly develop with time.

4.3.3.3 Complaints/dispute resolution

Under the PSR 2009, there were differences in the complaints handling procedures between payment services providers and firms that carried out other regulated financial activities. While the latter had to record complaints, compile complaint statistics and publish complaint data, the former did not have to do this.[164] However, businesses had to inform customers about their complaint procedures. The Financial Ombudsman Service ('FOS') further enabled customers to resolve complaints about payment services informally and out of court.[165] Consumer protection interests were thus slightly watered down due to the laxer complaints handling procedures for payment service providers; hence, a more neoliberal promotion consumer economic interests occurred. Indeed, new entrants into the market were not overburdened, but, in fact, treated less strictly. Nevertheless, the requirement to adopt complaints procedures and the ability to escalate complaints to the FOS without any legal fees reflects that social welfare-based consumer protection interests were not ignored.

[163] Ashta n 142.
[164] FSA, 'The FSA's role under the Payment Services Regulations 2009: Our approach', 2012, 108-109 <http://www.fca.org.uk/static/fca/documents/fsa-psd-approach-latest.pdf? accessed 28 May 2013.
[165] Ibid 108-110.

Under the PSR 2017, social welfare considerations are further heightened by setting out a clearer set of procedures for complaints handling.[166] Payment service providers now have to adopt dispute resolution procedures and reply to complaints within fifteen business days.[167] Where a complaint is upheld by the FOS, the FOS can award compensation of up to £150,000 to a consumer who has been deprived of money or for an investment loss or inconvenience, distress or other non-financial loss.[168] This is likely to spur payment service providers to act with additional vigilance and due care when delivering m-payment services and thus mitigates the risk to consumers.

In addition, private persons can, by virtue of s150 of the Financial Services and Markets Act 2000 ('FSMA'), bring actions for any contraventions by an authorised institution which result in a loss.[169] A 'private person' is defined under s3(1) of the FSMA (Rights of Action) Regulations 2001 as any person, who suffers a loss and the loss does not occur whilst he is pursuing a regulated activity or carrying on any business or acting as a shareholder.[170] If a private person successfully establishes that a loss is due to such a contravention, damages may be awarded.[171]

Customers may find it more practical to informally resolve complaints via the FOS since civil proceedings are costly and time-consuming.[172] The option of alternative dispute resolution through the FOS enables customers to pursue their rights and hold service providers to account. This promotes a social welfare-based consumer protection interest by

[166] Payments UK n 132, 9.
[167] Ibid.
[168] FOS, Compensation, 2013 <http://www.financial-ombudsman.org.uk/publications/technical_notes/compensation.html> accessed 28 May 2013.
[169] BCOBS, Schedule 5.
[170] *Sivagnanam v Barclays Bank Plc* (2015) EWHC 3985 (Comm).
[171] FSMA 2000, s138D; cf *Sivagnanam v Barclays Bank Plc* (2015) EWHC 3985 (Comm); B. Donnelly and J. Pratt, Mis-selling claims: Court of Appeal Guidance, Macfarlanes, 2010 <http://www.inhouselawyer.co.uk/index.php/litigation-a-dispute-resolution/8274-mis-selling-claimscourt-of-appeal-guidance> accessed 28 May 2013.
[172] G. Slapper and D. Kelly, *English Legal System 2009-2010* (8th ed, Routledge-Cavendish 2009) 183.

making the rights and protections available to consumers more tangible and easily accessible; in many cases, the mere threat that a consumer can easily enforce against the provider will be sufficient to ensure compliance. Indeed, consumers do not have to rely on private ordering, which suggests a dilution of a neoliberal approach being pursued. The majority of m-payments are likely to be low value transactions and thus a customer is less likely to wish to become involved in litigation given the stress, risk, and expense associated with this route.[173] In this respect, consumer protection, arguably, may not be as effective as expected and the risks posed by using technology for small transactions might still remain.

4.3.3.4 The role of the payment systems regulator and the furtherance of the consumer protection rationale

Customers are still indirectly protected since the Payment Systems Regulator ('PS Regulator')[174] is equipped with various powers to enforce these Regulations, including the right to order financial sanctions.[175] The objective of the PSR Regulator is threefold: Competition; innovation; and service user.[176] To this end, it has a broad range of powers including the power to obtain information or documents,[177] to conduct investigations[178], and to enter premises under warrant.[179] The existence of this office is indicative of an underlying policy of consumer protection as it provides a means of enforcement independent of complaints by affected consumers; the consumer interest is protected even where the

[173] F. Teruel, 'Low and Slow' Is How the Credit Card Fraudsters Roll', ThreatMetrix, 5 April 2018 <https://www.threatmetrix.com/digital-identity-blog/fraud-prevention/low-and-slow-is-how-the-credit-card-fraudsters-roll/> accessed 15 April 2019.
[174] Financial Services (Banking Reform) Act 2013, s40.
[175] PSR 2017, Regulations 108-117, particularly Regulation 85; see also BCOBS, Schedule 5.
[176] Financial Services (Banking Reform) Act 2013, s49.
[177] Financial Services (Banking Reform) Act 2013, s81.
[178] Ibid, ss83-84.
[179] Ibid, s88.

individual takes no action whatsoever to protect themselves. Paternalistic and interventionist legal regulations have thus been additionally adopted and thus promote social welfare considerations.

Whilst monetary sanctions may potentially involve large sums of money, it is questionable as to whether they might provide sufficient deterrent for m-payment providers, particularly if the financial gains from breaches of the Regulations exceed the penalties.[180] For example, Norwich Union was fined £1.26 million in December 2007 for not properly organising its risk management system, which exposed customers to an increased risk of fraud, showing that financial institutions are willing to put consumers' financial well-being in peril to make a profit.[181] Thus a neoliberal-oriented concept of regulation might still be seen to be at play. This is because the provider may make the economic assessment that the payment of the fines is less costly overall than the implementation of a proper risk management system. This may lead to the consumer protection objective not being realised as the payment of the fine does not benefit the wronged consumer.

Nonetheless, the PSR 2017 has created legal channels to protect customers and enable customers to enforce their rights and facilitate the resolution of complaints and disputes. There are, arguably, still issues in terms of the implementation of these procedures, especially in terms of more vulnerable customers or those facing errors in terms of smaller transactions. However, codes of conduct exist to shore up consumer protection, as discussed next.

[180] I. Walter 'Conflicts of interest and market discipline among financial service firms' (2004) *European Management Journal* 22(4), 361-376.
[181] FSA, 'FSA fines Norwich Union Life £1.26m for exposing its customers to the risk of fraud', 2007 <http://www.fsa.gov.uk/library/communication/pr/2007/130.shtml> accessed 29 March 2013.

4.3.4 Codes of conduct, consumer understanding and protection against unauthorised payment transactions

The PSR 2009 was supplemented by the FCA's Banking Conduct of Business Sourcebook ('BCOBS') and the voluntary Standards of Lending Practice 2016 for personal customers published by the British Bankers Association ('BBA'). Schedule 6 of the PSR 2017 provides that any breach of these rules of conduct might give rise to an action for damages under s150 of the FSMA 2000, thus giving the BCOBS some clout in terms of enforcement.

As with the PSR 2009[182] and the PSR 2017[183], the BCOBS addresses the issue of information asymmetry. The BCOBS Handbook requires that adequate information is given, that the right method of communication is used, as well as the utilisation of simple and easily understood language.[184] It further emphasises the importance of treating customers fairly, safeguarding their interests and providing for their informational needs, including ensuring that the material provided is 'clear, fair and not misleading.'[185]

As mentioned above, the complexity of the technology used in m-payment systems means that it is vital that m-payment providers make the nature of the risk and the rules involved clear in order to both protect and make liable the service's end users. Customers should be given enough notice when terms and conditions are changed.[186] Hence, service agreements have to adhere to these additional requirements. The BCOBS gives the customer some degree of rights where there has been a failure to provide necessary information about the specific application of the technology and systems involved and these rights may give rise to action for damages under s150 of the FSMA.

[182] PSR 2009, Part 59.
[183] PSR 2017, Part 6.
[184] BCOBS 4.1.1R.
[185] BCOBS 2.1.1G.
[186] BCOBS 4.1.2G.

4.3.3.1 Unauthorised payment transactions and how customers may still be vulnerable

As pointed out in chapter 3, information disclosure by itself does not sufficiently safeguard consumers, especially vulnerable ones. A neoliberal approach assumes that customers are able to adequately utilise information, an assumption which behavioural economists strongly refute for a number of reasons as noted in chapter 3.

However, the regulatory rules impose conditions to mitigate against the risk of unauthorised payments, whether by the financial institution or a third party, in pursuit of consumer protection: Refunds of unauthorised payments have to be issued 'within a reasonable time'.[187] The BCOBS reiterates the position taken in the PSR 2017, i.e., it states a cap of £35 on customers' liability when their payment instrument is stolen or lost, or is not kept safe.[188] This reinforces a more social welfare-based approach which limits the liability of the individual. A financial institution may only hold a customer fully liable for unauthorised payments for gross negligence and fraud, so business interests are also covered.[189] In this way, a balance is seemingly struck between allowing for economic expansion and mitigating the risks of consumers via a combination of the neoliberal and social welfare models.

[187] BCOBS 5.1.11R.
[188] BCOBS 5.1.12R.
[189] BCOBS 5.1.12(2)R.

4.3.3.2 The Standards of Lending Practice 2016 and consumer understanding

Apart from the BCOBS, the Standards of Lending Practice 2016 ('SLP'), a voluntary code sponsored by the BBA and the UK Cards Association,[190] apply to personal customers. The Lending Standards Board are responsible for the SLP.[191] The SLP provides additional independent guidance and governs services with consumers, but it only deals with current account overdrafts, credit cards and loans.[192] This means that the SLP has limited application since it arguably applies only to payment services, including m-payments, which involve the use of such credit facilities.

As a voluntary code, the SLP is only binding to the extent that its members have subscribed to it.[193] There are, however, no financial penalties or security consequences for a bank that is in breach of the code, other than censure from the Lending Standards Board itself.[194] This code, therefore, constitutes an example of private regulation by the banking sector that is typical of the neoliberal approach discussed in chapter 3, section 3.4, as it favours individual autonomy and self-regulation.

The extent to which a customer may rely upon the SLP in the case of disputes is of importance as it may be argued that a bank has acted against its own self-enforced rules of good practice. This may perhaps help to give rise to claims of negligence or a breach of contract. Voluntary codes, including the SLP, are not normally treated as implied terms, and

---

[190] Lending Standards Board, 'The Standards of Lending Practice, Personal Customers, July 2016, 1-12, 1 <https://www.lendingstandardsboard.org.uk/wp-content/uploads/2016/07/Standards-of-Lending-Practice-July-16.pdf> accessed 10 November 2016.

[191] The Prudential Regulation Authority ('PRA') and the Financial Conduct Authority ('FCA') replaced the FSA on 1 April 2013. See FSA, Regulatory Reform- background, 2013 <http://www.fsa.gov.uk/about/what/reg_reform/background> accessed 1 April 2013; BBC, UK financial regulation overhauled, 2013 <http://www.bbc.co.uk/news/business-21987829> accessed 27 May 2013.

[192] Lending Standards Board, 'The Standards of Lending Practice', 2016 <https://www.lendingstandardsboard.org.uk/the-slp/> accessed 10 November 2016; G.M. Andrews and R. Millett, *Law of Guarantees* (6th ed, Sweet & Maxwell 2012) 573.

[193] P. Hood, *Principles of Lender Liability* (OUP 2012) 230.

[194] Ibid.

therefore do not form part of the contract unless specifically incorporated.[195] They mainly form part of the background of reasonable expectation by reference to which the court would interpret the contract.[196] However, voluntary codes, such as, the SLP, have considerably less strength in that a bank may, from a risk management perspective, consider any cost of litigation which may arise from a breach of good practice could be less costly than implementing it. A bank may therefore choose to simply ignore the SLP. Nevertheless, as the SLP is not the only available tool within a matrix of regulatory measures to protect m-payment customers, this may not be a serious issue in terms of consumer protection. Indeed, another important legal measure to shield m-payment customers is the law governing unfair terms and conditions, which is discussed next.

4.4.1 The CRA 2015: Performance of a contract, unfair terms and consumer understanding

Institutions set out the applicable terms and conditions for m-payments in a written contract. Freedom of contract bestows private autonomy and forms one of the backbones of a market economy.[197] M-payment providers might limit their potential liability through tightly drafted m-payment service agreements which may reduce protection of consumers' rights.[198] However, such a neoliberal approach is restrained by the Consumer Rights Act 2015 ('CRA 2015') and the related case law which deals with unfair terms. It is, therefore, an expression of the social welfare consumer construct discussed in chapter 3, section 3.4. This section

[195] R. Shah et al, *Something to Believe In: Creating Trust and Hope in Organisations: Stories of Transparency, Accountability and Governance* (Routledge 2003) 155-156.
[196] Ibid.
[197] S. Grundmann and Y.M. Atamer, *Financial Services, Financial Crisis and General European Contract Law, Failure and Challenges of Contracting* (Kluwer Law International 2011) 56.
[198] *Midland Bank Ltd v Hett, Stubbs, Kemp & Co (A Firm)* (1979) Ch 384.

analyses the extent to which the CRA 2015 confers additional protection on customers who use new technologies.

It is examined to which extent consumers can challenge unfair terms and conditions contained in their m-payment service agreements under the CRA 2015. In light of the case law, section 4.4 highlights the ways in which UK regulation of this market has tried to balance neoliberal principles involving the development of consumer choice and a free market with notions of social welfare.

4.4.2 Contract law and tort law and the exclusion of liability

As discussed in section 4.3.2, m-payment providers must provide services with reasonable care and skill.[199] Reasonable care has to be taken when, e.g., carrying out an electronic payment order[200] and other functions.[201] While contractual liability arises from a breach of a term of the contract,[202] tortious liability results from non-contractual wrongdoing, such as, a breach of a duty of care in common law negligence.[203] This distinction is illustrated by Lord Scarman in *Tai Hing Cotton Mill v Liu Chong Hing Bank Ltd*[204] where he stated that, "the parties' mutual obligations in tort can[not] be greater than those to be found expressly or by necessary implication in their contract."[205]

---

[199] See CRA 2015, s2(3); *Overy* v *Paypal* (*Europe*) *Ltd* [*2012*] EWHC 2659 (QB), [2013] Bus LRD1; *Domsalla (t/a Domsalla Building Services) v Dyason* (2007) EWHC 1174 (TCC), (2007) BLR 348; see also CRA 2015 s49; Supply of Goods and Services Act 1982, s13 also implies a statutory duty to take care and skill, but this only applies to business to business dealings and not to business to consumer dealings.
[200] *Royal Products v Midland Bank* (1981) 2 Lloyds Rep 194, 198.
[201] J.S. Ziegel and S. Lerner, *New Developments in International Commercial and Consumer Law* (Hart Publishing 1998) 111.
[202] H. Beale et al, *Contract: Cases and Materials* (5th ed, OUP 2007) 3.
[203] C. Von Bar and U. Drobnig, *The Interaction of Contract Law and Tort Law and Property Law in Europe: A Comparative Study* (Sellier European Law Publishers 2004) 138.
[204] (1985) 2 All ER 947.
[205] Ibid 957-958.

Following this case, the scope of liability in m-payment service agreements cannot be more extensive in tort than in contract. Put differently, the contract defines the areas in relation to which a duty of care arises.[206]

A duty of care in tort generally arises when the following three-stage test is met[207]: It must be reasonably foreseeable that the defendant's behaviour causes damage to the claimant. There must exist sufficient proximity between the claimant and the defendant. It must be just, fair, and reasonable to impose a duty. However, m-payment providers are likely to use terms governing liability, access and usability of services that are subject to caveats so that they do not breach their duty of care by providing customers a ubiquitous right to a fail-proof system. For example, m-payment providers may qualify twenty-four-hour access to services in m-payment service agreements by stating exceptions, such as, updates, maintenance, cyber-attacks and force majeure events. The case of *Hedley Byrne v Heller*[208] highlights that it is possible to prevent the imposition of liability through the inclusion of a disclaimer, despite a finding of the common law duty of care having been breached.

Nonetheless, m-payment providers cannot incorporate exemption or limitation clauses into m-payment service agreements which contravene the CRA 2015.[209] Exemption clauses limit liability entirely while a limitation clause tries to restrict liability to a particular amount.[210] S65(2) of the CRA 2015 provides that negligence liability cannot be excluded by a person merely agreeing to or knowing about such a term, or receiving a consumer notice. This includes secondary contracts,[211] e.g., where a consumer has received the primary

[206] von Bar and Drobnig n 203, 203.
[207] *Caparo Industries plc v Dickman* (1990) UKHL 2.
[208] (1964) AC 465.
[209] Previously consumers were protected by virtue of the Unfair Contract Terms Act 1977 ('UCTA') and the Unfair Terms in Consumer Contracts Regulations 1999 ('UTCCR'). However, the UCTA no longer governs business to consumer contracts, whilst the UTCCR is replaced in its entirety by the CRA 2015.
[210] K. Kuhnel-Fitchen and T. Hough, *Optimize Contract Law* (Routledge 2014) 76.
[211] CRA 2015, s72.

internet banking service agreement and, additionally, enters into a m-payment service agreement.

Also, m-payment consumers do not only have to rely on negligence liability under the common law.[212] They can additionally rely on s49 of the CRA 2015 which implies a duty to supply services with reasonable care and skill. This duty is similar to one of the requirements under the Islamic good faith principle not to sell a thing which is defective, as discussed in chapter 3, section 3.6.1. When this statutory duty is breached, the CRA 2015, s54(3) provides the rights to demand repeat performance and a price reduction. More importantly within the context of m-payments, s54(7) stipulates that the remedies include, for instance, to seek monetary compensation. A term can thus not be used to exonerate or limit a m-payment provider for breaching this duty under a service contract.[213] Hence, the restriction or exclusion of remedies or rights is blacklisted.[214] Anything which has been written or said about the service is also considered to form part of the contract, except when conditions have been included.[215] Equally, under the Islamic good faith principle, discussed in chapter 3, section 3.6.1, anything said during the pre-contractual stage is taken into account.

In the m-payment context, UK consumers are thus assured that negligence liability and the duty to supply the services with reasonable care and skill [216], e.g., due to an operational mistake, cannot be excluded. The statutory right to have the service performed with reasonable care and skill, along with the tortious common law duty of care, confers on customers a high amount of protection in the m-payment context, which indicates a furthering

[212] CRA 2015, s65(4)(b).
[213] CRA 2015, s57.
[214] CRA 2015, s57; Competition & Markets Authority, 'Unfair contract terms guidance, Guidance on the unfair terms provisions in the Consumer Rights Act 2015', CMA 37, 31 July 2015, 1-144, 61.
[215] CRA 2015, s50.
[216] CRA 2015, s49 and s 65(4)(a)-(b).

of a social welfare-based model of consumer protection. Accordingly, a m-payment provider must shoulder some negligence liability.

Moreover, m-payment providers must also ensure that their contract terms and notices are prominent and transparent.[217] They must be worded in intelligible and plain language, as they can otherwise be challenged under Part 2, s62 of the CRA 2015.[218] These disclosure provisions are reflective of a market-based disclosure approach towards consumer protection, as e.g. advocated in the UN Guidelines on Consumer Protection, discussed in chapter 3, section 3.2. Nonetheless, the adoption of a fairness test in s62 tempers the classical assumption that a contract is a bargain between equals.[219] It results in the unfair term in the consumer contract or the unfair consumer notice not binding the consumer,[220] except if the consumer decides to rely on it.[221]

The fairness test goes some way to protect vulnerable parties and to a certain extent helps to realise fair outcomes.[222] The Law Commission explains that the main role of unfair terms laws is to avert that consumers face unfair surprises.[223] However, such legislation is not meant to resolve all issues which arise from a market place, including those which are the result of the consequences of consumer's poor decision making.[224]

As a result, the fairness test is not applied to all contract terms and notices and a term which is prominent and transparent[225] and "specifies the main subject matter of the contract"

[217] CRA 2015, ss 64(2) and 68.
[218] CRA 2015, s64(3).
[219] M.S. Hussain, 'The Reasonableness of the UCTA 1977's Test of Reasonableness' (2017) SSRN Electronic Journal, 1-4, 1 <10.2139/ssrn.3058489> accessed 1 March 2019.
[220] CRA 2015, s62(1)-(2).
[221] CRA 2015, s62(3).
[222] Hussain n 219.
[223] Law Commission, 'Unfair Terms in Consumer Contracts: a new approach?', Issues Paper, 25 July 2012, para.3.4.
[224] Ibid.
[225] CRA 2015, ss64(2) and s68.

or to assess "the appropriateness of the price payable...by comparison with the services supplied..." is excluded.[226] A prominent term is one which has been brought to an average "consumer's attention"[227], namely one "who is reasonably well-informed, observant and circumspect."[228] The term or notice is transparent if it is written in plain and intelligible language and is legible.[229]

Unfairness is found to exist when a term or notice is contrary to the notion of good faith and causes a significant imbalance in the parties' rights and obligations under the contract to the detriment of the consumer.[230] Courts consider "the nature of the subject matter of the contract", "all the circumstances existing when the term was agreed" and "all of the other terms"[231] and the non-exhaustive examples contained in Schedule 2.[232] However, the CRA 2015 does not define good faith because this is a flexible concept.[233] The UK approach reflects that English legislation has moved from the good faith principle to the principle of fairness when it comes to consumer protection, unlike the Islamic approach.

In *Director General of Fair Trading v First National Bank plc,*[234] Lord Bingham observed that 'good faith' necessitates, 'fair and open dealing'.[235] He explained that 'good faith' requires terms to be stated in their entirety and in a legible and clear manner, without any traps.[236] Onerous terms ought to be more prominent.[237] A consumer who is in need, has no experience, is unfamiliar or has insufficient leverage to bargain should, furthermore, not

[226] CRA 2015, s64(1).
[227] CRA 2015, s65(4).
[228] CRA 2015, s65(5).
[229] CRA 2015, s68(2).
[230] CRA 2015, s62(4) and (6).
[231] CRA 2015, s62(5)(a)-(b).
[232] J. Beatson, A.S. Burrows, J. Cartwright, *Anson's Law of Contract* (30th ed, OUP 2016) 223.
[233] L. Roach, *Card and James' Business Law* (4th ed, OUP 2016) 223.
[234] (2001) UKHL 52.
[235] Ibid at [17].
[236] Ibid.
[237] Ibid.

be exploited.[238] However, subsequent cases have construed 'good faith' more narrowly and this might undermine consumer protection in the risk-filled world of m-payment transactions.[239] Nonetheless, whilst under the Unfair Terms in Consumer Contracts Regulations 1999 it fell on the consumer to prove unreasonableness,[240] it appears that it now falls on the court to determine whether a term should be considered fair, despite a consumer not having pleaded this.[241] Such judicial oversight appears to be a proactive approach towards consumer protection. When comparing the Islamic good faith principle, discussed in chapter 3, section 3.6.1, it becomes apparent that the CRA 2015 and the therein contained fairness test are much more sophisticated and effective in regulating exclusion of liability clauses.

4.4.3 Possible issues with information disclosure and transparency and consumer understanding

Vulnerable consumers may be insufficiently protected because information disclosure and transparency may be inadequate protection mechanisms. As discussed in chapter 3, behavioural science research confirms that providing information is not enough, as customers often agree to standard contract terms without reading the contract.[242] However, as apparent from the analysis in the previous section, there are aspects of the CRA 2015 that go beyond a disclosure and transparency requirement which show some regard of social welfare considerations.[243] In particular, the CRA 2015 provides dispute resolution mechanisms (which will be compulsory in the financial services sector) to make rights more easily

[238] Ibid.
[239] *Mid Essex Hospital Services NHS Trust v Compass Group UK and Ireland Ltd (t/a Medirest)* (2013) EWCA Civ 200; *TSG Building Services plc v South Anglia Housing Ltd* (2013) EWHC 1151 (TCC).
[240] J. Poole, *Textbook on Contract Law* (13th ed, OUP 2016) 277.
[241] CRA 2015, s71; ibid (Poole).
[242] Chapter 3, pp126-130.
[243] E.g. see CRA 2015, s49.

enforceable and therefore more meaningful for consumers.[244] It has tightened the approach to unfair terms in service agreements where the consumer has little opportunity to negotiate to prevent abuse of this advantage by service providers.[245] In contrast, the analysis of the Islamic consumer protection jurisprudence in chapter 3, section 3.6, has demonstrated that no effective rights and remedies have been developed for consumers to challenge unfair clauses in service contracts, including m-payment service contracts.

4.4.4 Unauthorised payment transactions and ambiguous and unfair contract terms

The CRA 2015 provides safeguards for consumers by construing any ambiguous terms in a way which favours the consumer,[246] thereby retaining the approach taken in regulation 7(2) of the repealed Unfair Terms in Consumer Contracts Regulations 1999 ('UTCCR'). The CRA 2015 lists various terms which may be deemed unfair[247] and consumers may try to argue that some of these can be found in their m-payment service agreements.

For instance, m-payment providers cannot include terms which effectively limit or exclude the legal rights of the consumer in an inappropriate manner, i.e., they cannot contract out of their statutory obligations, including those under the PSR 2017.[248] However, the list of examples is not exhaustive. When such a term is found, it is not automatically deemed unfair.[249] Instead, this is best conceived as a grey, rather than black, list of unfair clauses, which is very similar to that contained in the UTCCR, except that additional examples have

[244] See section 4.3.3.3 above; Department for Business Innovation & Skills, 'Businesses get ready for new consumer laws', 2015, 1 <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/464208/Consumer_Rights_Act_2015_BIS_media_release.pdf> accessed 1 March 2019.
[245] See CRA 2015, Chapter 4.
[246] *Photo Production v Securicor* [1980] AC 827; *Ailsa Craig Fishing v Malvern Fishing* [1983] 1 WLR 964; CRA 2015, s69.
[247] CRA 2015, Schedule 2 Part 1.
[248] CRA 2015, Schedule 2, Part 1, para 2.
[249] J. O'Sullivan and J. Hilliard, *The Law of Contract* (7th ed, OUP 2016) 213.

been included.[250] Consequently, the examples indicate what may constitute prima facie cases of 'significant imbalance', though the courts may not necessarily consider any such term as causing a significant imbalance of information communication.[251]

As observed by Jackson LJ, the scope of the duty of good faith is heavily dependent on the context and this may effectively undermine consumer protection and policy attempts to further social welfare in this area.[252] For example, in *West v Ian Finlay & Associates,*[253] albeit a case that predates the CRA 2015, the court assessed whether a net contribution clause in a construction contract was fair. The Court of Appeal explained that, for a term to be deemed unfair and lacking in bad faith, mere imbalance was insufficient; there had to be a *significant* imbalance. O'Sullivan and Hilliard label this decision as 'surprisingly hard-nosed'.[254] Given that a consumer generally has little, if any, opportunity for negotiation and has to accept contractual terms on a 'take it or leave it' basis, the court's decision broadens the scope for service providers to take advantage of their position of power.[255] Accordingly, consumers may find it challenging to argue that a term in a m-payment service agreement is unenforceable which gives power to businesses, promoting a neoliberal conception of the law.

In respect of penalty clauses, i.e., a term 'which has the object or effect of requiring a consumer who fails to fulfil his obligations under the contract to pay a disproportionately high sum in compensation',[256] the position is different.[257] A term is a penalty clause when a secondary duty results in a detriment for the party who breaks the contract which is in excess

[250] See e.g. paras 5, 12 and 14 of Schedule 2, Part 1 of the CRA 2015; ibid.
[251] O'Sullivan and Hilliard n 249.
[252] *Mid Essex Hospital Services NHS Trust v Compass Group UK and Ireland Ltd (t/a Medirest)* (2013) EWCA Civ 200, at [112].
[253] (2014) EWCA Civ 316, (2014) BLR 324.
[254] O'Sullivan and Hilliard n 249.
[255] Ibid.
[256] CRA 2015, Schedule 2.
[257] Roach n 233, 320.

of what the innocent party legitimately expects to enforce its primary duty.[258] This requires assessing whether any legitimate business interests are furthered and safeguarded by the term and whether the term is unconscionable, exorbitant and profligate.[259] In the context of m-payments, however, customers who fail to adhere to their secondary duties, e.g., failing to maintain up-to-date antivirus software, should not be penalised excessively. This furthers a social welfare-based conceptualisation of the consumer as vulnerable, rather than circumspect in accordance with neoliberal philosophy. It is also consistent with the limitation of liability imposed on the consumer to £35 except in a case of gross negligence under the PSR 2017.[260] Both provisions prevent liability being transferred to the consumer even in circumstances where the consumer may have agreed (albeit possibly unwittingly) to assume this.

More extensive consumer protection is provided by the statutory obligations imposed on banks and payment institutions under the PSR 2017 than the common law. Under the common law, the consumer bears the burden of establishing the component elements of the tort of negligence in such situations, presenting evidential difficulties which would tend to undermine customer protection when using the new fiscal technologies.[261] Statutory interventions, such as, the PSR 2017 reverse this position.[262] Where the regulator finds a m-payment provider liable for failing to comply with the PSR 2017 (for example because of insufficient security procedures as discussed above), that finding can be relied on by the consumer in mounting a challenge to ambiguous or unfair terms.

[258] *Cavendish Square Holding BV v Makdessi; ParkingEye Ltd v Beavis* (2015) UKSC 67, (2015) 3 WLR 1383, at 32.
[259] Ibid per Lord Mance at [152].
[260] PSR 2017, Regulation 75.
[261] M. Spencer, J. Spencer, *Evidence* (4th ed, OUP 2015) 27.
[262] *Director General of Fair Trading v First National Bank plc* (2000) 1 All ER 240, per Lombe-Evans J at [254].

However, it may be argued that a term which permits m-payment providers to make subsequent changes to the 'characteristics of the subject matter' is an unfair term.[263] For example, the terms and conditions for the Pingit app provided that Barclays can make 'other small changes to the terms and conditions' and that users, 'who are not happy with these changes, [...] can cancel [their] registration or delete the app'.[264] It is conceivable that a similarly worded term which permits not just minor but also more substantive changes may be challenged. Equally, a term which permits the unilateral alteration of the provision of m-payment services without any good reason could be challenged by consumers.[265] For example, changes which affect the free-standing rights of the consumer, such as, the right to a refund, may not be validly altered by the m-payment provider's unilateral action. Similarly, a m-payment provider may not restrict or impose conditions upon its liability for either its own breaches or those of third parties which the m-payment provider relies upon to perform elements of the service promised to the consumer.[266] These examples indicate that the CRA 2015 provides customers with some protection from the risks of the new fiscal technologies, which promotes the social welfare model.[267]

4.4.3.1 Potential problems with the CRA 2015: Permitting m-payment providers to exclude liability

M-payment providers may counter-argue that none of the examples in Part 1 of Schedule 2 of the CRA 2015 are clearly laid out. If they can show that their terms specify the price or 'the

[263] CRA 2015, Schedule 2, Part 1, para12.
[264] Barclays, 'Pingit terms and conditions', 2016 <http://www.barclays.co.uk/Mobile/BarclaysPingittermsandconditions/P1242604890843> accessed 10 September 2016.
[265] CRA 2015, Schedule 2, Part 1, para13.
[266] CRA 2015, Schedule 2, Part 1, para17.
[267] CRA 2015, Schedule 2, Part 1, para19.

main subject matter of the contract', which are previously understood to be the contract's core terms,[268] consumers will not be able to challenge those terms. The underlying rationale for excluding the price and main subject matter of the contract from the purview of the CRA 2015 is to prevent price and quality control.[269] Burrows, however, comments that the 'main subject' exclusion is problematic as past case law highlights that it is difficult to determine what the substance of the contract is and this lessens consumer protection and social welfare.[270] Equally, Lord Steyn commented in *Director General of Fair Trading v First National Bank*[271] that, in the context of the UTCCR, there is a risk that 'endless formalistic arguments' may be pursued regarding whether a term is, in fact, a core term.[272]

The same argument may be made about the CRA 2015, particularly in relation to what constitutes the subject matter of a contract. This effectively increases the legal risks for customers using m-payment technologies. It may be necessary to reconsider the traditional conception of 'core terms' to reflect the realities of the m-payment market and the concerns which may compel consumers to choose to take advantage of this technology. For example, a consumer may rely on representations made as to the security provisions put in place by the provider when choosing either to use the service or selecting between providers. From the consumer perspective, these terms may be more significant than those traditionally conceived as 'core' terms, such as, pricing and performance of the core obligation. It is important that consumers' priorities and expectations when using m-payment services are taken into account in determining whether terms ought to be construed as core terms. Additionally, the strength of such arguments depends on previously decided cases where the courts have had to debate whether a term should be struck down because of perceived unfairness. Whilst the older cases

[268] CRA 2015, s64(1).
[269] A. Burrows, *Principles of the English Law of Obligations* (OUP 2015) 41.
[270] Ibid; see, e.g., *Suisse Atlantique v Rotterdamsche Kolen* [1967] 2 QB 361.
[271] (2001) UKHL 52.
[272] Ibid, at [34].

were decided under the repealed UTCCR, they are, nonetheless, indicative of the stance which courts may adopt in respect of the CRA 2015.[273]

In this connection, the case of *Office of Fair Trading v Abbey National plc and Others ('Abbey National')*[274] is particularly instructive. It dealt with the issue of the reasonable charges that banks might impose for providing banking services and, more particularly, when the customer overdraws on an account without a pre-arranged overdraft facility. The Office of Fair Trading (OFT)[275] sought to challenge the imposition of charges on customers for using an unauthorised overdraft on the basis that the fees were disproportionate to the costs incurred by the banks and amounted to a penalty and were thus unlawful. The court at first instance held that the charges, while not penalties, could be challenged under the UTCCR. The Court of Appeal then affirmed that it had jurisdiction to determine whether or not the charges were fair. However, the Supreme Court held that neither the courts nor the OFT could consider whether the fairness of the term as it related to charges for provision of a service by the banks. The term thus fell within Regulation 6(2)(b) of the UTCCR and was a core term which could not be subject to scrutiny under the UTCCR. Lord Walker acknowledged that the 'First National Bank shows that not every term that is in some way linked to monetary consideration falls within Regulation 6(2)(b). Paras (d), (e), (f) and (l) of the "greylist" in Schedule 2 to the 1999 Regulations are illustration of that'.[276]

In the m-payment context, the same issue may arise when a customer seeks protection against unfair terms by relying on the CRA 2015. One may argue that certain terms cannot be challenged since they are not listed as examples in Schedule 2, Part 1 of the CRA 2015 and/or concern the price or govern the subject matter of the contract. The lack of clarity regarding

[273] Poole n 127, 317.
[274] (2009) UKSC 6.
[275] Now the Competition and Markets Authority ('CMA').
[276] Above n 274, at para 7.

whether terms, particularly terms dealing with charges, are or are not core terms will pose a threat to consumer protection in the m-payment area.[277] To this extent, the discussion below relating to cases involving terms which impose charges on one of the contracting parties will show how the CRA 2015 may assist in resolving disputes over such terms, particularly in the context of m-payment services, when these had not been satisfactorily addressed under the UTCCR.

4.4.3.2 The *Abbey National* case*: A liberal approach towards consumer welfare*

In *Abbey National,* the Supreme Court found that core terms were generally restricted to matters, e.g., the loan amount, overdraft and/or the interest. Other additional terms imposing charges were not necessarily core terms and could thus be scrutinised.[278] However, it may prove more challenging to argue that terms dealing with, e.g., security of ICT systems, do not form part of the subject matter of a m-payment service agreement. It also appears more difficult to distinguish which terms fall within the purview of the subject matter and to distinguish core terms from non-core terms and terms concerning price. In this context, 'core terms' are restricted to setting out the essence of the consideration to be provided by each party to the contract, i.e., the service to be provided by the provider, and the price to be paid for it by the consumer. It is true that the consumers' rights would be compromised if courts were to construe what can be considered the concept of the 'subject matter' of the contract too broadly; the objective of the law would be evidently stymied.[279] Nevertheless, as discussed below, a narrow conception of 'core terms' can be problematic in the context of the m-payment sector. This is particularly so given that consumers may place great reliance on

[277] CRA 2015, s64.
[278] Also see *Falco Finance Ltd v Gough* (1999) CCLR 16.
[279] *Director General of Fair Trading v First National Bank* (2001) UKHL 52, at [12].

promises and representations made by the provider in relation to (for example) their security and authorisation procedures, even to the extent that they would not have used the service provider in the absence of these safeguards, only to find that they are not considered 'core' terms in law.

Indeed, *Abbey National* suggests that a robust approach towards consumer protection has not actually been endorsed. The fact that unauthorised overdraft charges added up to one third of the bank's' total income from current accounts possibly explains why, during the 2008 banking crisis, the court was disinclined to allow the matter to proceed to the European Court of Justice.[280] This decision appears to be a discretionary exercise, as opposed to a strict interpretation and application, of the law.[281]

The main issue with this decision for m-payments is that it may marginalise the CRA's usefulness in terms of consumer protection due to the Supreme Court's failure to narrowly construe what constitutes a core exemption. A similar construction of the 'main subject matter of the contract' will not benefit consumers. Instead, it serves business interests and is reflective of a neoliberal paradigm.

4.4.3.3 *Bairstow Eves London Central Ltd v Smith: A paternalistic approach towards consumer protection*

The difficulty of determining whether a term in a m-payment service agreement can be challenged as being unfair is further illustrated by *Bairstow Eves London Central Ltd v*

[280] J. Devenney and M. Kenny, *European Consumer Protection: Theory and Practice* (CUP 2012) 109.
[281] O. Amao, 'Judicial Discretion and Doing between the Banks and their Customers: A Critical Analysis of the Supreme Court Decision in Office of Fair Trading v Abbey National Plc and Others' (2011) *Web Journal of Current Legal Issues* 5, 1-15, 13.

Smith.[282] In this case, it was found that a term which resulted in a doubling of the commission if a payment was not made within a ten-day period did not constitute a core term, i.e., a price term. The contract involved an estate agency agreement. The parties only contemplated the doubling of commission as a default option if payment was not made, as opposed to being obligated to pay the doubled rate *per se*. The term was held to be ancillary and fairness thus could be assessed. Core terms concerning price were distinguished from ancillary terms.[283] Yet, 'core terms' are not conceptually very different from terms that are 'characteristic' and/or form the 'main subject matter' of a contract. Whilst the wording of terms may be different, it is unclear how a difference may be drawn in practical terms which may in turn have different impacts on consumer protection.[284] In the m-payment sector, judges may be unfamiliar with the nature of the services provided and have a less intuitive understanding of what consumers' expectations might be, thereby compounding these challenges. Further, the restrictive approach to interpreting terms which are open to review limits the powers of the courts to use contract or tort law to regulate contracts between m-payment providers and consumers. This in turn increases the pressure on legislative provisions.

4.4.3.4 *Bond v British Telecommunications plc: A liberal approach towards consumer welfare*

In *Bond v British Telecommunications plc*,[285] it was held that a 'charge for operating the total telecommunications service [...] [was] a charge for services rendered'. The term formed a core element for the service and could not be reviewed.[286] The determination of whether the provision deals with the issue of adequacy or price or remuneration can thus be difficult,

[282] (2008) EWHC 263.
[283] Poole n 127, 318.
[284] A. Burrows, *A Casebook on Contract* (5th ed, Hart Publishing 2016) 320.
[285] Unreported, 28 March 2008, Walsall CC.
[286] R. Lawson, *Exclusion Clauses and Unfair Contract Terms* (10th ed, Sweet & Maxwell 2011) 272.

particularly in the m-payment context and this possibly undermines consumer protection in this context. As was noted in relation to *Bairstow Eves*, the restrictive approach to construing terms which are open to review limits the powers of the courts to use common law tools to regulate contracts and provide a remedy where the imbalance of power between provider and consumer has been exploited.

Nonetheless, not all terms in the m-payment agreement will be considered as relating to the 'subject matter of the contract' as courts have not adopted such an approach towards core terms in the past.[287] Instead, core terms have been construed narrowly so that m-payment providers cannot simply label all of them as core terms.[288] M-payment providers may find it hard to label a term as relating to the subject matter of the contract, which may make it easier for consumers to challenge certain terms and promote social welfare interests.

Furthermore, under European law, consumer protection has to be guaranteed, even without consumers complaining about unfair terms,[289] but, as discussed, English law has adopted a more formalistic approach.[290] Accordingly, clauses that are necessary, and commonplace, to protect the interests of m-payment providers, and where it is not unreasonable for imposing such clauses, are likely to be considered fair.[291] The fact that a term may be more convenient for one party does not necessarily suggest unfairness.[292] Consequently, vulnerable m-payment customers may not be sufficiently protected as they are unlikely to challenge terms. In fact, even average or reasonably circumspect customers may not bring legal proceedings due to the difficulties which exist in establishing that a term is

[287] *Bankers Insurance Co Ltd v South* (2003) EWHC 380.
[288] *Director General of Fair Trading v First National Bank plc* (2001) UKHL 52.
[289] *Oceano Grupo Editorial SA v Murciano Quintero* C-244/98 to C/244/98.
[290] M. Chen-Wishart, 'Regulating Unfair Terms', *English and European Perspectives on Contract and Commercial Law: Essays in Honour of Hugh Beale*, October 2014, 105-130, 125 <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2709069> accessed 10 November 2016.
[291] *Broadwater Manor School v Davis*, unreported 8 January 1999, Worthing CC; Lawson n 187, 288.
[292] *Heifer International Inc v Helge Christiansen* (2007) EWHC 3015.

unfair. This erodes consumer protection across the board in this inherently risky new fiscal milieu and effectively promotes a neoliberal model where big business' interests prevail. Hence, whilst the CRA 2015 certainly is embedded with social welfare considerations, they may not actually provide a high degree of consumer protection.

However, very harsh clauses are likely to be found unfair[293] and even less harsh terms have sometimes been considered unfair so some consumer protection may still be seen to be provided. For example, an insurance agreement which required consumers to immediately communicate in writing all the particulars of their claims was found to be an unfair term, despite the insurance company being prejudiced if not provided with such information.[294] The full written disclosure requirement caused a significant imbalance in the parties' obligations to the insured's detriment. Following this authority, providers might be conscious to ensure that the demands they place on consumer are reasonable, in that they are not prohibitively onerous, and that a reasonable period of time is offered to comply with any requirements imposed.

Provided that contract terms comply with the substantive restrictions of the PSR 2017, particularly its extensive safeguarding requirements, it may not be unreasonable to impose obligations on customers, e.g., to inform their banks about the loss of their mobile phone or PIN without unreasonable delay. However, the unresolved question is whether a term which defines gross negligence strictly and prejudices a consumer would be considered contrary to the CRA 2015. In other words, the danger in respect of unauthorised m-payment transactions is that gross negligence and fraud are contractually defined in ways which undermine

[293] *Falco Finance Ltd v Michael Gough* Unreported 28 October 1998, Macclesfield CC; Lawson n 187, 295.
[294] *Bankers Insurance Co Ltd v South* (2003) EWHC 380; A. Carse and A. Padfield, 'Consumer insurance: The risks of contracting on unfair terms' (2012) *Journal of the British Insurance Law Association* 125, 64-69, 65.

consumer protection and which consumers cannot challenge as the question of liability may be ruled a core term.

Whilst the PSR 2017 ensures that risk is borne predominantly by m-payment providers, it does not require them to completely insure consumers against loss which is caused by their own negligence or fault, nor does it require customers to be absolved entirely of responsibility for their own welfare. The UK legal regime thus displays balance and concern for consumer welfare. This is not an inadequacy in the provisions of the PSR 2017, but rather a deliberate decision that the freedom of market players should not be entirely subjugated to consumer protection.

Moreover, as noted, the CRA 2015 requires transparency and consumers may, therefore, try to challenge terms which are not transparent and prominent,[295] and unfair.[296] Hence, m-payment service agreements must be transparent and not difficult for consumers to understand. Cases such as those considered in this chapter indicate how the concept of 'unfairness', particularly various manifestations of procedural and substantive unfairness, are being developed by the courts.[297] Even so, it is not clear what the transparency threshold is that has to be discharged in order for contract terms to be fair. Islamic jurists should also further develop the good faith principle in respect of exclusion clauses contained in m-payment service agreements.

For instance, clause 5.3 of the terms and conditions of Barclays' mobile app 'Pingit'[298] states that: 'If you want to cancel, recall, change or trace a payment, we can charge you a fee for this service as explained in our General Terms'. The question arises as to

[295] CRA 2015, s64(2).
[296] CRA 2015, ss 62, 64 and 68.
[297] *Director General of Fair Trading v First National Bank* (2001) UKHL 52, per Lord Bingham, at [17].
[298] Barclays n 264.

whether a term would fall foul of the CRA 2015 if the clause which imposes a fee is hidden in small print or held in a separate document where the link is not clearly signposted or provided. Obscuring access in terms of finding applicable charges, arguably, violates the concept of transparency. This answer would depend on whether or not the court embraces a more purposive approach towards consumer protection than seen in *Abbey National*,[299] in addition to well-established common law rules as to the incorporation of terms.[300] In this context, this approach entails that the court pays greater heed to the underlying objectives which the law seeks to achieve rather than the natural meaning of the language in which it is framed. This has the advantage of encouraging compliance with the spirit, not merely the letter, of the law.

However, courts have struck down terms for being unintelligible where the words resulted in uncertainty.[301] As was held in *Thornton v Shoe Lane* Parking, the requirements for incorporation of terms are particularly exacting where the term is highly adverse to the party against whom it is relied upon.[302] This approach is premised on the distinction between 'core' terms of the contract which are to be construed based primarily on the objective intentions of the parties and terms, such as, exclusion clauses which may be construed according to the principle of *contra preferentem.*[303] The distinction may seem at first glance to enhance consumer protection. Nonetheless, following *Abbey National*, freedom of contract will continue to be prioritised.[304] This reflects the emphasis placed by judges on this legal principle with which they were careful not to interfere. Such a stance towards the CRA 2015 may, therefore, make it difficult for consumers to successfully challenge unfair terms in m-

[299] Amao n 281, 10.
[300] See e.g. *Thornton v Shoe Lane Parking* [1971] 2 QB 163.
[301] *Scammel and Nephew Ltd v HC & JG Ouston* (1941) AC 251.
[302] Ibid.
[303] E. McKendrick, *Contract Law: Text, Cases, and Materials* (8th ed, OUP 2018) 409.
[304] Amao n 281, 10.

payment agreements and the risks posed to them when using such services, arguably, remains, thus undermining a more social welfare-based policy model.

Consumers do not necessarily have to bring their own proceedings as the FCA, as regulator, can also scrutinise terms.[305] Where proceedings are brought, the courts may consider the fairness of terms without the point being specifically pleaded by the parties.[306] Accordingly, there are elements of social welfare-oriented consumer protection underpinning the CRA 2015, as well as related case law. Notwithstanding that, the statutory provisions and relevant case law are driven by market considerations and neoliberal policy concerns. Indeed, another example of this business-focused approach which embeds social welfare needs is the approach towards data protection, which shall be discussed next.

4.5.1 Data and privacy protection of m-payment customers' data

In the m-payment context, consumer protection means safeguarding not only the funds, but also personal data of customers. Distinctions, however, should be drawn between data protection, confidentiality and privacy. Data protection is concerned with an individual's ability to control how data is collected, processed and/or used, rather than giving rights to privacy or confidentiality.[307] Institutions must protect their customers' data and this requires adhering to particular rules in relation to the processing of personal data and sensitive personal data.[308] The Data Protection Act 1998 ('DPA 1998') implements Directive 95/46/EC[309] and gives individuals rights over the control of their own personal data, as

[305] CRA 2015, s70, Schedule 3, para8(1)(d) and Schedule 5, paras4(d) and 11.
[306] CRA 2015, s71(2).
[307] See the Data Protection Act 1998.
[308] Ibid.
[309] Although it should be noted that data protection law within the UK stretches back to the mid-1980s, with the enactment of the Data Protection Act 1984.

defined in s1(1) of the DPA 1998.[310] The definition adopted in the DPA 1998 mirrors the one in Art. 2 of the 1995 Directive. Personal data is broadly defined and requires the individual to be identifiable from the data and to be alive.[311] (Though the GDPR entered into force in the UK by virtue of the doctrine of direct effect on 25 May 2018, the scope of this work is largely restricted to the law in the UK as at 1 May 2018 and discussion of the GDPR is limited in the thesis).

In *Durant v Financial Services Authority,*[312] the Court of Appeal adopted a narrow construction of personal data. A two-fold test was adopted which establishes data as being, firstly, 'biographical in a significant sense' and, secondly, information that has 'the putative data subject as its focus'.[313] Such an approach is not in the interests of m-payment users as the qualification makes it more difficult to protect a broad range of personal data; thus such consumer' data may still be at risk.

Whilst the DPA 1998 applied to m-payments, the Act was arguably insufficient to address the new privacy-related risks which could arise as a result of m-payment transactions. For instance, if banks team up with device manufacturers or mobile phone operators and customers become accustomed to using their mobile phones to pay for all their outgoings, these operators will collect extremely sensitive information, detailing comprehensively the preferences and profile information of the customer. This generates what has been labelled 'Big Data in payments.'[314] This information is likely to be of a high monetary value which, if

[310] Under the DPA 1998, s1(1) personal data includes 'data which relate to a living individual who can be identified from those data...or other information', such as any 'indication of the intentions of the data controller.'
[311] DPA 1998, s1(1).
[312] (2003) EWCA Civ 1746.
[313] *Durant v Financial Services Authority* (2003) EWCA Civ 1746, per Auld LJ at [28]; M.J. Taylor, 'Data Protection: Too Personal to protect?' (2006) *Scripted* 3(1), 72-81, 78 <http://www.law.ed.ac.uk/ahrc/script-ed/vol3-1/taylor.pdf> accessed 28 May 2013.
[314] Tata Consultancy Services Ltd, 'Big Data in Payments - Unparalleled Opportunity for Strategic Excellence.' White Paper, 2013, 1-6 <http://www.tcs.com/SiteCollectionDocuments/White%20Papers/Big-Data-Payments-0713-1.pdf> accessed 15 September 2016.

sold, might be utilised by marketing companies, insurance providers and other entities, thus promoting a neoliberal prioritisation of big business over individual welfare.[315]

4.5.2 Complexities concerning the definition of 'personal data'

Further complications may arise as not all data is considered 'personal data' within the definition of Directive 95/46/EC or the DPA 1998 but, which when taken together with other categories of individually 'non-personal' data, may form data from which an individual may become identifiable.[316] Any organisation that holds such data would then be categorised as a data controller under the law. M-payment service providers are likely to be operating systems along a long chain of technology which enables them to gather large amounts of data that they become responsible for as data controllers.

4.5.3 International data collection

The DPA 1998 applies to persons who process data or whose equipment is in the UK.[317] This may be problematic since personal data of a customer using m-payment services is passed along a chain of technology which is built from a range of systems and service providers. Due to the nature of packet-switching and routing technology, data may pass through jurisdictions with weaker or no data protection regulation.[318] Data may be transferred across borders with network traffic algorithms, e.g., through clouds, as discussed in chapter 1. This may mean that a m-payment transaction that takes place entirely within the UK may send

[315] Ibid.
[316] DPA 1998, s1.
[317] *Michael Douglas v Hello! Ltd (No. 2)* (2003) EWCA Civ 139.
[318] P.J. Springer, *Encyclopedia of Cyber Warfare* (ABC-Clio LLC 2017) 17.

personal data outside of it.[319] Directive 95/46/EC restricted the transfer of personal data to a third country outside of the European Economic Area ('EEA') if that country lacked sufficient data protection. To that end, the European Commission published a list of approved third countries which included Canada and Switzerland.[320] However, the US-EU Safe Harbour Framework was ruled inadequate since US law enforcement, national security and public interest requirements trump the safe harbour scheme, resulting in undertakings, such as, Facebook, not complying with the protective safeguards stipulated by it.[321]

Furthermore, data processing could only take place if at least one of the conditions in Schedule 2 was met, i.e., the data subject gave his/her consent, processing was required to contract for legal compliance or necessary to protect the vital interests of the data subject for governmental or judicial purposes or other legitimate purposes. In the case of m-payments, it would not be difficult to establish the existence of data processing by virtue of, e.g., the customer's consent. Payment service providers may make it a standard procedure to obtain their customers' express consent, although consent may be implied by the actions of the customer as the data subject.[322] Indeed, where sensitive personal data[323] is processed, Schedule 3 stated the conditions relevant to its processing, including the need for explicit consent to be given and that such data processing was of vital interest to the subject for legal compliance and the administration of justice. However, as pointed out in chapter 3, a legal

[319] Ibid.
[320] Directive 95/46/EC, Article 25(6); European Commission, 'Commission decisions on the adequacy of the protection of personal data in third countries.' 2016 <http://ec.europa.eu/justice/data-protection/international-transfers/adequacy/index_en.htm> accessed 15 September 2016.
[321] Case C-362/14 *Maximillian Schrems v Data Protection Commissioner*.
[322] DPA 1998, Schedule 3, para8.
[323] Under s2 of the DPA 1998, sensitive personal data includes information, such as an individual's political opinions or his racial or ethnic origin.

focus on obtaining consent represents a more neo liberal approach towards consumer protection, especially in light of ineffective participation alternatives in the economy.[324]

4.5.4 The DPA 1998 and data protection principles

Under the DPA 1998, data controllers had to adhere to eight data protection principles.[325] Data had to be processed fairly and lawfully and could only be obtained for one or more specified lawful purposes. It had to be adequate, relevant and not excessive, as well as accurate and up-to-date. The data could not be kept for longer than necessary and had to be processed in accordance with the data subject's rights. It had to be kept secure through technical and organisational measures and could not be sent outside the EEA if the data subjects were inadequately protected beyond this zone. Part II of the DPA 1998 set out the rights of data subjects and others[326] which included the following: Access to data; averting processing that causes damage or distress; correcting and destroying inaccurate data; and compensation.[327] The relevant exemptions to the DPA 1998 which m-payment providers could rely on were national security, crime and taxation, regulatory activities and disclosures required by law.[328]

M-payment providers also had to inform the Information Commissioner's Office ('ICO') that they were processing personal data.[329] Individuals could ask the ICO to assess whether the DPA 1998 had been breached.[330] An information notice could be served by the

[324] M. Rhoen, 'Big Data and Consumer Participation in Privacy Contracts: Deciding who Decides on Privacy' (2015) *Utrecht Journal of International and European Law* 31(80), 51–71, 65.
[325] DPA 1998, Schedule 1, Part I; D. Rowland and E. MacDonald, *Information Technology Law* (3rd ed, Routledge-Cavendish 2005) 347.
[326] E.g., credit reference agencies: DPA 1998, s8.
[327] DPA 1998, ss7-15.
[328] DPA 1998, Part IV.
[329] DPA 1998, s17.
[330] DPA 1998, s42.

ICO requesting all relevant data.[331] A breach of the DPA 1998 could result in damages being awarded if the data controller had not taken reasonable care.[332] Yet, the 1998 Act only penalised a failure to comply with an information notice.[333] Most penalties varied between £200 and £300 per contravention, which were equivalent to the amount of damages generally awarded to individuals.[334] These penalties appeared entirely inadequate as a deterrent for m-payment providers to protect data better. This, arguably, meant that consumer protection was limited in favour of big business.

However, following *Vidal-Hall v Google Inc,*[335] customers could invoke s13 of the DPA 1998 in order to seek damages when misuse of their personal information had caused them distress. Furthermore, since 2011, the ICO has required that data breaches are notified by service and network providers, thereby strengthening security for m-payment users and promoting a social welfare policy model.[336]

4.5.5 EU General Data Protection Regulation

The new EU legislation on data protection, the General Data Protection Regulation ('GDPR') (Regulation (EU) 2016/679), came into effect on 25 May 2018. The changes brought by the GDPR apply to m-payments. Fundamentally, the GDPR recognises the new risks which arise

[331] DPA 1998, s43.
[332] DPA 1998, s13.
[333] DPA 1998, s47.
[334] E.g. see Information Commissioner's Office, Annual Report 2006/2007, Information Guidance, 2007, 1-96, 58 <https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/231262/0646.pdf> accessed 29 March 2013; Information Commissioner's Office, 'Information Commissioner's Annual Report and Financial Statements 2011/12, in the Rights space- at the right time', 2012, 1-84, 32-33 <https://ico.org.uk/media/about-the-ico/documents/1042187/annual_report_2012.pdf > accessed 29 March 2013.
[335] (2015) EWCA Civ 311.
[336] Information Commissioner's Office, 'Guidance on data security breach management.' 2012, 1-8, 4 <https://ico.org.uk/media/1562/guidance_on_data_security_breach_management.pdf> accessed 15 September 2016; Information Commissioner's Office, 'Security of services', 2016 <https://ico.org.uk/for-organisations/guide-to-pecr/communications-networks-and-services/security-of-services/#securityobligations> accessed 15 September 2016.

in the big data era by spelling out new obligations for data processors, including the need to notify data controllers promptly about a breach, usually within a time limit of 72 hours, e.g., in the cases of identity theft, fraud and financial loss.[337]

More stringent rules are imposed with regard to the sharing of personal data, which is particularly important in the financial context. For example, the new regulation requires that the subject is not only informed of but gives informed and, importantly, continued consent to the sharing of personal information.[338] In light of the fact that transactions which take place within the UK may result in data being sent to servers located in third countries, it is important that data protection is also realised.[339] The GDPR addresses this particular issue by requiring data processors and controllers which are not located in the EU, but which offer services and goods in the EU, to adhere to these obligations.[340] The GDPR thus has an extraterritorial reach.[341]

It also introduces more stringent penalties including fines of up to 4% of global revenues or €20 million (whichever is the greater) for breaches of the Regulation.[342] This provides a stronger deterrent against breaches and does not require any action on the part of the consumer to enforce the service provider's obligations. Correspondingly, the GDPR also imposes additional safeguards, such as, requiring companies which collect and process personal data on a large scale (as will be the case for the majority of m-payment service providers) to hire a data protection officer.[343] Consequently, the GDPR adopts a social welfare approach that heightens consumer protection and mitigates the data risks posed to

[337] GDPR, Recitals 81&85.
[338] GDPR, Articles 4(11), 6-9.
[339] P.J. Springer, *Encyclopedia of Cyber Warfare* (ABC-Clio LLC 2017) 17.
[340] GDPR, Recital 23.
[341] GDPR, Article 115.
[342] GDPR, Article 83.
[343] GDPR, Article 97.

consumers as more onerous legal provisions are imposed. It is easier for customers as data subjects to withdraw their consent to processing following this and, in respect of sensitive data, consent must be explicit.[344] Nonetheless, it is unclear how effectively such requirements are in practice since m-payment users may have limited option but to consent if they wish to use the m-payment services.

The eight data protection principles contained in the DPA 1998 are mainly unaffected by the changes introduced by the GDPR.[345] Indeed, the exemptions to data protection obligations which m-payment providers can invoke have been further expanded. These include monitoring, inspection or regulatory functions connected to issues, such as, national security.[346] One could argue that this offers a potential loophole whereby consumers' data and their general protections may be legally undermined as it is difficult for a consumer to challenge a purported reliance on the 'national security' exemption by a m-payment provider. This is particularly so given that, even in the event of a legal challenge, the consumer may not be entitled to review documents and evidence supporting the provider's contention, as these companies are effectively given similar tools as domestic security agencies and the police.[347] This undermines the enforceability of the obligations imposed and may render the rights of the consumer academic.

The GDPR does not change the prohibition contained in the DPA 1998, which proscribes data being transferred to third countries with inadequate data protection

[344] GDPR, Recital 39.
[345] Information Commissioner's Office, 'Overview of the General Data Protection Regulation (GDPR).' 2016, 1-40, 5 <https://ico.org.uk/media/for-organisations/data-protection-reform/overview-of-the-gdpr-1-0.pdf> accessed 15 September 2016.
[346] GDPR, Article 23(1)(h).
[347] M. Rhoen, 'Beyond consent: improving data protection through consumer protection law' (2016) *Internet Policy Review* 5(1) <https://policyreview.info/articles/analysis/beyond-consent-improving-data-protection-through-consumer-protection-law> accessed 15 April 2019.

legislation.[348] However, it spells out various methods to overcome problems with international data transfers. M-payment service providers can, e.g., enter into model clauses, i.e., standard contractual provisions endorsed by the EU Commission, or adopt binding corporate rules, such as, codes of conduct.[349] These internal codes of conduct would then have to be followed by those within the m-payment ecosystem. Private, neoliberal measures, while favoured, are less intrusive. These solutions are important, particularly in light of the defunct US-EU Safe Harbour Framework, since they facilitate relatively safe cross-border sharing and transfer of data.[350] This chosen approach is likely to benefit the economic development of the m-payments industry. The GDPR could have better provided for the regulation of international data transfers; it would be better to regulate through legal consumer protection measures, instead of private options, consisting of government-approved model clauses and codes of conduct, as discussed in chapter 3, section 3.3 above. In this way, the principles of social welfare could be better embedded in lieu of a mainly neoliberal market focus.

Also, it is perhaps regrettable that the GDPR does not mandate that consumer advocacy groups be consulted before such codes of conducts or model clauses are devised.[351] The involvement of advocacy groups could, for instance, ensure that providers adopt strict cryptographic techniques in light of ever-increasing state surveillance, including spying on the most popular cloud services.[352] Consumer advocacy groups may also influence the shape

[348] T.F. Villeneuve et al, *Corporate Partnering: Structuring & Negotiating Domestic & International Strategic Alliances* (5th ed, Wolters Kluwer 2017) 2-45; GDPR, Article 115.
[349] L. Power, 'Getting to know the GDPR, Part 9 - Data transfer restrictions are here to stay, but so are BCR.' Field Fisher, 24 February 2016 <http://privacylawblog.fieldfisher.com/2016/getting-to-know-the-gdpr-part-9-data-transfer-restrictions-are-here-to-stay-but-so-are-bcr/> accessed 15 September 2016.
[350] Ibid.
[351] J. Kronqvist and M. Lehto, 'Adopting Encryption to Protect Confidential data in Public Clouds: A Review of Solutions, Implementation Challenges and Alternatives'. In N. Abouzakhar (eds), *ECCWS2015-Proceedings of the 14th European Conference on Cyber Warfare and Security, University of Hertfordshire, Hatfield, UK, 2-3 July 2015* (Academic Conferences and Publishing International Ltd 2015) 152.
[352] Ibid.

of regulations, e.g., advocating the inclusion of meta-data (i.e., 'data about data' such as the time and location at which the data relating to a transaction came into existence, or the number of transaction data files held in respect of a particular consumer) as personal data.[353] There are sound reasons for a broader definition since meta-data can reveal personal information about an individual's lifestyle and habits.[354] The lack of consumer influence is also arguably apparent from the fact that the term consumer protection is only mentioned once in the GDPR.[355]

One may conclude that the GDPR has at its heart the objective of engendering trust and confidence in markets by reassuring the public of stringent measures to protect the collection, processing, and use of data, as opposed to the consumer protection values which might at first blush appear to be its core objective.

4.5.6 The MLRs 2017 and FTR 2015 and the issue of protecting customers' data

Compliance with AML laws is a necessary prerequisite for most providers of m-payment services. On 26 June 2017, the Money Laundering Regulations ('MLRs') 2017 entered into force. The MLRs replace the Money Laundering Regulations 2007[356] and transpose the EU's Fourth Anti-Money Laundering Directive 2015/849.[357] These Regulations apply to banks,

[353] Ibid.
[354] Rhoen n 347.
[355] Ibid.
[356] D. Ormerod and D. Perry, *Blackstone's Criminal Practice 2018* (OUP 2017) B21.34.
[357] Directive (EU) 2015/849 of the European Parliament and of the Council of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, amending Regulation (EU) No 648/2012 of the European Parliament and of the Council, and repealing Directive 2005/60/EC of the European Parliament and of the Council and Commission Directive 2006/70/EC; ibid.

payment service providers, e-money institutions, e-money issuers[358] and others. However, this is subject to the caveat that a person engages in a financial activity which is not just 'occasional' or conducted on a 'very limited basis'.[359]

Payment service providers should specifically take note of Regulation 63 which imposes a duty to consider the guidelines given by the European Supervisory Authorities, pursuant to Article 25 of the EU Funds Transfer Regulation 2015[360] ('FTR 2015'). The FTR 2015 came into force on 26 June 2016[361] and ensures that Recommendation 16 of the Financial Action Task Force ('FATF') [362] is transposed.[363] Its objective is to ensure that all payments which are sent or received within the European Economic Area are fully traceable.[364] Under the FTR 2015, beneficiary and intermediary payment service providers must adopt effective measures to identify and collect the legally mandated information. That information consists of the names of the payer and payee, their respective bank accounts, as well as the payer's address,[365] and must be verified by the payer's payment service provider.[366] There are certain exceptions to these information requirements, e.g., in e-money

[358] MLRs 2017, Regulation 10.
[359] E.g., where the turnover is above £100,000 or the activity is not ancillary to the main business activity: See MLRs 2017, Regulation 15(3)(a)-(g).
[360] Regulation (EU) 2015/847.
[361] C. Westerhaus, 'Time to act: EU Funds Transfer Regulation 2015', Banking Technology, 9 August 2017 <http://www.bankingtech.com/896431/time-to-act-eu-funds-transfer-regulation-2015/> accessed 1 October 2017.
[362] FATF, 'International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation', The FATF Recommendations 2012, June 2012, 1-129 <http://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF%20Recommendations%202012.pdf> accessed 1 October 2017.
[363] D. Swanney, 'Prevention of money laundering/combating terrorist financing, 2017 Consultation Version, Guidance for the UK Financial Sector, Part III: Specialist Guidance', The Joint Money Laundering Steering Group, May 2017, 1-49, 4.
[364] Westerhaus n 361.
[365] FTR 2015, Article 4(1)-(2).
[366] FTR 2015, Article 4(4)-(5).

transfers below €1000[367] or reloadable e-money goods which are not in excess of €2,500 per year.[368]

Under the MLRs 2017, supervisory authorities in charge of the transfer of funds must monitor payment service providers to ensure adherence to the FTR 2015 and to urge them to notify violations as well as take measures to cooperate with other bodies, including overseas and coordinating activities.[369] Regulations 18 and 19 are particularly relevant in the context of m-payments as Regulation 18 requires risk assessments to be conducted by relevant persons and Regulation 19 requires 'policies, controls and procedures' to be adopted. These encompass a range of measures including due diligence, record keeping, amongst others. In addition, banks and payment service providers must regularly review and update these measures.[370] Written records must be kept of policies, controls and procedures and any changes made, as well as how relevant persons have been informed.[371] The MLRs 2017 and FTR 2015 are arguably aimed at institutions, e.g., m-payment providers, to ensure compliance with AML requirements rather than protection of consumers against money laundering.

As discussed in chapter 1, m-payment services are facilitated through several different stakeholders. It is, therefore, necessary that m-payments policies, controls and procedures are not inward-focused. Communications, including those relating to updates and changes, should be duly notified along the m-payment services chain and written records that are kept must be comprehensive. The different stakeholders ought to cooperate and coordinate so as to avoid gaps within policies, controls and procedures.

[367] So long as smaller transactions do not seem linked: FTR 2015, Article 5(4).
[368] Swanney n 363, 6.
[369] MLRs 2017, Regulation 63(1)(a)-(d)(i)-(iii).
[370] MLRs 2017, Regulation 19(1)(b).
[371] MLRs 2017, Regulation 19(1)(c)(i)-(iii).

Technological advancement, whilst offering many opportunities for improved services for consumers, also creates greater scope for generating, collecting, processing and use of data in m-payments. This, coupled with the increased obligation on financial institutions to conduct CDD, keep records, report beneficial ownership information will affect customers in their day-to-day use of banking services including payment services. The attempts of UK regulators to keep pace with these changes (albeit not always successfully) may be contrasted with the approach in SA outlined in chapter 5. There is also a more fundamental risk that the greater obligations imposed on financial institutions by the MLRs may have the unintended consequence of eroding customers' data protection rights by requiring greater transparency to combat the increased risks of money laundering.

An analysis of the MLRs shows that the underlying policy objective is business-friendly. This is illustrated by the inclusion of a proportionality requirement which can be found in Regulation 19(2)(a) which states that policies, controls and procedures should be commensurate with the type of business and its size. This business-friendly slant on traditional consumer protection principles ensures the compliance costs associated with providing consumer protection are not prohibitive, particularly for small or young entrants to the market, by adjusting its requirements to reflect what can realistically be expected of such a company. It is also in line with the economic interests of the consumer. The overall effect of the provisions is that providers are required to have in place a proactive system for the monitoring and reporting of suspicious activities which is as effective as can reasonably be achieved in view of the resources and capabilities of a company of that size and stature in question. On the other hand, it follows that a consumer may be entitled to different protection when dealing with different providers based upon criteria which are not obvious to them when making their initial selection. Unless the consumer is aware of legislative protections applicable when dealing with the company concerned (knowledge which cannot be

reasonably assumed), it will be exceptionally difficult to rely on legal protection when making decisions and assessing risk. Even if consumers were to have extensive knowledge about businesses, competition in the market may restrict consumer trust to a small number of well-known companies.

The AML requirements have been heightened by the MLRs 2017, which together with the FTR 2015, may deter certain newcomers from entering the market.[372] While the aim of the AML regime is to prevent, e.g., the payment system, from being used for money laundering purposes which may be prima facie beneficial to consumers, this comes with a cost; consumers may be concerned with the protection of their data and preservation of their privacy, which may in turn deter them from making use of new technologies. Consumers who are accustomed to using traditional banking systems are likely to be more reluctant to switch, even when the new technology offers significantly greater convenience because of these privacy concerns. [373] The provisions of the MLR were insufficient to entirely assuage these privacy concerns, though the new GDPR appears likely to go some way towards resolving its shortcomings, in particular through the requirement for meaningful and continuing consent which gives consumers greater confidence that they understand the implications of the terms they agree to, as discussed in section 4.5.5 above. It may be hoped that the heightened penalties of the GDPR will also increase consumer confidence in the deterrent effect of regulation. This is an important distinction: The GDPR is aimed at ensuring the proper collection, processing and use of data, and the obligations imposed by it may therefore be trumped by the need for disclosure of a customer's financial information when there is

[372] I. Sumkovski, 'The Optimal level of Anti-Money Laundering Regulation for the UK Banking Sector. Banks' Cost of Compliance, De-risking Problem and How to Implement Effective AML Systems and Controls' (2016/2017) Institute of Advanced Legal Studies, 1-54, 23 <https://sas-space.sas.ac.uk/6873/1/Final%20Dissertation_LLM%20ICGFREL_Igor%20Sumkovski_1544977.pdf> accessed 20 April 2019.
[373] J. Harvey, 'From a risk-based to an uncertainty-based approach to anti-money laundering compliance' (2017) *Security Journal* 39(1), 24-38.

suspicion of money laundering taking place by a customer's use of his account and transfer of funds. By contrast, the MLRs cannot be 'trumped' in this way.

Nevertheless, there remains the obstacle that consumers have no negotiating power and therefore have little choice but to agree to the terms offered to them if they wish to make use of the service; consent may be a somewhat empty protection in these circumstances. This challenge is particularly acute given that, as considered above, consumer protection is not the sole objective; indeed, the increased transparency and enhanced reporting obligations demanded by the MLR 2017 in an attempt to combat the increased risk of money laundering created by technological advancement may narrow the scope of protection available to consumers in respect of personal data and privacy.

4.6 Conclusion

In the future, it is foreseeable that the separation between banks and other non-bank entities in providing m-payment services will become less and less real, particularly when market consolidation takes place. The strongest players will undoubtedly want to offer the most extensive range of financial services and this ultimately means becoming credit institutions. In the short-term, the regulatory regime in the UK enables new entrants to enter the market, thereby fostering innovation and competition.

The EMR 2011 opens the door to a wide range of institutions to issue e-money, some of which might now enter what was traditionally the realm of the banks or regulated credit institutions. Hence, consumer economic interest is being furthered in neoliberal terms and that in turn, raises issues regarding the convergence of disparate industries. It further introduces a range of new legal challenges, including the regulation of communication

companies which wish to enter the payment services market. Introduction of e-money in the UK is likely to be of great importance in shifting the balance in terms of how the traditional banker-customer relationship operates as consumers can choose their financial services based on convenience, notwithstanding the possible risks involved. This fits with the neoliberal sense of customers as circumspect and responsible individuals, capable of making choices and understanding information.

Nevertheless, many different legal consumer protection measures exist for m-payment customers which promote social welfare-based policies. For instance, broader legal provisions foster substantive fairness through governing unfair contract terms and providing refunds to customers for unauthorised transactions. These types of measures encourage m-payment service providers to adopt strong technological and organisational procedures to mitigate risk and protect customer funds. However, as to whether the right policy balance has been struck, only time will tell.

The legislative landscape in the UK is still changing. The PSR 2017 creates a base level for the regulation of payments, including m-payments and service providers. Customers are protected while market expansion for new entrants is promoted. The adoption of regulatory security requirements mitigates against any risk which arises from providing account access to new market entrants, e.g., TPPs. While consumers are likely to benefit from additional competition, social welfare considerations are arguably also being promoted.

The GDPR serves to establish a more robust data protection regime than the DPA 1998. In particular, the requirement for consumer consent is made more meaningful by the positive acceptance and opt-in provisions. This enhances autonomy-based consumer protection, without restricting the freedom of activities available to market players (which remain free to use data as they have historically, subject to the consent of the individual

consumer). To some extent, the GDPR preserves the tailored approach formulated by the MLRs; obligations and penalties are linked to the size of the company in question, and proportionality between the costs and benefits of consumer protection is preserved.

Overall, a carefully thought-out consumer protection regime has been adopted which balances market interests with those of the consumer and which is still being incrementally developed. The next chapter analyses the legislative framework in SA, with a view of ascertaining how it compares with that of the UK and how the policy principles enshrined in UK law might be usefully implemented there.

CHAPTER 5

THE M-PAYMENT PROVIDER-CUSTOMER RELATIONSHIP IN THE M-PAYMENT ENVIRONMENT WITHIN SAUDI ARABIA

5.1 Introduction

SA's smartphone use is one of the highest in the world.[1] In 2017, it was estimated that the value of Saudi m-payment transactions was US$349m.[2] This figure is likely to grow by 52.3% to US$1,877m by 2021.[3] In terms of managing this growing part of the financial industry, recourse is made to Saudi laws, rules, regulations and the guidance provided by the Saudi Arabian Monetary Agency ('SAMA'), particularly the 2012 Regulatory Rules for Prepaid Payment Services, which are relevant to m-payments and the particular consumer protection rationales which come into play.

Chapter 4 explored how UK law is framed and the sources that regulate the rights and obligations of the m-payment provider and customer in m-payment transactions. In this chapter, the Saudi approach is compared with such UK laws and policy. As discussed before, in the UK, the consumer protection rationale has been carefully balanced with other priorities, e.g., promoting innovation, market growth and the potential expansion of the market to non-bank payment service providers. It is therefore argued that SA can draw inspiration from the balance which the UK has struck between pro-market reforms which

[1] European Travel Commission Digital Portal, 'Mobile/Smartphones, Rise of Mobile Internet Use in Middle East Region', 2014 <http://etc-digital.org/digital-trends/mobile-devices/mobile-smartphones/regional-overview/middle-east/> accessed 18 October 2014.
[2] Statista, 'Mobile Payments, Saudi Arabia', 2017 <https://www.statista.com/outlook/331/110/mobile-payments/saudi-arabia#> accessed 1 October 2017.
[3] Ibid.

encourage financial innovation and pro-consumer regulations protecting users of m-payment services.

As with chapter 4, this chapter identifies the consumer protection rationale that Saudi legislation has adopted or attempted to adopt in order to mitigate the risk to consumers. As discussed in chapter 3, the Sharia mandates that a social welfare policy must underpin the statutory and regulatory framework, but that framework should, nonetheless, still be business-friendly in light of Prophet Mohammed being a businessman. It should mean that losses from unauthorised m-payment transactions are allocated fairly and in accordance with the Islamic profit and loss sharing principle, discussed in chapter 3, section 3.6.3. Hence, Saudi Arabian law should prioritise social justice in line with the Islamic objective of 'establishing what is right and forbidding what is wrong'.[4] Fundamentally, SA m-payment customers should not bear the full cost of any loss that follows from an unauthorised transaction, as is currently the case. Consumers' data must also be protected in order to maintain privacy, as well as to protect consumers against breaches of their privacy.

Put differently, Islamic 'ethics, morality and behavioural admonitions' must not be deviated from.[5] In this context, it is particularly crucial for Islamic scholars to develop a consumer protection discourse, as discussed in chapter 3. They should utilise not only the broad social justice commands contained in the Sharia, but also the Islamic good faith principle currently applied in the context of contract law and which mandates that transactions are fair and honest. An Islamic test of fairness and honesty should be developed for the treatment of exclusion of liability exclusion and limitation clauses and the good faith principle could be utilised to achieve such a pro-consumer approach. As is apparent from the

[4] Quran 3:103, 109, 113; 9:71, 22:41; 31:17; cited from M.A. Khan, 'The Role of Islamic State in Consumer Protection' (2011) *Pakistan Journal of Islamic Research* 8, 31-44, 31.
[5] M.J.T. McMillen, 'Islamic Law Forum' (2008) *International Law* 42, 1017-1032, 1018.

analysis in chapter 4, English legislation has moved from the good faith principle to the principle of fairness when it comes to consumer protection, as illustrated by the CRA 2015. The Islamic good faith principle could thus fulfil a similar role to the UK Consumer Rights Act 2015 which promotes fairness. Hence, the Islamic good faith principle could be utilised to temper the classical notion of freedom of contract by ensuring that unfair terms are unenforceable.

Islamic scholars must also clarify the circumstances in which a m-payment transaction should be deemed *haram*. Furthermore, consumer rights and dispute resolution mechanisms should be developed, so that consumers can seek redress for unauthorised m-payment transactions and for failures to protect consumers' data, as well as breaches of their privacy. Only such an approach ensures that the Sharia is recognised as the most important source of law, [6] as well as being compatible with Article 6(a) of the Charter of the Saudi Arabian Monetary Agency ('SAMA') 1957. SAMA is required to act in a manner which does not conflict with the teachings of Islamic law, [7] which means adhering to the Hanbali version of Sharia law.[8] In other words, the Saudi central bank must regulate financial institutions in a Sharia-compliant manner and the Hanbali version of the Sharia is also deployed throughout this work.

[6] M. Ariff and M. Iqbal, *The Foundations of Islamic Banking: Theory, Practice and Education* (Edward Elgar Publishing Ltd 2011) 11; B. Maurer, *Mutual Life, Limited: Islamic Banking, Alternative Currencies, Lateral Reason* (Princeton University Press 2011) 32.
[7] Charter of the Saudi Arabian Monetary Agency 1957, Article 1(a)-(c); International Business Publications, *Saudi Arabia Central Bank & Financial Policy Handbook* (International Business Publications 2005) 150.
[8] S. Zuhur, *Saudi Arabia* (ABC-CLIO LLC, 2011) 176.

5.1.1 The structure of this chapter

This chapter firstly discusses how the emergence of technological innovation within the financial services sector has not resulted in the creation of new authorisation regimes, unlike in the UK where effectively 'limited banks',[9] i.e., payment institutions and e-money institutions have been created. It is emphasised that SA has failed to facilitate a m-payment third-party collaboration environment. This is also attributable to the failure to distinguish m-payment providers from banks in the old Banking Control Law 1966. The Electronic Transaction Law 2007 is analysed and highlights that it is insufficient to regulate third-party payment service providers.

The next section examines relevant sources of law which govern the rights and obligations of m-payment providers and customers in SA: The 2012 Regulatory Rules for Prepaid Payment Services are analysed, and it is highlighted how they fail to address the thorny issue of unauthorised m-payment transactions. The e-Banking Rules 2010 are scrutinised, and it is stressed that they reflect a neo-liberal consumer understanding and have also not been updated to account for new technological risks, including unauthorised m-payment transactions. Recourse is also made to the Manual of Combating Embezzlement & Financial Fraud & Control Guidelines 2008. It is identified that customers and, particularly their funds, are not adequately protected through these rules and guidelines when using these new technological forms of fiscal transactions.

The penultimate section assesses how consumers are protected against unfair terms by virtue of the 2013 Banking Consumer Protection Principles and Banking Consumers' Guide.

[9] A. Scupola, *Innovative Mobile Platform Developments for Electronic Services Design and Delivery* (Business Science Reference, 2012) 181.

The problem of utilising the principles and guide to seek compensation for unauthorised payments is stressed.

The final section looks at the issues of data protection and privacy, which are of particular importance as highly sensitive big data is collected during the provision of m-payment services, as discussed in chapter 2. It is identified that the Credit Information Law 2008 and the Consumer Credit Regulations 2006 fail to protect m-payment customers' data and do not protect consumers against breaches of their privacy. The section also provides a brief analysis of how the risk of money laundering is combated via the AML requirements (contained in the Anti-Money Laundering Law 2003) and the impact that these provisions may have on the balance between the prevention of money laundering and consumers' rights, or offer potential legal loopholes which may allow data to be accessed without consent, giving rise to related data protection issues.

All of this material provides a basis for the conclusion, of, firstly, whether SA's approach to m-payments should rightly adopt a social welfare approach in order to be compliant with Sharia law and principles and, secondly, whether Saudi legislation could usefully mirror the UK approach of combining neoliberal and more paternalistic models of consumer protection.

5.2.1 Background to m-payment regulation in Saudi Arabia

One would expect that the legal protection measures for customers in SA would exceed those of the UK on the grounds that a social welfare approach enables the law to be compliant with

Sharia more readily than a neoliberal consumer economic interest approach.[10] However, at present, Saudi Arabian laws are outdated and do not go as far as UK law in terms of adopting a social welfare approach for protecting consumers' interests. This is partly due to Saudi's law being currently related to Web 1.0 than Web 2.0 (as in the UK). Failing to keep up with technological change means that no protection is offered in respect of newly emerging risks, and service providers are easily able to evade regulation simply by updating the technological basis of their offering. The Saudi consumer protection rationale is also underdeveloped due to the religious-based legal system. As identified in chapter 3, this has limited the development of consumer rights due to Islam's focus on duties.[11] For instance, SA has not enacted a statute similar to the UK Consumer Rights Act 2015 ('CRA 2015'), tort law principles or a data protection law.

Islamic social welfare concepts that are enshrined in the Islamic business principles, such as the principle of good faith, have not been sufficiently transposed into the Saudi laws to challenge unfair contract terms which violate the consumer protection rationale. It is also unclear to what extent these Sharia law concepts are relied on by judges due to a lack of published cases. Even if these principles are being employed, without statutory clarification, these judgments will remain vague due to the lack of a doctrine of precedent, as established in the UK.

Fundamentally, the various legislation fails to adequately respond to the risk of unauthorised m-payment transactions and the protection of consumers' data in order to maintain privacy, as well as to protect consumers against breaches of their privacy, as detailed in chapter 2. As a result, the advantages for customers which flow from

[10] J.Q. Whitman, 'Consumerism Versus Producerism: A Study in Comparative Law' (2007) *Yale Law Journal* 117, 340-406, 356.
[11] G. Rice, 'Islamic ethics and the implications for business' (1999) *Journal of Business Ethics* 18, 345-358, 345.

technological innovation discussed in chapter 1 may be lost. The failure to update the legislative framework to promote innovation may also stifle economic growth in the rapidly advancing m-payment market. The potential for Fintech innovation to radically modernise the way in which m-payments can be conducted in SA may thus be hampered. SA's global position in 2012 as a 'leader nation in e-readiness' may, in addition, fail to be maintained without legislative reform.[12]

5.2.2 The m-payment third-party collaboration environment and the legal distinction concerning bank status and the problem with the Banking Control Law 1966

The Banking Control Law 1966 is the main banking law in SA. No other law has been enacted for new market entrants, as has been done in the UK. This is despite the fact that it is difficult to apply the 1966 Law to m-payment providers which are not banks. Article 1(a) defines banks as, 'any natural or juristic person practicing basically any of the banking business in the Kingdom'. It may be incorrect to label all m-payment service providers 'banks', since the services they provide are narrower than typical banking services. Simultaneously, the fact that m-payment service providers do not fall within existing statutory definitions of 'bank' (e.g., the definition in the Banking Control Law 1996),[13] means that they are effectively overlooked by the existing regime. The challenge is compounded by the lack of a conceptually clear definition of 'bank' or 'banking service', such as, the one provided by s2 of the UK Banking Act 2009.[14]

[12] Al Arabiya, 'Saudi Arabia leader nation in e-readiness: U.N. report', 3 August 2012. <http://english.alarabiya.net/articles/2012/08/03/230116.html> accessed 24 October 2014.
[13] Banking Control Law 1966, Articles 1(b) and 2(b).
[14] Banking Act 2009 (UK), s2.

As discussed in chapter 1, the multifarious nature of m-payment services infrastructures involves operations by various partners, even if a predominantly bank-led model emerged in the future. We saw in chapter 4 that English law distinguishes banks from payment service providers and e-money institutions, and imposes distinct requirements to protect customers from heightened technological risk. The PSR 2017 even goes further by providing that TPPs fall within the scope of these legislative provisions.

At present, the Banking Control Law 1966 fails to make any such distinctions and thus the statute appears outdated. A strict interpretation of the Banking Control Law 1966 highlights that the statute confers on SAMA extensive supervisory authority over institutions that are deemed 'banks' but not non-bank m-payment service providers and other associated parties that fall outside that definition.[15] Consumer economic interests are thus not promoted in neoliberal terms as the market remains closed to other entrants. While consumers may be better protected if m-payment services were only offered by banks (which is in any event largely the case at present in SA), this approach may stifle Fintech innovation in SA.

In addition, given that the holy Prophet Mohammed was a businessman and SAMA generally endorses conventional, as opposed to strict, Islamic banking,[16] the legislator ought to extend the Banking Control Law to payment and e-money institutions. In other words, it should define them and make it clear that these parties are also subject to the Banking Control Law, just like licensed moneychangers. Ideally though, SA should create distinct authorisation regimes for payment services as the UK has done, as discussed in chapter 4, sections 4.2.7 and 4.3.3. Without this, one of the central tenets of the Hanbali School,

[15] M.A. Ramady, *The Saudi Arabian Economy* (Springer 2010) 78.
[16] L. Etheredge, *Saudi Arabia and Yemen* (Britannica Educational Publishing 2011) 19.

namely to be 'liberal on economic and business issues', will not be realised.[17] This is preferable to merely extending the Banking Control Law, as its limited scope prevents it from accommodating innovations in the delivery of m-payment services. Attempts to base new regulation on the Banking Control Law would render the meaning of 'banking business' for the purposes of that legislation less meaningful and conceptually clear.

5.2.3 The Electronic Transaction Law 2007 and the non-regulation of third-party providers and related security and technological risks

Due to the lack of overarching coherence in Saudi regulation (by comparison with the UK, for example), it is necessary to consider a broader range of legislative provisions in order to gain a full understanding of the regulatory picture. In the absence of a purpose-designed regime, m-payment transactions may fall within any one (or more) of a disparate collection of statutes. As a result of the broad definition of 'electronic transactions' under Saudi legislation, one such statute is the Electronic Transaction Law 2007 ('ETL 2007'). The legislative intention of this law was to control, regulate and set out a legal framework in respect of electronic signatures and electronic transactions.[18] The objective was to facilitate e-commerce and the law is, therefore, not just directed at m-payment providers.

The ETL 2007 defines electronic transactions as 'any exchange, communication, contracting or other procedure, performed or executed, wholly or partially, by electronic means'.[19] The wording of the definition appears sufficiently inclusive as a m-payment

[17] A. Al Rajhi, A. Al Salamah, M. Malik, R. Wilson, *Economic Development in Saudi Arabia* (Routledge Curzon 2004) 14.
[18] Electronic Transaction Law 2007 ('ETL 2007'), Article 2; A.H. Boss and W. Kilian, *The United Nations Convention on the Use of Electronic Communications in International Contracts, An In-Depth Guide and Sourcebook* (Kluwer Law International 2008) 253.
[19] ETL 2007, Article 1(10).

transaction can be described as an exchange between a consumer and a merchant, or a communication between electronic devices, e.g., the mobile handset and the merchant platform, and a transaction can also be evidence that a contract has been concluded.

This law thus facilitates the advent of m-payments. It imposes various general conditions, even though m-payment providers can adopt additional measures so long as they do not contravene this law.[20] This law states that an electronic record is only considered original and integer when certain technical conditions and stipulated means are complied with.[21] The Implementing Regulations to the ETL 2007 explain that these conditions are met when documents are preserved in their original state, the electronic document has a digital certificate from an authorised service provider and the authorship of the data is secured.[22] These are general conditions for all types of electronic transactions and signatures. However, for m-payment transactions, sophisticated technical standards are required to enhance consumer protection against payment incidents, fraud and other abuse, particularly a strong form of customer authentication.[23] Authentication means adopting processes to verify and confirm that a device complies with certain features which make up its m-payment identity, as only this can result in the electronic record being original and integer.[24]

As noted in chapter 2, m-payment transactions are made possible through various stakeholders (banks/financial institutions, retailers/merchants, mobile network operators,

[20] ETL 2007, Article 4(3).
[21] ETL 2007, Article 8.
[22] Saudilegal, 'Electronic Transactions', 2016 <http://www.saudilegal.com/saudilaw/09_law.html> accessed 1 November 2016.
[23] European Banking Authority, 'Discussion Paper on future Draft Regulatory Technical Standards on strong customer authentication and secure communication under the revised Payment Services Directive (PSD2)', 2016, 1-31, 7 <https://www.eba.europa.eu/documents/10180/1303936/EBA-DP-2015-03+%28RTS+on+SCA+and+CSC+under+PSD2%29.pdf> accessed 1 November 2016.
[24] Smart Card Alliance, 'Security of Proximity Mobile Payments', A Smart Card Alliance Contactless and Mobile Payments Council White Paper, May 2009, 1-39, 25 <http://www.smartcardalliance.org/resources/pdf/Security_of_Proximity_Mobile_Payments.pdf> accessed 1 November 2016.

trusted service managers, mobile handset manufacturers and third-party payment service providers -'TPPs'). As explained in chapter 1, it is not enough to adopt just one authentication mechanism. Risk-based authentication, i.e., the adoption of multi-layered security, is important due to the complexities of this financial ecosystem.[25] A multi-factor authentication process (a multi-factor security protocol) ought to be adopted but without these security layers affecting interoperability and user-friendliness.[26]

In this context, it will be useful if ICT guidance was published in order mitigate consumer risk and promote social welfare.[27] This can take place at a range of different levels: At the most basic, e.g., providers may be required to simply inform consumers of the nature and extent of any risk to which they are exposed; at the most stringent, the provider may be required to limit or assume at least a portion of this risk themselves. The former approach reflects neoliberal values and may be insufficient to satisfy the requirements of Sharia in the context of the Saudi market. Nevertheless, it would represent an improvement on the current position.

The legislator could then make recourse to standards developed by specification organisations (e.g., the PCI Security Standards Council, EMVCo, the European Telecommunications Standards Institute, GSMA, OMA, the Near Field Communication Forum, and CDG).[28] Alternatively, they could use the EBA's regulatory technical standards on strong customer authentication and secure communications as a base from which to

[25] BBCA, 'How does PSD2 affect bank customers' digital identity?', BBVAOpen 4U, 1 August 2016 <https://bbvaopen4u.com/en/actualidad/how-does-psd2-affect-bank-customers-digital-identity> accessed 1 November 2016.
[26] A. Tiwari et al, 'A Multi-Factor Security Protocol for Wireless Payment - Secure Web Authentication Using Mobile Devices' (2011) *IADIS International Conference, Applied Computing* 2007, Salamanca, Spain, 160-167, 160; Smart Card Alliance n 24, 22; N. Vonthron, 'A2A interoperability: Understanding bank to mobile money transaction flows and technical solutions', GSMA, 10 December 2015 <http://www.gsma.com/mobilefordevelopment/programme/mobile-money/a2a-interoperability-understanding-bank-to-mobile-money-transaction-flows-and-technical-solutions> accessed 1 November 2016.
[27] Ibid (Smart Card Alliance) 9.
[28] Ibid 9-10.

develop its own guidance for the Saudi m-payment sector. However, as noted in chapter 3, effective consumer protection based on social welfare principles requires that laws are properly embedded.[29] Otherwise, the social welfare objectives of the Sharia are unlikely to be realised.

Moreover, under the ETL 2007, the task of authentication falls on certification service providers[30], namely, '[a] person licensed to issue digital certificates or perform any other service or task related thereto and to electronic signatures'.[31] Certification agents constitute 'the backbone of [digital] transactional activity', as these services deal with 'authentication, confidentiality, and non-repudiation'.[32] For this reason, certification providers are regulated through a licensing scheme operated by the Communications and Information Technology Commission.[33] Various conditions are imposed, e.g., to adopt secure means for issuance, delivery and storage.[34] These certification providers are regulated by the National Centre for Digital Certification within the Ministry of Communications and Information Technology.[35] This Centre supervises the adherence to applicable regulations and certification standards and criteria in line with international standards, for instance, the Information Technology – Technology – System Security Engineering – Capability Maturity Model ISO/IEC 21827/2002 and the Code of Practice for Information Security Management ISO/IEC 17799-2000.[36]

[29] J. Winn and N. Jondet, 'A "New Approach" to Standards and Consumer Protection' (2008) *Journal of Consumer Policy* 31, 459-472, 459.
[30] S. Mason, *Electronic Signatures in Law* (3rd ed, CUP 2012) 126.
[31] ETL 2007, Article 1(21).
[32] T.C. Glaessner et al, *Electronic Security: Risk Mitigation in Financial Transactions: Public Policy Issues* (World Bank 2002) 40.
[33] ETL 2007, Article 1(5).
[34] ETL 2007, Article 18.
[35] ETL 2007, Articles 16-17.
[36] H.R. Rao et al, *Managing Information Assurance in Financial Services* (IGI Publishing 2007) 99.

TPPs, namely Payment Initiation Service Providers ('PISPs') and Account Information Service Providers ('AISPs'), play a similarly important role to certification providers in the context of m-payments as they identify the consumer, authenticate the consumer's credentials (i.e., their username, password, one-time password and certificate) and authorise the m-payment transaction or, in the case of AISPs, give access to the retrieval of information.[37] It, therefore, appears prudent that they too should require licensing.[38] This is important to foster trust and guarantee the integrity of the m-payment system, especially since consumers provide log-in details to them and access to their accounts, which, in turn, gives rise to the risk of digital fraud and identity theft.[39] TPPs thus play a critical role since they own the digital identities of customers.[40] It is, therefore, essential that clear rules are devised which impose liability when TPPs are responsible for fraud and errors.[41] It is also essential that a contract is entered into between the PISPs and the AISPs and the consumer and that this is a transparent and clear agreement in order that the consumer be properly protected against the risks posed by the new technology and Sharia principles of social welfare are thus properly promoted.[42]

In view of the fact that the ETL 2007 cannot be evoked, it is necessary to introduce limitations on consumer liability in SA comparable to those which have been enforced in the UK, in order to prevent companies simply shifting their responsibilities to consumers through contract terms where the reality is that the consumer has little choice but to consent or lose

[37] BBCA n 25; European Banking Federation, 'European Banking Federation (EBF) Position Paper on the European Commission Proposal for a Revised Payment Services Directive (PSD2), Brussels, 8 November 2013, 1-16, 1-2 <http://www.ebf-fbe.eu/uploads/EBF_004743%20-%20EBF_004025%20-%20EBF%20position%20on%20PSD2_08Nov2013.pdf> accessed 1 November 2016.
[38] Ibid.
[39] Ibid.
[40] BBCA n 25.
[41] European Banking Federation n 37, 2.
[42] Ibid.

access to the service. At present, the statute provides that certification service providers are held responsible for the accuracy of the information when delivered; that they have to pay damages when this is not the case and persons have relied on this information as being bona fide.[43] However, at the time of writing there is no record of any consumer having sued a certification service provider. It is therefore difficult to speculate how effective a deterrent the provision provides. The lack of any existing case may indicate the absence of either a breach or enforcement, and it is hard to distinguish between these two scenarios.

The ETL 2007 also provides that certificate holders have to safeguard the confidentiality and integrity of the electronic signature system, adhere to particular conditions, furnish accurate information, inform the certification service provider of any changes and not use parts of a revoked or suspended certificate.[44] This provision is difficult to apply to the m-payment context since the role of customers in that context is different from that of certificate holders. Yet, TPPs ought to protect the confidentiality of a customer's digital identity and AIPs ought to retrieve accurate information, whilst customers ought to safeguard the security of their mobile devices and access to their m-payment apps.

The ETL 2007 lists ten offences,[45] which applies only to certification service providers; new offences would thus have to be formulated. Penalties are also spelled out. However, the current maximum fine of Riyals 5 million and a prison sentence of five years appear too low for the m-payment context, especially when serious violations have been committed and customers have suffered significant losses. Nicoletti, therefore, argues that

[43] ETL 2007, Article 20.
[44] ETL 2007, Article 22.
[45] ETL 2007, Article 23(1)-(10).

more specific and clearer regulations are desirable.[46] However, instead of amending the ETL 2007, it appears better to regulate third-party providers in a specific law for m-payments.

5.3.1 The sources of law which govern the rights and obligations of m-payment providers and their customers, including in respect of unauthorised m-payment transactions:

This section examines the sources of law which govern the rights and obligations of m-payment providers and customers in SA: The 2012 Regulatory Rules for Prepaid Payment Services, the e-Banking Rules 2010 and the Manual of Combating Embezzlement & Financial Fraud & Control Guidelines 2008. This is done to assess the current legal situation and the basis for future change. It is highlighted that m-payment customers and, particularly their funds, are not adequately protected through these different sources of rights when using these new technological forms of fiscal transactions.

5.3.2 The 2012 Regulatory Rules for Prepaid Payment Services and a failure to address the thorny issue of unauthorised payments

Before the adoption of the Regulatory Rules for Prepaid Payment Services 2012 ('RRPPS 2012'), there was no regulatory framework for prepaid cards. The intention was to promote payment services, which allow customers to buy services and commodities with different

[46] B. Nicoletti, *Mobile Banking: Evolution Or Revolution?* (Palgrave MacMillan 2014) 107.

types of electronic cash cards.[47] The rules enable customers to make use of prepaid services after opening an account and crediting it, thus clients can purchase services and goods or withdraw money or check their prepaid card account balances at ATMs.[48] The objective was also to promote smart e-governance, since the prepaid cards are utilised by the government to pay benefits and ensure that workers receive their wages.[49] For instance, in 2012, the Ministry of Labour created the Wage Protection System and many large businesses were required to adopt the so-called 'easypay system', a high-tech payroll, and use Saudi Investment Bank's electronic prepaid cards for their workers by late 2014.[50] The latter can use these cards to receive their wages, conduct financial transactions, send remittances, withdraw money at ATMs and top up mobile phones.[51]

The RRPPS 2012 define prepaid payment services as 'the holding of monetary value in a prepaid account/electronic record that can be utilised to purchase goods or services from one or more business who agrees to participate in the prepaid program'.[52] This is a narrow definition since emphasis is placed on money being prepaid. Consequently, the definition is insufficient to facilitate the emerging m-payment revolution which, in countries like the UK, empower customers also to conduct traditional banking services in a more convenient manner through their mobile phones. For instance, the Saudi rules do not cover situations where bank

---

[47] 'SAMA issues prepaid card services rules', *Saudi Gazette*, 22 July 2012 <http://www.saudigazette.com.sa/index.cfm?method=home.regcon&contentid=20120722130670> accessed 26 October 2014.

[48] Euromonitor International, 'Pre-Paid Cards in Saudi Arabia, Market Research', 22 August 2013 <http://www.marketresearch.com/Euromonitor-International-v746/Pre-Paid-Cards-Saudi-Arabia-7583184/> accessed 25 October 2014.

[49] N. Lloyd, 'The Wages Protection Program in Saudi Arabia - how will this affect your company', Simmons & Simmons LLP, 4 January 2016 <http://www.elexica.com/en/legal-topics/employment-and-benefits/04-the-wages-protection-system-in-saudi-arabia-how-will-this-affect-your-company> accessed 1 November 2016; The Saudi Investment Bank, 'Payroll Service', 2016 <https://www.saib.com.sa/en/content/payroll-service-0> accessed 1 November 2016.

[50] Ibid.

[51] Council of Ministers' Decision No.59 dated 28.3.1420H; Saudi Investment Bank, 'easypay, Your pay...your way', 2012, 1-10, 3-4 <https://www.saib.com.sa/sites/default/files/easypay-Brochure-English.pdf> accessed 28 October 2014.

[52] SAMA, Regulatory Rules for the Prepaid Payment Services in the Kingdom of Saudi Arabia, March 2012, 1-55, 8.

customers use their overdraft to make m-payments, leaving consumers open to risk in circumstances where the account used is not in credit (particularly problematic given that consumers in this category are arguably the most vulnerable in the first place).

Such an approach does not promote Fintech innovation and, therefore, appears unwise, especially when one of the benefits of the technology is that it can replace traditional debit and credit cards.[53] As discussed in chapter 4, section 4.2.1, financial services innovation is primarily taking place in the area of remote and proximity m-payments facilitated through apps, rather than in the prepaid card sector. One potential solution to this shortcoming would be to expand the definitions within the RRPPS 2012. However, this is non-ideal as the Rules were drafted to specifically address issues associated with prepaid cards and would not cover m-payments which do not involve the use of prepaid cards stored on mobiles. Prepaid cards need not necessarily include m-payments, and vice versa; redefinition of the Rules would therefore carry the risk of being a simply cosmetic rather than substantive change, making the regulatory gap more difficult to identify but failing to resolve it. Thus, Saudi Arabian legislators may need to draft a new set of rules that have wider application to payments services, including m-payment services, not merely in name but also in substance.

Moreover, the rules currently apply automatically to prepaid payment services providers and licensed banks, so long as SAMA does not issue a formal objection on the basis that application of the rules would be inappropriate or counterproductive in the context of a specific provider.[54] The current position is anomalous because, as discussed above, the Banking Control Law 1966 makes no mention of other institutions, apart from banks and money transmitters. The extension of the jurisdiction of the rules would arguably be based on a strained interpretation of the Banking Control Law. This is because the exchange of money

[53] C. Scardovi, *Restructuring and Innovation in Banking* (Springer 2016) 33.
[54] SAMA n 52, ibid 21.

for a prepaid card is not comparable to accepting deposits, and is not a core banking business, thus falling outside the scope of the Banking Control Law. It is, therefore, important to ensure that SAMA's mandate to supervise prepaid payment service providers, and even m-payment service providers and all associated stakeholders, is put on a statutory footing.

A distinction is made between open loop, restricted loop and closed loop payment services, i.e., multiple unrelated businesses which accept the same payment, a particular or more restricted set of businesses or just one business respectively.[55] Payment cards with a microprocessor, contactless payments equipped with NFC technology, mobile payments, internet wallets or magnetic stripe cards are considered prepaid instruments.[56] This definition is slightly restrictive since m-payments are increasingly conducted through Bluetooth, as opposed to NFC technology, as discussed in chapter 1. The rules do provide that the list of instruments is not exhaustive, so that does not constitute a problem. Nevertheless, the reference to 'internet wallets' is slightly clumsy and misleading as customers can have, e.g., client-side wallets which are stored on their computers, even when their computers are not connected to the internet.[57] As technology moves rapidly, it seems better to adopt a broad definition to describe the technology which can be used to make m-payment transactions. Again, the emphasis on prepaid instruments ought to be avoided.

The rules outline different acceptance models for the various types of loop services, such as, gift cards for closed loop prepaid payment services, public transport cards for restricted loop prepaid payment services and any other prepaid goods for open loop prepaid payment services.[58] By incorporating different prepaid cards, it was intended that the data of

[55] Ibid 8-9.
[56] Ibid 9-10.
[57] E. Griffor, *Handbook of System Safety and Security: Cyber Risk and Risk Management, Cyber Security, Threat Analysis, Functional Safety, Software Systems, and Cyber Physical Systems* (Elsevier 2017) 161.
[58] SAMA n 52.

Saudis who currently do not have bank accounts would be captured and it was likely that student, salary, expenses, gift and other cards would be appealing to a broad range of consumers.[59] However, such an approach did not promote what has been labelled 'mobile banking 2.0'[60] or 'Digital bank 2.0'.[61] The neoliberal consumer economic interest is not promoted through such an approach and Fintech innovation cannot fully promote consumer choice either due to its preoccupation with closed, restricted and open loop prepaid payment services.

By contrast, in the UK, customers can increasingly choose many different m-payment providers. They can pay remotely or in close proximity with their mobiles. This is very different to loading money on a card and then being able to either pay at one particular merchant or at various different ones.

Another weakness is that, whilst the rules cover all elements in respect of prepaid payments, they do not cover services which utilise the Saudi Arabian Payments Network[62] ('SPAN'). This is despite the fact that SPAN deals with a diverse range of transactions.[63] Banks which use SPAN are additionally required to comply with the SPAN Business Books, Operating Rules and Procedures.[64] However, the International Monetary Fund ('IMF') observes that SPAN cannot at present process transactions which have been directly

[59] Bank for International Settlements, 'Payment, clearing and settlement systems in Saudi Arabia', CPSS Red Book, 2012, 349-372, 356 <http://www.bis.org/cpmi/publ/d105_sa.pdf> accessed 25 October 2014.
[60] M. Cliffe, 'Mobile Banking 2.0: Six Ways The Experience Must Evolve', The Financial Brand, 9 February 2016 <https://thefinancialbrand.com/57103/mobile-banking-experience-innovation/> accessed 1 November 2016; B. Yurcan, 'Banks Position Themselves For Mobile Banking 2.0', Banktech, 13 May 2014 <http://www.banktech.com/channels/banks-position-themselves-for-mobile-banking-20/d/d-id/1297003?> accessed 1 November 2016.
[61] SAS Institute Inc, 'The Digital Bank 2.0', White Paper <http://www.sas.com/fi_fi/whitepapers/SAS-Whitepaper-The-Digital-Bank-2.html> accessed 1 November 2016.
[62] The SPAN is the sole payment system which links point of sale terminals and ATMS and connects them to the banks or credit card providers: SAMA, SPAN, 2015 <http://www.sama.gov.sa/en-US/PaymentSystem/Pages/SPAN.aspx> accessed 1 November 2016.
[63] Ibid.
[64] SAMA n 52, 8.

submitted through mobile phones or the internet.[65] As such, the system's capability has to be enhanced. SPAN also has no mechanism to report fraudulent transactions.[66] Instead, this data is held with the issuer and it is important to require issuers to notify all fraudulent transactions, so that SPAN can then identify those merchants who engage in fraud or suspicious transactions. [67] As mentioned in chapter 4, the PSR 2017 mandates that statistical data about fraud and details about mitigation measures are provided annually to regulatory authorities.[68] Such a requirement may be useful to improve SPAN and protect customers in accordance with social welfare principles and Sharia law.

Under the rules, a licensed bank can also act as so-called 'prepaid payment service issuing programme manager' and is responsible for reimbursing acquirers and various issuing activities, such as fraud investigation.[69] Banks can outsource these activities so long as the Rules on Outsourcing are complied with.[70] It is stipulated that banks may hire a programme manager, an issuing processor, a seller/distributor and a reload/load network.[71] However, banks have to assume full liability for outsourcing and, if considered appropriate, adopt additional methods to monitor compliance.[72] This is because issuers are required to continuously monitor prepaid payment service activities.[73]

Like the e-banking rules, the Regulatory Rules for Prepaid Payment Services adopt a bank-centric approach which, arguably, does not open up the m-payment market sufficiently

[65] International Monetary Fund, Saudi Arabia: Financial Sector Assessment Program Update—Detailed Assessment of Observance of the Basel Core Principles for Effective Banking Supervision, IMF Country Report No.13/213, July 2013, 33.
[66] Ibid.
[67] Ibid.
[68] Payments UK, 'The Second Payment Services Directive (PSD2)', July 2016, 1-20 <http://www.paymentsuk.org.uk/sites/default/files/PSD2%20report%20June%202016.pdf> accessed 10 September 2016.
[69] SAMA n 52, 5-6, 12-14.
[70] Ibid.
[71] Ibid 14-15.
[72] Ibid 20, 35.
[73] Ibid 35-36.

to promote neoliberal consumer economic interests. This approach is also in marked contrast to the UK, where competition is statutorily promoted by virtue of the Communications Act 2003, as discussed in chapter 4, section 4.2.3. Hence, no true collaboration model is permitted, despite this being the most likely avenue to realise ubiquitous m-payment services.

Furthermore, the rules define a licensed bank as an acquirer which has to either follow the SPAN Scheme Regulation or the Point-of-Sale scheme.[74] SPAN accepts prepaid payments.[75] Under the SPAN Scheme, an acquirer/bank has to have an agreement with SAMA in respect of ATM transactions.[76] Under the Point-of-Sale scheme, an acquirer/bank has to have an agreement with a merchant and SAMA.[77] Merchants are those linked to an acquirer/bank and are entitled to accept payments in accordance with their contracts with the acquirer/bank.[78] They also have merchant accounts with the acquirer/bank.[79] However, the requirement to follow either the SPAN Scheme Regulation or the Point-of-Sale scheme hinders technological innovation. In turn, the neoliberal consumer economic interest suffers.

As discussed in chapter 1, technology makes it possible to directly connect the debtor's bank, where a customer holds an account, with the merchant's creditor bank since consumer identification, authentication, as well as the transaction authorisation, can be carried out by other companies called TPPs under the PSR 2017 (UK). These TPPs then act as payment initiation service providers ('PISPs') and account information service providers ('AISPs'). Notwithstanding that opening up the market to new entrants may heighten consumer risk, this ultimately creates competition and market progression and SA, like the

[74] Ibid 16.
[75] Ibid 17.
[76] Ibid.
[77] Ibid.
[78] Ibid 16-17.
[79] Ibid 17.

UK, needs to find a suitable balance between neoliberal economic principles and social welfare ideas which protect the consumer.

In addition, as SPAN is incapable of processing transactions directly submitted through mobile phones or the internet,[80] this appears to be an ineffective tool to protect customers from risk. There is presently a *lacuna* in Saudi Arabian regulation in respect of m-payment transactions, giving rise to a risk which is perhaps inevitable given the piecemeal approach taken by the authorities. It is questionable whether the use of contractual methods to risk management as between a bank and a merchant is sufficient to shield consumers in social welfare terms as required under Sharia law. It would be better if a strong customer authentication requirement similar to that provided under the PSR 2017 is imposed on banks, payment service providers and TPPs.

The rules define retail and corporate payment products and give as examples, student cards, payroll cards, customer incentive cards, government entities payment products (e.g., social insurance accounts), and corporate payment products (e.g., employee benefits cards).[81] These products have to be disclosed to SAMA.[82] Yet, as explained in chapter 1, m-payments open the door to the replacement of cash, debit and credit cards, and the introduction of a host of new functionalities which are likely to substantially innovate banking products and are more far-reaching than the examples provided. It is important for SAMA to study the innovations which m-payment services make possible and revise their examples accordingly. This also necessitates a less restrictive, neoliberal approach towards m-payment services being adopted, as discussed above, in order to allow for innovation. In this context, SAMA must particularly recognise that consumer data, e.g. generated from m-payments, is

[80] International Monetary Fund n 65, 33.
[81] Ibid 18.
[82] Ibid 20.

developing into something very valuable for companies, comparable to a new form of "currency."[83]

The rules also stipulate various restrictions for the different types of prepaid payment systems. For example, cash cannot be withdrawn at ATMs when closed loop prepaid payment products and restricted loop prepaid payment services are used. [84] By contrast, in respect of open loop prepaid payment services, cash withdrawals and transfers, including cross-border transfers, may be made, even though these functions do not have to be provided.[85] It appears unnecessary to distinguish between closed, restricted and open loop prepaid payment services since the underlying idea behind m-payment transactions should be to empower customers to pay with their mobiles. Closed, restricted and open loop prepaid payment concepts belong to the era of prepaid telephone cards and gift vouchers, whilst open loop systems confer control, e.g., for employers who use it with their employees.[86] This does not mean that closed and open loop payment solutions have no role to play within m-payments. However, the prepaid limitation appears misplaced in light of the innovation which m-payments make possible.[87]

As discussed above and in chapter 1, payment intermediaries ('TPPs'), such as, digital wallet providers, establish a direct relationship between customers and the merchant's bank.[88] The way in which closed loop systems have been defined by the rules does not permit use of a typical closed loop system, such as, PayPal.[89] Customers can hold funds in a PayPal

[83] M. Rhoen, 'Beyond consent: improving data protection through consumer protection law' (2016) *Internet Policy Review*, 5(1) <https://policyreview.info/articles/analysis/beyond-consent-improving-data-protection-through-consumer-protection-law> accessed 15 April 2019.
[84] International Monetary Fund n 65, 19.
[85] Ibid 19.
[86] R.R. Dholakia, *Technology and Consumption: Understanding Consumer Choices and Behaviors* (Springer 2012) 147.
[87] C. Scardovi, *Restructuring and Innovation in Banking* (Springer 2016) 33.
[88] Ibid.
[89] Ibid.

account and then use these funds for in-store or online payments through their digital PayPal wallet.[90] It would be better if the terminology in respect of closed, restricted and open loop payment services was better aligned with industry trends. Otherwise, the analytical capabilities which m-payment technology make possible due to their ability to generate big data will be lost by the financial services industry in SA.

However, a distinction between closed, restricted and open loop prepaid payment services is useful in terms of combating money laundering and terrorist financing. This may be one of the reasons why the rules mandate that further information has to be obtained when funds can be transferred domestically or internationally.[91] However, less stringent requirements apply to closed loop prepaid payment products,[92] but face-to-face verification should take place when money laundering or terrorist financing is suspected.[93] Hence, a distinction is made between conducting a face-to-face verification and a simpler process which applies to more limited products, e.g., m-payment services, not tied to particular bank accounts or existing credit/debit cards issued by the bank.[94] Moreover, all products should adhere to the general rules governing AML and CTF.[95]

However, the analysis of the UK's AML law reveals that a more comprehensive approach has been adopted towards combating money laundering and terrorist financing. The reason is that the objective is not only to discharge CDD, but to ensure that all payments are fully traceable. SA should, therefore, either amend its AML Law. Alternatively, there should be a duty to collect information[96] via payment service providers, including banks, in the Regulatory Rules for Payment Services, a distinct regime covering prepaid payment services.

[90] Ibid.
[91] SAMA n 52, 36.
[92] Ibid 23.
[93] Ibid 36-37.
[94] Ibid 21-23, 34-35.
[95] Ibid 35.
[96] MLRs 2017, Regulation 15(3)(a)-(g).

Transparency would be significantly heightened if the name of the payer and payee, their respective bank account details, as well as the payer's address, were collected. Such an approach would also help to ensure that SA's law complies with FATF Recommendation 16[97] which deals with wire transfers.[98] This Recommendation urges countries to make sure that financial institutions obtain originator information and beneficiary information when wire transfers are made, as well as the related messages.

Another shortcoming which leaves Saudi m-payment customers unprotected is that the current RRPPS 2012 only contain provisions concerning data protection in respect of AML and the opening of bank accounts and related guidelines.[99] This appears wholly insufficient to shield m-payment customers in terms of 'big data' (i.e., information characterised by volume, velocity, and variety)[100] which m-payment transactions facilitate,[101] especially when no general data protection law exists in SA.[102] SA should enact a data protection law, or at least consider enacting rules for m-payment transactions similar to those which exist in respect of credit information (discussed below in section 5.5.2), in order to enact the social welfare provisions of Sharia law.

Another problem, albeit not one which undermines social welfare-based consumer protection, is that the RRPPS 2012 relate to distance selling contracts although m-payment

[97] FATF, 'International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation', The FATF Recommendations 2012, June 2012, 1-129 <http://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF%20Recommendations%202012.pdf> accessed 1 October 2017.
[98] Ibid 15.
[99] SAMA n 52, 37-38.
[100] A. De Mauro et al, 'A formal definition of Big Data based on its essential features' (2016) *Library Review* 65(3), 122-135, 122.
[101] A. Chambers and G. Rand, *The Operational Auditing Handbook: Auditing Business and IT Processes* (2nd ed, John Wiley & Sons Ltd 2010) 755.
[102] N. Al-Fawzan and O. Elsayed, 'Data Protection in the Kingdom of Saudi Arabia: A Primer', Latham & Watkins LLP, 2015, 1-2, 1 <https://www.lw.com/presentations/Data-Protection-in-the-Kingdom-of-Saudi-Arabia> accessed 1 November 2016.

transactions should not be construed as distance sales contracts.[103] This is because a distance selling contract is between the customer and the merchant who do not contract on a face-to-face basis but through remote means (e.g., online, telephone or post) for the *purchase* of goods/services whereas m-payment represents the use of, e.g., e-money, prepaid cards, credit/debit cards and/or electronic funds transfer, through a mobile with which the customer *pays* for goods/services. Issues in relation to distance selling ought rightly to be addressed in a specific law. However, equivalence in treatment between distance selling and m-payment services may be misplaced since the former deals with a very different type of contract.

Furthermore, the RRPPS 2012 provide that SAMA can investigate transactions, compliance problems, affiliates, books and accounts and impose sanctions for non-compliance with the rules.[104] However, overseeing m-payment systems is no easy task and the rules do not spell out the powers and policies of SAMA. It is important for SAMA to further develop its oversight arrangements, particularly with the view to strengthening social welfare-based consumer protection. Khiaonarong argues that this means adopting policies so that standards and requirements are clarified, and international standards are adopted.[105] In doing so, the regulator is equipped with sufficient powers to discharge its oversight duties, systematically and fairly enforcing oversight standards and working in close cooperation with other foreign regulators and authorities.[106] The IMF, therefore, proposes that ideally a specialised oversight unit or body should be created, as well as a payment system operations

[103] SAMA n 52, 38-39.
[104] Ibid 37.
[105] T. Khiaonarong, 'Oversight Issues in Mobile Payments', International Monetary Fund Working Paper No. 14/123, July 2014, 1-36, 15.
[106] Ibid.

unit.[107] Equally, the G20 High-Level Principles on Financial Consumer Protection require that specific oversight bodies are created to ensure financial consumer protection.[108]

For instance, in the UK, an independent Payment Systems Regulator was established by virtue of the Financial Services (Banking Reform) Act 2013, which, amongst other objectives, is responsible for ensuring that service-users' interests are safeguarded.[109] Financial consumer protection is further promoted through the FOS and the UK Competition and Markets Authority.[110] Equally, SA must create such bodies in order to protect consumers in terms of social welfare and Sharia law.

The rules also contain provisions so that customers can resolve disputes about billing errors.[111] Customers must challenge billing errors within 180 days.[112] When providing prepaid payment services, banks are given eighteen days to investigate any billing errors relating to a prepaid payment instrument.[113] Customers can also request documentary evidence from their bank.[114] Customers must be refunded where the bank determines that there was a billing error.[115] In the case of disputes, customers can escalate their complaint to SAMA.[116] If the customer is still not satisfied with SAMA's decision, it can request the Committee for Banking Disputes to review the case.[117] Both SAMA and the Committee have the power to enforce the bank's obligation to refund the customer for errors. Decisions by the

[107] International Monetary Fund, Saudi Arabia: Financial Sector Assessment Program Update—Detailed Assessment of Observance of the Basel Core Principles for Effective Banking Supervision, IMF Country Report No.13/213, July 2013, 6.
[108] OECD, G20 High-Level Principles on Financial Consumer Protection, Paris, OECD, October 2011, 1-7, 5.
[109] Financial Conduct Authority, Consultation Paper, A new regulatory framework for payment systems in the UK, PSR CP14/1, November 2014, 1-111, 3&7 <http://www.fca.org.uk/static/documents/psr/psr-cp14-1-cp-a-new-regulatory-framework-for-payment-systems-in-the-uk.pdf> accessed 17 May 2015.
[110] Ibid.
[111] SAMA n 52, 43-53.
[112] Ibid 46.
[113] Ibid 47.
[114] Ibid.
[115] Ibid.
[116] Ibid 48.
[117] Ibid.

Committee for Banking Disputes can be appealed in front of the Committee of Appeal for Banking Disputes and Violations. These appeal decisions are then final. A clear process has been created to challenge disputes and this offers some consumer protection. However, it may be noted that the scope of protection is less than in the PSR 2017 (UK), in which consumers are safeguarded against loss not only where there is a 'billing error' but also in all other circumstances which do not involve fraud or gross negligence. By contrast, the remedies provided by SAMA are restricted to errors on the part of the bank; there is therefore a 'gap' where the loss may have been caused by a third-party error, or by a fault for which responsibility cannot be attributed.

It is important to extend the dispute settlement process to cases where the prepaid payment instrument is lost or stolen, or the customer has failed to keep his/her personalised security features secure. It is essential that the rules address the thorny issue of negligence liability, which they fail to do at present. Instead, they only state that customers should be informed about any liability or limit if the payment device is misused, stolen or lost and that liability for any further amounts ceases after notifying the issuer.[118] Whilst the rules provide that unfair contracts terms are void, it is unclear how this point might be interpreted and whether, for instance, recourse might be made to the e-Banking Rules 2010, which require consumers to, e.g., install up-to-date antivirus software (as discussed in section 5.3.3 below). Legal uncertainty is thus created, and customers are hence not adequately protected against unauthorised m-payment transactions, but only against a much narrower operational risk which causes billing errors. This suggests a more neoliberal way of dealing with issues of legal responsibility which apparently views the consumer as circumspect individuals, thus not protecting the vulnerable or, arguably, adhering to Sharia law.

[118] SAMA n 52, 41-42, para.2.8.2.

There thus exist many issues with the RRPPS 2012. They fail to adhere to the Islamic business principle of allowing sellers and buyers to trade freely. The reason for this is that banks are being favoured and new entrants are being prevented from entering the emerging m-payment market. Social welfare is not promoted. Nor is consumers' economic interest being sufficiently facilitated, unlike in the UK where promotion of competition has been high on the policy agenda of the UK legislators, as discussed in chapter 4, section 4.2.3.

This analysis shows how the consumer protection interest is underdeveloped in many areas as SPAN fails to include m-payments and does not screen against fraud. AML requirements further require improvement. Customers have no guarantee that their financial information, including personal data, is adequately protected. No specialised payment system bodies have been created to protect consumers and a process for customers to challenge billing errors is the only form of legal recourse that has been created. However, the one of the most pressing topic of negligence liability has yet to be addressed. Consequently, the law needs to be further improved and the IMF recently strongly recommended that a 'comprehensive payment system law' be passed. This is needed in order to promote the principles of social welfare enshrined in Sharia law.[119]

[119] International Monetary Fund n 65, 4.

5.3.3 The e-Banking Rules 2010 and a neo-liberal consumer understanding and failure to update them to account for new technological risks, unauthorised m-payment transactions, and third-party providers

In April 2010, the banking technology department of SAMA issued e-banking rules.[120] These rules replaced the earlier Internet Banking Security Guidelines 2001.[121] The rules define e-banking, spelling out the evolution of e-banking and explaining the rules and their objectives, scope of application and date of application. SAMA defines e-banking as:

> Remote banking services provided by authorized banks, or their representatives through devices operated either under the bank's direct control and management or under the outsourcing agreement. In other words, e-banking is an umbrella term for the process by which a customer performs banking transactions electronically, without visiting a branch and it includes the systems that enable customers of banks, individuals or businesses, to access accounts, transact business or obtain information on financial products and services through a public or private network, including the Internet.[122]

M-payment transactions provided by banks and their agents thus fall within this definition as they enable customers to conduct their financial affairs without visiting a branch and through a system, which also relies on the internet. For the avoidance of doubt, it would be better if the rules expressly stated that they also applied to m-payments. The definition of e-banking, however, is sufficiently wide to accommodate m-payment offered by banks to customers, though not m-payment services offered by non-banks.[123]

---

[120] SAMA, E-Banking Rules, April 2010, 1-36, 1-3.
[121] Ibid 5.
[122] Ibid 4.
[123] Remote banking service is further defined as '[d]edicated banking service for which the Customer has explicitly registered and authorized; Service supplied using devices that are not under the control of the

The providers of m-payment services are not confined to banks as part of banking services under traditional statutory definitions and can extend to non-banks. Moreover, the definition provides that Automated Teller Machines ('ATMs') and phone banking services are not included within the definition. As discussed in chapter 1, m-phones may be used in future at ATMs and some prepaid electronic cards can already be used to settle transactions and withdraw money from them. It may even be possible, as in the UK, to use 'virtual' credit and debit cards to make payments via m-apps without the need for a physical card.[124] Hence, the definition of e-banking may have to be extended because the boundary will become further blurred in light of technological advances and Fintech innovations embedding credit card features within electronic payment cards held on portable devices.[125]

Currently, the rules apply to all banks licensed by SAMA, including subsidiaries and branches located abroad.[126] Banks can choose to provide e-banking directly or appoint representatives, provided that they adhere to SAMA's Rules on Outsourcing.[127] Such an approach makes it harder for a collaboration or operator-centric model to emerge since a bank-centric approach is endorsed.[128] However, a bank-centric approach may reduce competition which, in neoliberal terms, may not be in the interests of customers: It can lead to, e.g., poor, outdated and lower quality services.[129] Consequently, the consumer economic interest is not being promoted in free market terms.

Furthermore, the rules provide that senior management and the board of directors are accountable, customers must be educated and protected, their privacy secured, international

---

Provider; Service which demands the authentication of the Customer': SAMA, E-Banking Rules, April 2010, 1-36, 4.

[124] Google Pay, 2019 <https://pay.google.com/intl/en_uk/about/> accessed 15 April 2019.

[125] See Chapter 1.

[126] Ibid.

[127] Ibid, Chapter 1, 7.

[128] K. Al Agha et al, *Mobile and Wireless Networks* (ISTE Ltd and John Wiley & Sons Inc 2016) 235.

[129] P.M. Carare, 'Monopoly: Advantages and Disadvantages' (2011) Alexandru Ioan Cuza University, 1-6, 2 <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1787089> accessed 1 November 2016.

security standards adhered to, incidents managed and reported to SAMA, management be fully available and capacity must be built with regard to continuity planning.[130] However, no requisite legal procedures to enforce these rather broad assurances have been stipulated, thus leaving the risks to consumers unmitigated. For example, in the absence of a data protection law, it will be challenging for customers to seek remedies from banks for failing to protect their data. The rules are further unclear about the scope and extent to which customers may hold senior management and the board of directors accountable. In other words, no rights have really been conferred but, as noted in chapter 3, this may in part be due to Islam generally achieving adherence through imposition of duties rather than rights.[131]

By contrast, s150 of the FSMA 2000 (UK) stipulates that a breach of the rules of conduct may give rise to an action for damages, as discussed in chapter 4, section 4.3.3. Equally, customers can pursue proceedings when there is a failure to comply with any of the safeguarding requirements in the PSR 2017 (UK).[132] Real consumer protection based on Sharia principles of social welfare will only be realised if similar laws are enacted in SA which add weight to these e-banking rules. Otherwise, customers are unlikely to be able to invoke their rights and for these objectives to be achieved.

Another problem with the e-banking rules is that they fail to list the risks pertaining to apps, digital wallets (i.e. client-based and server-side wallets) and clouds, through which financial services are increasingly offered. The rules are very general and only mention different risk levels,[133] as well as the risks associated with fully transactional websites, information-only websites and information transfer websites.[134] This seems an outdated

[130] Ibid.
[131] Rice n 11, 345.
[132] PSR 2017, Regulation 23.
[133] Ibid 12-13.
[134] SAMA, E-Banking Rules, April 2010, 1-36, 12.

approach to take since m-payments are primarily conducted through apps. The rules should, therefore, be updated in order to ensure that the specific risks associated with m-payments are detailed in order to adequately protect the consumer.

Under these rules, the board of directors of a bank has a duty to identify and manage the different risks, adopt adequate risk management processes and policies, and conduct audits and internal checks.[135] This necessitates a risk analysis and quantification of risks.[136] When a particular risk materialises, the bank must consider how best to deal with the loss. It further means constantly monitoring and reviewing risks as they can change.[137]

However, as noted above, not all risks have been detailed. Whilst a complete list of risks is unrealistic, it is important that at least the more obvious risks are mentioned. Without this, banks may argue that they have discharged their duties when they have clearly failed to do so, leaving consumers potentially exposed to fraud, mischief and losses, all of which are forbidden under Sharia law.

It is also problematic to rely solely on banks to combat risks effectively. Although there is a strong argument that they *should*, banks are not necessarily information and communications technology experts. Hence, it may be better if the rules make clear that the respective partners of the bank are also obligated to identify and manage certain risks and adopt adequate risk management processes in order for the public to be properly protected.

In addition, the e-banking rules adopt fourteen principles, which are based on the Basel Risk Management Principles for Electronic Banking.[138] However, as highlighted by the 2013 G20 recommendations, and in the context of m-payments, SA should indicate how

[135] Ibid 13-14.
[136] Ibid.
[137] Ibid.
[138] SAMA, E-Banking Rules, April 2010, 1-36, 18.

banks comply with the Basel Committee on Banking Supervision's 'principles for the sound management of operational risk 2011'.[139] The Basel Committee recommendation imposes a number requirements based on the 'fundamental principles' of risk management, particularly an emphasis on the board of directors' essential role in establishing a 'strong risk management culture' throughout the whole organisation and the need for banks to develop, implement and maintain a fully integrated framework within their overall risk management processes which reflects the nature, size, complexity and risk profile of the company in question. Otherwise, it will be difficult to adequately protect customers from the heightened operational risks which arise from m-payment transactions, as discussed in chapter 2. At present, the fourteen principles are divided into the following three broad topics. The first three principles deal with board and management oversight while principles four to ten set out minimum security controls. Principles 11-14 address legal and reputational risk management.[140] SAMA should at a minimum add one more section specifically dedicated to operational and technological risk.

The e-banking rules could impose higher security thresholds in order to heighten customer protection. Presently, they provide that banks should adopt a strategic policy and clear processes for their internal audits and the testing of vulnerabilities, including ethical hacking of all applications, systems and networks.[141] Hence, banks should conduct penetration tests – also called white hat or ethical hacking – in order to identify security issues within the different components which facilitate e-banking.[142]

---

[139] Survey of National Progress in the Implementation of G20/FSB Recommendations, Saudi Arabia, 1-44, 43 <http://www.financialstabilityboard.org/implementation_monitoring/saudi_arabia_2013.pdf> accessed 20 October 2014.
[140] Ibid 18-25.
[141] SAMA, E-Banking Rules, April 2010, 1-36, 18.
[142] R. Mukhopadhyay and A. Nath, 'Ethical Hacking: Scope and challenges in 21st Century' (2014) *International Journal of Innovative Research in Advanced Engineering*, 1(1), 30-37, 30.

As discussed in chapter 4, section 4.3.2, under the PSR 2017 (UK), however, a security policy must be provided which consists of a comprehensive risk analysis.[143] It must be explained how fraud is being combated and the way in which personal and sensitive data is being kept secure.[144] In addition, incident management processes must be adopted, so that security and operational incidents can be detected and classified.[145] Statistical data about fraud, details about mitigation measures, security and operational risk assessments must also be provided to the regulator.[146] Regulatory technical standards on strong customer authentication and secure communication must also be complied with.[147] When these criteria are not met, customers cannot be held responsible for any losses, except when they commit fraud and this provides high levels of consumer protection.[148]

Like the PSR 2017, the Saudi e-banking rules require that banks report all high or medium risk security incidents.[149] Moreover, the Saudi e-banking rules state that banks must state the measures which will be taken to avoid the recurrence of such a problem. By contrast, the PSR 2017 mandates that affected customers must be informed.[150] This is a more social welfare-based and consumer-friendly approach than the one currently utilised in SA. Also, as argued before, it is important to extend these security duties to the different stakeholders within the ecosystem in order to maximise the use of their different forms of expertise.

Furthermore, the e-banking rules make clear that it falls on SAMA to assess whether risk management processes and security protocols are sufficiently thorough.[151] However, the task of scrutinising whether this is the case is not an easy one to discharge. Hence, the UK

[143] Payments UK n 68, 12.
[144] Ibid.
[145] Ibid.
[146] Ibid.
[147] Ibid.
[148] Ibid.
[149] SAMA, E-Banking Rules, April 2010, 1-36, 8.
[150] Ibid.
[151] Ibid.

has specifically created the office of the Payment Systems Regulator to do so.[152] SA should consider creating a similar body or, at least, a specialised department within SAMA. Initially, officers could receive support from third-party security auditors[153] until more capacity is developed. This may help with identifying whether banks' risk management plans have been implemented.

The e-banking rules do address the topic of consumer protection and the rights and liabilities of banks and customers are spelled out.[154] For instance, the e-banking rules require that banks: provide intelligible contracts to their customers; give advance notice of any disruption; explain the level of service clearly; and educate customers about the importance of adopting robust authentication mechanisms (e.g., choosing strong passwords).[155] However, these measures resemble the neoliberal paradigm which generally advocates disclosure. Chapter 3 highlighted that such an approach is premised on customers being reasonably circumspect although such a conceptualisation is strongly contested by behavioural economics. The social welfare objectives of the Sharia are, therefore, insufficiently realised. Hence, SAMA should formulate more far-reaching rights for customers in order to discharge its Sharia duty under Article 6(a) of the Charter of SAMA 1957.[156]

In that respect, it is important that SAMA requires banks to specify their obligations in the terms and conditions which they provide to their customers.[157] This should be done in a way which is easy to understand, so that customers are aware that they can hold banks liable in instances where the banks are in breach of their obligations as stipulated by SAMA, unless

[152] Payment Systems Regulator, 2017 <https://www.psr.org.uk/> accessed 1 October 2017.
[153] J. Linkous, 'Security Audit: The Pitfalls of Third-Party Assessments', RSA Conference, 9 September 2014 <https://www.rsaconference.com/blogs/security-audit-the-pitfalls-of-third-party-assessments> accessed 1 November 2016.
[154] SAMA, E-Banking Rules, April 2010, 1-36, 9.
[155] Ibid 9.
[156] As mentioned above, this provision requires it to act in a manner which does not conflict with the teachings of the Islamic law.
[157] SAMA, E-Banking Rules, April 2010, 1-36, 10-11.

there has been a failure or omission by the customer in safeguarding their personal information or fraud by the customer.[158]

The fourteen general obligations which banks owe to customers, such as potential liability for spreading viruses, can easily be extended to m-payments. SAMA should, however, clarify that these principles also apply to m-payments. However, some Saudi banks, e.g., Saudi Hollandi Bank, have adopted a set of terms and conditions which apply to their internet and m-banking services.[159] Although these do not mirror exactly the SAMA rules, they generally provide rights that are comparable (e.g., the circumstances in which service may be interrupted are broader). Terms and conditions provide a clear indication of the rights of the consumer but there is variance between various providers which may cause confusion and misunderstanding; a customer, who has previously dealt with one provider on the basis of their set of terms and conditions, may find that their rights are different when they switch to a different provider. This illustrates the importance of ensuring that consumers are adequately informed and educated so that they can make informed choices when deciding whether to switch service providers.

To some extent, education of customers is already required by the e-banking rules which states that banks must educate customers about, e.g., awareness and avoidance of online fraud.[160] However, the rules establishing the requirement for banks to bring these issues to the attention of customers are drafted with traditional internet banking, based on an old-fashioned web browser, in mind. No mention is made of apps, which are now predominantly used to provide m-payment services.[161] Hence, the e-banking rules fail to

[158] Ibid 11.
[159] Saudi Hollandi Bank, 'Terms and Conditions', 2016 <https://www.shb.com.sa/SHBFORMS/Terms/en/ribtermsen.htm> accessed 1 November 2016.
[160] SAMA, E-Banking Rules, April 2010, 1-36, 9-10.
[161] Innovation Edge, 'Mobile Banking', April 2012, 5.

address the question of where customers download such apps from and how to install them safely on their smartphones. This omission is in part due to the failure of Saudi regulators to update the law to reflect advances in technology. In the absence of satisfactory regulation, this is an issue which banks might take positive action to address individually through, e.g., formulation of their terms and conditions which go beyond SAMA's limited requirements. However, this approach heightens the need to make consumers aware of distinctions between the terms offered by different providers.

The existing e-banking rules are thus not adequate for m-payments. Moreover, the rules provide that banks are not responsible for customers failing to safeguard their passwords or other personal information.[162] The requirement to educate customers (e.g., advising them not to disclose personal information when they receive unsolicited emails or to unauthorised individuals,[163] or not using shared or public computers for banking, plus the importance of installing up-to-date antivirus software and a personal firewall)[164] means that customers are conceptualised as regulatory, circumspect subjects in a neoliberal sense.[165] By corollary, they are deemed capable rather than vulnerable, i.e., that they are capable of acting, or learning to act, responsibly. Thus, the protection model is drawn from elements of both neoliberal and social welfare conceptions of the consumer.

It may be argued that this is an inappropriate conception of the consumer in view that the e-banking rules do not require banks to make a refund to customers immediately in cases where there is a breach of their obligations to safeguard customers' funds and personal details. The lack of remedy afforded to customers in such circumstances reinforces the

[162] Ibid 11.
[163] SAMA, E-Banking Rules, April 2010, 1-36, 9-10.
[164] Ibid 10.
[165] I. Ramsay, 'Consumer Law, Regulatory Capitalism and the 'New Learning' in Regulation' (2006) *Sydney Law Review* 28(9), 9-35, 9 and 13.

underlying notion that customers make a choice and bear the risk of banks' non-compliance. The reason for this is that customers have not been equipped with any legal redress mechanism. Instead, they are simply assigned the duty to learn how to best protect themselves. Whilst such a learning duty is generally acceptable, the regulations should also entitle customers to seek a refund when they have discharged their duty to act responsibly.

As discussed in chapter 4, in the UK, an unauthorised transaction must be refunded in full.[166] Customers' liability is limited to £35 where the payment instrument has been lost or stolen or they have not kept secure their personalised security feature.[167] This right arises automatically so long as customers make a complaint within eight weeks[168] and they have not been grossly negligent or fraudulent. A review of the e-banking rules in SA demonstrates that a similar procedure of limiting customers' liability in cases of unauthorised transactions (e.g., when cyber criminals have appropriated money from their accounts) has been omitted. Consequently, vulnerable customers are not protected as it is extremely difficult to hold banks accountable and consumer protection and the social welfare aspects of Sharia law are not being met. Whilst customers can complain to SAMA, they cannot evoke any right to a refund like in the UK. Furthermore, it is unclear how SAMA would resolve such disputes, so it may mean that the evidential burden falls on customers. However, it is difficult for customers to demonstrate that they have adequately safeguarded their passwords and banks may also be reluctant to publicise that their systems have been hacked. This would make it difficult for customers to prove that they were victims of cyber criminals who have exploited weaknesses within the m-payment infrastructure.

[166] PSR 2017, Regulation 76.
[167] PSR 2017, Regulation 77.
[168] PSR 2017, Regulation 80.

Other questions also remain in terms of attributing responsibility. For example, the banking rules do not address whether customers should be held entirely liable or proportionately liable, together with banks, when they have not switched on their antivirus programmes or their firewall is not up-to-date or they have used public computers, despite the advice of their banks. Cyber criminals may then gain unauthorised access because of such oversights. It is also unclear whether the SAMA rules are duly incorporated into the terms and conditions of the contract between bank and customer. The rules do not state that banks cannot exclude any of their stipulated obligations. This leaves a degree of uncertainty as to whether the rules are incorporated as contract terms by implication unless excluded, or must be actively incorporated in the same manner as self-regulatory and voluntary codes of conduct. The Islamic good faith and profit and loss sharing principles may be evoked to strike down unfair terms, yet, as discussed above, SAMA does not fulfil the role of a Sharia court and adopts instead a modern, neoliberal approach towards banking.

The e-banking rules, therefore, provide general guidance, but do not address the thorny questions noted above. This creates uncertainty for customers who have to resort to challenging their banks when problems occur, and this undermines consumer protection. Moreover, the e-banking rules do not explain how disputes can be resolved. The issue of customers resolving disputes was criticised by the G20 in 2013.[169] In response, SA confirmed the importance of 'financial inclusion working committees' to further strengthen consumer protection, and a Consumer Protection Department was established within SAMA.[170] However, no consumer protection law exists to date, though a draft bill for a law was prepared in 2014, which would create an independent body responsible for monitoring

[169] Survey of National Progress in the Implementation of G20/FSB Recommendations n 139.
[170] Ibid.

unethical practices.[171] By 2017, this bill had still not yet been adopted, thus weakening the case that SA is going to adopt a social welfare-based approach to consumer protection which accords with Sharia law.[172]

It would, therefore, be useful if the rules required banks to make customers aware in their terms and conditions that they can escalate complaints to SAMA's Consumer Protection Department. Ideally, an easy process should be outlined by banks which customers could follow when they feel that their rights as set out in the e-banking rules have not been upheld. In this context, it may be important to require banks to alert customers that their rights and obligations are spelled out in the e-banking rules. Without these changes, customers appear to be insufficiently protected and the social welfare objective of the Sharia is unlikely to be met.

5.3.4 The Manual of Combating Embezzlement & Financial Fraud & Control Guidelines 2008 and the failure to address risks arising from third-party collaboration, particularly unauthorised m-payment transactions

In 2008, SAMA issued the important 'Combating Embezzlement Manual.'[173] The manual defines fraud as, 'any act involving deceit to obtain a direct or indirect financial benefit by the perpetrator or by others with his help, causing a loss to the deceived party'.[174] This broad definition can be applied to the m-payment context to mitigate the risk posed to consumers.

---

[171] Zawya, 'Consumer protection law under Shoura study', 12 November 2014 <https://www.zawya.com/story/Consumer_protection_law_under_Saudi_Shoura_study-ZAWYA20141112035028/> accessed 18 May 2015.
[172] Shoura, 'Shoura discusses consumer protection law', Saudi Gazette, 5 October 2017 <http://saudigazette.com.sa/article/178256/Shoura-discusses-consumer-protection-law> accessed 20 April 2019.
[173] SAMA, Manual of Combating Embezzlement & Financial Fraud & Control Guidelines 2008, 1-51, 1 <http://www.sama.gov.sa/sites/samaen/RulesRegulation/Rules/Pages/prevention_of_fraud_v21.pdf> accessed 26 October 2014.
[174] Ibid 7, para.2(2).

However, the manual could be further updated since, at present, the section about the role of technology is rather terse[175] and technological risk which causes unauthorised m-payment transactions is heightened in the context of m-payments, as discussed in chapter 2. Currently, the manual requires banks to adopt a plan to combat and prevent fraud and imposes eight specific conditions, e.g., to develop and implement a strategy to combat fraud, as well as a control policy.[176] A similar approach has been adopted in the UK where authorised companies have to demonstrate that risk is properly managed through internal control mechanisms.[177]

Social welfare-based consumer protection could be further strengthened if other parties involved in the provision of m-payment services, such as, merchants and mobile network operators, were also required to adopt similar plans to combat fraud, even bank- or operator-centric systems,[178] as discussed in chapter 1. Cyber fraudsters can attack banks, merchants/agents, mobile network operators and TPPs, or use weaknesses within a mobile handset or the application programming interface ('API'). In other words, security risks emanating from third parties may cause losses to customers. The scope of the manual should, therefore, be extended in order to fully meet the social welfare principles of Sharia law.

Otherwise, customers are insufficiently protected if only banks must combat and prevent fraud, especially in a collaborative financial model.[179] As a bank is only responsible for a small aspect of the m-payment ecosystem, it is important that other parties which are responsible for the mobile handset, payment applications or other ecosystem functions[180] take steps to combat and prevent fraud. These steps could be commensurate with their respective

[175] Ibid 10.
[176] Ibid 9-10.
[177] PSR 2017, Regulation 6(6).
[178] Al Agha et al n 128, 235.
[179] Ibid.
[180] Smart Card Alliance n 24, 9.

roles by including a proportionality requirement in order to promote consumer protection that fits with Sharia law. Alternatively, banks could formulate strategies which allocate responsibility amongst different stakeholders and this would represent a more neoliberal, business-friendly approach.[181] However, it may be challenging to carry out effectively the task of explaining risks, as well as the mitigation strategies of various sources in an inclusive manner.[182]

Irrespective of whether the information is presented by banks or other stakeholders, specific types of risk (e.g., DoS attacks, server impersonation attacks, eavesdropping, data alteration and stolen devices) within the m-payment ecosystem should be identified in order to allocate responsibility to the party best placed to prevent and combat that risk.[183] For instance, those responsible for the app or device security should consider where risks emanate from[184] and then develop and implement appropriate strategies and policies accordingly.[185] Due to the collaborative nature of this form of commerce, it is also important that their individual plans complement each other. Each party has to know which particular type of risk it is assuming responsibility for and SAMA should be informed. It is questionable whether the role of SAMA should be more involved, e.g. by taking the lead in setting rules and guidelines to identify which of the parties should have responsibility and oversight of managing particular types of risk. This could offer one means of providing the type of risk handling envisaged by Saha and Sanyal below.

---

[181] A. Saha and S. Sanyal, 'Review of Considerations for Mobile Device based Secure Access to Financial Services and Risk Handling Strategy for CIOs, CISOs and CTOs' (2015) *International Journal of Advanced Networking and Applications*, 6(4), 2427-2434, 2427.
[182] Ibid.
[183] Also see chapter 3, section 3.4.
[184] A.-S. Pathan, *Security of Self-Organizing Networks: MANET, WSN, WMN, VANET* (Taylor and Francis Group 2011) 148.
[185] M.G. Harvey, *Wireless Next Generation Networks: A Virtue-Based Trust Model* (Springer 2014) 4.

Specific anti-fraud policies should be developed so that security weaknesses do not arise; consumer risk will thus be lessened, and Sharia law adhered to. Saha and Sanyal opine that a risk-handling strategy for financial services provided via mobile devices requires that stakeholders within the m-payment structure identify particular fraud risks, detailing the approach towards dealing with these risks, setting out the degree of risk acceptance and ways to mitigate risks and developing and implementing strategies to address these different risks.[186] Hence, clear risk handling procedures must be adopted for different vulnerabilities and threats if consumers are to be properly protected.[187]

Even if the 2008 Manual is not extended to all stakeholders, it should at a minimum require banks to formulate comprehensive strategies which corresponding stakeholders have to adopt so that there is a joined-up approach to combat and prevent fraud in m-payments transactions. However, given the complex nature of an m-payments services network, it is argued that such a task is better discharged by the respective stakeholders than banks alone.[188] Alternatively, SAMA could issue regulatory technical standards to prevent and combat fraud, similar to those published by the EBA, as discussed in sections 4.3-4.4 of chapter 4. Respective parties could also be required to show that they have obtained certain trustmarks.[189] As noted in chapter 3, trustmarks prove that certain technical standards have been met. More responsible norms of business behaviour would thus be created which, in turn, would safeguard customers against fraud and further the social welfare principles of Sharia law.

[186] Saha and Sanyal n 181, 2427.
[187] Ibid 2429.
[188] Ibid 2436.
[189] G.-P. Calliess, 'Transnational Consumer Law: Co-Regulation of B2C-E-Commerce' (2007) Law Research Institute Research Paper Series 3(3), 1-54, 6.

5.4.1 The 2013 Banking Consumer Protection Principles and Banking Consumers' Guide and the problem of utilising the principles and guide to seek compensation for unauthorised payments and data breaches

In June 2013, SAMA adopted banking consumer protection principles, as well as a financial consumer protection implementation model. These principles entered into force on 1 September 2013 and are mandatory for all banks supervised by SAMA.[190] Eight principles have been adopted for internet and ATM banking services and four principles deal with errors.[191] These principles are further supplemented by key commitments.[192] The 2013 principles provide a complaints process whereby complaints can be brought by consumers to SAMA's Consumer Protection Department.[193] Broadly, these principles seek to ensure that consumers who have dealings with licensed financial institutions "receive the expected level of fair treatment, honesty, and ease of access to financial products and services'.[194] This is achieved through a complimentary framework of non-binding policy principles which financial institutions are encouraged to achieve, and directives/regulations with which they are required to comply. However, because the definitions used in the Principles and Guide often lags behind developments in technology, it is unclear whether the principles apply to m-payment services, in which case the usefulness of the complaints process to deal with m-payment disputes may be limited. SAMA should therefore provide clarification. This is particularly important due to the limited level of consumer protection provided by the 2012 Regulatory Rules for Prepaid Payment Services. Given that the 2012 Regulatory Rules limit disputes to billing errors, customers are likely to find it difficult to rely on these principles in

[190] Ibid 7.
[191] SAMA, Consumer Protection Department, Banking Consumer Protection Principles, June 2013, 1-28, 21 <http://www.anb.com.sa/pdf/banking/Banking_Consumer_Protection_Code_SAMA_English.pdf> 24 September 2014.
[192] Ibid 13.
[193] Ibid 2.
[194] Ibid 4.

cases where they are victims of online fraud or when other rules have been breached. For this reason, it should be made clear whether complaints relating to m-payment disputes can be made to the Consumer Protection Department. Moreover, in light of the terms and conditions of banks, such as, SABB[195], as discussed above, it is important for SAMA to enforce these consumer protection principles. At present, these principles do not clarify whether fines will be imposed for non-compliance. SAMA's Consumer Protection Department should publish information about the rates of non-compliance by banks and the sanctions imposed.

The banking consumer's guide was 'designed to ensure that banks meet SAMA's strategic objectives in promoting transparency, fairness and ease of access to financial products and services for consumers, especially in the resolution of consumer complaints.'[196] The guide's ten principles are modelled on the G20 High Level Principles on Financial Consumer Protection 2011:[197] Equitable and fair treatment; disclosure and transparency; financial education and awareness; behaviour and work ethics; protection against fraud; protection of privacy; complaints handling; competition; third parties and conflict of interest.[198]

However, as discussed in chapter 3, the G20 High Level Principles on Financial Consumer Protection 2011 focuses on providing consumers with important information rather than substantive rights (e.g., to a minimum standard of protection, or to access to dedicated dispute resolution mechanisms to enforce obligations against the service provider). Hence, they are best viewed as a neoliberal version of consumer protection as the market is free to

[195] SABB, 'SABB Mobile - Mobile Banking', 2017 <http://www.sabb.com/en/everyday-banking/ways-to-bank/sabb-mobile/> accessed 1 October 2017.
[196] A. Polat and A.A. Alsaif, 'Consumer Protection in Banking: Investigating the 10 High Level Principles of G20 in Saudi Arabia' (2014) *Journal of Applied Finance & Banking* 4(3), 195-215, 196.
[197] Survey of National Progress in the Implementation of G20/FSB Recommendations n 139.
[198] Saudi Arabian Monetary Agency, Consumer Protection Department, Banking Consumer Protection Principles, June 2013, 1-28 <http://www.anb.com.sa/pdf/banking/Banking_Consumer_Protection_Code_SAMA_English.pdf> 24 September 2014.

dictate the terms on which consumers interact with service providers, and the role of the state is limited to ensuring that the consumer is sufficiently informed to act rationally in their own interests. They, therefore, would not achieve genuine Sharia compliance in terms of providing social welfare to consumers.

The banking consumer's guide reflects the typical Islamic approach to moral issues. It outlines consumers' responsibilities, e.g., notifying banks of unauthorised transactions, and the corresponding obligations of the banking service provider (e.g., reversing the value of the transaction or to limit the potential loss of the consumer, save in a case of fraud).[199] In other words, the focus of the guide is on the duties rather than rights of consumers. As these responsibilities are worded in very general terms, they could be applied to m-payment transactions. Equally, the consumer protection principles which banks have to follow are very broad and could easily be extended to the m-payment context.

Various banks have published their own banking consumers' guides, which detail their customers' financial rights and responsibilities.[200] Although to some extent these individual bank guides mirror the 2013 principles published by SAMA, they do not uniformly do so and there are, therefore, also some disparities between them. Despite the assurances in these guides, some banks exclude liability from fraud to the greatest extent possible and it is uncertain whether the SAMA principles render these wide exclusion clauses void. SAMA should, therefore, clarify whether their banking consumer protection principles and banking consumer's guide take precedence and are implied in the terms and conditions of the contracts of banks as this would provide more robust protection for consumers.

[199] Ibid 10-11.

[200] See, e.g., Saudi Hollandi Bank, Your Financial Rights and Responsibilities, The Banking Consumers' Guide, 2014 <http://www.shb.com.sa/en/pdf/consumerProtection/Guide%20en.pdf> 24 September 2014; Al Ahlie, 2014 <http://www.alahli.com/en-us/Documents/Financial_Rights_of_Bank_Customers_EN.pdf> 24 September 2014; National Commercial Bank, 'Your Financial Rights and Responsibility, Our commitment to the protection of customer interests', 2014 <http://www.alahli.com/en-us/Pages/Consumer-Protection.aspx> accessed 25 October 2014.

5.5.1 Data and privacy protection of m-payment customers' data

SA currently only protects credit information but not data in general[201] and recourse is made to the Credit Information Law 2008 and thereafter the Consumer Credit Regulations 2006 in order to ascertain its approach. In the final section, it is analysed how money laundering is addressed and whether the objective of money laundering undermines consumers' rights in relation to data protection.

5.5.2 The Credit Information Law 2008 and the failure to protect m-payment customers' data

The Credit Information Law 2008 ('CIL 2008') protects credit information and its enforcement is overseen by SAMA.[202] This law is rooted in Islamic principles, as the Prophet Mohammed was clear that debts have to be repaid and it is permissible to speak about those who fail to do this.[203] Equally, when false information is being reported, the Saudi Hanbali School considers that damages may be sought.[204] This law regulates the manner in which credit information can be collected and exchanged, and establishes that credit information has to be protected, especially to prevent unauthorised disclosure or usage.[205] The law sets out the principles which govern the gathering of credit information, their exchange and establishes

[201] DLA Piper, Data Protection Laws of the World, Saudi Arabia, 2019 <https://www.dlapiperdataprotection.com/index.html?t=law&c=SA> accessed 25 April 2019.
[202] See esp. CIL 2008, Article 11; Saudi Credit Bureau, 'Horizons in Credit, Credit in Saudi Arabia', 2013, 1-9, 3 <http://www.simah.com/Documents/PDF/Booklet9A.pdf> accessed 22 October 2014.
[203] M. Al-Bukhair, *Translation of Sahih Bukhair* (translation M. Khan), Volume 3, 41/572; M. Bin Al-Hajjaj, Being Traditions of the Sayings and Doings of the Prophet Muhammad as narrated by his Companions and Complied under the Title Aljami-US-Sahih 25/2387 (translation A. H. Siddiqui, Arabic House for Printing and Publishing, and Distribution 1972).
[204] M. Alhajjawi, *Aliqna in the Jurisprudence on Ahmed Bin Hanbal (The Convincing) 2/354* (A. Alsubki, The Knowledge Publishing House); M.A.A. Alhaidary, 'Measuring Compensation from Credit Reporting Damage: A Comparison of Islamic, Saudi, and American Law in Light of Credit Information Reporting Acts', University of Kansas, 2012, 1-300, 24 <https://kuscholarworks.ku.edu/bitstream/handle/1808/9855/Alhaidary_ku_0099D_12164_DATA_1.pdf?sequence=1&isAllowed=y> accessed 22 October 2014.
[205] CIL 2008, Article 2; ibid (Alhaidary).

protective safeguards for consumers.[206] Credit information encompasses details of the amount and nature of loans made, outstanding balances, the nature of security or guarantees taken, and the borrower's creditworthiness, amongst other things.[207] Though broad, this definition may not capture the data generated by a m-payment transaction.

The law helps businesses and consumers to obtain finance too, since the asymmetrical information structure between borrowers and lenders becomes reduced, thereby helping to create a more efficient credit market.[208] This statute further deals with credit information rather than information (e.g., automated data) more generally. Consequently, the law covers a very specific type of information, i.e., credit transactions and the repayment history of consumers in relation to leases, credit cards, instalment purchases, loans and credit sales.[209] It does not extend to m-payment transactions unless these use credit information, such as, credit card details.[210]

In light of the failure to adopt a data protection law, such as the GDPR, discussed in chapter 4, section 4.5.4, m-payment consumers' data, privacy and security are thus at great risk. Data protection is only guaranteed to a limited extent by virtue of Article 17 of the Basic Law of Governance 1992 and some other sectoral laws.[211] As discussed in chapter 1, the advent of m-payment transactions enables the capture of big data,[212] which makes it possible

[206] International Business Publications n 7, 71.
[207] CIL 2008, Article 2.
[208] K. Hanware, 'Saudi Credit Bureau banks on sophisticated mechanisms', *Arab News*, 20 October 2014 <http://www.arabnews.com/news/646971> accessed 10 May 2015.
[209] CIL 2008, Article 1; Saudi Credit Bureau, 'Horizons in Credit, Credit in Saudi Arabia' n 63.
[210] PSR 2017, Regulation 64, Schedule 8, para. 1.
[211] E. Read and T. Alsheikh, 'Data protection in Saudi Arabia: overview', Practical Law, 2012 <http://uk.practicallaw.com/4-520-9455> accessed 1 November 2016.
[212] J. Liu et al, 'Assessing the Opportunities and Challenges with Big Data in the Mobile Payments Ecosystem' (2015). Workshop on Internet and Big Data Finance 2015. Research Collection School of Information Systems, 1-7, 2 <http://ink.library.smu.edu.sg/cgi/viewcontent.cgi?article=3944&context=sis_research> accessed 1 November 2016.

to understand customers' behaviour.[213] When such data is misused, it can affect the privacy and security of consumers.[214] The collection of large quantities of personal consumer data for financial gains by m-payment providers ought to be, therefore, regulated, just like credit information.

The Islamic basis for extending protection from credit information to personal data is that the Quran clearly forbids fraud and mischief. For example, Sura Shu'ara 26, verses 181 to 183 state: 'Give just measure, and cause no loss (to others by fraud)/And weigh with scales true and upright/And withhold not things justly due to men, nor do evil in the land, working mischief'. The lack of personal data protection is indicative of a weaker social welfare approach to consumer protection as it increases the likelihood of fraud and other mischief for consumers. For this reason, Islamic scholars and legislators could utilise this fundamental holy command to create data protection laws, including for m-payment transactions.

The other option would be to widen the scope of Article 1 of the CIL 2008, so that m-payment transactions are included. However, in light of the scope of this law, which clearly suggests that it only applies to credit information, it is better to address this in a new statute altogether with similar provisions to those contained in the CIL 2008 being imposed on those providing m-payment services. The collection and exchange of m-payment transaction information would also generate a more complete picture about the financial status of customers and this may enable SA to maintain its World Bank Credit Depth of Information

[213] C. Hauser, 'How Big Data is Transforming Mobile Payments and What This Means for Retailers and Users', Wirecard, 12 November 2015 <https://blog.wirecard.com/how-big-data-is-transforming-mobile-payments-and-what-this-means-for-retailers-and-users/> accessed 1 November 2016.
[214] J. Filipe and M.S. Obaidat, *E-Business and Telecommunications: International Conference, ICETE 2008: Porto, Portugal, July 2008, Revised Selected Papers* (Springer-Verlag 2009) 92.

Index's results in the future, which were eight out of eight in 2013 to 2014, with eight being the highest.[215]

In 2004, the Saudi Credit Bureau ('SIMAH') was set up to provide commercial and consumer information services and its Research and Advisory Centre utilises data to address issues and develop products.[216] SIMAH is responsible for maintaining and collecting credit information about corporate entities and consumers.[217] It functions as a data aggregator as it collects credit information from banks and issues official credit reports when requested.[218] However, credit information companies can provide credit information services in addition to SIMAH, so long as they have been awarded a licence.[219] Both act like credit reference agencies and help banks, retailers and mobile companies to quickly assess the creditworthiness of a potential borrower.

In the future, businesses which collect data about m-payment transactions can also offer important insights about customer behaviour.[220] Whilst this data is not concerned with the ability to repay, it is arguably more far-reaching and can be utilised in different ways. For example, retail offers can be individualised based on personal data.[221] In light of the fact that the Prophet Mohammed clearly favoured trade, this new data market needs to be regulated in an Islamic way, but, as discussed in chapter 3, adherence to the principles of good faith, honesty and fairness must be ensured. One way to achieve this is to supervise all those entities which collect and handle such information, possibly through a new body similar to

[215] World Bank, 'Depth of credit information index (0=low to 8=high)', 2015 <http://data.worldbank.org/indicator/IC.CRD.INFO.XQ/countries> accessed 10 May 2015.
[216] Saudi Credit Bureau, 'Reducing risk: Nabil A Al Mubarak, CEO, Saudi Credit Bureau (SIMAH), on the role of credit risk mana', 2013 <http://www.simah.com/en/NewsDetail.aspx?news_id=Uq4oqo8lLRU=> accessed 20 October 2014.
[217] Ibid.
[218] SIMAH, 'About Us', 2016 <https://www.simah.com/English/About-Us> accessed 1 November 2016.
[219] CIL 2008, Article 1.
[220] Hauser n 213.
[221] Ibid.

the SIMAH. The adoption of a data protection law, including m-payment transaction data, together with the creation of an office like the ICO in the UK would heighten consumer protection in line with a social welfare approach. SA should ensure that it takes steps to transpose the OECD's G20 High-Level Principles on Financial Consumer Protection, as discussed in chapter 3. These principles strike a balance which would be appropriate in SA by calling on governments to create financial consumer protection frameworks, yet at the same time acknowledge that customers must have obligations.

The Islamic *haram* doctrine is also, arguably, violated without such a law being in place as data protection breaches heighten the risk of customers losing funds. Sensitive big data which is generated through m-payment transactions is currently insufficiently protected and businesses are not legally incentivised to exercise due diligence and care to prevent customer data being lost. However, many Quranic verses emphasise that individuals must be protected, especially against undue interference.[222] Consequently, Islamic scholars should require customer data generated from m-payment transactions to be afforded similar protection to credit information. For instance, the CIL 2008 requires that credit information must be kept confidential,[223] that complaint mechanisms are created[224] and customers must consent to the creation of credit records.[225] Customers are also permitted to complain to a committee for a failure to correct their report.[226] Article 12 of the CIL 2008 provides that there will be a violation in eight instances, e.g., when credit information is used for unauthorised purposes. Any violation can result in a fine and/or a temporary licence

[222] S. Mancuso, 'Consumer Protection in E-Commerce Transactions: A First Comparison between European Law and Islamic Law' (2007) *Journal of International Commercial Law and Technology* 2(1), 1-8, 4.
[223] CIL 2008, Article 6.
[224] CIL 2008, Article 8(2).
[225] CIL 2008, Article 9(1).
[226] CIL 2008, Article 9(7).

revocation or suspension.[227] However, unlike under UK law considered in chapter 4, section 4.5, the CIL 2008 is silent on providing any remedies to the consumer whose information has been subject to unauthorised use; the penalty is paid to the regulator as a punishment rather than to the consumer as compensation.[228] This gives rise to a lacuna in the Saudi regime of consumer protection, as enforcement actions brought through the Committee provide no remedy to the wronged party.

The Minister of Finance forms committees in order to determine disputes between consumers and credit information companies, banks and other public and private entities which have collected and handled credit information in order to assess whether the law has been violated.[229] These committees also determine the appropriate sanctions and their decisions can be appealed in the courts.[230] Once a decision has been reached, those who have suffered loss because of a breach may seek damages.[231]

A similar set-up for m-payment transaction information is crucial to protect the personal data of customers which is, arguably, as sensitive as their credit information. The UK approach towards data protection, particularly the GDPR, could serve as a blueprint. Such legal intervention from the state is essential to further the social welfare objectives of the Sharia. Without this, the Saudi stance on information from m-payment transactions resembles the neoliberal paradigm and lacks the needed social welfare aspect to support the country's Islamic ethics.

Furthermore, in the future, it is necessary that data obtained from m-payment systems is fed into SIMAH's national data pool. At present, corporate credit information from most

[227] CIL 2008, Article 13.
[228] Ibid.
[229] CIL 2008, Article 14.
[230] Ibid.
[231] CIL 2008. Article 15.

commercial banks is fed into this.[232] Through this pool, SIMAH assesses the risk of default exposure and whether the capital adequacy requirements of Basel II and III are met. In 2009, the Saudi Credit Information Company was created by Saudi banks and SAMA to further help banks to determine credit risk.[233] M-payment data integration may help to promote financial stability which is essential for mitigating the risks posed to m-payment customers. It may help create new big data business opportunities and help to assess consumer's trustworthiness far beyond their credit score.[234] Businesses can advertise more tailored offers to consumers, increasing their attractiveness and avoiding a situation where the consumer is shown content they are uninterested in.[235] However, it may be necessary to ensure regulatory safeguards are in place so that these potential consumer benefits are realised and not simply taken advantage of by service providers.[236]

5.5.3 The Consumer Credit Regulations 2006 and the failure to protect m-payment customers' data

In 2006, SAMA adopted Consumer Credit Regulations ('CCR 2006') which require consumer information to be kept private and confidential.[237] They also spell out what information has to be furnished as part of consumer credit or related agreements, and set the annual percentage, profit and borrowing rates.[238] It explains what constitutes unfair terms in

[232] Saudi Credit Bureau n 216.
[233] Oxford Business Group, *The Report, Saudi Arabia 2010* (Oxford Business Group 2011) 71.
[234] B. Marr, 'Chinese Social Credit Score: Utopian Big Data Bliss or Black Mirror on Steroids?' Forbes, 21 January 2019 <https://www.forbes.com/sites/bernardmarr/2019/01/21/chinese-social-credit-score-utopian-big-data-bliss-or-black-mirror-on-steroids/#5962880048b8> accessed 25 April 2019.
[235] T.M. Le and S.-Y. Liaw, 'Effects of Pros and Cons of Applying Big Data Analytics to Consumers' Responses in an E-Commerce Context' (2017) *Sustainability* 9, 1-19, 1.
[236] Ibid.
[237] CCR 2006, Article 2.
[238] CCR 2006, Article 4.

the context of consumer credit agreements.[239] The Regulations further provide for joint and several liabilities, as well as the assignments of rights and early repayments.[240] The Regulations also applies to consumer credit and related agreements that are offered online.

As it is likely that, in future, m-payment services may extend to consumer credit and not just prepaid payments (as is currently the position), these provisions will remain relevant. However, at present, they do not offer protection to customers who make m-payments and so the social welfare aspects of Sharia law are not being met in this respect.

5.5.4 The Anti-Money Laundering Law 2003 and the issue of protecting customers' data

Following 9/11 in the United States, SA passed the Anti-Money Laundering Law 2003 ('AML') in order to criminalise money laundering, terrorist financing, terrorist organisations and terrorist acts.[241] Under this law, banks are required to establish mechanisms to identify and report suspicious transactions and freeze accounts.[242] Moreover, record-keeping and reporting requirements were enhanced and the *hawala* system, which is an informal trust-based funds transfer system, has been subjected to compulsory licensing.[243] A financial intelligence unit ('FIU') was also created to analyse suspicious transaction reports and banks are now required to submit as part of their AML and counter-terrorist financing initiatives

[239] CCR 2006, Article 5.
[240] CCR 2006, Article 6.
[241] Saudi Embassy, 'Summary of FATF Report and Conclusions', 14 June 2004 <http://www.saudiembassy.net/archive/2004/statements/page9.aspx> accessed 1 May 2015; SAMA, 'A Report on Initiatives and Actions Taken by Saudi Arabia to Combat Terrorist Financing and Money Laundering', April 2004, 1-22, 3 <http://www.saudiembassy.net/files/PDF/SAMA_INITIATIVES_BY_KSA_UP_DATED_APRIL_2004.pdf> accessed 1 May 2015.
[242] Z.D. Merritt, *Combating Terrorism: U. S. Agencies Report Progress Countering Terrorism and Its Financing in Saudi Arabia, but Continued Focus on Counter Terrorism Financing Efforts Needed* (Washington DC, United States Government Accountability Office 2010) 31-32.
[243] M. El Qorchi et al, *Informal Funds Transfer Systems: An Analysis of the Informal Hawala System* (International Monetary Fund 2003) 6.

('CTF') any suspicious transaction reports to this unit.[244] Money laundering offences are tried in Sharia courts and there have been successful prosecutions.[245] The AML Law 2003 was further supplemented by: the Rules governing AML and Combating Terrorist Financing of 2003, 2008 and 2012; the AML and Counter-Terrorism Financing Rules for Financing Companies 2012; and the 2013 Implementing Regulations of the AML Law.

SA's AML and CTF laws are largely in line with the FATF standards.[246] A Mutual Evaluation Report by the FATF describes the legal AML regime as 'quite robust', but observes that the legal regime for combating the financing of terrorism is 'not as developed.'[247] The AML Law also applies to m-payment systems, as made clear by various FATF reports.[248] An analysis of the AML Law 2003 shows that the law is wide enough to accommodate suspicion-based reporting relating to m-payments since anyone who commits money laundering, for instance, or who conducts any transaction involving funds or proceeds with the knowledge that they are the result of a criminal activity or have an illegitimate or illegal source or who assists, facilitates, colludes or covers up such transactions, is culpable.[249] The AML Law further clarifies this, stating that 'anyone who carries out or

[244] B. Mendelsohn, *Combating Jihadism: American Hegemony and Interstate Cooperation in the War on Terrorism* (University of Chicago Press 2009) 128.
[245] I.A. Odeh, *Anti-Money Laundering and Combating Terrorist Financing for Financial Institutions* (Dorrance Publishing Co Inc 2010) 55.
[246] Merritt n 242, 31-32; Mendelsohn n 244, 126.
[247] FATF, 'Mutual Evaluation of the Kingdom of Saudi Arabia', 1 February 2012 <http://www.fatf-gafi.org/countries/s-t/saudiarabia/documents/mutualevaluationofthekingdomofsaudiarabia.html> accessed 2 May 2015.
[248] FATF, 'Report on New Payment Methods', 13 October 2006, 1-44 <http://www.fatf-gafi.org/media/fatf/documents/reports/Report%20on%20New%20Payment%20Methods.pdf> accessed 3 May 2015; FATF, 'Money Launder Using New Payment Methods', FATF Report, October 2010, 1-117 <http://www.fatf-gafi.org/media/fatf/documents/reports/ml%20using%20new%20payment%20methods.pdf> accessed 3 May 2015; FATF, 'Guidance for a Risk-Based Approach, Prepaid Cards, Mobile Payments and Internet-Based Payment Services', June 2013, 1-47 <http://www.fatf-gafi.org/media/fatf/documents/recommendations/guidance-rba-npps.pdf> accessed 2 May 2015.
[249] Anti-Money Laundering Law 2003, Article 2(a)&(e).

participates commits money laundering and that this also extends to chairmen of institutions, employees and others, including hired hands'.[250]

Reference to non-financial institutions ensures that the scope is broad enough to cover payments and e-money institutions. The term 'hired hands' can also extend to other parties within the m-payment infrastructure. Obligations can thus be imposed on m-payment providers to make suspicious activity reports ('SARs') if a customer uses m-payment services and instructs a bank to transfer funds. However, these are insufficiently robust in comparison with international standards, e.g., the UK's AML law combating money laundering and terrorist financing. SA should either amend its AML Law or insert into the Regulatory Rules for Payment Services (discussed at section 5.3.2) a duty to collect information[251] via payment service providers. The AML law and the interlinked Regulatory Rules should be revised to incorporate a coherent system of definitions to ensure that there are not gaps created by technicalities in the language of the legislation. Further, in order to give the regime teeth, real and accessible remedies must be available to consumers who are harmed by the regulatory breaches of service providers. This might encompass issues from breaches of privacy and data protection to failure to provide the requisite protections against fraud.

Furthermore, it would be useful for SAMA to issue specific guidance for m-payment service providers. At present, even an individual service provider might have difficulty in identifying whether and to what extent they fall within the scope of the regulation. This is because m-payment transactions create novel AML situations, as explained by the FATF in its 'Guidance for a Risk-Based Approach, Prepaid Cards, Mobile Payments and Internet-Based Payment Services.'[252] For instance, criminals may use stolen mobile phones to

[250] Anti-Money Laundering Law 2003, Article 3.
[251] MLRs 2017, Regulation 15(3)(a)-(g).
[252] FATF, 'Guidance for a Risk-Based Approach' n 248.

perpetrate money laundering and terrorist financing. Cyber criminals may also hack the accounts of other customers in order to launder money or finance terrorism, thus putting consumers at considerable risk. Accordingly, consumer protection based on social welfare principles would be heightened if SAMA was to issue more specific guidance for m-payment services.

In the UK, guidelines have been issued for payment service providers by the European Supervisory Authorities, so that payments are fully traceable. One significant improvement of SA's AML framework which may be advanced based on international comparison would, therefore, be to mandate that payment service providers collect the name of the payer and payee and their respective bank account details, as well as the payer's address, when more than 4,000 SAR are transferred, or more than 11,000 SAR worth of goods are purchased per year through reloadable payment cards. This should be in addition to the existing CDD requirements outlined in section 5.3.2. To date, SA has disappointingly not implemented many of the sound recommendations made by the FATF.[253] The AML framework could be enhanced if provision is made requiring AML risk assessments to be conducted to determine whether a transaction is suspicious and may require an SAR, and that subsequently written policies, controls and procedures would be put in place to mitigate identified risks. In addition, it should be required that these policies, controls and procedures were regularly reviewed and updated. Staff should also be provided with these policies, controls and procedures and receive training in how to follow them. Implementation of these changes would provide a starting point for ensuring that some of the inherent risks of m-payments to ordinary consumers would be assuaged and adherence to the Sharia principles of social welfare would be improved. Placing additional requirements, such as, collection of the

[253] FATF, 'Anti-money laundering and counter-terrorist financing measures, Kingdom of Saudi Arabia', Mutual Evaluation Report, September 2018, 1-243, 3.

name, address, and details of consumers making m-payment transactions above certain thresholds limits the risk to which both payer and payee are potentially exposed at the expense of the service provider, and carrying out CDD if necessary. Although it may be argued that this would in fact represent the reinforcing of a neoliberal position of improving market efficiency by building public confidence in such markets through stricter AML laws, this would only be the case as a means to achieve the ultimate end of improving consumer protection, a potential resolution to the policy conflict which was identified in chapter 4, section 4.6.

5.5 Conclusion

This chapter examined the law governing the use of m-payment applications in SA. SA's approach towards m-payments has not been as liberal as that in the UK. The reason for this is that the Banking Control Law 1966 has not been updated, making it impossible for new parties to enter the emerging m-payment market. Equally, the 2012 Regulatory Rules for Prepaid Payment Services are bank-centric so that Fintech innovation is being stifled. The 2012 Rules adopt a very restrictive business model, more akin to gift cards than the varied forms that m-payment services can take. The Rules are, arguably, close to the UK regime for e-money institutions in that both address the carrying of e-money business. However, the 2012 Rules do not properly liberalise the m-payment market, thereby curtailing consumer choice in a neoliberal sense since only prepaid payment services can be offered. As a result, many of the advantages which m-payment services bring for customers are being squandered.

SA is presently pursuing a producerist stance which protects banks. Producerism, as chapter 3 argues, does not promote the consumers' interests in the economic realm. It should be borne in mind that Prophet Mohammed was a great supporter of trade, which has led the

Hanbali School to take a normally liberal stance in respect of business matters. There thus exist fundamental reasons for legislators to abandon this trade-hindering approach.

One way to achieve this is to amend the Banking Control Law 1966 and to clarify that SAMA is responsible for regulating institutions which offer m-payment services, including TPPs and e-money institutions. In addition, there should be a new authorisation regime for these institutions, as in the UK. Steps should be taken to facilitate consumerism by allowing interested businesses to make use of telecommunications networks in order to make available m-payment services. Technology is a great driver of progress and economic growth, which, in turn, would promote social welfare in line with Sharia demands.

The Electronic Transaction Law also only facilitates e-commerce but does not confer protection on customers who use m-payment services. The underlying basis of this Web 1.0 law (which regulates the relationship between certification service providers and certificate holders) is ill-equipped to govern the new relationships created through the m-payment ecosystem. In other words, a new payment services law is required which defines m-payment transactions and addresses how such transactions are original and integer.

Consequently, SA's laws, regulations, rules and guidance are currently based on the Web 1.0 version. The legal responses to many issues that arise are outdated and have not evolved, as appropriate, to the Web 2.0 version, like in the UK. In the near future, new technological innovation will further facilitate Web 3.0, an even more dynamic and interactive World Wide Web.[254] It is essential for SA to substantially reform its banking laws to keep abreast with such developments. Otherwise, the risk is that businesses will offer new

[254] P. Duhan and A. Singh, *M-Commerce: Experiencing the Phygital Retail* (Apple Academic Press Inc 2019) para.1.4.2.

services without an appropriate regulatory framework being put in place to protect consumers.

The analysis reveals that there is currently little to no law, rules, regulations or guidance that specifically address m-payment in SA, particularly unauthorised m-payment transactions and protection of consumer data and their privacy, including against privacy breaches. Banks are using wide exclusion clauses when they offer m-payment services and their scope is not curtailed by unfair terms legislation, such as the CRA 2015 in the UK. This appears to be because the Islamic jurisprudence governing unfair contractual terms is insufficiently developed, as discussed in chapter 3, section 3.6. Customers have therefore been granted very few rights which is unsurprising due to Islamic scholars typically focusing on duties, as opposed to rights. Consequently, the appropriate channels and procedures for resolving consumer disputes are still largely underdeveloped and the social welfare aspect of Sharia law is not being adhered to in this area.

The failure to pursue a liberal policy orientation towards the opening up of the m-payment sector has not resulted in additional protection for m-payment customers. Instead, it is more accurate to state that a non-interventionist legal consumer protection approach has been adopted. No specialised body similar to the UK Payment Systems Regulator has been created. Customers cannot settle disputes easily through an ombudsman service, as in the UK. No efforts have been made to make up for failures through private ordering, e.g., by setting up voluntary codes, such as, the UK Standards of Lending Practice 2016.

Whilst the Regulatory Rules for Prepaid Payment Services are a sound first step, they are insufficient to facilitate the emerging m-payment revolution and are unlikely to greatly benefit customer choice. They do not adequately protect customers against heightened technological risk as the most pressing topic of negligence liability has not been addressed.

No right to a refund has been granted except in the case of billing errors, which massively undermines consumer protection and the social welfare principles of Sharia law. The disputes settlement procedure is also unduly limited to those cases which fall within the narrow scope of billing errors. The Banking Consumer Protection Principles and Banking Consumers' Guide may also be difficult to evoke in the context of m-payment transactions without further clarification. The reason is that they are most likely to be treated as soft law which does not override unfair exclusion clauses. Ideally, these principles and guide should be rooted in the Sharia, such as the good faith principle, the *haram* and *halal* concepts and the profit and loss sharing principle, in order to confer meaningful protection to m-payment consumers. However, as discussed in chapter 3, the requisite Islamic pro-consumer protection jurisprudence must firstly be promulgated.

Furthermore, banks' terms and conditions do not seem to accord with the principles. It is unclear whether the banking consumer guides and banking consumer protection principles take priority over the exclusion clauses in the terms and conditions of banks. The other issue with these principles is that they are modelled on the G20 High Level Principles on Financial Consumer Protection 2011, which are reflective of a neoliberal approach. For this reason, the Banking Consumer Protection Principles and Banking Consumers' Guide are not fully compatible with the social welfare objective of the Sharia.

Moreover, consumer protection has been significantly marginalised because customers' data is inadequately protected by m-payment providers in the big data era. The Credit Information Law only protects credit but not m-payment information as no data protection law exist which customers can evoke. This is despite the fact that the advent of m-payments generates large datasets which profile customers much more precisely than ever

before.[255] As a result, the security of this far-reaching personal data is much more at risk. There are no legislative provisions which customers can evoke to compel m-payment providers to not misutilise or safeguard their data or compensate them for losses suffered due to security or third-party failures.

All these issues highlight that reforms to existing laws in SA are needed and more particularly, the adoption of an improved payment system law is urgently needed in order to honour the primary source of law, the Sharia which is supreme over civil law. This particularly requires that m-payment customers are conceptualised as vulnerable individuals, though capable of learning, as further discussed in the Conclusion.

[255] K. Pousttchi and Y. Hufenbach, 'Enabling evidence-based retail marketing with the use of payment data - the Mobile Payment Reference Model 2.0' (2013) *International Journal of Business Intelligence and Data Mining* 8, 19-44, 19.

CHAPTER 6

CONCLUSION

6.1 Concluding comments

This work has employed a positivist ontology to explore the ways in which the law protects banking customers from the risks of m-payments in SA, particularly unauthorised m-payment transactions and data protection of such transactions, through the lens of comparisons between Saudi and UK approaches to this challenge.

The opening chapter of this work elaborated on the nature and potential of this new technology, highlighting its unique benefits to consumers in terms of convenience and accessibility, and its potential to open up a new market which brings great benefits to those economies which are able to embrace it.

The challenge presented by m-payments is often underestimated and poorly understood by regulators. Chapter 2 thus set out in greater detail the complex risks associated with Fintech innovation, in particular the heightened risk of fraud, theft, money laundering, and breaches of data security. It was emphasised that the legal questions of how to protect consumers when it comes to unauthorised m-payment transactions and how to safeguard consumers' data in order to maintain privacy and protect against breaches of their privacy are particular salient for legislators to address.

It is well-established and widely accepted that regulators have a responsibility to protect consumers from exploitation by potentially malign market forces. The literature review in chapter 3 set out the theoretical bases and justifications for this responsibility, as well as the countervailing policy considerations such as the general economic advantages of encouraging free trade, competition, and innovation. That these principles apply in the context of m-payment is self-evident, but how they should be balanced and realised is a more controversial question. The complexity of contractual relationships and the wide array of stakeholders with competing interests makes this a particularly thorny field for regulators. The picture is further complicated in the context of the Saudi Arabian market, where Sharia principles are also considered an imperative element of market and financial service regulation. Sharia law requires that consumers are safeguarded in a variety of ways, including by adhering to the good faith principle, the concepts of *halal* and *haram,* and the profit and loss sharing principle. The writings of Islamic scholars on the subject of consumer protection, both broadly and specifically in the context of m-payments, were referred to in this analysis to illustrate what the implications of these principles might be for the regulation of the Fintech sector.

In this context, chapter 4 analysed the regulation of m-payment services firstly in the UK and secondly in chapter 5 in SA. The UK regulatory environment generally favours the neoliberal values of innovation and market competition, whilst at the same time offering significant protection to consumers.

On the other hand, the regulatory picture in SA is less promising. The Saudi approach to the Fintech sector has, as might perhaps be expected, been less liberal than that of the UK.

However, this has not brought the strong consumer protection which it might be hoped could accompany a restrictive regulatory approach. Not only does it fail to serve the interests of the economy by enabling the growth of a sector with huge potential, and failed consumers by depriving them of the practical benefits which m-payment services offer, but perhaps more seriously it has failed to meet the requirements of Sharia law in a number of respects. Most importantly, it presently falls short in providing consumers protection against unauthorised m-payment transactions by permitting that customers bear the full cost of any loss that follows from an unauthorised transaction and by failing to protect consumers' data and their privacy.

6.2 Key findings

The next sections present the key findings, firstly in section 6.2.1 about the (in)adequacy of existing Saudi regulation of m-payments discussed in chapter 5, particularly its defects in compliance with Sharia law and its failure to keep pace with technological change. Thereafter, section 6.2.2 discusses the extent to which the UK approach might provide a useful model in seeking to improve the regulation of m-payment services that is Sharia compliant and discusses its advantages and disadvantages, as well as the challenges of regulator transplantation.

6.2.1 Shortfalls in the current Saudi Arabia regulatory regime for m-payments

A key purpose of this work has been to consider the areas which the Saudi legislator will need to address in order to provide a more robust legal framework in which Saudi m-payment providers can deliver m-payment services to consumers in a way which adequately deals with the risks in a Sharia compliant manner. Chapter 5 set out the substance of the key provisions in Saudi law, and measured these against the Sharia requirements which the law sought to attain. Chapter 5 further demonstrated the areas of the existing Saudi legal regime that fell short of the ideal social welfare approach by a significant margin.

The Sharia requires that social welfare policy should provide the lynchpin of any statutory and regulatory framework.[1] At the same time, these policy imperatives should be balanced with encouraging business, enterprise, and economic growth, as Islam is pro-commerce.[2] Saudi Arabian law should, therefore, prioritise social justice in line with the Islamic objective of 'establishing what is right and forbidding what is wrong';[3] Islamic 'ethics, morality and behavioural admonitions' must not be deviated from.[4] This reflects the fact that the Sharia is the most important source of law,[5] and shapes both the broad concepts applicable in this field (such as the good faith principle), and specific legislative enactments

[1] M. Tamadonfar, *Islamic Law and Governance in Contemporary Iran: Transcending Islam for Social, Economic and Political Order* (Lexington Books 2015) 100.
[2] QFinance, *Islamic Finance: Instruments and Markets* (Bloomsbury Publishing 2010) 147.
[3] M.A. Khan, 'The Role of Islamic State in Consumer Protection' (2011) *Pakistan Journal of Islamic Research* 8, 31-44, 31, citing the Quran 3:103, 109, 113; 9:71, 22:41; 31:17.
[4] M.J.T. McMillen, 'Islamic Law Forum' (2008) *International Law* 42, 1017-1032, 1018.
[5] M. Ariff and M. Iqbal, *The Foundations of Islamic Banking: Theory, Practice and Education* (Edward Elgar Publishing Ltd 2011) 11; B. Maurer, *Mutual Life, Limited: Islamic Banking, Alternative Currencies, Lateral Reason* (Princeton University Press 2011) 32.

such as Article 6(a) of the Charter of the Saudi Arabian Monetary Agency ('SAMA') 1957. [6] In SA, this means adhering to the Hanbali version of Sharia law.[7]

For the detailed reasons identified in the preceding chapter, Saudi legislation has fundamentally failed to respond to the various risks and challenges identified in chapter 2, particularly unauthorised m-payment transactions and data protection, that are associated with m-payment and in a manner which complies with these Islamic concepts. A stark illustration of this defect is the failure of the 2010 e-Banking Rules in SA to provide consumers with recourse for redress in the event that they are targeted by cyber criminals who have appropriated money from their accounts. The rights of the consumers are limited to raising a complaint with SAMA (the resolution of which remains uncertain) and do not extend to any right to a refund or compensation from the payment service provider responsible.

Even where protections do exist, chapter 5 demonstrates that banks can easily evade these simply by invoking an exclusion clause when offering m-payment services. In the absence of any specific rules, regulations, or even voluntary guidance to address the challenges and risks of m-payment, the effect is that the sector is almost entirely unregulated and the level of protection available to consumers is below even what they might expect to receive when using traditional banking services. This is compounded by a false sense of

[6] Charter of the Saudi Arabian Monetary Agency 1957, Article 1(a)-(c); International Business Publications, *Saudi Arabia Central Bank & Financial Policy Handbook* (International Business Publications 2005) 150.
[7] S. Zuhur, *Saudi Arabia* (ABC-CLIO LLC 2011) 176.

security amongst consumers, which results from the usually stringent approach of Islamic jurisprudence to banking.[8]

Moreover, it is highly arguable that the restrictive market conditions which are created by existing regulations are inconsistent with overarching Islamic principles. As noted in chapter 3, Islam and particularly the Hanbali School normally take a liberal approach to business matters. There are thus good reasons for legislators to abandon a trade-hindering approach, particularly in relation to a service, such as, m-payment, which has inherent benefits for consumers. The provision of m-payment services offers freedom and convenience to customers. That also supports the advancement of the Fintech sector as a whole which offers much more widespread benefits.

How can Saudi regulators resolve these challenges? Perhaps the greatest challenge facing Saudi regulators is that the law is heavily outdated and legislative processes have struggled to keep up with the rate of change in the m-payment sector. Unlike UK law, Saudi laws have not kept abreast with technological advances. The Saudi consumer protection rationale is underdeveloped due to the religious-based legal system. As identified in chapter 3, this has limited the development of consumer rights due to Islam's focus on duties.[9] A comprehensive reform therefore offers the most realistic prospect of bringing Saudi regulation into line with Sharia requirements. The following two sections discuss the utility of the UK as a model in undertaking such an extensive reform. This analysis is undertaken with the caveat that the UK is able to offer a framework which encourages trade, flexibility,

[8] Khan n 3, 31, citing the Quran 3:103, 109, 113; 9:71, 22:41; 31:17.
[9] G. Rice, 'Islamic ethics and the implications for business' (1999) *Journal of Business Ethics* 18, 345-358, 345.

and market growth, whereas the Saudi Arabian legislator should pursue different values of social welfare and consumer protection.

6.2.2 The value of the UK as a model for regulating m-payment systems

Chapter 4 offered a doctrinal analysis of the UK legal framework concerning m-payment services. As indicated at the outset of chapter 4, this legal evaluation helps to provide a basis for a comparative analysis with the Saudi legal framework and to interrogate the thesis' central research question of whether SA could be positively influenced by the UK model.

The UK approach to regulating m-payments has various advantages. Fundamentally, it promotes the neoliberal values of innovation and market competition, but also simultaneously offers significant protection to consumers. Moreover, the UK approach has proven highly adaptable in response to changing market conditions; legislation has evolved as the sector has matured. This places the UK in a strong position to meet the next generation of Fintech advances.[10] The overall assessment of UK regulation is therefore positive; a carefully considered regime is provided which finely balances market interests with those of the consumer and is sufficiently flexible to accommodate incremental development.

However, there are certain disadvantages with the UK approach which can serve as a useful warning to other legislators, such as, the Saudi Arabian government, regarding the

[10] Capgemini and BNP Paribas, 'World Payment Report', 14th ed, 2018, 1-56, 31 <https://worldpaymentsreport.com/wp-content/uploads/sites/5/2018/10/World-Payments-Report-2018.pdf> accessed 10 February 2019; K.-C. Claus, 'How convergence is transforming payment services', Ernst & Young, 24 May 2018 <https://www.ey.com/en_gl/digital/how-convergence-is-transforming-payment-services> accessed 13 February 2019.

potential pitfalls of m-payment regulation. For example, chapter 4, section 4.5.6, outlined the ongoing debate about the effectiveness of the AML requirements contained in the MLRs 2017. Given the increasing demand for transparency, the MLRs 2017 raises a tension between AML and consumer protection, particularly in terms of data protection. It has even been suggested that the AML provisions could be actively detrimental to consumer interests by providing legal uncertainties which permit companies to access customer data without consent or even the knowledge of the individuals concerned.[11] This illustrates the risk of unintended consequences when regulating a complex and fast-moving market, such as, m-payment services, which in turn can create uncertainty for companies as to the legal position, and undermine the ability of consumers to act rationally in their own best interests. The UK approach is to a certain extent premised on the assumption of consumer rationality which is not necessarily realistic in m-payment where many consumers lack understanding of how technology operates and what their legal rights may be. The law alone cannot resolve this challenge as it is a societal issue which reflects both the pace of change of technology and the degree of attention which consumers give, or is willing to give, in deciding which types of financial services to use. However, what the law *can* do is proceed on the basis of an accurate and realistic impression of consumer rationality, rather than designing a regulatory regime with the 'perfect' consumer in mind.

Moreover, the use of voluntary codes of conduct in preference to compulsory standards is inconsistent with Sharia principles in so far as it reflects the prioritisation of

[11] See e.g., T. Zalan and E. Toufaily, 'The Promise of Fintech in Emerging Markets: Not as Disruptive' (2017) *Contemporary Economics* 11(4), 415-430.

commercial and economic incentives to shield this new sector from the full force of the law until it becomes better established. Voluntary codes may have the benefit of reducing the risk of stifling innovation. An obvious issue with voluntary codes, however, is that even enterprises which subscribe to the code can flout their commitments with little or no consequence. In other words, the implication of soft law/bank guides into the contract with the consumer is that they therein contained rights and duties are not enforceable. This leaves consumers with the 'worst of both worlds' as the code provides the appearance of protection and subscription gives the enterprise the impression of legitimacy, leading the consumer be more trusting than they otherwise might, whilst in reality there is no or little substantive protection. It also creates the impression that regulators are not 'serious' about consumer protection, as voluntary codes may lack any teeth. Companies may take advantage of their reticence and be emboldened to push the boundaries of acceptable behaviour. For this reason, it is essential that statutory obligations are at least imposed on general purpose networks in order to protect customers and financial stability. Users of general purpose networks are more vulnerable as they are generally less likely to have specialist knowledge of the services they choose to use and of the legal protections available in respect of any transactions they choose to enter into.

It must be also emphasised that a regulatory transplantation of the UK model poses various challenges. The considerations which drive UK politics namely, to strike a balance between pro-consumer regulations protecting users of m-payment services and pro-market reforms encouraging financial innovation are not necessarily the same considerations which drive Saudi Arabian politics. Legislation must always be specific to the jurisdiction in which

it is to be implemented.[12] However effectively the approach might work in the UK, it does not mean that a direct transplantation of provisions is likely to offer similarly positive results in SA. The challenges of translation are particularly acute given the vastly different social, economic, and political contexts of the UK and SA. The UK operates as a liberal democracy and generally favours a capitalist approach to market regulation.[13] By contrast, SA is a religious state and policy makers are required to take into account the requirements of Sharia law, which should include extensive consumer protection and public welfare considerations.[14] Also, the UK follows a common law legal system and decides cases based on precedents, whereas SA lacks this common law heritage.[15] SA would therefore be unable to mirror the UK approach in this regard without a much broader and more far-reaching overhaul of its legal system.

Notwithstanding the challenges of regulatory transplantation, the UK approach can perhaps provide a positive example, particularly in respect of its flexibility and responsiveness to shifting social, political, and economic pressures. UK policy has not rigidly adhered to any single approach, but has evolved over time. The permissive approach which provided the basis for the UK's initial response to the emerging challenges presented by m-payment services, as previously embodied in the PSR 2009, enabled the UK to promote development and innovation, most notably in the form of Fintech. However, as the market developed, a second generation of legislation was introduced to reflect growing concerns

[12] F. Bignami and D. Zaring, *Comparative Law and Regulation: Understanding the Global Regulatory Process* (Edward Elgar 2016) 26.
[13] B. Jones and P. Norton, *Politics UK* (8th ed, Routledge 2014) 576.
[14] M.M. Keshavjee and R. Abdulla, 'Family Law to Finance'. In A.B. Sajoo (eds.), *The Shari'a: History, Ethics and Law* (IB Tauris & Co Ltd 2018) Chapter 7.
[15] R. Miller and F. Cross, *The Legal Environment Today* (5th ed, Thomson Learning 2007) 16.

about its social and economic impact. The PSR 2017 also addressed new services such as PIS and AIS which simply had not been contemplated at the time of the PSR 2009. This allowed concerns about protecting consumers from fast-paced and unregulated developments to be addressed, whilst preserving strong competition within the financial services market and the economic growth which this ultimately enables.[16]

For example, the UK regulatory regime has constantly revised the definitions of key terms, e.g., e-money (which definition was recently updated by the EMR 2011), to ensure that the relevance of legislative provisions is maintained as the market and technology develops.[17] This reflected the need to expand protection to include any value which is stored magnetically to undertake payment transactions and is used as tender by legal and natural persons, as well as value which is stored on IT servers and on plastic cards.[18]

The UK approach illustrates two key principles which could prove highly valuable for Saudi Arabian legislators in addressing the regulatory challenges presented by the development of the m-payment sector. Firstly, the weight and nature of policy considerations are not constant and fluctuate with changes in the market, advancements in technology, and broader social developments. Likewise, the regulatory response must not be set in stone but must be capable of adapting to changing circumstances, and should be kept under regular

[16] P.A. Salz, *The Netsize Guide 2009: Mobile Society & Me, when worlds combine* (Netsize 2009) 102; S. Romero, 'The unstoppable growth of digital banking: 3 billion users by 2021', BBVA, 22 February 2017 <https://www.bbva.com/en/unstoppable-growth-digital-banking-3-billion-users-2021/> 19 November 2017.
[17] Directive 2009/110/EC on the taking-up, pursuit and prudential regulation of the business of electronic money institutions amending Directives 2005/6-/EC and 2006/48/EC and repealing Directive 2000/46/EC.
[18] HM Treasury, 'Laying of regulations to implement the new E-Money Directive, a consultation document.' October 2010, 1-112, 10 <https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/81328/emoney_directive_consultation.pdf> accessed 10 September 2016.

review to determine whether updates are necessary. In this context, it is important for the Saudi Arabian legislator to continuously take into account regulatory responses from around the world. The reason is that there exist not only the three options of placing all of the loss from an unauthorised payment either with the consumer (as SA currently does) or with the service provider or opting for a hybrid allocation (as the UK has done). In other words, while this research has focused on the UK as a model for regulating m-payment systems and has examined its regulatory response, other jurisdictions may also offer interesting solutions which might better fit the Saudi Arabian context.

Hence, Saudi Arabia should not confine itself to these three options. It must conduct a far-reaching review of the possible legislative and regulatory options to the problem of loss allocation. This will help SA to devise a legislative response which best fits its social, economic, and political context. Secondly, what is apparent from the UK regulatory regime is that it is possible to formulate policies which balance competing policy interests without necessarily prioritising only one. Again, this balance can be adapted over time to reflect changing needs.

The next section presents the recommendations and reform proposals.

6.3 Recommendations and Proposals: Areas for reform in order to provide a more robust legal framework for protecting consumers using m-payment services

In summary, the existing Saudi regulation of m-payment services is deficient in two principal respects. Firstly, they fail to provide protection, which the Sharia law demands, to consumers

who might be less aware of the potential risks of FinTech, particularly against unauthorised m-payment transactions and 'datafication'[19], from mercenary corporations. In particular, as noted in chapter 3, they fail to ensure that wealth creation confers rights on persons in a way that promotes unity within society through high business standards.[20] Secondly, existing Saudi laws not only neglect to facilitate market innovation, competition, and the growth of the Fintech sector, but actively inhibit these processes. Again, this is contrary to the fundamental principles of Islam, and is not in the interests of the Saudi nation or individual consumers who might otherwise enjoy the benefits of m-payments. The root cause of these failings lies primarily in the failure of regulators to adopt a specialised regime to address the unique challenges posed by m-payment services. They, instead, attempt to shoehorn regulation of the newly emerged Fintech sector into existing banking regulations which were manifestly inadequate to manage the risks of a technology which was not even contemplated at the time they were drafted. This problem has become compounded over time, as m-payment services have grown ever further from traditional banking and the challenge faced by Saudi regulators in 'catching up' with the technology has grown ever more daunting.

It is apparent that the Saudi regulatory regime is in urgent need of reform. Notwithstanding the need for caution in pursuing any proposed regulatory transplant, SA can adopt a number of broad principles from the UK's approach which have been structured thematically to reflect the challenges identified in the Introduction chapter.

---

[19] M. Rhoen, 'Beyond consent: improving data protection through consumer protection law' (2016) *Internet Policy Review* 5(1) <https://policyreview.info/articles/analysis/beyond-consent-improving-data-protection-through-consumer-protection-law> accessed 15 April 2019.
[20] H. Abdalati, *Islam in Focus* (2nd ed, Dar Al-Elm Printing and Publishing Co 1985) 10.

A complete review of relevant aspects of Saudi law should take place to ensure overarching compliance with Sharia principles. The starting point for any such review is to identify the ideal position which SA hopes to achieve through regulation of the m-payments sector, drawing on the requirements of both Sharia law and the needs of the market if the Fintech sector is to thrive in the country. This review should then proceed to characterise the defects identified above in greater detail, along with any other areas in which it appears that Saudi regulation has fallen short of the preferred position. It will be necessary to consider the reasons for these shortcomings, both on an immediate level (i.e., that the primary reason for many of the failures is the neglect of updating the law to accommodate advances in mobile technology) and on a secondary level (broader features of the Saudi legal system which may inhibit the type of review and incremental reform which successful regulation of this sector requires). In respect of the latter, Islamic scholars should particularly focus on utilising the good faith principle to develop an Islamic fairness jurisprudence which can be applied to unfair contract terms and to devise more pro-consumer legislation, including in the field of data protection.

6.3.1 Balancing Consumer Protection and Market Innovation

UK law may be drawn on as an illustration of how consumer protection values can co-exist, and even support, strong competition within the market. One way to achieve this is to amend the Banking Control Law 1966, so that it clarifies that SAMA is responsible for regulating those which offer m-payment services, including TPPs and e-money institutions. This could also be an opportunity to introduce more efficient and effective provisions by which

consumer protections might be enforced, or to strengthen the powers of enforcement/mandate available to SAMA. For example, an Ombudsman service for resolution of consumer disputes has been introduced in the UK to facilitate the resolution of disputes and the enforcement of consumer rights. Introduction of comparable measures would make those rights which are protected by SAMA more meaningful. Similarly, the e-Banking Rules 2010 might be amended to complement the reformed regime in respect of e-money issuers. This could include, for example, provision to ensure that the service providers are required to make consumers aware of their rights and the straightforward mechanisms by which they can be enforced; mere awareness on the part of consumers is likely to have some effect in ensuring compliance by providers.

Alternatively, it might be preferable to create a new regime from first principles to cover the authorisation and supervision of payment service institutions, rather than implementing reforms within the existing framework of the Banking Control Law 1966. This option would take more time and would be more resource intensive, but it has the advantage of marking a 'fresh start' and allowing a coherent regime to be developed from the outset. In order to reap the full benefits of this investment, it would be desirable to replace the e-Banking Rules 2010 as part of the same process. In this way, policy makers can consider the desired balance between consumer protection and market innovation to best meet the country's needs and design legislation specifically intended to implement this, rather than seeking to adapt pre-existing measures which did not envisage the desired balance. In order to put together a more appropriate regime for regulating this area in a more social welfare-oriented approach to consumer protection, the areas and provision that the new statute

replacing the BCL 1966 and the E-banking Rules should incorporate, at a minimum, a coherent regime of definitions drawn along lines which would be (at least relatively) intuitive to consumers. Consumer rights, including in particular protections in the event of unauthorised transactions, should be clearly differentiated based on these definitions in ways which the consumer can understand in advance of making a decision about which service provider they wish to use. The UK approach provides a valuable model in this respect. Management of information is another important issue which must be addressed; this encompasses both provision of information to the consumer to resolve the challenges of information asymmetry, and protection of consumer data which as illustrated by the MLRs must be counterbalanced against the need to protect against the increased risk of money laundering which technology creates. The GDPR, balanced out by the MLR 2017, again provides a valuable model on which Saudi Arabian legislators might begin to build a regime providing the necessary balance. These specific recommendations are discussed in greater depth below. As discussed in chapter 3, one way to achieve this is to require compliance with regulatory technical standards which are firmly embedded with the consumer protection interest. TPPs must be licensed, just like certification service providers, since they hold the digital identities of customers. New provisions should be introduced to set out clearly the situations when liability will be imposed, as otherwise there exists too much uncertainty, rendering the service *haram*. The law should further mandate that customers are entitled to a prompt refund whenever fraud or other operational errors occur. A contract ought to be entered into between the TPPs and customers which clearly formulates the parties' respective rights and duties in accordance with the Islamic principle of good faith. Other obligations ought to be imposed on TPPs, especially to protect customers' digital identities and

appropriate sanctions have to be spelled out when TPPs and their collaborators fail to comply with their respective duties. This will incentivise the stakeholders within the m-payment ecosystem to adopt robust processes throughout the complicated architecture of this enterprise.

Moreover, the Combating Embezzlement Manual could extend the obligations to other stakeholders within the m-payment infrastructure, i.e. these parties should identify respective fraud risks and mitigation measures. Alternatively, banks could describe how these other partners combat fraud. The burden of this task may be shared between service providers, who should have an obligation to self-declare, and state institutions which should undertake monitoring (perhaps on a sampling or 'spot check' basis to minimise the demands on this task).

The AML Law could be further reformed. Whilst it can be applied to the m-payment context, m-payment transactions create new opportunities for criminals and terrorists to launder money and this also puts consumers at risk. For this reason, it is important to gather more information and to transpose FATF Recommendation 16, as previously discussed. Naturally this must be matched by improved protection of data and privacy in response to the increased risks created. It would also be useful for SAMA to issue specific guidance

modelled on the FATF recommendations entitled 'Prepaid Cards, Mobile Payments and Internet-Based Payment Services.'[21]

6.3.2 Institutional Competence

New authorisations schemes should be required for payment services institutions, as in the UK. Steps could be taken to facilitate consumerism by allowing new entrants to make use of telecommunications networks in order to make available m-payment services. Once these principles have been implemented broadly, the necessary statutory clarifications must be put in place to ensure that they are effected in practice. The Saudi government might consider adopting the broad categories which have been adopted in the UK (e.g., in respect of the boundaries of 'PS provider' and 'PS institution') following careful consideration.

6.3.3 Adherence to Sharia Values

Guidance should be provided for the application of Islamic principles in the context of m-payment contracts, particularly exclusion and limitation clauses. This would resolve the imbalance of negotiating power between consumer and service provider. The good faith principle should be specifically defined and identified as core principles in any new statutory rules so as to preserve the Sharia as the touchstone of fairness and common sense and ensure operators comply with the spirit and not merely the letter of the law. It should thus be

[21] Financial Action Task Force, 'Guidance for a Risk-Based Approach, Prepaid Cards, Mobile Payments and Internet-Based Payment Services', June 2013, 1-47, 3 <http://www.fatf-gafi.org/media/fatf/documents/recommendations/guidance-rba-npps.pdf> accessed 1 March 2015.

developed to address the extent to which Sharia law will impose or permit the exclusion of liability of m-payment providers to their customers. Provision of further guidance would encourage companies to act consistently with the intentions of legislators (particularly Islamic companies which are eager to operate consistently with Sharia values, but lack the understanding or expertise to do so, that is assuming that compliance with Saudi regulation inevitably entails compliance with Sharia principles). This could be done by adopting statutory restrictions that are comparable to those for the enforcement of unfair contract terms in the CRA 2015 and UCTA 1977 (UK).

6.3.4 Keeping Pace with Technological Change

This area of law should be kept under review to identify when changes in social or market conditions mean that it is no longer as effective as it could be in fulfilling its intended purpose. Mechanisms and procedures should be put in place to ensure that the necessary changes to the law can be implemented in a timely, efficient, and effective manner. These might be formalised as the regulatory regime matures. Promising options may include:

- A specialised body, such as the UK Payment Systems Regulator, to allow m-payment customers to settle disputes easily and quickly (as for example is provided by the UK ombudsman service). This might build on the work of the Consumer Protection Department which has already been established within SAMA[22] and could even make

[22] Survey of National Progress in the Implementation of G20/FSB Recommendations, Saudi Arabia, 1-44, 43 <http://www.financialstabilityboard.org/implementation_monitoring/saudi_arabia_2013.pdf> accessed 20 October 2014.

use of the 2014 draft bill for the creation of an independent body responsible for monitoring unethical practices (which remains unimplemented at the time of writing).[23]

- An advisory body or committee charged with monitoring developments in the Fintech sector and making recommendations as to how the law might respond.

6.4 Significance of these findings

The fundamental problem with the Saudi legislature regime is that it has failed to identify and respond to the specific challenges raised by m-payments, as distinct from traditional banking operations. This is epitomised by the failure to reform, or indeed to update in any way, the 1966 Banking Control Law, which is manifestly inadequate for the Fintech era. SAMA has similarly failed to shift its focus away from the traditional banking sector towards emerging services, despite indications that m-payment constitutes the fastest growing element of the financial sector.[24] The result is that the market is severely restricted, with companies permitted to offer only a limited range of services and innovation severely stifled. Even those enactments which have purported to update the law have often fallen short. In particular, the 2012 Regulatory Rules for Prepaid Payment Services offer little relief for the Fintech sector, instead maintaining the status quo bank-centric approach.

[23] Zawya, 'Consumer protection law under Shoura study', 12 November 2014 <https://www.zawya.com/story/Consumer_protection_law_under_Saudi_Shoura_study-ZAWYA20141112035028/> accessed 18 May 2015.
[24] A.A. Shaikh and H. Karjaluoto, 'Mobile banking adoption: A literature review' (2015) *Telematics and Informatics 32* (1), 129-142, 129.

This is detrimental not only to the Saudi economy as a whole, which given its high rate of smart phone use[25] might have had the potential to become a leader in this emerging sector, but also individual consumers who are unable to access the benefits of technological advancement which they might otherwise enjoy. This is inconsistent with Sharia values in a number of respects.

First and foremost, Saudi regulation fall short of the standard of consumer protection which Sharia demands in its approach to m-payment, the stifling of the market and economic growth is also fundamentally inconsistent with Islamic principles. The starting point is that reasonable protection against unethical treatment should be established by the law, particularly in the context of a newly emerged and high-tech sector where many consumers are likely to be uninformed as to the risks. Secondly, as is alluded to earlier in the work, the Hanbali School is normally liberal in legislating to address business matters. There thus exist fundamental reasons for legislators to abandon this trade-hindering approach. The overall conclusion of this assessment of Saudi regulation is therefore that it is in need of significant reform.

Finally, these discussions were drawn together in the closing chapter to consider the relative strengths and weakness of UK and Saudi regulation of m-payments and the ways in which the latter might learn from the former notwithstanding the different social, cultural, and economic contexts of the two jurisdictions. Indeed, on closer inspection of the law and policy in each country, it becomes apparent that the values which arise from these two

[25] Arab News, 'Saudi Arabia has almost double international rate of smartphones', 20 December 2017 <http://www.arabnews.com/node/1211721/saudi-arabia> accessed 10 February 2019.

different contexts are not so far apart after all; both the UK and SA are concerned to balance the interests of consumer protection and encouragement of market growth of innovation.

A number of recommendations were made as to how SA might benefit from the example of the UK in order to reform its own consumer protection regulatory regime, in particular in enhancing its consumer protection provisions and in updating its law to reflect advances in technology and the maturing of the Fintech sector, whilst maintaining or strengthening compliance with Sharia principles.

6.5 Further Research

This work has been restricted in its scope to consideration of m-payment services. As alluded to above, the regulatory context in SA is significantly different to that in the UK. Perhaps most obviously, SA is an Islamic nation in which the financial sector and economic regulation is moulded by a significant extent by the requirements of Sharia law. An interesting avenue for further research would be to consider how other Islamic countries have effected Sharia compliant regulation of m-payments and the successes and failures which have accompanied their attempts to do so.

However, there are many other social differences which distinguish the challenge faced by UK legislators from that of their Saudi counterparts in respect of regulating m-payment services. In particular, SA has one of the highest rates of smartphone use anywhere

in the world[26], and has a reasonably developed m-banking sector.[27] It may therefore be helpful to draw comparisons between SA and other nations with a comparable degree of technological advancement, in particular smart phone use, in order to identify other potentially valuable regulatory models. Ideally, a number of alternative models would be available to allow regulators to compare the success of each and select the most favourable elements as the basis for a new Saudi Arabian regime.

More generally, the m-payment market is amongst the most significant and fast-paced developments in financial services of modern times.[28] In light of this, it is desirable in general that further research should be completed into the likely future developments of this market, the regulatory challenges which may lie ahead, and pre-emptive solutions which might be adopted to address these.[29]

[26] European Travel Commission Digital Portal, 'Mobile/Smartphones, Rise of Mobile Internet Use in Middle East Region', 2014 <http://etc-digital.org/digital-trends/mobile-devices/mobile-smartphones/regional-overview/middle-east/> accessed 18 October 2014.
[27] Arab Advisors Group, 'Remote banking services adoption in Saudi Arabia', 30 May 2012 <http://www.arabadvisors.com/Pressers/presser-300512.htm> accessed 19 October 2014.
[28] PWC, 'Financial Services Technology 2020 and Beyond: Embracing disruption', 2016, 1-48 <https://www.pwc.com/gx/en/financial-services/assets/pdf/technology2020-and-beyond.pdf> accessed 29 April 2019.
[29] Ibid.

BIBLIOGRAPHY

BIBLIOGRAPHY

Legislation

Saudi Arabia Legislation

Anti-Money Laundering Law 2003

Banking Control Law 1966

Charter of the Saudi Arabian Monetary Agency 1957

Consumer Credit Regulations 2006

Credit Information Law 2008

Electronic Transaction Law 2007

Financial Services (Banking Reform) Act 2013

Regulations for Consumer Financing 2014

Saudi Credit Information Law 2008

UK Legislation

Banking Act 2009

Communications Act 2003

Consumer Credit Act 1974

Consumer Rights Act 2015

Data Protection Act 1984

Data Protection Act 1998

Electronic Money (Miscellaneous Amendments) Regulations 2002

Electronic Money Regulations 2011

Financial Services (Banking Reform) Act 2013

Financial Services (Banking Reform) Act 2013

Financial Services and Markets Act (Regulated Activities) Order 2001 (Statutory Instrument 2001/544) (Statutory Instrument 2001/544)

Financial Services and Markets Act 2000

Financial Services and Markets Act 2000 (Carrying on Regulated Activities by Way of Business) Order 2000 (Statutory Instrument 2001/1177)

Financial Services and Markets Act 2000 (Carrying on Regulated Activities by Way of Business)(Amendment) Order 2014 (Statutory Instrument 2014/3340)

Financial Services and Markets Act 2000 (Prescribed Financial Institutions) Order 2013

Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017

Payment Services Regulations 2009

Privacy and Electronic Communications (EC Directive) Regulations 2003

Sale of Goods Act 1979

Supply of Goods and Services Act 1982

Unfair Contract Terms Act 1977

Unfair Terms in Consumer Contracts Regulations 1999

Wireless Telegraphy Act 2006

US Legislation

US Truth in Lending Act of 1968

US Electronic Funds Transfer Act of 1978

South Korea Legislation

Electronic Financial Transaction Act No. 11087

Kenyan Legislation

National Payment Systems Act 2011

EU legislation

Communications Act 2003

Directive (EU) 2015/849 of the European Parliament and of the Council of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, amending Regulation (EU) No 648/2012 of the European Parliament and of the Council, and repealing Directive 2005/60/EC of the European Parliament and of the Council and Commission Directive 2006/70/EC

Directive 2000/46/EC of the European Parliament and the Council on the taking up and prudential supervision of the business of e-money institutions

Directive 2002/19/EC of the European Parliament and of the Council of 7 March 2002 on access to, and interconnection of, electronic communications networks and associated facilities

Directive 2002/21/EC of the European Parliament and of the Council of 7 March 2002 on a common regulatory framework for electronic communications networks and services

Directive 2006/48/EC of the European Parliament and of the Council of 14 June 2006 relating to the taking up and pursuit of the business of credit institutions

Directive 2007/64/EC on payment services in the internal market amending Directives 97/7/EC, 2002/65/EC, 2005/60/EC and 2006/48/EC and repealing Directive 97/5/EC, OJ L 319/1

Directive 2009/110/EC on the taking-up, pursuit and prudential regulation of the business of electronic money institutions amending Directives 2005/6-/EC and 2006/48/EC and repealing Directive 2000/46/EC

Directive 2009/140/EC of the European Parliament and of the Council of 25 November 2009 amending Directives 2002/21/EC on a common regulatory framework for electronic communications networks and services, 2002/19/EC on access to, and interconnection of, electronic communications networks and associated facilities, and 2002/20/EC on the authorisation of electronic communications networks and services, which amended both the Access and Framework Directive

Directive 2014/17/EU of the European Parliament and of the Council of 4 February 2014 on credit agreements for consumers relating to residential immovable property and amending Directives 2008/48/EC and 2013/36/EU and Regulation (EU) No 1093/2010

Directive 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC (Text with EEA relevance)

Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data

European Union Funds Transfer Regulation 2015/847

General Data Protection Regulation (Regulation (EU) 2016/679)

Treaty on the Functioning of the European

Case Law

UK cases

Agip (Africa) Ltd v Jackson (1989) 3 WLR 1367

Baden v Societe Generale (1983) BCLC 325

Bairstow Eves London Central Ltd v Smith (2008) EWHC 263

Bankers Insurance Co Ltd v South (2003) EWHC 380

Belmont Finance Corp Ltd v Williams Furniture Ltd (No 2) (1980) 1 All ER 393

Bond v British Telecommunications plc, Unreported, 28 March 2008, Walsall CC

Broadwater Manor School v Davis, unreported 8 January 1999, Worthing CC

Caparo Industries plc v Dickman (1990) UKHL 2

Cavendish Square Holding BV v Makdessi; ParkingEye Ltd v Beavis (2015) UKSC 67, (2015) 3 WLR 1383

Director General of Fair Trading v First National Bank (2001) UKHL 52

Director General of Fair Trading v First National Bank plc (2000) 1 All ER 240

Domsalla (t/a Domsalla Building Services) v Dyason (2007) EWHC 1174 (TCC), (2007) BLR 348

Durant v Financial Services Authority (2003) EWCA Civ 1746

Falco Finance Ltd v Gough (1999) CCLR 16

Falco Finance Ltd v Michael Gough Unreported 28 October 1998, Macclesfield CC

Greenwoods v Martins Bank (1933) AC 51

Hedley Byrne v Heller (1964) AC 465

Heifer International Inc v Helge Christiansen (2007) EWHC 3015

Interfoto Picture Library Ltd v Stiletto Visual Programmes Ltd [1989] QB 433

Joachimson v Swiss Bank Corporation (1921) 3 KB 110

Libyan Arab Foreign Bank v Bankers Trust & Pharaon v BCCI (1989) AC 80

Lipkin Gorman v Karpnale Ltd (1992) 2 AC 548

London Joint Stock Bank v Macmillan and Arthur (1918) AC 777

Michael Douglas v Hello! Ltd (No. 2) (2003) EWCA Civ 139

Mid Essex Hospital Services NHS Trust v Compass Group UK and Ireland Ltd (t/a Medirest) (2013) EWCA Civ 200

Midland Bank Ltd v Hett, Stubbs, Kemp & Co (A Firm) (1979) Ch 384

Oceano Grupo Editorial SA v Murciano Quintero C-244/98 to C/244/98

Office of Fair Trading v Abbey National plc and Others (2009) UKSC 6

Overy v *Paypal* (*Europe*) *Ltd* [*2012*] EWHC 2659 (QB), [2013] Bus LRD1

Royal Products v Midland Bank (1981) 2 Lloyds Rep 194

Scammel and Nephew Ltd v HC & JG Ouston (1941) AC 251

Sivagnanam v Barclays Bank Plc (2015) EWHC 3985 (Comm)

Smith v Lloyds TSB Bank (2000) 2 All ER (Comm) 693

Suisse Atlantique v Rotterdamsche Kolen [1967] 2 QB 361

Tai Hing Cotton Mill Ltd v Liu Chong Hing Bank (1986) AC 80

Tai Hing Cotton Mill v Liu Chong Hing Bank Ltd (1985) 2 All ER 947

Thornton v Shoe Lane Parking [1971] 2 QB 163

TSG Building Services plc v South Anglia Housing Ltd (2013) EWHC 1151 (TCC)

Vidal-Hall v Google Inc (2015) EWCA Civ 311

West v Ian Finlay & Associates (2014) EWCA Civ 316, (2014) BLR 324

European Case Law

Case C-362/14 *Maximillian Schrems v Data Protection Commissioner*

Saudi Arabia Case Law

Abdullah Girgi Beserani v Ismale Fawzi Abu Khadra (1996) Board of Grievance, Case No. 2195

Decisions

Saudi decisions

Council of Ministers' Decision No.59 dated 28.3.1420H

Ministry of Interior, Circular No.10207

Guidelines

Commission guidelines on market analysis and the assessment of significant market power under the Community regulatory framework for electronic communications networks and services, Official Journal C 165, 11/07/2002 P. 0006 - 0031

International Chamber of Commerce Code on Advertising and Marketing Communication Practices 2011

OECD Guidelines for Protecting Consumers from Fraudulent and Deceptive Commercial Practices Across Borders 2003

OECD, G20 High-Level Principles on Financial Consumer Protection, Paris, OECD, October 2011

UN Guidelines on Consumer Protection 2016

Guidance

General

Bank for International Settlements, 'Basel Committee on Banking Supervision, Consultative Document, Operational Risk', Supporting Document to the New Basel Capital Accord, 2001, 1-30 <http://www.bis.org/publ/bcbsca07.pdf> accessed 28 October 2013

Basel Committee, 'Risk management for electronic banking and electronic money activities', March 1998, 1-25 <https://www.bis.org/publ/bcbsc215.pdf> accessed 1 September 2016

FATF, 'International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation', The FATF Recommendations 2012, June 2012, 1-129 <http://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF%20Recommendations%202012.pdf> accessed 1 October 2017

FATF, 'Anti-money laundering and counter-terrorist financing measures, Kingdom of Saudi Arabia', Mutual Evaluation Report, September 2018, 1-243

Financial Action Task Force, ‘Guidance for a Risk-Based Approach, Prepaid Cards, Mobile Payments and Internet-Based Payment Services’, June 2013, 1-47 <http://www.fatf-gafi.org/media/fatf/documents/recommendations/guidance-rba-npps.pdf> accessed 1 March 2015

Financial Conduct Authority, ‘Mobile banking and payments -supporting an innovative and secure market’, Thematic Review TR13/6, August 2013, 1-12 <http://www.fca.org.uk/your-fca/documents/thematic-reviews/tr13-6> accessed 12 October 2013

Financial Conduct Authority, 'Payment Services and Electronic Money - Our Approach, The FCA’s role under the Payment Services Regulations 2017 and the Electronic Money Regulations 2011', September 2017, 1-237

Financial Conduct Authority, The Perimeter Guidance Manual, Chapter 3A, Guidance on the scope of the Electronic Money Regulations 2011, 1-14 <https://www.handbook.fca.org.uk/handbook/PERG/3A.pdf> accessed 10 November 2016

Mobile Financial Services Working Group, 'Mobile Financial Services, Consumer Protection in Mobile Financial Services' (2014) Guideline Note No.13, 1-15 <http://www.afi-global.org/sites/default/files/publications/mfswg_guideline_note_7_consumer_protection_in_mfs.pdf> accessed 1 September 2016

UK Guidance

Information Commissioner's Office, 'Guidance on data security breach management,' 2012, 1-8 <https://ico.org.uk/media/1562/guidance_on_data_security_breach_management.pdf> accessed 15 September 2016

Financial Conduct Authority’s Banking Conduct of Business Sourcebook

Financial Conduct Authority, 'The FCA's role under the Electronic Money Regulations 2011', June 2013, 1-113 <https://www.fca.org.uk/publication/archive/emoney-approach.pdf> accessed 10 November 2016

Payment Systems Regulator, 'Discussion paper: Data in the payments industry', June 2018, 1-66 <https://www.psr.org.uk/sites/default/files/media/PDF/PSR-Discussion-paper-Data-in-the-payments-industry-June-2018.pdf> accessed 5 July 2019

Standards of Lending Practice 2016

Swanney, D., 'Prevention of money laundering/combating terrorist financing, 2017 Consultation Version, Guidance for the UK Financial Sector, Part III: Specialist Guidance', The Joint Money Laundering Steering Group, May 2017, 1-49

Saudi Arabia Guidance

Saudi Arabian Monetary Agency, Consumer Protection Department, Banking Consumer Protection Principles, June 2013, 1-28 <http://www.anb.com.sa/pdf/banking/Banking_Consumer_Protection_Code_SAMA_English.pdf> 24 September 2014

Saudi Arabian Monetary Agency, E-Banking Rules, April 2010, 1-36

Saudi Arabian Monetary Agency, Manual of Combating Embezzlement & Financial Fraud & Control Guidelines 2008, 1-51 <http://www.sama.gov.sa/sites/samaen/RulesRegulation/Rules/Pages/prevention_of_fraud_v21.pdf> accessed 26 October 2014

Saudi Arabian Monetary Agency, Regulatory Rules for Prepaid Payment Services in the Kingdom of Saudi Arabia, March 2012, 1-55

Saudi Arabian Monetary Agency, SPAN, 2015 <http://www.sama.gov.sa/en-US/PaymentSystem/Pages/SPAN.aspx> accessed 1 November 2016

International Guidance

Financial Action Task Force, 'Guidance for a Risk-Based Approach, Prepaid Cards, Mobile Payments and Internet-Based Payment Services', June 2013, 1-47 <http://www.fatf-gafi.org/media/fatf/documents/recommendations/guidance-rba-npps.pdf> accessed 2 May 2015

Financial Action Task Force, 'International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation', The FATF Recommendations 2012, June 2012, 1-129 <http://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF%20Recommendations%202012.pdf> accessed 1 October 2017

Books

Abdalati, H., *Islam in Focus* (2nd ed, Jeddah, Dar Al-Elm Printing and Publishing Co 1985)

Ahsanullah, H. T., *Turning Point: Breaking the Shackles of Dependant Thinking a Personal Journey in Discovering God and Myself* (Bloomington, Authorhouse 2013)

Ahson, S., Ilyas, M., *RFID Handbook, Applications, Technology, Security, and Privacy* (Boca Raton, CRC Press 2008)

Akbarzadeh, S., and MacQueen, B., 'Framing the debate on Islam and human rights', in Islam and Human Rights in *Practice: Perspectives across the Ummah* (Abingdon, Taylor & Francis 2008)

Al Agha, K., Pujolle, G., Yahiha, T. A., *Mobile and Wireless Networks* (London and Hoboken, ISTE Ltd and John Wiley & Sons Inc 2016)

Al Rajhi, A., Al Salamah, A., Malik, M., Wilson, R., *Economic Development in Saudi Arabia* (Abingdon, Routledge Curzon 2004)

Al-Ali, *The Meaning of the Glorious Quran* (Jeddah, Islamic Books 1934)

Al-Bukhair, M., *Translation of Sahih Bukhair* (translation M. Khan), Volume 3, 41/572

Aldohni, A. K., *The Legal and Regulatory Aspects of Islamic Banking: A Comparative Look at the United Kingdom and Malaysia* (Abingdon, Routledge 2011)

Alhajjawi, M., *Aliqna in the Jurisprudence on Ahmed Bin Hanbal (The Convincing) 2/354* (A. Alsubki, The Knowledge Publishing House)

Al-Jayyousi, O.R., *Islam and Sustainable Development: New Worldviews* (Routledge 2016)

Allums, S., *Designing Mobile Payment Experiences: Principles and Best Practices for Mobile Commerce* (Sebastopol, O'Reilly Media Inc 2014)

Andenas, M., Chiu, I. H.-Y., *The Foundations and Future of Financial Regulation: Governance for Responsibility* (Abingdon, Routledge 2014)

Andenas, M., Fairgrieve, D., *Courts and Comparative Law* (Oxford, Oxford University Press 2015)

Andrews, G. M., and Millett, R., *Law of Guarantees* (6th ed, London, Sweet & Maxwell 2012)

Anolli, M., Beccalli, E., Giordani, T., *Retail Credit Risk Management* (Basingstoke, Palgrave MacMillan 2013)

Ariff, M., and Iqbal, M., *The Foundations of Islamic Banking: Theory, Practice and Education* (Cheltenham, Edward Elgar Publishing Ltd 2011)

Atilgan, A., *Global Constitutionalism: A Socio-legal Perspective* (Berlin Springer 2018)

Ayari et al, B., 'Delay-Aware Mobile Transactions'. In U. Brinkschulte et al (eds), *Software Technologies for Embedded and Ubiquitous Systems: 6th IFIP WG 10.2 International Workshop, SEUS 2008, Anacarpi, Capri Island, Italy, October 2008, Proceedings* (New York, Springer 2008)

Baamir, S., *Shari'a Law in Commercial and Banking Arbitration: Law and Practice in Saudi Arabia* (Farnham, Ashgate Publishing Ltd 2010)

Baldoni, R., and Chockler, G., *Collaborative Financial Infrastructure Protection, Tools, Abstractions, and Middleware* (Berlin, Springer-Verlag 2012)

Bar, von C., Drobnig, U., *The Interaction of Contract Law and Tort and Property Law in Europe: A Comparative Study* (Munich, European Law Publishers GmbH 2004)

Bayuk, J. L., Healey, J., Rohmeyer, P., Sachs, M.H., Schmidt, J., Weiss, J., *Cyber Security Policy Guidebook* (John Wiley & Sons Inc 2012)

Beale, H., Bishop, W.D., Furmston, M.P., *Contract: Cases and Materials* (5th ed, Oxford, Oxford University Press 2007)

Beatson, J., Burrows, A. S., Cartwright, J., *Anson's Law of Contrac*t (30th ed, Oxford, Oxford University Press 2016)

Beck, T., Maimbo, S. M., *Financial Sector Development in Africa, Opportunities and Challenges* (Washington DC, The World Bank 2011)

Baghdadi, Y., *ICT for a Better Life and a Better World: The Impact of Information and Communication Technologies and Organizations and Society* (Cham, Springer 2019)

Bhala, R., *Understanding Islamic Law* (Danver, LexisNexis 2011)

Bhatia, K.L., *Textbook on Legal Language and Legal Writing* (Universal Law Publishing Co Pvt Ltd 2010)

Bignami, F., and Zaring, D., *Comparative Law and Regulation: Understanding the Global Regulatory Process* (Cheltenham, Edward Elgar 2016)

Bin Al-Hajjaj, M., Being Traditions of the Sayings and Doings of the Prophet Muhammad as narrated by his Companions and Complied under the Title Aljami-US-Sahih 25/2387 (translation A. H. Siddiqui, Beirut, Arabic House for Printing and Publishing, and Distribution 1972)

Birch, K., *A Research Agenda for Neoliberalism* (Cheltenham, Edward Elgar 2018)

Boss, A.H., Kilian, W., *The United Nations Convention on the Use of Electronic Communications in International Contracts, An In-Depth Guide and Sourcebook* (AH Alphen aan den Rijn, Kluwer Law International 2008)

Boyd-Barrett, O., *Communications Media, Globalization, and Empire* (Herts, John Libbey Publishing Ltd 2016)

Boydell, S., and Braidwood, R., *Preliminary Physics, Cambridge Checkpoints 2012* (Cambridge, Cambridge University Press 2011)

Burrows, A., *A Casebook on Contract* (5th ed, Oxford, Hart Publishing 2016)

Burrows, A., *Principles of English Commercial Law* (Oxford, Oxford University Press 2015)

Cartwright, P., *Banks, Consumers and Regulation* (Oxford, Hart Publishing 2004)

Cartwright, P., *Consumer Protection in Financial Services* (London, Kluwer Law International 1999)

Cartwright, P., *Consumer Protection and the Criminal Law: Law, Theory, and Policy in the UK* (Cambridge, Cambridge University Press 2004)

Cerna, M., Svobodova, L., Hrusa, P., 'Quality in Mobile Payment Service in India' in Arpan Kumar Kar, P. Vigneswara Ilavarasan, M.P. Gupta, Yogesh K. Dwivedi, Matti Mäntymäki,

Marijn Janssen, Antonis Simintiras, Salah Al-Sharhan (eds), *Digital Nations – Smart Cities, Innovation, and Sustainability: 16th IFIP WG 6.11 Conference on e-Business, e-Services, and e-Society, i3E 2017, Delhi, India, November 21-23, 2017, Proceedings* (Cham, Springer 2017)

Chambers, A., Rand, G., *The Operational Auditing Handbook: Auditing Business and IT Processes* (2nd ed, Chichester, John Wiley & Sons Ltd 2010)

Chell, D., Erasmus, T., Colley, S., Whitehouse, O., *The Mobile Application Hacker's Handbook* (Indianapolis, John Wiley & Sons Inc 2015)

Choudhry, M., *The Principles of Banking* (Singapore, John Wiley & Sons Singapore Pte Ltd 2012)

Cohen, L., Manion, L., Morrison, K., *Research Methods in Education* (7th ed, Routledge 2011)

Conklin, W.E., *The Invisible Origins of Legal Positivism: A Re-Reading of a Tradition* (Kluwer Academic Publishers 2001)

Consolvo, S., Bentley, F. R., Hekler, E. B., Phatak, S. S., Mobile User Research: A Practical Guide (Williston, Morgan & Claypool 2017)

Cownie, F., *Legal Academics: Cultures and Identities* (Oxford, Hart Publishing 2004)

Curwen, P., and Whalley, J., *Mobile Telecommunications in a High-Speed World, Industry Structure, Strategic Behaviour and Socio-Economic Impact* (Farnham, Gower Publishing Ltd 2010)

Dagan, H., and Heller, M., *The Choice Theory of Contracts* (Cambridge, Cambridge University Press 2017)

Daidj, N., *Developing Strategic Business Models and Competitive Advantage in the Digital Sector* (Hershey, IGI Global 2015)

Dawson, M., and Omar, M., *New Threats and Countermeasures in Digital Crime and Cyber Terrorism* (Hershey, IGI Global 2015)

Delimatsis, P., and Herger, N., *Financial Regulation at the Crossroads: Implications for Supervision, Institutional Design and Trade* (AH Alphen aan den Rijn, Kluwer Law International 2011)

De Wit, G., The Character of Technological Change and Employment in Banking: A Case – Study of Dutch Automated Clearing House (Bgc) (Pinter, 1990)

Devenney, J., and Kenny, M., *European Consumer Protection: Theory and Practice* (Cambridge, Cambridge University Press 2012)

Dholakia, R.R., *Technology and Consumption: Understanding Consumer Choices and Behaviors* (London, Springer 2012)

DiMatteo, L.A. and Hogg, M., *Comparative Contract Law: British and American Perspectives* (Oxford, Oxford University Press 2016)

DiVanna, J.A., *Understanding Islamic Banking, The Value Proposition That Transcends Cultures* (Cambridge, Leonardo and Francis Press Ltd 2006)

Doherty, E.P., *Digital Forensics for Handheld Devices* (Boca Raton, CRC Press 2013)

Dorfleitner, G., Hornuf, L., Schmitt, M., Weber, M., *FinTech in Germany* (London, Springer 2017)

Dubey, A., and Misra, A., *Android Security, Attacks and Defenses* (Boca Raton, Taylor & Francis Group LLC 2013)

Duhan, P., and Singh, A., *M-Commerce: Experiencing the Phygital Retail* (Palm Bay, Apple Academic Press Inc 2019)

Durovic, M. and Micklitz, H.W., *Internationalization of Consumer Law: A Game Changer* (London, Springer 2016)

Ellinger, E.P., Lomnicka, E., Hare, C., *Ellinger's Modern Banking Law* (5th ed, Oxford, Oxford University Press 2011)

El Qorchi, M., Maimbo, S.M., Wilson, J. F., *Informal Funds Transfer Systems: An Analysis of the Informal Hawala System* (Washington DC, International Monetary Fund 2003)

Essvale Corporation Ltd, *Business Knowledge in IT in Global Retail Banking, the Complete Handbook for IT Professionals* (London, Essvale Corporations Ltd 2011)

Estreicher, S., and Sherwyn, D., *Alternative Dispute Resolution in the Employment Arena: Proceedings of the New York University 53rd Annual Conference on Labor* (London, Kluwer Law International 2004)

Etheredge, L., *Saudi Arabia and Yemen* (New York, Britannica Educational Publishing 2011)

Feintuck, M., and Varney, M., *Media Regulation, Public Interest and the Law* (2nd ed, Edinburgh, Edinburgh University Press 2006)

Filipe, J., and Obaidat, M.S., *E-Business and Telecommunications: International Conference, ICETE 2008: Porto, Portugal, July 2008, Revised Selected Papers* (Berlin, Springer-Verlag 2009)

Fikentscher, W., *Modes of Thought: A Study in the Anthropology of Law and Religion* (2nd ed, Tubingen, Mohr Siebeck 2004)

Forte, A.D.M., *Good Faith in Contract and Property* (Oxford, Hart Publishing 1999)

Gilchrist, G., *Learning iBeacon* (Birmingham, Packt Publishing 2014)

Gimigliano, G., *Bitcoin and Mobile Payments: Constructing a European Union Framework* (Basingstoke, Palgrave Macmillan 2016)

Gkoutzinis, A., *Internet Banking and the Law in Europe, Regulation, Financial Integration and Electronic Commerce* (Cambridge, Cambridge University Press 2006)

Glaessner, T.C., Kellermann, T., McNevin, V., *Electronic Security: Risk Mitigation in Financial Transactions: Public Policy Issues* (Washington DC, World Bank 2002)

Giordano Ciancio, A., 'Fairness in Consumer Law: A Vague, Flexible Notion' in V.K. Bhatia, J. Engberg, M. Gotti, D. Heller (eds) *Vagueness in Normative Texts* (Oxford, Peter Lang 2005)

Goldmann, P., *Financial Services, Anti-Fraud Risk and Control Workbook* (Hoboken, John Wiley & Sons Inc 2010)

Goldring, J., Maher, L., McKeough, J., Pearson, G., *Consumer Protection Law* (5th ed, Leichhardt, The Federation Press 1998)

Gordley, J., 'The functional method' in P. G. Monateri (eds), *Methods of Comparative Law* (Cheltenham, Edward Elgar 2012)

Griffor, E., *Handbook of System Safety and Security: Cyber Risk and Risk Management, Cyber Security, Threat Analysis, Functional Safety, Software Systems, and Cyber Physical Systems* (London, Elsevier 2017)

Grundmann, S., and Atamer, Y.M., *Financial Services, Financial Crisis and General European Contract Law, Failure and Challenges of Contracting* (Kluwer Law International 2011)

Harvey, M.G., *Wireless Next Generation Networks: A Virtue-Based Trust Model* (New York, Springer 2014)

Hassan, M.K., and Rashid, M., *Management of Islamic Finance: Principle, Practice, and Performance* (Bingley, Emerald Publishing Limited 2019)

Hassan, K., and Mahlknecht, M., *Islamic Capital Markets: Products and Strategies* (Chichester, John Wiley & Sons Ltd 2011)

Hendry, M., *Near Field Communications Technology and Applications* (Cambridge, Cambridge University Press 2014)

Hernich, A., *Foundations of Query Answering in Relational Data Exchange* (Berlin, Logos Verlag GmbH 2010)

Hill-Smith, A., *Consumer Credit: Law and Practice* (2nd ed, Abingdon, Routledge 2015)

Hood, P., *Principles of Lender Liability* (Oxford, Oxford University Press, 2012)

House of Commons, *Committee on Standards and Privileges, Privilege: Hacking of Members' mobile phones, Fourteenth Report of Session 2010-11* (London, TSO Shop 2011)

Howells, G., and Ramsay, I., *Handbook of Research on International Consumer Law* (2nd ed, Cheltenham, Edward Elgar 2018)

Hunter, C., and Cowan, D., *Integrating Socio-Legal Studies Into the Law Curriculum* (Basingstoke, Palgrave MacMillan 2012)

Husa, J., 'Research Designs of Comparative Law - Methodology or Heuristics?' in M. Adams, D. Heirbaut (eds) *The Method and Culture of Comparative Law: Essays in Honour of Mark Van Hoecke* (Oxford, Hart Publishing 2014)

Information Resources Management Association, *Banking, Finance, and Accounting: Concepts, Methodologies, Tools, and Applications* (Hershey, Business Science Reference 2015)

International Business Publications, *Saudi Arabia Central Bank & Financial Policy Handbook* (Washington DC, International Business Publications 2005)

Islam, Md. T., 'The Theological Foundations of Islamic Banking: A Critical Review' in M. Zulkhibri and T.A.A. Manap (eds), *Islamic Finance, Risk-sharing and Macroeconomic Stability* (Cham, Springer 2019)

Jedidia, K.B., 'How can Islamic banks achieve social justice?' A discourse. In T. Azid and L. Sunar (eds(, *Social Justice and Islamic Economics: Theory, Issues and Practice* (Abingdon, Routledge 2019) Chapter 5

Joshi, V.C., *E-Finance: The Future is Here* (2nd ed, London, Sage 2010)

Jones, B., and Norton, P., *Politics UK* (8th ed, Abingdon, Routledge 2014)

Jonsson, D., *Islamic Economics and the Final Jihad, The Muslim Brotherhood to the Leftist/Marxist - Islamist Alliance* (USA, Xulon Press 2006)

Kettell, B., *Introduction to Islamic Banking and Finance* (Hoboken, John Wiley & Sons 2011)

Khan, M.F., and Porzio, M., *Islamic Banking and Finance in the European Union: A Challenge* (Cheltenham, Edward Elgar Publishing Ltd 2010)

Khan, M.M., *Sahih Al Bukhair* (Beirut, Dar Al Arabi 1985)

Keshavjee, M.M., and Abdulla, R., 'Family Law to Finance' in A. B. Sajoo (eds.), *The Shari'a: History, Ethics and Law* (London, IB Tauris & Co Ltd 2018) Chapter 7.

Khosrow-Pour, M., *E-Commerce for Organizational Development and Competitive Advantage* (Hershey, IGI Global 2013)

Khosrow-Pour, M., *Encyclopedia of Information Science and Technology* (3rd ed, Hershey, Information Resources Management Association 2014)

Kidner, R., *Casebook on Torts* (12th ed, Oxford, Oxford University Press 2012)

King, B., *Bank 3.0, Why Banking Is No Longer Somewhere You Go, But Something You Do* (Singapore, Marshall Cavendish Business 2013)

Kommers, P., Isaias, P., Issa, K., The Evolution of the Internet in the Business Sector: Web 1.0 to Web 3.0 (Hershey, IGI Global 2015)

Kronqvist, J., and Lehto, M., 'Adopting Encryption to Protect Confidential data in Public Clouds: A Review of Solutions, Implementation Challenges and Alternatives' in N. Abouzakhar (eds), *ECCWS2015-Proceedings of the 14th European Conference on Cyber Warfare and Security, University of Hertfordshire, Hatfield, UK, 2-3 July 2015* (Reading, Academic Conferences and Publishing International Ltd 2015)

Keshavjee, M.M., *Islam, Sharia and Alternative Dispute Resolution: Mechanisms for Legal Redress in the Muslim Community* (New York, I.B. Tauris & Co Ltd 2013)

Kshetri, N., Fredriksson, T., Rojas Torres, D. C., *Big Data and Cloud Computing for Development: Lessons from Key Industries and Economies in the Global South* (Abingdon, Routledge 2017)

Kuhnel-Fitchen, K., Hough, T., *Optimize Contract Law* (Abingdon, Routledge 2014)

Lawson, R., *Exclusion Clauses and Unfair Contract Terms* (10th ed, London, Sweet & Maxwell 2011)

Lemstra, W., and W.H. Melody, W.H., *The Dynamics of Broadband Markets in Europe: Realizing the 2020 Digital Agenda* (Cambridge, Cambridge University Press 2015)

Lerner, T., *Mobile payment* (Wiesbaden, Springer 2013)

LeRoy Miller, R., *Business Law Today, Comprehensive Edition, Text & Cases* (11th ed, Boston, Cengage Learning2017)

Lewis, M.K., Ariff, M., Mohamad, S*., Risk and Regulation of Islamic Banking* (Edward Elgar 2014)

Lima Marques, C., Wei, D., *Consumer Law and Socioeconomic Development: National and International Dimensions* (Cham, Springer 2017)

Lloyd, I., *Information Technology Law* (7th ed, Oxford, Oxford University Press 2014)

Lodder, A.R., Murray, A.D., *EU Regulation of E-Commerce: A Commentary* (Cheltenham, Edward Elgar Publishing 2017)

Macleod, J., *Consumer Sales Law, The Law Relating to Consumer Sales and Financing of Goods* (London, Cavendish Publishing Ltd 2002)

Makin, P., 'Regulatory Issues around Mobile Banking in Organisation for Economic Co-operation and Development' in OECD (eds), *The Development Dimension ICTs for Development: Improving Policy Coherence* (Paris, OECD Publishing 2010)

Malloy, M.P., *Banking Law and Regulation* (2nd ed, New York, Wolters Kluwer 2016)

Mannan, M.A., *Islamic Economics: Theory and Practice* (London, Hodder and Stoughton 1986)

Mason, S., *Electronic Signatures in Law* (3rd ed, Cambridge, Cambridge University Press 2012)

Matthaus-Maier, I., von Pischke, J.D., *New Partnerships for Innovation in Microfinance* (Berlin, Springer-Verlag 2009)

Maurer, B., *Mutual Life, Limited: Islamic Banking, Alternative Currencies, Lateral Reason* (Princeton, Princeton University Press 2011)

McConville, M., Hong Chui, W., *Research Methods for Law* (Edinburgh, Edinburgh University Press 2007)

McKendrick, E., *Contract Law: Text, Cases, and Materials* (8th ed, Oxford, Oxford University Press 2018)

Mendelsohn, B., *Combating Jihadism: American Hegemony and Interstate Cooperation in the War on Terrorism* (Chicago, University of Chicago Press 2009)

Merritt, Z.D., *Combating Terrorism: U. S. Agencies Report Progress Countering Terrorism and Its Financing in Saudi Arabia, but Continued Focus on Counter Terrorism Financing Efforts Needed* (Washington DC, United States Government Accountability Office 2010)

Michaels, R., 'The Functional Method of Comparative Law' in Mathias Reimann and Reinhard Zimmermann (eds), *The Oxford Handbook of Comparative Law* (Oxford, Oxford University Press 2006)

Micklitz, H.-W., 'European Consumer Law' in E. Jones, A. Menon, and S. Weatherill (eds), *The Oxford Handbook of the European Union* (Oxford, Oxford Handbooks Online, 2013)

Miller, R., and Cross, F., *The Legal Environment Today* (5th ed, London, Thomson Learning 2007)

Miryala, R.K., Ramana Reddy, M.V., *Trends, Challenges & Innovations in Management - Volume III* (Hyderabad, Zenon Academic Publishing 2015)

Monateri, P.G., *Methods of Comparative Law* (Edward Elgar 2012)

Morley, D., Parker, C.S., *Understanding Computers: Today and Tomorrow* (15th ed, Stamford, Cengage Learning 2015)

Mulcahy, L., and Tillotson, J., *Contract Law in Perspective* (4th ed, London, Cavendish Publishing Ltd 2004)

Murdoch, S.J., Becker, I., Abu-Salma, R., Anderson, R., Bohm, N., Hutchings, A., Sasse, M. A., Stringhini, G., 'Are payment card contracts unfair?' In J. Grossklags and B. Preneel (eds), *Financial Cryptography and Data Security* (Heidelberg: Springer 2016) 600-608.

Mtenzi, F.J., Oreku, G.S., Lupiana, D.M., Yonazi, J.J., *Mobile Technologies and Socio-Economic Development in Emerging Nations* (Hershey, IGI Global 2018)

Murray, A., *Information Technology Law: The Law and Society* (3rd ed, Oxford, Oxford University Press 2016)

Muruganand, S., Kunasekaran, K.K.H., James, D., *Proceedings of the International Conference on Interdisciplinary Research in Electronics and Instrumentation Engineering, 11-12 August 2015* (Chennai, ICIREIE 2015)

Nahari, H., Krutz, R.L., *Web Commerce Security: Design and Development* (Indianapolis, Wiley Publishing Inc 2011)

Nebbia, P., *Unfair Contract Terms in European Law: A Study in Comparative and EC Law* (Oxford, Hart Publishing 2007)

Neef, D., *Digital Exhaust: What Everyone Should Know About Big Data, Digitization, and Digitally Driven Innovation* (New Jersey, Pearson Education 2015)

Nguyen, T., Goyal, A., Manicka, S., Nadzri, M.H.M., Perepa, B., Singh, S., Tennenbaum, J., *IBM Redbooks, IBM MobileFirst in Action for mGovernment and Citizen Mobile Services* (New York, International Business Machines Corporation 2015)

Nicoletti, B., *Cloud Computing in Financial Services* (Basingstoke, Palgrave Macmillan 2013)

Nicoletti, B., *Mobile Banking: Evolution Or Revolution?* (Basingstoke, Palgrave Macmillan 2014)

Nicoletti, B., *The Future of FinTech: Integrating Finance and Technology in Financial Services (*London, Palgrave Macmillan 2017)

Nottage, L., 'Product safety regulation.' In G. Howells, I. Ramsay and T. Wilhelmsson (eds). *Handbook of International Consumer Law and Policy* (Cheltenham, Edward Elgar 2010)

Odeh, I. A., *Anti-Money Laundering and Combating Terrorist Financing for Financial Institutions* (Pittsburgh, Dorrance Publishing Co Inc 2010)

O'Donovan, J., *Lender Liability* (London, Sweet & Maxwell 2005)

OECD, *Consumer Policy Toolkit* (Paris, OECD Publishing 2010)

Oriyano, S.-P., Gregg, M., *Hacker Techniques, Tools, and Incident Handling* (Jones & Bartlett Learning 2011)

Ormerod, D., Perry, D., *Blackstone's Criminal Practice 2018* (Oxford, Oxford University Press 2017)

Örücü, E., *The Enigma of Comparative Law: Variations on a Theme for the Twenty-First Century* (Springer & Business Media 2004)

O'Sullivan, J., and Hilliard, J., *The Law of Contract* (7th ed, Oxford, Oxford University Press 2016)

Oxford Business Group, *The Report, Saudi Arabia 2010* (Oxford, Oxford Business Group 2011)

Ozatac, N., and Gökmenoglu, K. K., *Emerging Trends in Banking and Finance: 3rd International Conference on Banking and Finance Perspectives* (London, Springer 2018)

Padmalatha, S., and Paul, J., *Management of Banking & Financial Service* (2nd ed, London, Pearson 2010)

Pan, Y.-C., Jacobs, A., Tan, C., Askool, S., 'Extending Technology Acceptance Model for Proximity Mobile Payment via Organisational Semiotics' in K. Liu, K. Nakata, W. Li, C. Baranauskas (eds), *Digitalisation, Innovation, and Transformation* (Cham, Springer 2018)

Park, J. J., et al, *IT Convergence and Services, ITCS 2011 & IRoA 2011* (London, Springer 2012)

Parry, D., Nordhausen, A., Howells, G., Twigg-Flesner, C., *The Yearbook of Consumer Law 2009* (London, Routledge 2008)

Pathan, A.-S., *Security of Self-Organizing Networks: MANET, WSN, WMN, VANET* (Boca Raton, Taylor and Francis Group 2011)

Patil, M. B., *Basic Electronics Devices and Circuits* (Delhi, PHI Learning Private Ltd 2013)

Penttinen, J. T. J., *The Telecommunications Handbook: Engineering Guidelines for Fixed, Mobile and Satellite Systems* (Chichester, John Wiley & Sons Ltd 2015)

Platteau, J.-P., *Islam Instrumentalized, Religion and Politics in Historical Perspective* (Cambridge, Cambridge University Press 2017)

Penttinen, J. T. J., *Wireless Communications Security: Solutions for the Internet of Things* (Chichester, John Wiley & Sons Ltd, 2017)

Poole, J., *Casebook on Contract Law* (13th ed, Oxford, Oxford University Press 2016)

Porzio, C., 'Islamic banking versus conventional banking' in M. F. Khan and M. Porzio (eds), Islamic Banking and Finance in the European Union, A Challenge (Cheltenham, Edward Elgar 2010)

Popkova, E. G., Ragulina, Y. V., Bogoviz, A. V., *Industry 4.0: Industrial Revolution of the 21st Century* (Cham, Springer 2019)

QFinance, *Islamic Finance: Instruments and Markets* (London, Bloomsbury Publishing 2010)

Quirk, P. and Rothchild, J. A., 'Consumer Protection and the Internet' in G. Howells, I. Ramsay and T. Wilhelmsson, *Handbook of Research on International Consumer Law* (Cheltenham, Edward Elgar 2010)

Radin, M. J., *Boilerplate: The Fine Print, Vanishing Rights, and the Rule of Law* (Princeton, Princeton University Press 2013)

Ramady, M.A., *The Saudi Arabian Economy* (Springer 2010)

Ramadan, H. M., *Understanding Islamic Law: From Classical to Contemporary* (Lanham, AltaMira Press 2006)

Ramsay, I., *Advertising Culture and the Law: Beyond Lies, Ignorance and Manipulation* (London, Sweet & Maxwell 1997)

Ramsay, I., 'Changing Policy Paradigms of EU Consumer Credit and Debit Regulation.' In D. Leczykiewicz and S. Weatherill (eds). *The Image of the Consumer in EU Law* (Bloomsbury, Hart 2016)

Rao, H. R., Gupta, M., Upadhyaya, S., *Managing Information Assurance in Financial Services* (Hershey, IGI Publishing 2007)

Resatch, F., *Ubiquitous Computing: Developing and Evaluating Near Field Communication Applications* (Wiesbaden, Springer 2010)

Rida et al, A., *RFID-Enabled Sensor Design and Applications* (Norwood, Artech House 2010)

Roach, L., *Card and James' Business Law* (4th ed, Oxford, Oxford University Press 2016)

Roberts, A., Stephan, P. B., Versteeg, M., Verdier, P.-H., *Comparative International Law* (Oxford, Oxford University Press 2018)

Rouse, J., et al, *Hacking Exposed Mobile: Security Secrets & Solutions* (New York, McGraw Hill Professional 2013)

Rowland, D., and MacDonald, E., *Information Technology Law* (3rd ed, Abingdon, Routledge-Cavendish 2005)

Salz, P. A., *The Netsize Guide 2009: Mobile Society & Me, when worlds combine* (London, Netsize 2009)

Samani, R., et al, *CSA Guide to Cloud Computing: Implementing Cloud Privacy and Security* (London, Elsevier 2015)

Scardovi, C., *Restructuring and Innovation in Banking* (London, Springer 2016)

Schuller, B., 'Social peace via pragmatic civil rights -the Scandinavian model of consumer law' in H. W. Micklitz (eds) *The Many Concepts of Social Justice in European Private Law* (Cheltenham, Edward Elgar 2011)

Scupola, A., *Developing Technologies in E-Services, Self-Services, and Mobile Communication: New Concepts* (Hershey, Information Science Reference 2011)

Scupola, A. *Innovative Mobile Platform Developments for Electronic Services Design and Delivery* (Hershey, Business Science Reference 2012).

Schoon, N., *Islamic Banking and Finance* (London, Spiramus Press Ltd 2009)

Siddiqi, A. H., *Sahih Muslim, Volume III, Book IX* (Jeddah, undated)

Singhal, S., *WAP-the Wireless Application Protocol: Writing Applications for the Mobile Internet* (Boston, Addison-Wesley 2001)

Slapper, G., and Kelly, D., *English Legal System 2009-2010* (8th ed, Abingdon, Routledge-Cavendish 2009)

Smith, A., *An Inquiry into the Nature and Causes of the Wealth of Nations* (W. Strahan and T. Cadell 1776)

Springer, P.J., *Encyclopedia of Cyber Warfare* (Santa Barbara, ABC-Clio LLC 2017)

Stertz, F., Mangler, J., S. Rinderle-Ma, S., 'NFC-Based Task Enactment for Automatic Documentation of Treatment Processes' in Iris Reinhartz-Berger, Jens Gulden, Selmin Nurcan, Wided Guédria, Palash Bera (eds.), *Enterprise, Business-Process and Information Systems Modeling* (London, Springer 2017)

Stewart, J. M., *Comp TA Security + Review Guide* (2nd ed, Indianapolis, Wiley & Sons 2011)

Stokes, E., 'Double Movements in the Regulation of New Technologies: The Case of Nanotechnology' in B. Lange, F. Haines, D. Thomas (eds), *Regulatory Transformations: Rethinking Economy-Society Interactions* (Oxford, Hart Publishing 2015)

Sunnahn Al-Termizi, Hadith Books, Ministry of Islamic Affairs, Endowments, Dah'wah and Guidance, Saudi Arabia

Suresh, P., and Paul, J., *Management of Banking and Financial Services* (2nd ed, New Delhi, Dorling Kindersley (India) Pvt Ltd 2010)

Tamadonfar, M., *Islamic Law and Governance in Contemporary Iran: Transcending Islam for Social, Economic and Political Order* (London, Lexington Books 2015)

Téllez, J., Zeadally, S., *Mobile Payment Systems: Secure Network Architectures and Protocols* (Cham, Springer 2017)

Thanasegaran, H., *Good Faith in Insurance and Takaful Contracts in Malaysia, A Comparative Perspective* (Springer 2016).

Todoroki, E., et al, *Making Remittances Work: Balancing Financial Integrity and Inclusion* (Washington DC, The World Bank 2014)

Trentman, F., *'Empire of Things: How We Became a World of Consumers, from the Fifteenth Century to the Twenty-First* (New York, Harper 2016)

Turner, R. S., *Neo-Liberal Ideology, History, Concepts and Policies* (Edinburgh, Edinburgh University Press 2008)

Valdar, A., *Understanding Telecommunications Networks* (London, Institution of Engineering and Technology 2006)

Van der Meulen, N. S., *Financial Identity Theft: Context, Challenges and Countermeasures* (The Hague, TMC Asser Press 2011)

Van Greuning, H., and Iqbal, Z., *Risk Analysis for Islamic Banks* (Washington DC, The World Bank 2008)

Van Hoecke, M., *Methodologies of Legal Research: Which Kind of Method for What Kind of Discipline?* (Oxford, Hart Publishing 2011)

Venardos, A. M., *Islamic Banking and Finance in South-East Asia: Its Development and Future* (3rd edn, Singapore, World Scientific Publishing Co Pte Ltd 2012)

Vermaat, M. E., et al, *Discovering Computers 2014, Technology in a World of Computers, Mobile Devices, and the Internet* (Boston, CengageBrain 2013)

Villeneuve et al, T. F., *Corporate Partnering: Structuring & Negotiating Domestic & International Strategic Alliances* (5th ed, New York, Wolters Kluwer 2017)

Von Bar, C., and Drobnig, U., *The Interaction of Contract Law and Tort Law and Property Law in Europe: A Comparative Study* (Munich, Sellier European Law Publishers 2004)

Wandhofer, R., 'European Payments: A Path Towards the Single Market for Payments' in B. Batiz-Lazo and L. Efthymiou (eds), *The Book of Payments: Historical and Contemporary Views on the Cashless Society* (London, Palgrave Macmillan 2016)

Weatherill, S., 'Who is the "average consumer?" In S. Weatherill and I. Bernits (eds), *The regulation of unfair commercial practices under EC Directive 2005/29: New rules and new techniques* (Oxford: Hart Publishing 2007)

Wernaart, B., *The Enforceability of the Human Right to Adequate Food: A Comparative Study* (Wageningen, Wageningen Academic Publishers 2013)

Weyl, W. E., *The New Democracy: An Essay on Certain Political and Economic Tendencies in the United States* (New York, Harper & Row 1912, 1964)

Wild, C., et al, *Electronic Mobile Commerce Law, An analysis of trade, finance, media and cybercrime in the digital age* (Hertfordshire, University of Hertfordshire Press 2011)

Willett, C., *Fairness in Consumer Contracts: The Case of Unfair Terms* (2nd ed, Abingdon, Routledge 2016)

Williams, T., 'Continuity, not Rupture: The Persistence of Neoliberalism in the Internationalization of Consumer Finance Regulation' in T. Wilson (eds). *International Responses to Issues of Credit and Over-indebtedness in the Wake of Crisis* (eds) (Abingdon, Routledge 2013)

Wilson, R., *Legal, Regulatory and Governance Issues in Islamic Finance* (Edinburgh, Edinburgh University Press Ltd 2012)

Xiao, J. J., *Consumer Economic Wellbeing* (London, Springer 2015)

Xu, J., *Managing Digital Enterprise: Ten Essential Topics* (Paris, Atlantis Press 2014)

Yang et al, L. T., *Handbook on Mobile and Ubiquitous Computing: Status and Perspective* (Boca Raton, CRC Press 2012)

Zetsche, D.A., Buckley, R.P., Arner, D.W., Barberis, J.N., 'From Fintech to TechFin: The Regulatory Challenges of Data-Driven Finance' (2017) European Banking Institute Working Paper Series 3, No.6, 1-36

Zweigert, K., and Kotz, H., *An introduction to comparative law* (Oxford, Oxford University Press 1998)

Zhang, M. Y., Dodgson, M., *High-tech Entrepreneurship in Asia: Innovation, Industry and Institutional Dynamics in Mobile Payments* (Cheltenham, Edward Elgar 2007)

Ziegel, J. S., and Lerner, S., *New Developments in International Commercial and Consumer Law* (Oxford, Hart Publishing 1998)

Zuhur, S., *Saudi Arabia* (Santa Barbara, ABC-CLIO LLC 2011)

Reports

Board of Trade, Final Report of the Committee on Consumer Protection (Molony Committee) Cmnd 1781/1962

Capgemini and BNP Paribas, 'World Payment Report', 14th ed, 2018, 1-56, 31 <https://worldpaymentsreport.com/wp-content/uploads/sites/5/2018/10/World-Payments-Report-2018.pdf> accessed 10 February 2019

Competition & Markets Authority, 'Unfair contract terms guidance, Guidance on the unfair terms provisions in the Consumer Rights Act 2015', CMA 37, 31 July 2015, 1-144

European Commission, 'Report from the Commission to the European Parliament, the Council and the European Economic and Social Committee, First Report on the application of Directive 2005/29/EC of the European Parliament and of the Council of 11 May 2005 concerning unfair business-to-consumer commercial practices in the internal market and amending Council Directive 84/450/EEC, Directives 97/7/EC, 98/27/EC and 2002/65/EC of the European Parliament and of the Council and Regulation (EC) No 2006/2004 of the European Parliament and of the Council ('Unfair Commercial Practices Directive'), Brussels, COM(2013) 139 final, 14 March 2013, 1-31

World Economic Forum, 'A Blueprint for Digital Identity, The Role of Financial Institutions in Building Digital Identity', August 2016, 1-108 <http://www3.weforum.org/docs/WEF_A_Blueprint_for_Digital_Identity.pdf> accessed 1 May 2017

Financial Action Task Force, 'Money Launder Using New Payment Methods', FATF Report, October 2010, 1-117 <http://www.fatf-

gafi.org/media/fatf/documents/reports/ml%20using%20new%20payment%20methods.pdf> accessed 3 May 2015

International Monetary Fund, Saudi Arabia: Financial Sector Assessment Program Update—Detailed Assessment of Observance of the Basel Core Principles for Effective Banking Supervision, IMF Country Report No.13/213, July 2013

Law Commission, 'Unfair Terms in Consumer Contracts: a new approach?', Issues Paper, 25 July 2012

OECD, 'Report on Consumer Protection in Online and Mobile Payments', 17 August 2012, 1-45

McAfee Labs, '2013 Threats Predictions', Report, 2013, 1-16 <http://www.mcafee.com/uk/resources/reports/rp-threat-predictions-2013.pdf> accessed 20 December 2013

Sir Mark Walport, *FinTech Futures: The UK as a World Leader in Financial Technologies*, Report of the UK Government Chief Scientific Adviser, March 2015, 1-68

UNCTAD, *Information Economy Report 2007-2008: Science and Technology for Development: The new paradigm of ICT* (New York and Geneva, United Nations 2007)

Zhu, X., *Emerging Champions in the Digital Economy: New Theories and Cases on Evolving Technologies and Business Models* (Singapore, Springer 2019)

Articles

Abbamonte, G.B., 'The Unfair Commercial Practices Directive: An Example of the New European Consumer Protection Approach' (2006) *Columbia Journal of European Law* 12 (3), 695-712

Abu Bakar, E., Amin, N., 'Consumer Protection under Islamic Law in the Service Industry' (2011) *International Journal of Social Policy and Society* 8, 37-49

Ahmat, K.A., 'Emerging Cloud Computing Security Threats' (2015) City University of New York, 1-4 <https://arxiv.org/ftp/arxiv/papers/1512/1512.01701.pdf> accessed 5 March 2019

Albaqme, A.S., 'Consumer Protection under Saudi Arabia Law' (2014) *Arab Law Quarterly* 29, 158-175

Al-Fawzan, N., Elsayed, O., 'Data Protection in the Kingdom of Saudi Arabia: A Primer', Latham & Watkins LLP, 2015, 1-2 <https://www.lw.com/presentations/Data-Protection-in-the-Kingdom-of-Saudi-Arabia> accessed 1 November 2016

Alhaidary, M.A.A., Measuring Compensation from Credit Reporting Damage: A Comparison of Islamic, Saudi, and American Law in Light of Credit Information Reporting Acts, University of Kansas, 2012, 1-300 <https://kuscholarworks.ku.edu/bitstream/handle/1808/9855/Alhaidary_ku_0099D_12164_DATA_1.pdf?sequence=1&isAllowed=y> accessed 22 October 2014

Akbar Khan, M., 'Consumer Protection and the Islamic Law of Contract' (2011) *Islamabad Law Review* 2(2), 62-73

Alqarni, A., 'Saudi Consumers' Experience toward the Role of the Government Agencies as Service Providers in Ensuring their Consumer Rights' (2016) *International Journal of Business and Social Sciences* 7(9), 72-76

Amao, O., 'Judicial Discretion and Doing between the Banks and their Customers: A Critical Analysis of the Supreme Court Decision in Office of Fair Trading v Abbey National Plc and Others' (2011), 5 *Web Journal of Current Legal Issues*, 1-15

Anderson, R., and Moore, T., 'The economics of information security' (2006) *Science* 314, 610-613

Arnone, M., Bandiera, L., 'Monetary Policy, Monetary Areas, and Financial Development with Electronic Money', IMF Working Paper WP/04/122, July 2004

Asay, M., 'Why Your iPhone Will Inevitably Catch a Virus', Hack, 5 September 2013 <http://readwrite.com/2013/09/05/kaspersky-the-ios-malware-dam-will-break/> accessed 1 September 2016

Ayob, H., 'Consumer Protection in Islam: An Overview' (2014) *Malaysian Journal of Consumer and Family Economics*, 1-10

Baker, T. and Siegelman, P., 'Protecting Consumers from Add-On Insurance Products: New Lessons for Insurance Regulation from Behavioral Economics' (2013) *University of Pennsylvania Law School Research Paper* No. 13-1, 1-61

Bank for International Settlements, 'Payment, clearing and settlement systems in Saudi Arabia', CPSS Red Book, 2012, 349-372 <http://www.bis.org/cpmi/publ/d105_sa.pdf> accessed 25 October 2014

Bar-Grill, O., 'The Behavioral Economics of Consumer Contracts' (2008) *Minnesota Law Review* 92, 749-802

Bashir, M., Hayes, C, Lambert, A. D., Kesan, J. P., 'Online privacy and informed consent: The dilemma of information asymmetry' (2016) *Proceedings of the Association for Information Science and Technology* 52(1), 1-10 <https://onlinelibrary.wiley.com/doi/full/10.1002/pra2.2015.145052010043> accessed 20 April 2019

Batista, C., et al, International Experiences of Mobile Banking Regulation, International Growth Centre Policy Brief 36012, January 2012, 1-15 <http://www.theigc.org/wp-content/uploads/2015/03/Batista-Et-Al-2012-Policy-Brief.pdf> accessed 1 September 2016

Becker, I., Hutchings, A., Abu-Salma, R., Anderson, R., Bohm, N., Murdoch, S. J., Sasse, M. A., and Stringhini, G., 'International comparison of bank fraud reimbursement: customer perceptions and contractual terms' (2017) *Journal of Cybersecurity* 3(2), 109-125

Be'er, H., Metaphor, 'A (real) real-life Stagefright exploit', Exploit, 1-38 <https://www.exploit-db.com/docs/39527.pdf> accessed 1 September 2016

Ben-Shahar, O. and Schneider, C. E., 'The Failure of Mandated Disclosure' (2011) *University of Pennsylvania Law Review* 159(3), 101-204

Bohm, N., Brown, I., Gladman, B., 'Electronic commerce: Who carries the risk of fraud' (2000) The Journal of Information, Law and Technology, 3 <https://warwick.ac.uk/fac/soc/law/elj/jilt/2000_3/bohm/> accessed 10 April 2019

Borroni, A., C. Tabor, C., 'Caveat Emptor's Current Role in Louisiana and Islamic Law: Worlds Apart yet Surprisingly Close' (2009) *Journal of Civil Law Studies* 2(1), 61-100

Brand, O., 'Conceptual Comparisons: Towards a Coherent Methodology of Comparative Legal Studies' (2007) *Brooklyn Journal of International* Law 32, 405-466

Calboli, I., 'A Call for Strengthening the Role of Comparative Legal Analysis in the United States' (2017) *Saint Johns Law Review* 90(3), 609-638

Calliess, G.-P., 'Transnational Consumer Law: Co-Regulation of B2C-E-Commerce' (2007) *Law Research Institute Research Paper Series* 3(3), 1-54

Carare, P. M., 'Monopoly: Advantages and Disadvantages' (2011) Alexandru Ioan Cuza University, 1-6 <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1787089> accessed 1 November 2016

Carse, A., and Padfield, A., 'Consumer insurance: the risks of contracting on unfair terms' (2012) *Journal of the British Insurance Law Association* 125, 64-69

Castro, D., et al, 'Embracing the Self-Service Economy' (2010) *Information Technology & Innovation Foundation*, 1-54 <http://ssrn.com/abstract=1590982> accessed 22 December 2013

Cavoukian, A., 'Mobile Near Field Communications (NFC) "Tap 'n Go" Keep it Secure & Private, Information and Privacy Commissioner Ontaria', Canada, 2013, 1-22 <http://www.ipc.on.ca/images/Resources/mobile-nfc.pdf> accessed 29 December 2013

Certified Ethical Hacker, 'Ethical Hacking and Countermeasures Version 6, Module XXXVI, Hacking Mobile Phones, PDA and Handheld Devices', 2008, 1-90 <http://blurredlogic.net/data/tut/Ethical_HackingV6/CEH-v6_Instructor_slides/CEHv6%20Module%2036%20Hacking%20Mobile%20Phones,%20PDA%20and%20Handheld%20Devices.pdf> accessed 30 December 2013

Chen-Wishart, M., 'Regulating Unfair Terms', *English and European Perspectives on Contract and Commercial Law: Essays in Honour of Hugh Beale*, October 2014, 105-130 <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2709069> accessed 10 November 2016

Choi, S. B., Han, N. H., Bae, M. K., Bae, J. H., 'Towards A Better Understanding of Good Faith Concept in Islamic Contract Law' (2018) *International Journal of Engineering & Technology* 7(4), 247-253

Chun, S.-H., 'E-Commerce Liability and Security Breaches in Mobile Payment for e-Business Sustainability' (2019) *Sustainability* 11, 715-733

Cloud Security Alliance, 'Security Guidance for Critical Areas of Mobile Computing', November 2012, 1-60 <https://downloads.cloudsecurityalliance.org/initiatives/mobile/Mobile_Guidance_v1.pdf> accessed 1 September 2016

Collins, H., 'Harmonisation by Example: European Laws against Unfair Commercial Practices' (2010) *The Modern Law Review* 73(1), 89-118

Competition & Markets Authority and the Office of Communications, 'Memorandum of understanding between the Competition and Markets Authority and the Office of Communications - concurrent competition powers, 2 February 2016, 1-21 <https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/502645/Ofcom_MoU.pdf> accessed 10 November 2016

Consumer International, 'Decision Making in the Global Market: Trade, Standards and the Consumer', 2005, 1-152

Cooter, R. D., and Rubin, E. L., 'A Theory of Loss Allocation for Consumer Payments' (1987) *Texas Law Review* 66(3), 63-130

Daly, A., and Scardamaglia, A., 'Profiling the Australian Google Consumer: Implications of Search Engine Practices for Consumer Law and Policy' (2017) *Journal of Consumer Policy*, 1-22

De Mauro, A. Greco, M. and Grimaldi, M. A formal definition of Big Data based on its essential features. (2016) *Library Review* 65(3), 122-135.

Delgadillo, L. M. 'An Assessment of Consumer Protection and Consumer Empowerment in Costa Rica' (2013) *Journal of Consumer Policy* 36, 59-86

Demombynes, G., Thegeya, A., 'Kenya's Mobile Revolution and the Promise of Mobile Savings' (2012) *World Bank Policy Research Working Paper* No.5988, 1-32 <http://ssrn.com/abstract=2017401> accessed 5 January 2014

Department for Business Innovation & Skills, 'Businesses get ready for new consumer laws', 2015, 1 <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/464208/Consumer_Rights_Act_2015_BIS_media_release.pdf> accessed 1 March 2019

Department for Culture, Media and Sport, 'Implementing the revised EU Electronic Communications Framework, Impact Assessment', April 2011, 1-204 <https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/77643/Implementing_revised_EU_ElectronicCommunicationsFramework_IA.pdf> accessed 10 November 2016

Dorfman, R.S., 'The Regulation of Fairness and Duty of Good Faith in English Contract Law: A Relational Contract Theory Assessment' (2013) *Leeds Journal of Law & Criminology* 1(1), 91-116

Drinkwater, D. 'RBS and NatWest to let mobile customers sign-in with biometrics', SC Magazine, 18 February 2015 <https://www.scmagazineuk.com/rbs-and-natwest-to-let-mobile-customers-sign-in-with-biometrics/article/537599/> accessed 15 December 2017.

Eberle, E. J., 'The Method and Role of Comparative Law' (2009) *Washington University Global Studies Law Review* 8(3), 451-486

Edmonds, T., 'High Cost Consumer Credit', House of Commons Briefing Paper, Number 05849, 15 July 2014, 1-48

Edwards, C., 'Freedom of Contract and Fundamental Fairness for Individual Parties: The Tug of War Continues' (2009) *UMKC Law Review* 77(3), 647-696

Elkarkouri, D, 'Pre-Contractual Liability in Islamic Construction Contracts' (1992) *International Construction Law Review* 4, 544-551

Epstein, R. A., 'Behavioral Economics: Human Errors and Market Corrections' (2006) *University of Chicago Law Review* 73, 111-132

Epstein, R. A., 'The Neoclassical Economics of Consumer Contracts' (2008) *Minnesota Law Review* 92, 803- 835

Esposito, F., 'A Dismal Reality: Behavioural Analysis and Consumer Policy' (2017) *Journal of Consumer Policy* 40, 193-216

Esmaeili, H., 'On a Slow Boat Towards the Rule of Law: The Nature of Law in the Saudi Arabian Legal System' (2009) *Arizona Journal of International & Comparative Law* 26(1), 1-47

European Banking Authority, 'Discussion Paper on future Draft Regulatory Technical Standards on strong customer authentication and secure communication under the revised Payment Services Directive (PSD2)', 2016, 1-31 <https://www.eba.europa.eu/documents/10180/1303936/EBA-DP-2015-03+%28RTS+on+SCA+and+CSC+under+PSD2%29.pdf> accessed 1 November 2016

European Banking Federation, 'European Banking Federation (EBF) Position Paper on the European Commission Proposal for a Revised Payment Services Directive (PSD2), Brussels, 8 November 2013, 1-16 <http://www.ebf-fbe.eu/uploads/EBF_004743%20-%20EBF_004025%20-%20EBF%20position%20on%20PSD2_08Nov2013.pdf> accessed 1 November 2016

European Commission, 'Commission decisions on the adequacy of the protection of personal data in third countries.' 2016 <http://ec.europa.eu/justice/data-protection/international-transfers/adequacy/index_en.htm> accessed 15 September 2016

EY, 'The heightened threat of cyber attacks is fueling payment losses - how should your business respond? April 2018, 1-4 <https://www.ey.com/Publication/vwLUAssets/EY-convergence-of-payments-and-cybersecurity/$File/EY-convergence-of-payments-and-cybersecurity.pdf> accessed 10 July 2019

Facciolo, F. J., 'Unauthorized Payment Transactions and Who Should Bear the Losses' (2008) *Chicago-Kent Law Review* 83(2), 605-631

Farah, Y, 'Allocation of jurisdiction and the internet in EU law' (2008) *European Law Review* 33(2), 257-270

Faure, M. G., and Luth, H. A., 'Behavioural Economics in Unfair Contract Terms' (2011) *Journal of Consumer Policy* 34, 337-358

Feng, Y., et al, 'Price Competition in an Oligopoly Market with Multiple IaaS Cloud Providers' (2014) *IEEE Transactions on Computers* 63(1), 59-73

Financial Conduct Authority, Consultation Paper, A new regulatory framework for payment systems in the UK PSR CP14/1, November 2014, 1-111 <http://www.fca.org.uk/static/documents/psr/psr-cp14-1-cp-a-new-regulatory-framework-for-payment-systems-in-the-uk.pdf> accessed 17 May 2015

Financial Stability Board, Consumer Finance Protection with particular focus on credit, 26 October 2011, 1-53

Flaming, M., et al, 'Agent Management Toolkit, Building a Viable Network of Branchless Banking Agents, Technical Guide' (2011) Consultative Group to Assist the Poor (CGAP)/The World Bank, 1-171 <http://www.cgap.org/sites/default/files/CGAP-Technical-Guide-Agent-Management-Toolkit-Building-a-Viable-Network-of-Branchless-Banking-Agents-Feb-2011.pdf> accessed 1 September 2016

Foster, N.H.D., 'Islamic Commercial Law: An Overview (II)' (2007) *InDret: revista per a analisi del dret* 1, 405-425

Frankenberg, G., 'Critical Compromises: Rethinking Comparative Law' (1985) *Harvard International Law Journal* 26(2), 411-456

Gait, A.H., Worthington, A.C., 'A Primer on Islamic Finance: Definitions, Sources, Principles and Methods' University of Wollongong, School of Accounting and Finance, Working Paper Series, No. 07/05, 1-27

Gawas, V.M., 'Doctrinal legal research method a guiding principle in reforming the law and legal system towards the research development' (2017) *International Journal of Law* 3(5), 128-130

Geva, B., 'Consumer Liability in Unauthorised Electronic Funds Transfers' (2003) *Canadian Business Law Journal*, 207-281

Gidlöf, K., Wallin, A., and Holmqvist, K., and Møgelvang-Hansen, P., 'Material Distortion of Economic Behaviour and Everyday Decision Quality' (2013) *Journal of Consumer Policy* 36, 389-402

Gross, D.B. and Souleles, N.S., 'Do Liquidity Constraints and Interest Rates Matter for Consumer Behavior? Evidence from Credit Card Data' (2002) *Quarterly Journal of Economics* 117(1), 149-185

GSMA, 'Safeguarding Mobile Money: How providers and regulators can ensure that customer funds are protected', January 2-16, 1-31 <http://www.gsma.com/mobilefordevelopment/wp-content/uploads/2016/01/2016_GSMA_Safeguarding-Mobile-Money_How-providers-and-regulators-can-ensure-that-customer-funds-are-protected.pdf> accessed 10 November 2016

Habib, R.A.K., 'Consumer Policy in Less Developed Countries: A Saudi Arabian Context', PhD Thesis, University of Glasgow, 1988

Hache, A.C.B., and Ryder, N., 'Tis the season to (be jolly?) wise-up to online fraudsters. Criminals on the Web lurking to scam shoppers this Christmas: A critical analysis of the United Kingdom's legislative provisions and policies to tackle online fraud' (2011) *Information & Communications Technology Law* 20, 35-56

Harvey, J. 'From a risk-based to an uncertainty-based approach to anti-money laundering compliance' (2017) *Security Journal* 30(1), 24-38.

Haselsteiner, E., Breitfuss, K., 'Security in Near Field Communication (NFC), Strengths and Weaknesses', undated, 1-11 <http://ece.wpi.edu/~dchasaki/papers/Security%20in%20NFC.pdf> accessed 27 December 2013

Helveston, M.N., 'Consumer Protection in the Age of Big Data' (2016) *Washington University Law Review* 93(4), 859-917

Hinds, D., 'Micropayments: A technology with a promising but uncertain future' in (eds) N. Mallat, M. Rossi and V.K. Tuunainen, 'Mobile Banking Services' (2004) *Communications of the ACM* 47(5), 42–46

HM Treasury, 'Laying of regulations to implement the new E-Money Directive, a consultation document.' October 2010, 1-112 <https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/81328/emoney_directive_consultation.pdf> accessed 10 September 2016

Hnaif, A., Alia, M.A., 'Mobile Payment Method Based on Public-Key Cryptography' (2015) *International Journal of Computer Networks and Communications Security* 7(2), 81-92

Hodgson, G.M., 'On the Limits of Rational Choice Theory' (2012) *Economic Thought* 1, 94-108

Hoofnagle, C. J., Urban, J.M., Li, S., 'Mobile Payments: Consumer Benefits & New Privacy Concerns' (2012) University of California, 1-19 <https://ssrn.com/abstract=2045580> accessed 5 March 2019

Horvath, A.S., Agrawal, R., 'Trust in cloud computing', *South East Conference*, 9-12 April 2015, 1-8

Husa, J., 'Farewell to Functionalism or Methodological Tolerance?' (2009) University of Helsinki, 1-25 <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1488669> accessed 10 February 2019

Hussain, M.S., 'The Reasonableness of the UCTA 1977's Test of Reasonableness' (2017) *SSRN Electronic Journal*, 1-4 <10.2139/ssrn.3058489> accessed 1 March 2019

Hutchinson, T., 'Valé Bunny Watson? Law Librarians, Law Libraries and Legal Research in the Post-Internet Era' (2014) *Law Library Journal* 106(4), 579-592

Incardona, R. and Poncibo, C., 'The Average Consumer, The Unfair Commercial Practices Directive, and the Cognitive Revolution' (2007) *Journal of Consumer Policy Issue* 30(1), 21-38

Information Commissioner's Office, 'Information Commissioner's Annual Report and Financial Statements 2011/12, in the Rights space- at the right time', 2012, 1-84 <https://ico.org.uk/media/about-the-ico/documents/1042187/annual_report_2012.pdf> accessed 29 March 2013

Information Commissioner's Office, 'Overview of the General Data Protection Regulation (GDPR).' 2016, 1-40 <https://ico.org.uk/media/for-organisations/data-protection-reform/overview-of-the-gdpr-1-0.pdf> accessed 15 September 2016

Information Commissioner's Office, Annual Report 2006/2007, Information Guidance, 2007, 1-96 <https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/231262/0646.pdf > accessed 29 March 2013

Innovation Edge, 'Mobile Banking', April 2012, 1-3

International Financial Consumer Protection Organisation, 'Online and mobile payments, An overview of supervisory practices to mitigate security risks', January 2018, 1-79 <http://www.finconet.org/FinCoNet_SC3_Report_Online_Mobile_Payments_Supervisory_Practices_Security_Risks.pdf> accessed 6 July 2019

Jansen, J., and Leukfeldt, R., 'Phishing and Malware Attacks on Online Banking Customers in the Netherlands: A Qualitative Analysis of Factors Leading to Victimization' (2016) *International Journal of Cyber Criminology* 10(1), 79–91

Jones, R., 'Regulator warns of dangers of mobile banking', The Guardian, 27 August 2013 <https://www.theguardian.com/money/2013/aug/27/dangers-mobile-banking-regulator> accessed 1 September 2016

Kaikkonen, A., Roto, V., 'Navigating in a mobile XHTML application' (2003) *Proceeding CHI '03 Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, 329-336

Karl, D.J., 'Islamic Law in Saudi Arabia: What Foreign Attorneys Should Know' (1991) *The George Washington Journal of International Law and Economics* 25(1), 131-170

Kashyap, A.K., Rajan, R. and Stein, J.C., 'Banks as liquidity providers: An explanation for the coexistence of lending and deposit-taking'(2002) *The Journal of Finance* 57(1), 33-73

Kelly, A.M., and Beaumont, A., 'Freedom After Neoliberalism' (2018) *Open Library of Humanities*, 1-26

Kessler, F., 'The Protection of the Consumer under Modern Sales Law, Part 1, A Comparative Study' (1964-1965) *Yale Law Journal* 74, 262-285

Khan, M.A., 'The Role of Islamic State in Consumer Protection' (2011) *Pakistan Journal of Islamic Research* 8, 31-44

Khan, M.A., 'Consumer Protection in Islamic Law (Shariah): An Overview' (undated) 45(31), 77-100 <http://pu.edu.pk/images/journal/szic/PDF/English/6-%20Muhammad%20Akbar%20Khan%20Final%20Draft%20of%20Research%20Paper.pdf> accessed 10 February 2019

Khiaonarong, T., 'Oversight Issues in Mobile Payments', *IMF Working Papers 14/123*, 2014, 1-35

Kurtz, C., Wittner, F., Semmann, M., Schulz, W., Böhmann, T., 'The Unlikely Siblings in the GDPR Family: A Techno-Legal Analysis of Major Platforms in the Diffusion of Personal Data in Service Ecosystems' (2019) *Proceedings of the 52nd Hawaii International Conference on System Sciences*, 5059-5068

Lake, A. J., 'Risk management in Mobile Money: Observed Risks and Proposed Mitigants for Mobile Money Operators', International Finance Corporation/World Bank Group, November 2013, 1-22

Latin, H., '"Good" Warnings, Bad Products and Cognitive Limitations' (1994) *University of California Law Review* 41, 1193-1295

Lauer, K., et al, 'Bank Agents: Risk Management, Mitigation, and Supervision' (2011) *CGAP Focus Note* 75, 1-24

Le, T.M., and Liaw, S.-Y., 'Effects of Pros and Cons of Applying Big Data Analytics to Consumers' Responses in an E-Commerce Context' (2017) *Sustainability* 9, 1-19

Legrand, P., 'The Impossibility of 'Legal Transplants' (1997) *Maastricht Journal of European and Comparative Law* 4(2), 111-124

Lelieveldt, S., 'Which future for electronic money in Europe, Lelieveldt Consultancy, 2015, 1-4

Lending Standards Board, 'The Standards of Lending Practice, Personal Customers, July 2016, 1-12 <https://www.lendingstandardsboard.org.uk/wp-content/uploads/2016/07/Standards-of-Lending-Practice-July-16.pdf> accessed 10 November 2016

Lim, C.J.F., Koh, B., Lee, D., 'Exploring Mobile Peer-to-Peer Payment Adoption: The Effects of SNS and Native Mobile Banking Apps Usage' (2018) *PACIS 2018 Proceedings*, 109-118

Liu, J., Kaufman, R. J., Ma, D., 'Assessing the Opportunities and Challenges with Big Data in the Mobile Payments Ecosystem' (2015). Workshop on Internet and Big Data Finance 2015. Research Collection School of Information Systems, 1-7

<http://ink.library.smu.edu.sg/cgi/viewcontent.cgi?article=3944&context=sis_research> accessed 1 November 2016

Lu, L., 'Decoding Alipay: mobile payments, a cashless society and regulatory challenges' (2018) *Butterworths Journal of International Banking and Financial Law*, 40-43

Lukonga, I., 'Fintech, Inclusive Growth and Cyber Risks: Focus on the MENAP and CCA Regions', IMF Working Paper, WP/18/201, 2018

Luminzu Mudiri, J., 'Fraud in Mobile Financial Services', MicroSave, 2014, 1-48 <http://www.microsave.net/files/pdf/RP151_Fraud_in_Mobile_Financial_Services_JMudiri.pdf> accessed 1 September 2016

Macdonald, E., 'Unifying Unfair Terms Legislation' (2004) *The Modern Law Review* 67(1), 69-93

Malik, M.S., and Mustafa, W., 'Controversies that make Islamic banking controversial: An analysis of issues and challenges' (2011) *American Journal of Social and Management Issues* 2(1), 41-46

Malisa, L., et al, 'Detecting Mobile Application Spoofing Attacks by Leveraging User Visual Similarity Perception' (2015) *International Association for Cryptologic Research*, 1-17 <https://eprint.iacr.org/2015/709.pdf> accessed 1 September 2016

Mallat, C., 'Commercial Law in the Middle East: Between Classical Transactions and Modern Business' (2000) *American Journal of Comparative Law* 48(1), 81-141

Mancuso, S., 'Consumer Protection in E-Commerce Transactions: A First Comparison between European Law and Islamic Law' (2007) *Journal of International Commercial Law and Technology* 2(1), 1-8

Mann, R. J., 'Contracting' for Credit' (2006) *Michigan Law Review* 104, 899-932

Mann, R. J., 'Making Sense of Payments Policy in the Information Age' (2005) *Georgetown Law Journal* 93, 633-673

Masters, B. and Moore, E. 'E-money' challenge for high street banks', The Financial Times, 14 April 2013 <https://www.ft.com/content/88d9b378-a1fa-11e2-ad0c-00144feabdc0> accessed 13 December 2017

McIlraith, G., 'How to Ensure Mobile Banking App Security', BankTech, 2013 <http://www.banktech.com/risk-management/how-to-ensure-mobile-banking-app-securit/240163093> accessed 28 October 2013

McKinsey&Company, 'McKinsey on Payments', Number 16, March 2013, 1-46

McMillen, M.J.T., 'Islamic Law Forum' (2008) *International Law* 42, 1017-1032
Micklitz, H.-W., 'Social Justice and Access Justice in Private Law', *EUI Working Papers Law* 2011/02, 1-44

Mirjanich, N., 'Digital Money: Bitcoin's Financial and Tax Future Despite Regulatory Uncertainty' (2014) *De Paul Law Review*, 64(1), 213-248

Mobile Financial Services Working Group, 'Mobile Financial Services, Consumer Protection in Mobile Financial Services' (2014) Guideline Note No.13, 1-15 <http://www.afi-global.org/sites/default/files/publications/mfswg_guideline_note_7_consumer_protection_in_mfs.pdf> accessed 1 September 2016

Morris, D., and Al Dabbagh, M., 'The development of consumer protection in Saudi Arabia' (2004) *International Journal of Consumer Studies* 28(1), 2-13

Mukhopadhyay, R., Nath, A., 'Ethical Hacking: Scope and challenges in 21st Century' (2014) *International Journal of Innovative Research in Advanced Engineering* 1(1), 30-37

Myers, M.L., 'Adam Smith's Concept of Equilibrium' (1976) *Journal of Economic Issues* 10(3) 560-575

Nath, K., Dhar, S., Basishtha, S., 'Web 1.0 to Web 3.0 - Evolution of the Web and its various challenges' (2014) *ICROIT 2014 - Proceedings of the 2014 International Conference on Reliability, Optimization and Information Technology*, 86-89

Newcomb Hohfeld, W., 'Some Fundamental Legal Conceptions as Applied in Judicial Reasoning' (1913) *Yale Law Journal* 23(1), 16-59

Pandy, S., Crowe, M., 'What's New with Regulation in the Mobile Payment and Fintech Space?' Federal Reserve Bank of Boston, MPIW Meeting with Regulators Report, 25 May 2017, 1-7 <http://www.asbasupervision.com/es/bibl/x-lecturas-recomendadas/1507-lr229/file> accessed 2 September 2017

Paterson, J. M., and Brody, 'G., "Safety Net" Consumer Protection: Using Prohibitions on Unfair and Unconscionable Conduct to Respond to Predatory Business Models' (2015) *Journal of Consumer Policy* 38, 331-355

Payments UK, 'The Second Payment Services Directive (PSD2)', July 2016, 1-20 <http://www.paymentsuk.org.uk/sites/default/files/PSD2%20report%20June%202016.pdf> accessed 10 September 2016

Peng, S., et al, 'Smartphone Malware and Its Propagation Modeling: A Survey' (2013) *IEEE Communications Surveys & Tutorials* 16(2), 925-941

Polat, A., Alsaif, A. A., 'Consumer Protection in Banking: Investigating the 10 High Level Principles of G20 in Saudi Arabia' (2014) *Journal of Applied Finance & Banking* 4(3), 195-215

Polk, D., 'Lex et Brexit - The Law and Brexit', Wardwell LLP, 9 July 2016, 1-7

Poncibò, C., 'Networks to Enforce European Law: The Case of the Consumer Protection Cooperation Network' (2012) *Journal of Consumer Policy* 35, 175-195

Pousttchi, K., and Hufenbach, Y., ‘Enabling evidence-based retail marketing with the use of payment data - the Mobile Payment Reference Model 2.0’ (2013) *International Journal of Business Intelligence and Data Mining* 8, 19-44

Posner, R. A., 'Rational choice, behavioural economics, and the law' (1998) *Stanford Law Review* 50, 1551–1575

PWC, 'Financial Services Technology 2020 and Beyond: Embracing disruption', 2016, 1-48 <https://www.pwc.com/gx/en/financial-services/assets/pdf/technology2020-and-beyond.pdf> accessed 29 April 2019

Qasim, H., Abu-Shanab, E., 'Drivers of mobile payment acceptance: The impact of network externalities' (2016) *Information Systems Frontiers* 18(5), 1021-1034

Ramsay, I., '"A very intrusive proposition"? - the long and winding road to payday loan price controls', Credit Debt and Insolvency, October 2013 <https://creditdebtandinsolvency.wordpress.com/2014/07/22/a-very-intrusive-proposition-the-long-and-winding-road-to-payday-loan-price-controls/> accessed 1 July 2017

Ramsay, I., 'Consumer credit regulation after the fall: international dimensions' (2012) *Zeitschrift für Europäisches Unternehmens- und Verbraucherrecht Journal of European Consumer and Market Law* 1, 24–34

Ramsay, I., 'Consumer Law, Regulatory Capitalism and the 'New Learning' in Regulation' (2006) *Sydney Law Review* 28, 9-35

Ramsay, I., 'Regulation and the Constitution of the EU Single Market: The Contribution of Consumer Law' (2011) *Canadian Business Law Journal* 50, 322-355

Ramsay, I., 'To Heap Distress Upon Distress?' Comparative Reflections on Interest-Rate Ceilings' (2010) *University of Toronto Law Journal* 60, 707-730

Rhoen, M., 'Beyond consent: improving data protection through consumer protection law' (2016) *Internet Policy Review* 5(1) <https://policyreview.info/articles/analysis/beyond-consent-improving-data-protection-through-consumer-protection-law> accessed 15 April 2019

Rhoen, M., ‘Big Data and Consumer Participation in Privacy Contracts: Deciding who Decides on Privacy’ (2015) *Utrecht Journal of International and European Law* 31(80), 51–71

Rice, G., 'Islamic ethics and the implications for business' (1999) *Journal of Business Ethics* 18, 345-358

Rosenberg, A., ‘Better than cash? Global proliferation of payment cards and consumer protection policy’ (2006) *Columbia Journal of Transnational Law* 44, 520-578

Saha, A., Sanyal, S., ‘Review of Considerations for Mobile Device based Secure Access to Financial Services and Risk Handling Strategy for CIOs, CISOs and CTOs’ (2015) *International Journal of Advanced Networking and Applications* 6(4), 2427-2434

Saudi Arabian Monetary Agency, ‘A Report on Initiatives and Actions Taken by Saudi Arabia to Combat Terrorist Financing and Money Laundering’, April 2004, 1-22 <http://www.saudiembassy.net/files/PDF/SAMA_INITIATIVES_BY_KSA_UP_DATED_APRIL_2004.pdf> accessed 1 May 2015

Saudi Credit Bureau, ‘Horizons in Credit, Credit in Saudi Arabia’, 2013, 1-9 <http://www.simah.com/Documents/PDF/Booklet9A.pdf> accessed 22 October 2014

Saudi Investment Bank, ‘easypay, Your pay...your way’, 2012, 1-10 <https://www.saib.com.sa/sites/default/files/easypay-Brochure-English.pdf> accessed 28 October 2014

Shaikh, A.A., and Karjaluoto, H., ‘Mobile banking adoption: A literature review’ (2015) *Telematics and Informatics* 32 (1), 129-142

Sheftali, J., et al, 'Bank Litigation Liabilities', Guildhall Chambers, 2010, 1-8 http://www.guildhallchambers.co.uk/files/BankLitigationLiabilities_NeilLevy_LucyWalker_JackieSheftali_MatthewArnold&BaldwinLLP_October_2010.pdf> accessed 10 November 2016

Singh Grewal, D., and Purdy, J., 'Introduction: Law and Neoliberalism' (2015) *Law and Contemporary Problems*, 1-23 <https://scholarship.law.duke.edu/lcp/vol77/iss4/1/> accessed 15 April 2019

Smart Card Alliance, 'Security of Proximity Mobile Payments', A Smart Card Alliance Contactless and Mobile Payments Council White Paper, May 2009, 1-39 <http://www.smartcardalliance.org/resources/pdf/Security_of_Proximity_Mobile_Payments.pdf> accessed 1 November 2016

Smith, P., ‘Comparisons between Low Power Wireless Technologies, Bluetooth low energy, ANT, ANT+, RF4CE, ZigBee, Wi-fi, Nike+, IrDA and NFC, CSR Whitepaper’ (2013), 1-29 <http://www.csr.com/sites/default/files/white-papers/comparisons_between_low_power_wireless_technologies.pdf> accessed 29 December 2013

Soederberg, S., 'The US Debtfare State and the Credit Card Industry: Forging Spaces of Dispossession' (2013) *Antipode* 45(2), 493-512

Solin, M., Zerzan, A., 'Mobile Money: Methodology for Assessing Money Laundering and Terrorist Financing Risks' (2010) GSMA Discussion Paper, 1-35 <http://www.gsma.com/mobilefordevelopment/wp-content/uploads/2012/03/amlfinal35.pdf> accessed 1 September 2016

Sonne, P., ‘Data-Security Expert Kaspersky: There Is No More Privacy’, *The Wall Street Journal*, 3 September 2013 <http://www.wsj.com/articles/SB10001424127887324432404579053091175949708> accessed 1 September 2016

Sophos, ‘Security Threat Report 2012, Seeing the Threats Through the Hype’, 2012, 11-31 <http://www.sophos.com/medialibrary/PDFs/other/SophosSecurityThreatReport2012.pdf> accessed 1 September 2017

SPD Bank, 'NFC and Mobile Bank 2.0', GSMA (2013), 1-20 <http://www.gsma.com/mobilecommerce/wp-content/uploads/2013/07/3.-XUE-JIANHUA-Pudong-Dev-Bank.pdf> accessed 29 October 2013

Stapleton, J., Poore, R. S., 'Tokenization and Other Methods of Security for Cardholder Data' (2011), 20(2) *Information Security Journal: A Global Perspective*, 91-99

State of New Hampshire Department of Information Technology (2012), 7(1) *Monthly Security Tips Newsletter*, 1-2 <http://www.nh.gov/doit/cybersecurity/resources/documents/nl1201-emerging-trends.pdf> accessed 27 December 2013

Sumkovski, I., 'The Optimal level of Anti-Money Laundering Regulation for the UK Banking Sector. Banks' Cost of Compliance, De-risking Problem and How to Implement Effective AML Systems and Controls' (2016/2017) Institute of Advanced Legal Studies, 1-54 <https://sas-space.sas.ac.uk/6873/1/Final%20Dissertation_LLM%20ICGFREL_Igor%20Sumkovski_1544977.pdf> accessed 20 April 2019

Survey of National Progress in the Implementation of G20/FSB Recommendations, Saudi Arabia, 1-44 <http://www.financialstabilityboard.org/implementation_monitoring/saudi_arabia_2013.pdf> accessed 20 October 2014

Swanney, D., 'Prevention of money laundering/combating terrorist financing, 2017 Consultation Version, Guidance for the UK Financial Sector, Part III: Specialist Guidance', The Joint Money Laundering Steering Group, May 2017, 1-49

Tabakovic, A., 'The prepaid mobile wallet: A powerful product for an impatient ecosystem' (2014) *Journal of Payments Strategy & Systems* 8(3), 254-263

Tahir, S., 'Current Issues in the Practice of Islamic Banking, International Institute of Islamic Economics of the International Islamic University', Islamabad, 2003, 1-8 <http://www.sbp.org.pk/departments/ibd/Lecture_8_Related_Reading_1.pdf> accessed 5 October 2014

Tata Consultancy Services Ltd, 'Big Data in Payments - Unparalleled Opportunity for Strategic Excellence.' White Paper, 2013, 1-6 <http://www.tcs.com/SiteCollectionDocuments/White%20Papers/Big-Data-Payments-0713-1.pdf> accessed 15 September 2016

Taylor, E., 'Mobile payment technologies in retail: a review of potential benefits and risks' (2016) *International Journal of Retail and Distribution Management*, 44(2), 159-177

Taylor, M. J., 'Data Protection: Too Personal to protect?' (2006) *Scripted* 3(1), 72-81 <http://www.law.ed.ac.uk/ahrc/script-ed/vol3-1/taylor.pdf> accessed 28 May 2013

Tiwari, A., Sanyal, S., Abraham, A., Knapskog, S. J., Sanyal, S., 'A Multi-Factor Security Protocol for Wireless Payment - Secure Web Authentication Using Mobile Devices' (2011) *IADIS International Conference, Applied Computing* 2007, Salamanca, Spain, 160-167

Trzaskowski, J., 'Behavioural Economics, Neuroscience, and the Unfair Commercial Practises Directive' (2011) *Journal of Consumer Policy* 34, 377-392

Valant, J., 'Consumer protection in the EU, Policy overview', *European Parliamentary Research Service*, September 2015, 1-24

Van Alsenoy, B., Verdoodt, V., Heymany, R., Ausloos, J., 'From social media service to advertising network, A critical analysis of Facebook's Revised Policies and Terms', 23 February 2015, 1-61 <https://www.law.kuleuven.be/citip/en/news/item/facebooks-revised-policies-and-terms-v1-1.pdf> accessed 10 March 2019

Van Boom, W.H., 'Price Intransparency, Consumer Decision Making and European Consumer Law' (2011) *Journal of Consumer Policy* 34, 359-376

Volmar, M. N., and Helmdach, K. I., 'Protecting consumers and their data through competition law? Rethinking abuse of dominance in light of the Federal Cartel Office's Facebook investigation' (2018) *European Competition Journal*14(2-3), 195-215

Walter, I., 'Conflicts of interest and market discipline among financial service firms' (2004) *European Management Journal* 22(4), 361-376.

Warren, E., 'Unsafe at Any Rate' (2007) *Democracy Journal* 5, 1-15

Watson, A., 'Legal Transplants and Law Reform' (1976) *Law Quarterly Review* 92, 79-84

Weber, R.H., Darbellay, A., 'Legal Issues in Mobile Banking' (2010) *Journal of Banking Regulation* 11, 129-145

Whitman, J.Q., 'Consumerism Versus Producerism: A Study in Comparative Law' (2007) *The Yale Law Journal* 117, 340-406

Wilhelmsson, T., 'Various Approaches to Unfair Terms and Their Background Philosophies' (2008) *Juridica International* XIV, 51-57

Williams, T., 'Empowerment of Whom and for What? Financial Literacy Education and the New Regulation of Consumer Financial Services' (2007) *Law & Policy* 29(2), 226-256

Winn, J., and Jondet, N., 'A "New Approach" to Standards and Consumer Protection' (2008), *Journal of Consumer Policy*, 31, 459-472

Xu, J., *Digital Payment Systems, Managing Digital Enterprise* 2014, 159-175

Zahid, A., Shapiee, R., Sohaib Mukhtar, S., Syed Munawar Shah, S. M., 'Good faith in international commercial contracts under un sale convention and Islamic law: A brief comparison' (2016) *International Journal of Applied Business and Economic Research* 14(13), 9075-9183

Webpages

Al Ahlie, 2014 <http://www.alahli.com/en-us/Documents/Financial_Rights_of_Bank_Customers_EN.pdf> 24 September 2014

Al Arabiya, 'Saudi Arabia leader nation in e-readiness: U.N. report', 3 August 2012 <http://english.alarabiya.net/articles/2012/08/03/230116.html> accessed 24 October 2014

Allen, K., 'UK finance industry dominates European scene', Financial Times, 5 September 2018 <https://www.ft.com/content/88cdec40-b03c-11e8-8d14-6f049d06439c> accessed 10 February 2019.

Alpari, 'Mobile trading', 2013 <http://www.alpari.co.uk/trading-platforms/mobile-trading> accessed 29 October 2013

Apple UK, 'Find it all in Wallet.' 2017 <https://www.apple.com/uk/apple-pay/> accessed 23rd November 2017

Arab Advisors Group, 'Remote banking services adoption in Saudi Arabia', 30 May 2012 <http://www.arabadvisors.com/Pressers/presser-300512.htm> accessed 19 October 2014

Arab News, 'Saudi Arabia has almost double international rate of smartphones', 20 December 2017 <http://www.arabnews.com/node/1211721/saudi-arabia> accessed 10 February 2019

Asimakopoulos, P., 'Report: the size, depth & growth opportunity in UK capital markets', New Financial, May 2018 <https://newfinancial.org/report-the-size-depth-growth-opportunity-in-uk-capital-markets/> accessed 5 July 2019

Attard, A., 'A Novel Card-Present Payment Scheme using NFC Technology', Royall Holloway, University of London, 2010-2011, 1-98 <http://www.ma.rhul.ac.uk/static/techrep/2012/MA-2012-07.pdf> accessed 27 December 2013

Bachelor, L., 'Contactless card fraud is too easy, says Which?' Guardian, 23 July 2015 <http://www.theguardian.com/money/2015/jul/23/contactless-card-is-too-easy-says-which> accessed 17 July 2015

Barclays, 'Barclays Mobile Banking app', 2013 <http://www.barclays.co.uk/BarclaysMobileBanking/BarclaysMobileBankingapp/P1242609123821> accessed 28 October 2013

Barclays, 'Pingit terms and conditions', 2016 <http://www.barclays.co.uk/Mobile/BarclaysPingittermsandconditions/P1242604890843> accessed 10 September 2016

BBC, UK financial regulation overhauled, 2013 <http://www.bbc.co.uk/news/business-21987829> accessed 27 May 2013

BBCA, 'How does PSD2 affect bank customers' digital identity?', BBVAOpen 4U, 1 August 2016 <https://bbvaopen4u.com/en/actualidad/how-does-psd2-affect-bank-customers-digital-identity> accessed 1 November 2016

BBVA, 'Mobile Banking, New Experience in the Post PC Era', Innovation Edge, April 2012, 1-67

BBVA, 'Mobile Payments, Paying with a mobile device', Innovation Edge, November 2012

Benyon, D., ‘Banks fear in increase in financial crime’, Risk.Net, 2008 <http://www.risk.net/operational-risk-and-regulation/news/1499571/banks-fear-increase-financial-crime> accessed 28 October 2013

Boden, R., 'Barclays and Starbucks promote contactless in UK', NFC World, 18 June 2015 <https://www.nfcworld.com/2015/06/18/336077/barclays-and-starbucks-promote-contactless-in-uk/> accessed 1 March 2019

Boden, A., 'Explaining PSD2 without TLAs is tough!' Starling Bank, 9 October 2015 <https://www.starlingbank.com/explaining-psd2-without-tlas-tough/> accessed 10 September 2016

Borison, R., ‘PayPal challenges NFC with bluetooth-enabled mobile payments’, Mobile Commerce Daily, 2013 <http://www.mobilecommercedaily.com/paypal-gives-nfc-a-run-for-its-money-with-new-bluetooth-mcommerce-option> accessed 30 December 2013

Brignall, M., 'Barclays launches Pingit money-sending service for smartphones', The Guardian, 16 February 2012 <https://www.theguardian.com/money/2012/feb/16/barclays-pingit-money-sending-smartphone> accessed 1 November 2016

Cabrai, A. R., 'ApplePay launches in UAE and 3 other countries today', Khaleej Times, 24 October 2017 <https://www.khaleejtimes.com/technology/apple-pay-is-now-in-the-uae> accessed 16 November 2017

Campbell, F., 'Contactless payments continue to grow in the UK', Mobile Transaction, 2 January 2019 <https://www.mobiletransaction.org/contactless-payments-uk/> accessed 1 March 2019

Chesworth, N., ‘Be smart, stay safe: security and mobile banking’, The Telegraph, 2013 <http://www.telegraph.co.uk/sponsored/finance/natwest-mobile-banking/10292506/smartphone-security-mobile-banking.html> accessed 28 October 2013

Chin, J., 'Bank Negara plans minimum standards for mobile payments, more safeguards', The StarOnline, 12 April 2018 <https://www.thestar.com.my/business/business-news/2018/04/12/bank-negara-plans-minimum-standards-mobile-payments-more-safeguards/> accessed 13 February 2019

Claus, K.-C., 'How convergence is transforming payment services', Ernst & Young, 24 May 2018 <https://www.ey.com/en_gl/digital/how-convergence-is-transforming-payment-services> accessed 13 February 2019

Cliffe, M., 'Mobile Banking 2.0: Six Ways The Experience Must Evolve', The Financial Brand, 9 February 2016 <https://thefinancialbrand.com/57103/mobile-banking-experience-innovation/> accessed 1 November 2016

Collinson, P., ‘Don't bank on your phone - it could be hacked by Zeus 'trojan horse'’, The Guardian, 2011 <http://www.theguardian.com/money/2011/jul/22/smartphones-hacked-zeus-malware> accessed 28 October 2013

Communications Act 2003, Explanatory Notes <http://www.legislation.gov.uk/ukpga/2003/21/notes/division/2> accessed 10 November 2016

Daily Record, ‘HMV customers furious as collapsed music chain refuse to honour vouchers and gift cards’, 2013 <http://www.dailyrecord.co.uk/news/uk-world-news/hmv-cutomers-angry-as-music-chain-1535990> accessed 28 May 2013

Deloitte, ‘HMV Administration-FAQ’, 2013 <http://www.deloitte.com/view/en_GB/uk/services/corporate-finance/restructuring-services/updates-for-insolvencies/hmv/4d244ad0cd24c310VgnVCM2000003356f70aRCRD.htm> accessed 2 April 2013

Discover Digital Arabia, 2013 <http://www.ddarabia.com/statistics/> accessed 18 October 2014

DLA Piper, Data Protection Laws of the World, Saudi Arabia, 2019 <https://www.dlapiperdataprotection.com/index.html?t=law&c=SA> accessed 25 April 2019

DM Wallet Summit, ‘Digital Wallet Opportunity’, 2013 <http://www.dmwsummit.com/digital-wallet-opportunity/> accessed 13 October 2013

Donnelly, B., and Pratt, J., ‘Mis-selling claims: Court of Appeal Guidance’, Macfarlanes, 2010 <http://www.inhouselawyer.co.uk/index.php/litigation-a-dispute-resolution/8274-mis-selling-claimscourt-of-appeal-guidance> accessed 28 May 2013

Dorfman, R.S., 'The Regulation of Fairness and Duty of Good Faith in English Contract Law: A Relational Contract Theory Assessment', The New Jurist, 13 October 2015 <http://newjurist.com/fairness-in-english-contract-law.html> accessed 7 July 2019

Dunkley, E., 'UK banks seek to Zapp Apple with digital payment services', Financial Times, 7 July 2015 <https://www.ft.com/content/4bc7b682-23e0-11e5-9c4e-a775d2b173ca> accessed 10 November 2016

Elias, A.A., 'Sharia, Fiqh, and Islamic Law explained', 18 April 2013 <https://abuaminaelias.com/is-the-sharia-a-single-code-of-law-an-explanation-of-sharia-fiqh-and-islamic-law/> accessed 19 November 2017

Epstein, S., 'Is the fintech industry killing mobile payments?' Finextra, 16 August 2016 <https://www.finextra.com/blogposting/12976/is-the-fintech-industry-killing-mobile-payments> accessed 1 September 2017

Epstein, Z., 'Major security holes found in 90% of top mobile banking apps’, BGR, 14 January 2014 <http://bgr.com/2014/01/14/mobile-banking-apps-security-vulnerabilities/> accessed 1 September 2016

ETSI, 'Certification Authorities and other Trust Service Providers', 2016 <http://www.etsi.org/technologies-clusters/technologies/security/certification-authorities-and-other-trust-service-providers> accessed 1 November 2016

Eur-Lex, 'Access to electronic communications networks', 10 September 2015 <http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=URISERV%3Al24108i> accessed 10 November 2016

Euromonitor International, 'Pre-Paid Cards in Saudi Arabia, Market Research', 22 August 2013 <http://www.marketresearch.com/Euromonitor-International-v746/Pre-Paid-Cards-Saudi-Arabia-7583184/> accessed 25 October 2014

European Banking Authority, 'Consultation on the Guidelines on the criteria on how to stipulate the minimum monetary amount of the professional indemnity insurance under PSD2', 22 September 2009 <https://www.eba.europa.eu/news-press/calendar?p_p_id=8&_8_struts_action=%2Fcalendar%2Fview_event&_8_eventId=1586016> accessed 10 September 2016

European Banking Authority, 'EBA seeks input on strong customer authentication and secure communication under PSD2', 8 December 2015 <https://www.eba.europa.eu/-/eba-seeks-input-on-strong-customer-authentication-and-secure-communication-under-psd2> accessed 10 September 2016

European Commission, 'E-money', 2013 <http://ec.europa.eu/internal_market/payments/emoney/> accessed 28 May 2013

European Payment Institutions Federation, 'What is a Payment Institution?', 2019 <https://paymentinstitutions.eu/the-payment-institutions-sector/about/> accessed 1 March 2019

European Travel Commission Digital Portal, 'Mobile/Smartphones, Rise of Mobile Internet Use in Middle East Region', 2014 <http://etc-digital.org/digital-trends/mobile-devices/mobile-smartphones/regional-overview/middle-east/> accessed 18 October 2014

Financial Action Task Force, 'Mutual Evaluation of the Kingdom of Saudi Arabia', 1 February 2012 <http://www.fatf-gafi.org/countries/s-t/saudiarabia/documents/mutualevaluationofthekingdomofsaudiarabia.html> accessed 2 May 2015

Financial Action Task Force, 'Guidance for a Risk-Based Approach, Prepaid Cards, Mobile Payments and Internet-Based Payment Services', June 2013 <http://www.fatf-gafi.org/media/fatf/documents/recommendations/Guidance-RBA-NPPS.pdf> accessed 1 November 2016

Financial Conduct Authority, Payment Services Institutions, 2013 <http://www.fca.org.uk/firms/firm-types/payment-services-institutions> accessed 28 May 2013

Financial Ombudsman Service, Compensation, 2013 <http://www.financial-ombudsman.org.uk/publications/technical_notes/compensation.html> accessed 28 May 2013

Financial Services Authority, ‘FSA fines BNPP Private Bank £350,000 for weak anti-fraud controls’, 2007 <http://www.fsa.gov.uk/library/communication/pr/2007/060.shtml> accessed 29 March 2013

Financial Services Authority, ‘FSA fines Nationwide £980,000 for information security lapses’, 2007 <http://www.fsa.gov.uk/library/communication/pr/2007/021.shtml> accessed 29 March 2013

Financial Services Authority, ‘FSA fines Norwich Union Life £1.26m for exposing its customers to the risk of fraud’, 2007 <http://www.fsa.gov.uk/library/communication/pr/2007/130.shtml> accessed 29 March 2013

Financial Services Authority, ‘The FSA's role under the Payment Services Regulations 2009: Our approach’, 2012 <http://www.fca.org.uk/static/fca/documents/fsa-psd-approach-latest.pdf> accessed 28 May 2013

Financial Services Authority, ‘Regulatory Reform- background’, 2013 <http://www.fsa.gov.uk/about/what/reg_reform/background> accessed 1 April 2013

Financial Services Authority, 'Tracked changes version of the FSA's role under the Electronic Money Regulations 2011: Our approach', April 2013 <http://www.fsa.gov.uk/static/pubs/international/draft-approach-emoney.pdf> accessed 1 April 2013

Finextra, 'Virgin Money to launch pre-paid MasterCard', 18 November 2016 <https://www.finextra.com/newsarticle/17133/virgin-money-to-launch-pre-paid-mastercard> accessed 10 November 2016

Fintechnews Middle East, 'A Glimpse into Fintech in Saudi Arabia', 25 March 2019 <https://fintechnews.ae/3734/saudiarabia/fintech-saudi-arabia-overview/> accessed 5 July 2019

Firpo, J., 'E-Money - Mobile Money - Mobile Banking - What's the Difference?', The World Bank, 21 January 2009 <http://blogs.worldbank.org/psd/e-money-mobile-money-mobile-banking-what-s-the-difference> accessed 10 November 2016

FSA Handbook, Electronic Money <http://fsahandbook.info/FSA/html/handbook/ELM/4> accessed 29 March 2013

FSA, Payment Services Regulations, 2013 <http://www.fsa.gov.uk/doing/regulated/banking/psd> accessed 1 April 2013

Glazer, E., Farrell, M., 'Big U.S. Banks Face Increase in Attempted Cyberattacks', 30 September 2018 <https://www.wsj.com/articles/big-u-s-banks-face-increase-in-attempted-cyberattacks-1538317920> accessed 5 March 2019

Gonsalves, A., ‘What Apple's iBeacon rollout doesn't say’, ComputerWorld, 2013 <http://blogs.computerworld.com/mobile-security/23256/what-apples-ibeacon-rollout-doesnt-say> accessed 20 December 2013

Google Pay, 2019 <https://pay.google.com/intl/en_uk/about/> accessed 15 April 2019

Google Play, 'Riyad Mobile', 2017 <https://play.google.com/store/apps/details?id=riyad.bankingapp.android> accessed 1 October 2017

Google Wallet, 'Shop, Save. Pay. With your phone', 2013 <http://www.google.co.uk/wallet/index.html> accessed 29 December 2013

Green, T., 'Zapp and Paym - just what is the difference?' Mobile Money Revolution, 25 March 2014 <http://www.mobilemoneyrevolution.co.uk/zapp-and-paym-just-what-is-the-difference/> accessed 10 November 2016

Groenfeldt, T., 'How London Achieved, And Maintained, Its Leadership In International Finance', Forbes, 2 February 2017 <https://www.forbes.com/sites/tomgroenfeldt/2017/02/02/how-london-achieved-and-maintained-its-leadership-in-international-finance/#30c67b48e86b> accessed 11 February 2019

Hanware, K., 'Saudi Credit Bureau banks on sophisticated mechanisms', Arab News, 20 October 2014 <http://www.arabnews.com/news/646971> accessed 10 May 2015

Hauser, C., 'How Big Data is Transforming Mobile Payments and What This Means for Retailers and Users', Wirecard, 12 November 2015 <https://blog.wirecard.com/how-big-data-is-transforming-mobile-payments-and-what-this-means-for-retailers-and-users/> accessed 1 November 2016

Hinkel, T., 'Banks Beware: Operational Risk Increasing', Bank Systems & Technology, 2012 <http://www.banktech.com/risk-management/banks-beware-operational-risk-increasing/240005678> accessed 28 October 2013

HM Revenue & Customs, 'Financial Services Authority to supervise small electronic money issuers' <http://www.hmrc.gov.uk/mlr/news/supervision-semi-fsa.htm> accessed 25 July 2013

Husain, A., 'Contract in Islamic Commercial and Their Application in Modern Islamic Financial System', Global Islamic Finance, 30 September 2008 <http://www.global-islamic-finance.com/2008/09/contract-in-islamic-commercial-and.html> accessed 23 September 2017

iBeaconInsider, 'What is iBeacon? What are iBeacons?' 2016 <http://www.ibeacon.com/what-is-ibeacon-a-guide-to-beacons/> accessed 10 November 2016

Information Commissioner's Office, 'Security of services', 2016 <https://ico.org.uk/for-organisations/guide-to-pecr/communications-networks-and-services/security-of-services/#securityobligations> accessed 15 September 2016

Islamic Information Center, '15 Prohibitions of Speculation in Islam', 2019 <https://azislam.com/prohibitions-of-speculation-in-islam> accessed 15 March 2019

KPMG, 'UK global leader for fintech investment in H1 2018', 31 July 2018 <https://home.kpmg/uk/en/home/media/press-releases/2018/07/uk-global-leader-for-fintech-investment-in-h1-2018-.html> accessed 10 February 2019

Khandelwal, S., 'New Exploit to 'Hack Android Phones Remotely' threatens Millions of Devices', The Hacker News, 16 March 2016 <http://thehackernews.com/2016/03/exploit-to-hack-android.html> accessed 1 September 2016

Klein, A., 'SIM-ple: Mobile Handsets Are Weak Link in Latest Online Banking Fraud Scheme', Security Intelligence, 13 March 2012 <https://securityintelligence.com/sim-ple-mobile-handsets-are-weak-link-in-latest-online-banking-fraud-scheme/> accessed 1 September 2016

Konolafe, B., 'NDIC issues deposit insurance guidelines for mobile money', Vanguard, 18 January 2016 <http://www.vanguardngr.com/2016/01/ndic-issues-deposit-insurance-guidelines-for-mobile-money/> accessed 10 November 2016

Lambert, R., 'How effective is antivirus software on smartphones?' IT Security, 2012 <http://www.techrepublic.com/blog/it-security/how-effective-is-antivirus-software-on-smartphones/7629/> accessed 28 October 2013

Lanxon, N., 'Facebook to Make Mobile Payments Service Available Outside U.S.', Bloomberg, 6 November 2017 <https://www.bloomberg.com/news/articles/2017-11-06/facebook-to-make-mobile-payments-service-available-outside-u-s> accessed 1 March 2019

Leighton, B., 'NFC mobile payments: overcoming the barriers for banks', Banking Technology, 2013 <http://www.bankingtech.com/151452/nfc-mobile-payments-overcoming-the-barriers-for-banks/> accessed 29 October 2013

Lending Standards Board, 'The Standards of Lending Practice', 2016 <https://www.lendingstandardsboard.org.uk/the-slp/> accessed 10 November 2016

Liard, M., Gupta, R., 'NFC vs Current Mobile Payment Alternatives, Transaction World Magazine', 2013 <http://www.transactionworld.net/articles/2013/may/global-nfc.html> accessed 20 December 2013

Linkous, J., 'Security Audit: The Pitfalls of Third-Party Assessments', RSA Conference, 9 September 2014 <https://www.rsaconference.com/blogs/security-audit-the-pitfalls-of-third-party-assessments> accessed 1 November 2016

Lloyd, N., 'The Wages Protection Program in Saudi Arabia - how will this affect your company', Simmons & Simmons LLP, 4 January 2016 <http://www.elexica.com/en/legal-topics/employment-and-benefits/04-the-wages-protection-system-in-saudi-arabia-how-will-this-affect-your-company> accessed 1 November 2016

Marr, B., 'Chinese Social Credit Score: Utopian Big Data Bliss or Black Mirror on Steroids?' Forbes, 21 January 2019 <https://www.forbes.com/sites/bernardmarr/2019/01/21/chinese-social-credit-score-utopian-big-data-bliss-or-black-mirror-on-steroids/#5962880048b8> accessed 25 April 2019

Marria, V., 'What A Cashless Society Could Mean For The Future', Forbes, 21 December 2018 <https://www.forbes.com/sites/vishalmarria/2018/12/21/what-a-cashless-society-could-mean-for-the-future/#e40fc1332638> accessed 10 February 2019

Martin, J. A., '7 reasons mobile payments still aren't mainstream', CIO Insider, 7 June 2016 <http://www.cio.com/article/3080045/payment-processing/7-reasons-mobile-payments-still-arent-mainstream.html> accessed 10 November 2016

McMillin, D., 'Massive mobile banking growth', Bankrate, year? <http://www.bankrate.com/financing/banking/massive-mobile-banking-growth/> accessed 13 October 2013

Muchmore, M., 'The Best Mobile Payment Apps', PC Mag, 2 April 2018 <https://www.pcmag.com/roundup/358553/the-best-mobile-payment-apps> accessed 20 April 2019

Murphy, C., 'Saudi to codify Sharia 'for clarity', The National, 21 July 2010 <https://www.thenational.ae/world/mena/saudi-to-codify-sharia-for-clarity-1.518063> accessed 10 February 2019

Murrant, S., 'Pingit will be marginalized by Pam, Verdict Financial, 15 May 2014 <http://www.verdictfinancial.com/pingit-will-be-marginalized-by-paym/> accessed 10 November 2016

Naraine, R., 'Exploit beamed via NFC to hack Samsung Galaxy S3 (Android 4.0.4)', Zero Day, 19 September 2012 <http://www.zdnet.com/article/exploit-beamed-via-nfc-to-hack-samsung-galaxy-s3-android-4-0-4/> accessed 1 September 2016

National Commercial Bank, 'Your Financial Rights and Responsibility, Our commitment to the protection of customer interests', 2014 <http://www.alahli.com/en-us/Pages/Consumer-Protection.aspx> accessed 25 October 2014

NatWest, 'NatWest App not Updating Balances Over Weekends', Communities Natwest, 31 August 2015 <http://www.communities.natwest.com/t5/Ways-to-Bank/NatWest-App-Not-Updating-Balances-Over-Weekends/td-p/41285> accessed 1 September 2016

Near Field Communication Forum, 2013 <http://www.nfc-forum.org/home/> accessed 28 October 2013

NFC Forum, 'Our Members NFC', 2019 <https://nfc-forum.org/about-us/our-members/> accessed 5 March 2019

O2, O2 Momey <http://www.o2.co.uk/money> accessed 10 November 2016

O'Harrow, R., 'Hacking tool kits, available free online, fuel growing cyberspace arms race', Washington Post, 2013 <http://www.washingtonpost.com/investigations/hacking-tool-kits-available-free-online-fuel-growing-cyberspace-arms-race/2012/11/12/1add77a4-21e6-11e2-ac85-e669876c6a24_story.html> accessed 8 January 2014

Oxford Dictionary, 'Fintech', 2017 <https://en.oxforddictionaries.com/definition/fintech> accessed 20 May 2017

Paym, 'The UK's Mobile Payment System', 2019 <https://paym.co.uk/> accessed 2 March 2019

Payment Systems Regulator, 2017 <https://www.psr.org.uk/> accessed 1 October 2017

PayPal <https://www.paypal.com/uk/home> accessed 1 July 2015

PayPal, 'We get where you're coming from.' 2017 <https://www.paypal.com/en/webapps/mpp/country-worldwide> accessed 25 November 2017

Pingit, 2019 <https://www.pingit.com/> accessed 1 February 2019

Pinola, M., '5 Main Types of Mobile Payments', Lifewire, 20 October 2016 <https://www.lifewire.com/main-types-of-mobile-payments-2377766> accessed 10 November 2016

Power, L., 'Getting to know the GDPR, Part 9 - Data transfer restrictions are here to stay, but so are BCR', Field Fisher, 24 February 2016 <http://privacylawblog.fieldfisher.com/2016/getting-to-know-the-gdpr-part-9-data-transfer-restrictions-are-here-to-stay-but-so-are-bcr/> accessed 15 September 2016

Press Trust of India, 'Hackers come up with new tricks to attack bank accounts', 2013 <http://ibnlive.in.com/news/hackers-come-up-with-new-tricks-to-attack-bank-accounts/422343-11.html> accessed 28 October 2013

Radwan, S., 'Islamic Banking: Why Transparency Matters', International Sharia Research Academy for Islamic Finance, Wahed, 14 June 2017 <https://journal.wahedinvest.com/islamic-banking-why-transparency-matters/> accessed 1 September 2017

Read, E., Alsheikh,T., 'Data protection in Saudi Arabia: overview', Practical Law, 2012 <http://uk.practicallaw.com/4-520-9455> accessed 1 November 2016

Responsible Digital Payments Guidelines. July 2016, 1-28 <http://www.cashlearning.org/downloads/btca-responsibledigitalpaymentsguidelinesandbackground-(1).pdf> accessed 1 September 2016

Romero, S., 'The unstoppable growth of digital banking: 3 billion users by 2021', BBVA, 22 February 2017 <https://www.bbva.com/en/unstoppable-growth-digital-banking-3-billion-users-2021/> 19 November 2017

Rouse, M., 'WAP (Wireless Application Protocol)', TechTarget.com, 2017 <http://searchmobilecomputing.techtarget.com/definition/WAP> accessed 15 November 2017

Rushton, K., 'O2 to launch mobile money transfer app to rival Barclays' Pingit', The Telegraph, 27 February 2012 <http://www.telegraph.co.uk/finance/newsbysector/mediatechnologyandtelecoms/telecoms/9109155/O2-to-launch-mobile-money-transfer-app-to-rival-Barclays-Pingit.html> accessed 10 November 2016

Russell, J., 'Apple is 'working rapidly' to launch Apple Pay in more countries in Asia and Europe', TechCrunch, 26 May 2016 <https://techcrunch.com/2016/05/26/apple-is-working-

rapidly-to-launch-apple-pay-in-more-countries-in-asia-and-europe/> accessed 10 November 2016

Russon, M-A., 'NatWest online banking flaw enables hackers to drain bank accounts by stealing your smartphone', IB Times, 7 March 2016 <http://www.ibtimes.co.uk/natwest-online-banking-flaw-enables-hackers-drain-bank-accounts-by-stealing-your-smartphone-1548002> accessed 1 September 2016

SABB, 'SABB Mobile - Mobile Banking', 2017 <http://www.sabb.com/en/everyday-banking/ways-to-bank/sabb-mobile/> accessed 1 October 2017

Sahih International <https://quran.com/16/91> accessed 10 February 2019

Sahih International <https://quran.com/55/9> accessed 10 February 2019

Sahih International <https://quran.com/17/35> accessed 10 February 2019

SAMA, 'Saudi Arabian Monetary Authority Launches Fintech Saudi with the Objective to Make the Kingdom a Pioneer in the Financial Technology Sector', 1 May 2018 <http://www.sama.gov.sa/en-US/News/Pages/news30042018.aspx> accessed 5 July 2019

Sanchez, A., 'Personal banking apps leak info through phone', 8 January 2014, IOActive <http://blog.ioactive.com/2014/01/personal-banking-apps-leak-info-through.html> accessed 1 September 2016

SAS Institute Inc, 'The Digital Bank 2.0', White Paper <http://www.sas.com/fi_fi/whitepapers/SAS-Whitepaper-The-Digital-Bank-2.html> accessed 1 November 2016

Saudi Arabian Monetary Authority, 'Saudi Arabian Monetary Authority Launches FintechSaudi with the Objective to Make the Kingdom a Pioneer in the Financial Technology Sector', 1 May 2018 <http://www.sama.gov.sa/en-US/News/Pages/news30042018.aspx> accessed 6 March 2019

Saudi Credit Bureau, 'Reducing risk: Nabil A Al Mubarak, CEO, Saudi Credit Bureau (SIMAH), on the role of credit risk', 2013 <http://www.simah.com/en/NewsDetail.aspx?news_id=Uq4oqo8lLRU=> accessed 20 October 2014

Saudi Embassy, 'Summary of FATF Report and Conclusions', 14 June 2004 <http://www.saudiembassy.net/archive/2004/statements/page9.aspx> accessed 1 May 2015

Saudi Gazette, 'SAMA issues prepaid card services rules', 22 July 2012 <http://www.saudigazette.com.sa/index.cfm?method=home.regcon&contentid=20120722130670> accessed 26 October 2014

Saudi Hollandi Bank, 'Terms and Conditions', 2016 <https://www.shb.com.sa/SHBFORMS/Terms/en/ribtermsen.htm> accessed 1 November 2016

Saudi Hollandi Bank, Your Financial Rights and Responsibilities, The Banking Consumers' Guide, 2014 <http://www.shb.com.sa/en/pdf/consumerProtection/Guide%20en.pdf> 24 September 2014

Saudi Investment Bank, 'Payroll Service', 2016 <https://www.saib.com.sa/en/content/payroll-service-0> accessed 1 November 2016

Saudilegal, '2. Islamic Contract Law', 2018 <http://www.saudilegal.com/saudilaw/02_law.html> accessed 15 February 2019

Saudilegal, 'Electronic Transactions', 2016 <http://www.saudilegal.com/saudilaw/09_law.html> accessed 1 November 2016

Schneider, I., '5 Critical Strategies for Mobile Banking Security', BankTech, 2012 <http://www.banktech.com/risk-management/5-critical-strategies-for-mobile-banking/240003902> accessed 28 October 2013

Shoura, 'Shoura discusses consumer protection law', Saudi Gazette, 5 October 2017 <http://saudigazette.com.sa/article/178256/Shoura-discusses-consumer-protection-law> accessed 20 April 2019

Sidel, R., 'Mobile Bank Heist: Hackers Target Your Phone', The Wall Street Journal, 26 August 2016 <http://www.wsj.com/articles/mobile-bank-heist-hackers-target-your-phone-1472119200> accessed 1 September 2016

SIMAH, 'About Us', 2016 <https://www.simah.com/English/About-Us> accessed 1 November 2016

Snell, K., 'Who Needs a Cayman Account When You've Got Bitcoin?' *Politici Morning Tax*, 9 August 2013 <http://www.politico.com/tipsheets/morning-tax/2013/08/who-needs-a-cayman-account-when-youve-got-bitcoin-graves-investigating-irs-small-business-letters-011385> accessed 1 September 2016

Sonawane, K., 'Mobile Payment Market Expected to Reach $ 4,574 Billion by 2023', Allied Market Research, February 2018 <https://www.alliedmarketresearch.com/press-release/mobile-payment-market.html> accessed 5 March 2019

Sposito, S., 'Mobile Bank Accounts May Be Vulnerable from SIM Card Hack', American Banker, 2013 <http://www.americanbanker.com/issues/178_141/mobile-bank-accounts-may-be-vulnerable-from-sim-card-hack-1060802-1.html> accessed 28 October 2013

Statista, 'Mobile Payments, Saudi Arabia', 2017 <https://www.statista.com/outlook/331/110/mobile-payments/saudi-arabia#> accessed 1 October 2017

Statista, 'Number of NFC and non-NFC mobile proximity payment users worldwide from 2014 to 2019 (in millions)', The Statistical Portal, February 2016 <https://www.statista.com/statistics/557959/global-mobile-proximity-payment-users/> accessed 14 September 2017

Symantec, ‘SpyEye Bot versus Zeus Bot’, 2010 <http://www.symantec.com/connect/blogs/spyeye-bot-versus-zeus-bot> accessed 23 December 2013

The Wall Street Journal, 'How Mobile Money Drives Economic Growth', 2017 <http://www.wsj.com/ad/article/mlf-how-mobile-money-drives-economic-growth> accessed 16 December 2017

Thompson, J., ‘U-turn on HMV gift cards as its survival hopes improve’, The Independent, 2013 <http://www.independent.co.uk/news/business/news/uturn-on-hmv-gift-cards-as-its-survival-hopes-improve-8460995.html> accessed 2 April 2013

Tugby, L., 'Sainsbury's to launch scan-and-go smartphone shopping app', RetailWeek, 15 April 2015 <https://www.retail-week.com/sectors/grocery/sainsburys-to-launch-scan-and-go-smartphone-shopping-app/5073990.article> accessed 15 September 2017

UK Cards Association, 'UK Card Payments Summary 2017', 2017, 1-4 <http://www.theukcardsassociation.org.uk/wm_documents/UK%20Card%20Payments%202017%20-%20Summary%20FINAL.pdf> accessed 1 September 2017

V3.co.uk, 2013 <http://www.v3.co.uk/v3-uk/news/2291042/mobile-banking-services-pose-major-security-risks-warns-financial-watchdog> accessed 28 October 2013

VISA, ‘BBVA and Visa launch first commercial solution for cloud-based mobile payments’, 2015 <http://www.visaeurope.com/newsroom/news/bbva-and-visa-launch-first-commercial-solution-for-cloud-based-mobile-payments> accessed 18 July 2015

VISA, ‘Visa Ready for Mobile Payments’, 2014 <https://technologypartner.visa.com/VisaReady/MobilePayments.aspx> accessed 20 August 2015

Vonthron, N., 'A2A interoperability: Understanding bank to mobile money transaction flows and technical solutions', GSMA, 10 December 2015 <http://www.gsma.com/mobilefordevelopment/programme/mobile-money/a2a-interoperability-understanding-bank-to-mobile-money-transaction-flows-and-technical-solutions> accessed 1 November 2016

Warman, M., 'Orange and Barclaycard launch ‘Quick Tap’ mobile phone payments', The Telegraph, 20 May 2011 <https://www.telegraph.co.uk/technology/news/8525031/Orange-and-Barclaycard-launch-Quick-Tap-mobile-phone-payments.html> accessed 10 February 2019

Westerhaus, C., 'Time to act: EU Funds Transfer Regulation 2015', Banking Technology, 9 August 2017 <http://www.bankingtech.com/896431/time-to-act-eu-funds-transfer-regulation-2015/> accessed 1 October 2017

Williams, R., 'How to set up Apple Pay', The Telegraph, 14 July 2015 <http://www.telegraph.co.uk/technology/apple/11737576/How-to-set-up-Apple-Pay.html> accessed 10 November 2016

World Bank, ‘Depth of credit information index (0=low to 8=high)’, 2015 <http://data.worldbank.org/indicator/IC.CRD.INFO.XQ/countries> accessed 10 May 2015.

Worth, D., ‘Mobile banking services pose major security risks, warns financial watchdog’, V3.co.uk, 2013 <http://www.v3.co.uk/v3-uk/news/2291042/mobile-banking-services-pose-major-security-risks-warns-financial-watchdog> accessed 28 October 2013

Yurcan, B., 'Banks Position Themselves For Mobile Banking 2.0', Banktech, 13th May 2014 <http://www.banktech.com/channels/banks-position-themselves-for-mobile-banking-20/d/d-id/1297003?> accessed 1 November 2016

Zapp, 'Barclays Pingit set to be first bank app live with Zapp', 7 July 2015 <http://www.zapp.co.uk/blog/2015/07/barclays-pingit-set-be-first-bank-app-live-zapp-2> accessed 10 November 2016

Zawya, ‘Consumer protection law under Shoura study’, 12 November 2014 <https://www.zawya.com/story/Consumer_protection_law_under_Saudi_Shoura_study-ZAWYA20141112035028/> accessed 18 May 2015.