University of Kent

Kent Academic Repository

Zheng, Jiamin, Deng, Yue, Chen, Jessica, Li, Shujun, Zou, Yixin and Li, Jingjie (2026) *Characterizing Scam-Driven Human Trafficking Across Chinese Borders and Online Community Responses on RedNote*. In: CHI '26: Proceedings of the 2026 CHI Conference on Human Factors in Computing Systems. . ACM ISBN 979-8-4007-2278-3.

Downloaded from
https://kar.kent.ac.uk/114786/ The University of Kent's Academic Repository KAR

The version of record is available from
https://doi.org/10.1145/3772318.3791786

This document version
Publisher pdf

DOI for this version

Licence for this version
CC BY (Attribution)

Additional information

Versions of research works

Versions of Record
If this version is the version of record, it is the same as the published version available on the publisher's web site. Cite as the published version.

Author Accepted Manuscripts
If this document is identified as the Author Accepted Manuscript it is the version after peer review but before type setting, copy editing or publisher branding. Cite as Surname, Initial. (Year) 'Title of article'. To be published in ***Title of Journal*** , Volume and issue numbers [peer-reviewed accepted version]. Available at: DOI or URL (Accessed: date).

Enquiries
If you have questions about this document contact ResearchSupport@kent.ac.uk. Please include the URL of the record in KAR. If you believe that your, or a third party's rights have been compromised through this document please see our Take Down policy (available from https://www.kent.ac.uk/guides/kar-the-kent-academic-repository#policies).

Characterizing Scam-Driven Human Trafficking Across Chinese Borders and Online Community Responses on RedNote

Jiamin Zheng
University of Edinburgh
Edinburgh, United Kingdom
jiamin.zheng@ed.ac.uk

Yue Deng*
Department of Computer Science and Engineering, The Hong Kong University of Science and Technology
Hong Kong, China
ydengbi@connect.ust.hk

Jessica Chen
University of Edinburgh
Edinburgh, United Kingdom
J.Chen-265@sms.ed.ac.uk

Shujun Li
University of Kent
Canterbury, United Kingdom
s.j.li@kent.ac.uk

Yixin Zou
Max Planck Institute for Security and Privacy
Bochum, Germany
yixin.zou@mpi-sp.org

Jingjie Li
University of Edinburgh
Edinburgh, United Kingdom
jingjie.li@ed.ac.uk

Abstract

A new form of human trafficking has emerged across Chinese borders, where individuals are lured to Southeast Asia with fraudulent job offers and then coerced into operating online scams. Despite its massive economic and human toll, this scam-driven trafficking remains underexplored in academic research. Through qualitative analysis of 158 RedNote posts, we examined how Chinese online communities respond to this threat. Our findings reveal that perpetrators exploit cultural ties to recruit victims for cybercriminal roles within self-sustaining compounds, using sophisticated manipulation tactics. Survivors face serious reintegration barriers, including family rejection, as the cultural values that enable trafficking also hinder their recovery. While communities present protective strategies, efforts are complicated by doubts about the reliability of support and cross-border coordination. We discuss key implications for prevention, platform governance, and international cooperation against scam-driven trafficking. Warning: This paper contains descriptions of physical, psychological, and sexual abuse.

CCS Concepts

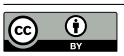
• **Human-centered computing** → *Empirical studies in HCI*; • **Security and privacy** → *Human and societal aspects of security and privacy*.

Keywords

Human trafficking, scam, China, Southeast Asia, social media, RedNote

ACM Reference Format:
Jiamin Zheng, Yue Deng, Jessica Chen, Shujun Li, Yixin Zou, and Jingjie Li. 2026. Characterizing Scam-Driven Human Trafficking Across Chinese Borders and Online Community Responses on RedNote. In *Proceedings of CHI Conference on Human Factors in Computing Systems (CHI '26).* ACM, New York, NY, USA, 25 pages. https://doi.org/10.1145/3772318.3791786

*This work was conducted while the author was a visiting PhD scholar at the Max Planck Institute for Security and Privacy.



This work is licensed under a Creative Commons Attribution 4.0 International License.
CHI '26, Barcelona, Spain
© 2026 Copyright held by the owner/author(s).
ACM ISBN 979-8-4007-2278-3/2026/04
https://doi.org/10.1145/3772318.3791786

1 Introduction

The rapid expansion of digital technologies has transformed human trafficking into hybrid forms of exploitation that extend beyond traditional labor and sexual coercion. Increasingly, traffickers deploy technology-enabled tactics that are broader, faster, and harder to detect. This phenomenon, often described as "cyber slavery" [60], involves individuals deceived by promises of lucrative jobs, trafficked across borders, and forced to work in scam compounds running large-scale online fraud operations.

Recent reports highlighted China as one of the primary sources of human trafficking. In 2023 alone, Chinese authorities announced the arrest of over 50,000 fraud suspects and the disruption of organized networks in Myanmar's border region [59]. A report published by the Office of the United Nations High Commissioner for Human Rights (OHCHR) in 2023 estimated that hundreds of thousands of people are trapped in cyber-scam compounds across Southeast Asian countries near Chinese borders, such as Cambodia, Myanmar, and Laos, generating approximately $43.8 billion annually for criminal networks [77]. At least 120,000 individuals were reportedly forced into scam labor in Myanmar and another 100,000 in Cambodia [77]. This modern form of human trafficking blurs the victim-perpetrator boundary [116], as trafficked individuals are compelled to commit crimes against others while being victims themselves.

Technology plays a dual role in this ecosystem. Traffickers exploit mobile phones, social media platforms, and encrypted communication tools to recruit, control, and monitor victims [85, 101]. However, with increasing usage of social media [95], it provides vital spaces where survivors, families, and concerned users share warnings, coordinate rescue efforts, and build collective knowledge about trafficking operations, mirroring the broader online safety and well-being research showing how users and communities develop narratives around experiences of risks and protective strategies and provide peer support [50, 130].

Despite its severity, scam-driven human trafficking remains critically underexplored in the academic literature. Existing work in this setting has largely examined institutional responses and broader sex and labor exploitation [79, 102], along with compound structures, governance dynamics, and legal responses [44, 77, 111]. Empirical studies show that traffickers recruit educated, digitally skilled victims through fake job advertisements, operate within layered criminal networks enabled by weak governance, and force victims to conduct scripted online fraud under violent enforcement regimes [44, 52, 63, 64]. Regional studies have traced how cyber-fraud industries have migrated from China into Southeast Asia, supported by weaker governance, complicit local authorities, and money-laundering infrastructures [12, 24, 61].

Building on prior work examining institutional responses or isolated survivor accounts, we focus on how victims and communities themselves perceive risks and develop protective strategies in the digital space of scam-driven human trafficking. From this lens, we can understand how different stakeholders exchange information and support across the full trafficking lifecycle, as well as the cultural and socio-technical dynamics that shape community responses when institutional interventions prove inadequate. Specifically, we address four research questions:

- **RQ1:** What *recruitment tactics* for scam-driven human trafficking do RedNote users recognize?
- **RQ2:** What *exploitation and control mechanisms* in scam-driven human trafficking are shared by RedNote users?
- **RQ3:** What *post-trafficking outcomes and reintegration challenges* are identified by RedNote users affected by scam-driven human trafficking?
- **RQ4:** How do RedNote users share and evaluate *protective strategies* against scam-driven human trafficking?

To answer these questions, we conducted a qualitative content analysis based on 158 posts sampled from RedNote, a popular Chinese social media platform that has recently become a valuable data source for researchers [18, 115, 129]. Our findings reveal how perpetrators weaponize Chinese kinship ties and filial duties throughout the trafficking lifecycle. During recruitment (**RQ1**), scammers' strategies extend beyond generic social ties identified by prior work [52, 63]: they exploit trust embedded in kinship and cultural expectations, while the boundary between voluntary participation and coercion becomes blurry for victims. While certain groups are especially vulnerable, including "left-behind youth"—rural children whose migrant-worker parents leave them with a weak social safety net, even highly skilled individuals are not immune and are specifically targeted in recruitment for multilingual abilities or other competencies valuable to scam operations. Once trafficked (**RQ2**), survivors endure continuous, multi-layered abuse in scam compounds, while operators further weaponize kinship and cultural ties to extract ransoms from families. Upon escape, survivors seeking reintegration (**RQ3**) face family rejection, uncertain legal consequences, and public shaming for being "greedy" or "gullible," in stark contrast to the sympathy typically afforded to abuse survivors [84]. When institutional channels prove inadequate, RedNote users develop their own protective strategies (**RQ4**), including grassroots rescue networks and targeted warnings for vulnerable groups. These community efforts raise broader awareness and address gaps left by formal support systems.

Situating our work within the HCI literature [86, 89, 100, 119], we discuss pathways to protect survivors of scam-driven human trafficking, including culturally and socially informed digital safenets, content moderation on traumatizing topics and narratives, and efforts related to cross-border rescue.

For the rest of the paper, we review related work on human trafficking and online safety discourse (§2), then describe our qualitative methodology for analyzing RedNote posts (§3). We present findings organized by our four research questions (§4) and discuss implications for culturally informed interventions, platform design, and cross-border support systems (§5).

2 Background and Related Work

Below, we introduce the background for our study on scam-driven human trafficking, a pressing threat that involves deceiving victims through false employment promises and coercing them into cybercrime operations across international borders.

2.1 Exploitation in Human Trafficking

Exploitation in human trafficking has historically been framed around sexual and labor exploitation, including physical violence, psychological manipulation, and economic coercion [48, 78]. More than half of survivors report physical or sexual abuse, while psychological coercion creates emotional dependencies that isolate victims from support networks [70, 79, 102]. Economic mechanisms such as debt bondage, confiscation of documents, and wage withholding further entrench dependency and limit mobility [101]. These practices are shaped by inequalities, with marginalized groups disproportionately targeted and subjected to slavery-like conditions [58, 98]. Beyond sex and labor exploitation, trafficking also involves forms of exploitation such as domestic servitude, organ trafficking, and criminal exploitation, though these remain comparatively underresearched [14]. Recent work has highlighted that victims are increasingly coerced into illicit activities such as cybercrime, which blurs the boundary between victims and perpetrators [116].

With the rapid development of China's economy and societal transformation, fraud has also exhibited a trend towards digitalization. As Chinese authorities intensify cross-border crackdowns and repatriations with Southeast Asian partners, Chinese nationals remain a major share of both victims and perpetrators in scam compounds [26]. Victims deceived with fraudulent job offers are coerced into cyber-fraud operations within heavily guarded compounds, facing strict quotas, extended hours, and violent punishments for noncompliance [41, 42]. Testimonies have shown that traffickers train victims to fabricate online identities and carry out "pig-butchering" scams that combine romantic persuasion with fraudulent investment schemes [75, 93, 116, 123]. Wang [116] showed how trafficked workers undergo coerced identity shifts that sustain their dual status as both exploited and criminalized.

While recent research has relied primarily on interviews, NGO reports, and legal proceedings, less attention has been paid to how Chinese survivors and communities interpret these exploitative

practices in digital spaces. Our study addresses this gap by examining how users recognize, describe, and evaluate the mechanisms of scam-driven human trafficking through RedNote data.

2.2 Human Trafficking in the Digital Era

Human trafficking is defined as the exploitation of individuals through force, fraud, or coercion for involuntary labor or sexual activity [110]. Kleemans and Smit [49] conceptualized trafficking as a linear process involving recruitment, transportation, and exploitation. Digital technologies have transformed the methods traffickers use to recruit, control, and exploit victims. Mobile phones, social media platforms, and chat applications are central tools for contacting victims, advertising services, and coordinating transactions in sex and labor trafficking contexts [51]. Technology also amplifies coercion beyond traditional forms of physical and psychological abuse. As Stephenson et al. [101] demonstrated, human traffickers exert real-time control of survivors via location trackers such as Apple's FindMy, covert monitoring apps, and contact surveillance.

While the existing scholarship on sex and labor trafficking emphasizes recruitment through social media and escort websites, scam-driven trafficking in Asia operates through "forced criminality," wherein victims are deceived into cyber-fraud operations where they are compelled to use digital tools to target new victims, effectively turning coercion into a scalable digital labor system, a phenomenon journalists referred to as "cyber slavery" [35, 41, 93]. These operations are concentrated in border regions such as Myawaddy in Myanmar, where numerous scam compounds have been documented. Regional work traces how cyber-fraud industries moved from China to Southeast Asia, exploiting weak governance and legal loopholes. Franceschini et al. [24] detailed this shift through a case study of Sihanoukville, Cambodia, while others described protection by political elites in Cambodia and military-linked actors in Myanmar [61, 111]. Institutional reports frame scam compounds as part of transnational organized crime. In 2023, OHCHR [77] called for cross-border cooperation and emphasized the non-punishment principle for coerced victims.

While news reports highlight rapid growth in scam compounds and mass trafficking into cyber-fraud hubs with statistics [69, 88, 125, 126], empirical studies add more granular views. Luong [63] analyzed Vietnamese case files and police interviews and showed that traffickers target educated victims through fake job adverts in layered criminal networks. Jesperson et al. [44] studied eight Southeast Asian countries and identified enabling institutional and economic conditions, including targeting highly educated workers, reversed migration flows from wealthier to poorer countries, and dual victimization of both trafficked workers and scam targets. Lazarus et al. [52] drew from a Bangladeshi survivor's testimony to outline six stages from recruitment to escape and show how victims are coerced into scripted online fraud.

In terms of institutional support for human trafficking survivors, counter-trafficking efforts in the US rely on hotlines, communication apps, and online awareness campaigns that allow victims and families to seek help remotely and enable NGO coordination [23], while institutional support for Chinese human-trafficking victims heavily relies on law enforcement and official anti-scam apps [30, 127]. However, rising evidence has shown that people have found these channels limited or inaccessible, thus turning to social media to share information, mobilize support, and seek help directly under public safety crisis [5, 83, 95]. This trend highlights that social media is not only a site of risk, where traffickers recruit and exploit, but also a critical source of support and community resilience.

For methodologies, news coverage tends to focus on high-profile cases and rescue operations, which could be subject to media ideology and political environments [103]. Past academic research has documented trafficking organizations, economic impacts, and survivor experiences, mostly through interviews and official reports outside China [44, 52, 63, 64]. Chinese Internet users' own perspectives on how they understand risks, exchange support, and navigate reintegration in everyday digital spaces remain understudied, despite being a major victim group and a primary trafficker nationality [63]. Our study addresses this gap by analyzing posts on RedNote, a Chinese social media platform where users actively discuss safety risks, help-seeking, and reintegration under crisis in their own narratives.

2.3 User Perception and Online Safety Discourse

Online communities develop their understandings of risk through shared narratives, warnings, and interpretive frameworks that often operate alongside or in tension with official safety guidelines [50, 72, 120]. Research on adolescent online safety has demonstrated how users interpret linguistic and emotional cues to distinguish safe from unsafe interactions [4], while research on family dynamics has highlighted tensions between trust, autonomy, and protective strategies [31]. These perspectives underscore that users are not passive targets but actively co-construct safety practices in digital spaces. Research in security and privacy has shown how online discussions can reveal everyday safety concerns and coping strategies, from smart homes to software development [3, 6, 54, 56, 107, 112, 122]. In particular, human-centered security research has examined how users detect online scams leveraging URLs and browser security indicators [19, 21, 97, 106] and the barriers users encounter during their sense-making process [20, 74, 119]. Recent work has also leveraged online forums to analyze scam-related discourse, showing that communities collaboratively dissect fraudulent tactics, reconstruct scam lifecycles, and share step-by-step prevention guidance [76]. Community resources can update faster than institutional advisories and offer granular, platform-specific advice. These investigations highlight how personal narratives on digital platforms often serve as user-driven strategies for interpreting, flagging, or resisting perceived harms.

Cultural and political contexts further influence online safety discourses, particularly for sensitive or controversial topics [18, 108, 132]. In the Chinese context, Deng et al. showed how filial piety motivated people to seek online safety advice for parents [18], and He et al. discovered that social media commodified the safety concerns of Chinese women [33]. This is also manifested in the moderation policies of online platforms, which drove Chinese users to use indirect expression and re-appropriate hashtags when articulating threats and maintaining online safe spaces [65, 80, 115, 124]; while weaker moderation can also push communities to create local safety norms and workaround practices [92]. These patterns are relevant

to trafficking-related discussions, which share features with other forms of online exploitation, such as grooming and sextortion [90].

Prior work explains how individuals actively interpret risks, co-construct safety narratives and adapt to platform governance. However, much existing research in HCI focuses on phishing and general forms of online fraud in Western contexts. Emerging studies in China have begun to analyze social media users' discourse and responses to both public and individual safety crises, including the COVID-19 pandemic [62], mental health issues [130], and gender-specific harms [33], highlighting how these dynamics are shaped by unique cultural, social, and technological environments in China. Scam-driven human trafficking in China, however, extends far beyond individual safety risks in contexts like email-based phishing, and instead represents a systematic public crisis involving sophisticated digital and physical fraud schemes, the exploitation of digital labor, and ambiguous online governance spaces and support systems. Despite its complexity and societal impact, there remains a lack of holistic research examining how Chinese Internet users respond to different phases of scam-driven human trafficking and collectively construct protective discourses in this rapidly evolving, sensitive, and often contentious context. Addressing this gap motivates our study.

3 Method

To understand human trafficking driven by scams from a user-centric perspective, we collected relevant posts on RedNote, a major Chinese social network, and conducted qualitative content analysis to uncover insights at different stages of scam-driven human trafficking.

3.1 Data Source

We chose social media platforms as our data source for studying scam-driven trafficking discourse because they capture diverse user narratives about the full life-cycle of trafficking experiences in an ecologically valid setting. Specifically, we selected RedNote, a rapidly growing Chinese social media platform launched in 2013 that combines features from Instagram and TikTok, supporting lifestyle-oriented content through text, photos, and videos [40, 105]. By 2025, RedNote had over 300 million monthly active users, with a user base largely composed of young people, who are disproportionately targeted by trafficking [8, 113]. RedNote has gained increasing attention in HCI research as the study site for Chinese users on topics related to online safety and discourse analysis of personal experiences [18, 33, 55, 115]. It particularly aligns with our research objectives as RedNote emphasizes individual perspectives and global experiences of Chinese users within a unified app [128], which allows analysis of firsthand accounts of experiences and protection practices regarding cross-border scam-driven human trafficking. In contrast, other platforms such as Douyin (the domestic version of TikTok) maintain separate domestic and international versions or host limited relevant content. Our preliminary exploration indicates that RedNote posts contain richer personal narratives about scam-driven human trafficking. Searches on Weibo, another candidate mainstream social media platform in China returned fewer such narratives and were dominated by official announcements, likely a result of the platform's content moderation policies [133, 134], making it less suitable for our purposes.

3.2 Data Collection

To identify posts relevant to scam-driven human trafficking from RedNote, we collected publicly available content from RedNote using MediaCrawler [73], which queries RedNote's web API to automate keyword-based search and post download. To mitigate biases introduced by personalized recommendations, we used a fresh RedNote account for data collection. RedNote's search feature relies on contextual similarity rather than strict keyword matching [18].

Our search term selection drew upon the trafficking-related literature, media reports, and online discussions to ensure we covered a diverse topic representation for different aspects and stages of scam-driven human trafficking. We include 26 keywords under four main groups of key terms: (1) core trafficking terminology ("`human trafficking`"), (2) scam-related terms ("`high-paying labor`" and "`overseas job scam`"), (3) geographic targets that incorporate specific high-risk regions frequently mentioned in trafficking discourse ("`Northern Myanmar`" and "`Myawaddy campus`"), and (4) victim experience terminology that captures first-hand narratives ("`trafficking experience`" and "`abduction experience`"). We started with terms that are broad in scope, formed and tested more specific terms by snowball sampling from the key terms and tags in the collected samples initially. Data collection was completed in January 2025, and a total of 6,639 posts were retrieved.

We used a comprehensive keyword set to cover more posts from different perspectives, as each search returned around 200 to 300 posts. We collected posts by searching each of the 26 terms. Our data exploration showed that posts containing particular tags about entertainment and lifestyles (e.g., dramas and food recommendations) are largely irrelevant to user narratives of scam-driven human trafficking. Therefore, we excluded posts associated with these tags. As a result, our collected posts include keywords and tags subject to the logic `(human trafficking OR high-paying labor OR ... OR Cambodian scam) AND NOT (Korean drama OR Daily drama-watching OR ... OR Food and fun)`. We show the list of keywords and excluded tags in Appendices A and B, respectively. After removing duplicated entries using each post's unique ID, we retained a dataset that includes 4,499 posts, with post dates ranging from December 2018 to January 2025.

3.3 Data Filtering and Sampling

Despite initial scoping using key terms and tags, the dataset still contained posts that were irrelevant to scam-driven human trafficking, e.g., human trafficking without connections to scams. We discussed and established the relevance criteria that a post should contain relevant information about scams and human trafficking, or cross-border human trafficking between China and Southeast Asia that is connected to scam operations. These posts include types such as users' first-hand experiences, commentary on related news, and information-seeking posts. We employed a Chinese LLM (large language model) `qwen2.5-3b` to complement our manual efforts to identify relevant data points, following prior work that adopts similar semi-automated approaches [120].

We developed a prompt (Appendix C) for `qwen2.5-3b` to identify candidate posts for subsequent manual validation. Final inclusion decisions were made by the authors through close verification. We ran `qwen2.5-3b` locally over the full corpus of 4,499 posts and retrieved 1,955 candidate posts for manual review.

To assess screening quality, we randomly sampled 100 posts from the full corpus (44 predicted as relevant by the model and 56 predicted as irrelevant) and had the first two authors independently annotate relevance as ground truth, using a deliberately permissive inclusion criterion that considers borderline posts as relevant candidates. For example, we treated posts that mention scam-driven human trafficking only via hashtags as relevant candidates for manual filtering. This permissive criterion was designed to evaluate the model's ability to flag any post that plausibly fell within our final inclusion scope. Inter-rater agreement was high (Cohen's $\kappa = 0.98$), indicating consistent application of the criteria. The model achieved 84% accuracy and a false negative rate of 8.8% in identifying candidate posts for human validation. Upon closer manual examination, we found that posts missed by the filter model were typically borderline or low-information cases (e.g., `#human_trafficker` appeared in the hashtags, but the body text discussed unrelated topics or lacked substantive detail). These missed posts therefore would not contribute confident, substantive information even if included in the qualitative analysis.

Using `qwen2.5-3b`, we obtained a subset of 1,955 candidate posts from our dataset. We drew random samples from the candidate posts and then jointly validated and further refined the samples by the first two authors as the coders. We removed posts unrelated to scam-driven human trafficking and excluded those without substantive information (e.g., scam reports with no link to overseas trafficking and scam compounds and domestic missing-person cases without suspected trafficking to scam compounds) and resolved ambiguous cases during team meetings. As a result, our final data sampled and coded for analysis included 158 posts, during which we reached data saturation [96] when establishing our codebook used in thematic analysis using the first 93 posts sampled.

3.4 Qualitative Content Analysis

We conducted open coding for our thematic analysis. Our initial codes are built on Kleemans and Smit's linear model of recruitment, transportation, and exploitation in human trafficking [49]. Nevertheless, existing models missed the details in the user narratives of scam-driven trafficking documented on social media. To derive fine-grained codes and insights, the first author first familiarized themselves with the dataset and developed initial codes and themes. The second author jointly coded the dataset and contributed to the code refinement and interpretations. The two coders worked closely together, meeting weekly to reconcile disagreements and ambiguities in the codes and definitions. The wider team was involved throughout the process to review the codebook and help refine the coding scheme. The first author then reapplied the updates and revisions to the coded data, ensuring consistency. The two coders established our initial codebook using 60 posts, for which we applied axial coding [15] to identify associated codes and form a hierarchy. After that, we further coded data and monitored data saturation [96]. We observed data saturation using 93 posts, after which we continued to code 65 posts.

Throughout the analysis, we adopted a reflexive thematic analysis approach [7], treating researchers as active interpreters rather than interchangeable coders applying fixed categories. The varied expertise within our team in HCI, online security and safety, and cybercrime supported a richer understanding of nuances in the data. Following qualitative practice in HCI [67], we prioritized iterative discussion and collective sense-making rather than independent coding agreement. Inter-rater reliability metrics are not appropriate for this analytic approach [7] because IRR assumes stable categories and would constrain the interpretive flexibility needed to capture the complexity of user narratives. We provide our codebook in Appendix D, which includes 52 codes and 91 fine-grained sub-codes.

3.5 Ethical Considerations

Our research was approved by the Ethics Committee of the School of Informatics, University of Edinburgh. We paid careful attention to ensuring ethical research practices, particularly in handling sensitive content and user information, although the posts are already publicly available. We removed all usernames and identifiers when presenting our analysis. We further paraphrased and manually translated our quotes from Chinese to English to minimize re-identification of post authors via direct searches on RedNote. Each quoted post in our reported findings is indexed by a unique label (e.g., `P-e8Y`), where `P` denotes *Post* and the alphanumeric suffix was randomly generated. These labels serve solely to distinguish between different posts. Our analysis focuses on aggregate insights, and we did not attempt to or intend to trace, contact, or profile individual users. To reduce the risk of undue platform strain, we did not collect more than 300 posts per day. The Chinese LLM we used is hosted locally without sharing data with a third party. Our study team members were informed of the topic and concerns for analyzing the potentially triggering content, and we carefully monitored the mental well-being of team members throughout the project. Team members took structured breaks to limit prolonged exposure to sensitive materials and rotated between different tasks. Institute-provided counseling services were available to the research team throughout the project. Our study aims to benefit and inform stakeholders to reduce future safety harms for online users.

3.6 Limitations

Our study has several limitations. First, our dataset is drawn exclusively from RedNote, a single Chinese social media platform. While RedNote provides rich and diverse narratives of scam-driven human trafficking, these accounts may not represent experiences discussed on other platforms or offline contexts. Relatedly, our keyword-based crawling approach, which is limited by RedNote's search interface as well as content policy, may lead to bias in the post distribution. Thus, we encourage future work to cross-compare multiple platforms and derive a more comprehensive understanding of the online ecosystems. Our filtering combined automated classification with manual validation. While the model achieves a good accuracy, automated classification may have excluded some relevant posts that refer to incidents of scam-driven human trafficking but contain too little textual information to assess their relevance. Additionally,

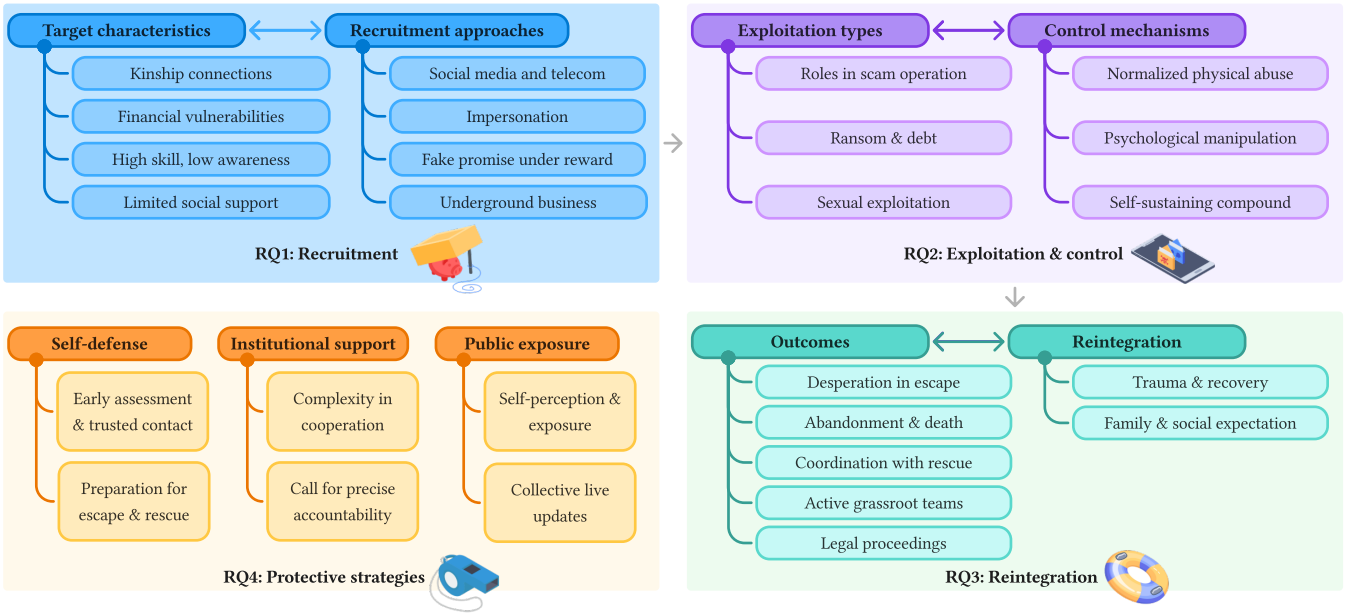


Figure 1: Overview of our findings mapped to scam-to-trafficking phases and research questions: RQ1 characterizes recruitment targets and approaches, RQ2 summarizes exploitation and control mechanisms, RQ3 captures post-trafficking outcomes and reintegration barriers, and RQ4 outlines protective strategies, including self-defense, institutional support, and public exposure.

our analysis focuses on textual elements of safety discourse, and we encourage future work to examine multimodal data such as images and videos, which may shed light on different communication strategies and offer complementary insights. Last, our qualitative analysis centers on self-reported narratives shared by those who voluntarily post on social media, and these voices may differ from those that remain silent due to barriers, including trauma, memory lapses, or self-preservation.

4 Findings

Our findings provide a comprehensive understanding of how scam-driven trafficking is understood and discussed on social media in China. We first report findings around recruitment tactics for scam-driven cross-border human trafficking recognized by RedNote users in §4.1. We then describe results from our analysis on the exploitation and control mechanisms shared by RedNote users in §4.2. Then, findings about the post-trafficking outcomes and reintegration challenges identified by users affected by scam-driven trafficking are presented in §4.3. Finally, we show how RedNote users share and evaluate protective strategies against scam-driven human trafficking in §4.4. Figure 1 shows an overview of our findings.

4.1 RQ1: Recruitment

In this section, we discuss the recruitment tactics for scam-driven cross-border trafficking as recognized and discussed by RedNote users. RedNote users have identified a range of targeted tactics, leveraging people's differing cultural, financial, and educational backgrounds in China (§4.1.1) when recruiting or defrauding people for scam-driven human trafficking (§4.1.2).

4.1.1 Target characteristics. RedNote posts collectively reveal four key target characteristics that perpetrators exploit. Our analysis showed that recruitment scams consistently leverage people's financial vulnerabilities and traditional Chinese kinship culture. Perpetrators specifically look for potential victims who possess skills for scam operations while having limited protection against exploitation.

Kinship and cultural connections. In multiple cases, perpetrators exploited family ties and cultural connections when approaching initial targets and abusing trust. P-e8Y gave an example of a recruitment scam spread through family networks. The target carried the thought that *"there is no way my [her] own sister would scam me [the target]"*, who also received ¥50,000 upfront from her sister, luring her, and eventually several other senior family members, to migrate to Cambodia for fraud working.

Community interpretations on RedNote suggest that such exploitation operates through the unique kinship ties in China [13] where shared local identities, family and clan reputations, and lineage-based networks provide falsely justified legitimacy and recruitment opportunities. Multiple RedNote posts point out that the perpetrators and victims are from the Fujian Province, which is a major hub of overseas migration from China and is associated with one of the largest online scam networks globally [1]. For example, in P-Nh4, a proclaimed insider commented that *"almost all managers are Fujianese"* for a scam compound in the Shan State, Myanmar. Another poster condemned these perpetrators and thought they *"brought massive negative impacts to the clan and the society and would possibly deserve expulsion from their pedigrees"*, which further showcases how the traditional kinship culture shapes people's understanding of modern cybercrime (P-Jo7).

Beyond initial recruitment, P-U0v discusses that victims' kinship ties can be further unwillingly exploited during forced recruitment scam production, as the perpetrators will be *"squeezing the last bit of use from victims and forcing them to proclaim to relatives and friends their infinite success abroad"* to lure more victims to scam compounds. This example further reflects the broader social codes in China, i.e., the so-called guanxi [11], where perpetrators exploit based on reciprocal obligations, honor, and mutual trust, extending the recruitment channel from close family members to others in the network, e.g., *"camaraderie of a friend"* (P-5mn, P-B9j).

Individual and generational financial vulnerabilities. Perpetrators consistently exploit victims' aspirations for financial advancement by crafting deceptive employment opportunities that appear to align with personal backgrounds and career interests. One case describes a mother's account of her son, who became disillusioned with unstable factory employment and the desire to pay medical bills for her. The son was subsequently targeted by a *"game company"* in Yunnan, resonating her son's interest in e-commerce and *"professional background"* in gaming, with a monthly salary of over ten thousand Chinese Yuan (¥), but ended up trafficking her son to Myanmar (P-H7j). Multiple other survivors shared the same financial hardship or the desire to *"make a big fortune"* (P-w81). Some posts questioned if the described financial vulnerabilities and aspirations are simply greed, describing survivors as *"freeloaders"* (P-N8k). Beyond individual vulnerability, RedNote users connected individual financial vulnerabilities to generational economic crisis, revealing their concerns in social safety nets and labor market instability. For instance, they called for *"strengthening protection of workers' rights"* (P-v68) for removing the financial driver of being lured into scam-driven human trafficking. They also recognized the inefficacy of policing strategies such as border control because *"Yunnan border guards can't stop people who think they can make money"* (P-p6a).

High skill potential but low awareness. Traffickers deliberately target individuals from a mix of educational and age backgrounds who possess the skills or potential to be converted into scam workers. The targets perpetrators look for include multilingual people (P-A6z) to reach prospective victims internationally. Targets also include teenagers and college students who are digitally literate, e.g., with social media platforms such as Kuaishou, who can be trained quickly for fraud production. These young targets are often depicted as lacking adequate social experience, legal understanding, and geographical awareness against scams, especially during travels abroad, which is illustrated by *"followed online acquaintances from Guangdong to Guangxi and then across borders, only realizing belatedly that they were being trafficked"* (P-J1v).

Limited social protection and support. Perpetrators target populations with high mobility to travel but limited social protections at home and abroad. These targets include *"left-behind children,"* a large population of Chinese children who stay in rural hometowns while their parents work in urban areas [47] (P-J1v), as well as tourists who *"had no idea why they are sent to borders between Thailand and Myanmar"* or got trafficked by the *"travel partners"* they just met (P-5yt). Additionally, RedNote users also offered travel warnings specific to women, e.g., *"especially single and beautiful girls,"* who might lack the physical strength to fight against street-kidnapping for sexual exploitation in the scam compounds (P-1VH). The post also commented that *"no one will look after you"* during their travels.

4.1.2 Recruitment approaches. Perpetrators often combine multiple tactics to create more convincing deceptions that make it harder for potential victims to recognize the danger.

Communication transiting targets across multiple channels exploiting digital governance blindspots. Social media arised as the dominant channel for perpetrators to broadly disseminate fraudulent job advertisements and romantic interests, and to gradually cultivate trust of the target in the perpetrator. These social media platforms include apps that are not officially allowed in China, for example, Facebook and Telegram, which are often referred to in coded language such as *"面子书"* ("face book" – Facebook) and *"飞机群"* ("airplane group" – Telegram) (P-3BQ and P-t3u). Additionally, posters discussed seeing recruitment posts on several domestic social media apps in China other than RedNote, such as Douyin and WeChat (P-z3p and P-v3S). Telephone calls are used for more direct and urgent communication, and when used along with other social media channels, they create a veneer of formality for business-related recruitment scams, e.g., directly with the *"boss"* (P-3BQ). One user described how *"initial contact through chat on Douyin, creates romantic emotional bonding and then introduces fake investment websites"* (P-z3p). Posts reveal that perpetrators strategically choose platforms with weaker governance mechanisms. For instance, one poster warned others (P-1Jy) by saying *"they generally use chat software that Chinese people don't commonly use, because there's no strict control mechanism."* This pattern shows that recruitment shifts to foreign platforms with less oversight. When communication moves across platforms, users receive no indication that they are crossing into spaces with weaker protections, allowing the trust built on regulated platforms to carry over without recognizing the risk.

Sophistically organized impersonation. Perpetrators impersonate distant relatives, authority figures, corporate representatives, or romantic partners when luring potential targets. Such impersonation can be sophistically organized, e.g., posing as clients to approach freelance workers such as dancers, magicians, makeup artists, and photographers, offering overseas work opportunities with *"accommodation and flights provided"* through seemingly normal business inquiries. More specifically, a news report indicated that perpetrators would run a seemingly legitimate business and later traffic targets to Cambodia for scam work *"during a corporate retreat"*, involving a group of impersonators (P-5mn).

Fake promises under upfront rewards. We observed that perpetrators are willing to pay for an upfront reward to lure targets and leverage their financial vulnerabilities, especially in fraudulent recruitment and investment opportunities. These upfront rewards include passport renewal fees (P-3BQ), free travel and transportation (P-B9j), advanced training payment (e.g., *"gave her 50k to receive manicure training"*), and express loan or startup budget (P-e8Y). These apparent benefits convince potential victims that they are entering profitable arrangements. However, survivors recounted how these promises are later transformed into mechanisms

of entrapment, with upfront rewards reinterpreted as debts and leveraged for control once victims arrive at scam compounds.

Willful participation in underground business. Our analysis reveals that trafficking recruitment deliberately exploits the boundaries between legitimate high-paying opportunities and underground business in China and Southeast Asia. Posts reveal several smuggling schemes leveraged by perpetrators to attract people (*"smuggling gold"*), courier services for high-value, export-controlled goods (*"transporting edible bird's nests"* [71] for *"¥15k per trip"*), or other semi-legitimate cross-border trade that promises exceptional returns (P-E8q). This exploits victims' intentions for *"quick money"* to be tempted, as they may see this work involve bending rules and would not constitute serious criminality. Another underground business mentioned is the *"debt trap,"* and a user suspected that some targets may have intended to *"get something for nothing"* and never intended to repay the loans. In particular, several posts explicitly accused survivors' informed participation in scam work, who *"went specifically for rebate fraud"* (P-SI6). The same post also claimed that a large proportion of *"about 90% are not real victims but participate in overseas fraud activities."* Similarly, P-9og openly questioned other survivors' proclaimed innocence by saying that *"he dares to write, and you dare to believe it."*

4.2 RQ2: Exploitation and Control

We observed that RedNote users share accounts of diverse tactics that traffickers employ to exploit and control victims.

4.2.1 Exploitation Types. Trafficked victims are exploited for their physical and intellectual labor in scam production, alongside additional financial and sexual values.

Trafficked victims transformed into specialized roles within scam operations. Our analysis reveals that survivors are transformed into scam workers in specialized organizational roles, along with the perpetrators. Labor is structured around scam production quotas, with survivors assigned to various operations including phone scams and chat-based fraud, social media farming, and romance grooming. One survivor described being *"required to add 5 customers (scam targets) online every day"* (P-Q1T). Training in using specific scam tactics is given when new "fraud workers" [survivors] receive training with scripts and materials: *"Given a thick stack of conversation materials to memorize, plus twenty phones to play various identities"* (P-Gy2). One victim documented that they got trained for a multi-stage romance scam targeting women aged 35-60 with a predetermined geographic area and timeline: *"The scam uses a military veteran's persona and gaming to build trust, then foster fake romantic ties of 'husband and wife' before pushing a 4-day money making cycle. Avoiding remote regions like Yunnan and Guizhou"* (P-z3p). The exploitation of young victims is particularly striking, with one observer noting (P-Q1T) *"I've seen the youngest dog pusher and agent at 19 years old, using a childish voice to impersonate a nearly 40-year-old middle-aged man,"* demonstrating how traffickers force even teenager victims to adopt false personas far beyond their years. Victims may eventually get "promoted" to management roles within scam compounds, such as enforcers of disciplinary actions or coordinators for scam operations. The term *"Piglets (猪仔)"* is used by traffickers and within the online community to refer to trafficked victims, framing them as livestock within a trading system for labor exploitation between different scam operations and compounds. Victims reported inflation of their *"buy-out cost"* upon transfer between scam compounds, with documented cases showing *"my buy-out cost increasing from $1,300 to $13,000"* (P-HF3). This commodification extends to the most extreme forms of exploitation, with survivors reporting witnessing *"organ harvesting"* and describing the compounds as places where victims face the ultimate threat of bodily dismemberment when they become unprofitable or uncooperative (P-x9a and P-5Ig).

Ransom demands and debt manipulation targeting victims' families. Exploitation extends beyond forced labor and commodification of the victim to their families through ransom demands and debt manipulation, described as *"squeezing the last bit of use from victims"* by one survivor (P-U0v). Ransom videos showing tortured and pleas of victims are sent to families, pushing already impoverished families deeper into debt, with families lamenting *"Never mind 300,000 [RMB], our rural family can't even come up with 30,000."* In several posts (e.g., P-Q9F), victims initially pursued higher wages to cover family medical bills, yet their families ultimately sold assets and borrowed heavily to make up the ransom amount, revealing a vicious cycle where economic desperation leads to victimization, and victimization creates even greater economic desperation. Some posts also reference established price ranges, such as *"Ransom is often between 200,000 and 400,000 RMB."* Ransom demands also create uncertainty and moral pressure. Relatives worry that pleas for help may be secondary scams but fear the cost of ignoring them. Many turn to RedNote to crowdsource verification and advice. One user created *"an alt account"* for anonymity and wrote: *"several friends say it's a scam, but it's hard to determine when it involves someone's life—if it's not a scam, my little cousin might get trapped, and I don't know whether to lend this [money emoji]")* (P-GW6). Another one asked, *"My relatives were scammed in the Myanmar Industrial Park! I see this kind of help request every now and then. Can they really be saved?"* (P-i3h). These narratives show families using the platform to narrate financial and emotional strain and to collectively reason about whether, and how to respond to ransom demands.

Sex exploitation in parallel with scam operations. Our findings reveal that female victims face additional exploitation within scam-driven trafficking. While initially forced into fraud work, women face sexual exploitation threats when resisting productivity demands, whereas males face physical punishments like beatings and electric shocks. Male perpetrators leverage romantic relationships and power imbalance for sexual exploitation and control. One post (P-Gy2) described a case where a scam operator *"has more than ten girls under his command,"* who *"often pretends to be tall, rich and handsome online to gain the trust of girls, and then takes them to Myawaddy, Myanmar."* Physical attributes become commodification criteria that determine the exploitation pathway, where *"slightly prettier girls will be targeted by supervisors, directors, and team leaders"* (P-xL7). Those who refuse fraud work or fail to meet performance metrics face immediate transfer to *"clubs,"* where phone access is eliminated entirely, severing their final communication lifeline (P-xL7). The term *"handrail girl (扶手女)"* is a localized

label that refers to women who, after being drugged or coerced, were forced into auxiliary sexual roles in brothels.

4.2.2 Control Mechanisms. To exploit victims in a "sustainable" manner, perpetrators apply a range of physical and psychological control.

Normalized physical abuse. Violence functions as a normalized productivity enforcement tool explicitly tied to fraud quotas and rule compliance within scam-driven trafficking operations. Multiple first-person accounts described punishment regimes where survivors face systematic physical abuse for failing to meet performance targets, with one post stating (P-0gV) *"if you miss targets you are shocked and beaten."* A post by a self-proclaimed victim in diary-like format documented mass punishment and shaming exercises involving *"frog jump"* drills with *"over a hundred people"* and brutal punishment of two young escapees (aged 14 and 17), with the 14-year-old electrocuted on the forehead and ear *"for nearly a minute"* before confinement in a coffin-sized *"black room."* Seemingly innocent phrases like *"eating popsicles"* and *"drinking bubble tea"* mask descriptions of brutal torture methods involving dismemberment and violence (P-5Ig).

The psychological impact manifests through behavioral conditioning, as evidenced by a 17-year-old victim who *"developed the habit of immediately lying face down with buttocks raised in preparation for beating upon waking each morning,"* demonstrating how physical control transforms victims from resistance to resignation (*"Since I'm already here, I might as well just do the job")* (P-0gV). Prolonged work hours requiring 700–800 scam calls per day create physical and psychological burnout, pushing victims from initial resistance toward resigned compliance.

Psychological manipulation by exploiting cultural values and drugs. Our analysis reveals how perpetrators exploit cultural values and create dependency to maintain victim compliance. As one pro-claimed survivor (P-uY1) states: *"She deceived all the agents by saying they were her younger brothers, saying how could her sister treat you badly . . . carefully look at those who follow her, one by one either taking drugs or becoming inhuman and ghostlike, or mentally unclear."* This false familial manipulation of perpetrators positioning themselves as elder siblings exploits the Chinese Confucian principle of filial piety and fraternal duty [81] that positions older siblings as figure deserving respect and obedience from younger family members, making resistance feel like a betrayal of core cultural values. This also exploits victims' need for protection in isolated environments while undermining their autonomy through drug dependency and psychological destabilization. Posts showed that victims eventually exhibit *"willingness to give money to traffickers"* (P-th4) and resist rescue attempts after prolonged conditioning. Perpetrators additionally use drugs to enhance psychological manipulation and ensure compliance, through forced consumption of *"happy water with drugs," "drugged water,"* or Ketamine (P-w9M).

Self-sustained compound facility for isolation and control. Our analysis further reveals survivors or insiders describing how the scam compound facilities enable isolation and control. Some survivors described the scam compound as *"prison-like"* with constant surveillance and degrading conditions, such as *"sleeping on bare wooden boards . . . with cameras in the toilets and showers under 24/7 surveillance, leaving us no privacy at all"* (P-f90). The long-term effect is a *"zombified"* workforce that has little energy left to resist. In contrast to the harsh work conditions, some users depicted compounds as self-contained cities with victims describing *"Compounds features casinos, KTV, entertainment centers, banks, supermarkets, everything is available"* (P-Gy2), which allows victims to slowly become accustomed to their captivity. One post provided an insider perspective on their lives as a contracted scam worker: *"the bonus I received was not much. I earned money from the compound and spent it in the compound, leaving nothing to take home"* (P-K2M).

4.3 RQ3: Post-Trafficking and Reintegration

Below we analyze the barriers people face when escaping from the scam compounds and reintegrating into their normal lives.

Post-Trafficking Outcomes. Our analysis reveals a complex landscape of post-trafficking outcomes, ranging from successful escape and rescue to abandonment, re-trafficking, and death. For those who return, the path to reintegration is fraught with significant medical, legal, and social challenges.

Desperation in escape. Escape attempts represent an act of desperation and victims' final chance for survival. Some victims resort to severe self-harm, as documented by an awareness spreader: *"some are willing to break their hands and feet to jump from buildings to escape"* (P-7TG), while others sent desperate social media pleas for help: *"This is my only chance to send a distress signal, perhaps also the last time, please save us"* (P-J3T). However, even successful escapes often lead to recapture as one escapee *"was sold by locals to local armed forces,"* while recaptured face even more brutal punishment as a deliberate deterrent, including being *"beaten unconscious multiple times per day and having boiling water poured on them"* (P-C1C).

Abandonment, being re-trafficked and death under extreme pressure. Our analysis reveals how perpetrators dispose of victims who become unprofitable or lack useful skills. One post stated, *"If you're illiterate or can't type, they'll just beat you up and dump you on the roadside to fend for yourself"* (P-K2M). However, escape or release does not guarantee freedom, as many survivors face re-trafficking to other compounds: *"I was sold by human traffickers to the Myawaddy fraud park, where I was sold more than ten times"* (P-E9y). Others documented the extreme working conditions of *"17–18 hours of forced work per day with corporal punishment"* that left victims *"dying like slaves"* (P-J3T), while others die from *"exhausted to death by the high pressure"* (P-7aC), overwork, or *"Beaten to death, tortured to death, and even committed suicide"* (P-C1C).

Coordination with institutional rescue and public support. RedNote users documented how institutional rescue efforts achieved notable success through international coordination, yet face significant barriers. Interventions often involve coordinated police, where *"Thai authorities are coordinating with the Chinese embassy in Thailand"* (P-v68), diplomatic channels, and family advocacy. Successful cases often involve multi-national cooperation, as documented when *"Thai police successfully arrested one of the suspects... Thai authorities are coordinating with the Chinese Embassy in Thailand to send the victim back to China"* (P-v68).

Several families shared detailed information, including departure timeline and locations, with some publicly expressing willingness to pay for ransom (P-9zh): *"younger sister was trafficked to Myawaddy on September 15...I hope the company that has her won't beat or scold her. Please just confirm your safety; compensation is negotiable."* However, failures may occur due to victim non-cooperation, as in one case where, despite *"cooperation of police from two countries, [they] finally found the child at Myanmar customs, but he seemed to have been brainwashed... unwilling to contact parents and friends"* (P-th4), demonstrating how psychological manipulation can undermine successful interventions. Furthermore, rescue effectiveness varies significantly by survivors' choice, with many opting for personal networks (through WeChat) over authorities. This is evidenced in a news report where victims *"did not choose to call police"* but rather *"sought help from friends through WeChat."* Reports indicate that survivors who escaped suffer serious psychological damage and distrust outsiders, with some choosing silence over reporting due to death threats from perpetrators and concerns about collusion in the rescue teams (P-Zj0).

Active presence of grassroots rescue teams. Beyond formal law enforcement channels, our analysis highlights the emergence of grassroots rescue networks operating through RedNote. These self-proclaimed *"anti-trafficking rescue teams"* actively advertise service timelines such as *"response times as fast as '20 minutes' for driver deployment"* and *"will act within 48 hours and rescue within 3 days"* (P-H7j, P-UU2). To further establish credibility, some agree to authenticate via trusted intermediaries, e.g., *"Cap Uncle (帽子叔叔, slang referring to the police)"* (P-F2H, P-9zh, and P-e9F) as well as signing formal *"service agreements"* (P-1nS) with families. These teams offer detailed accounts of past successful rescue cases and rescue procedures, including border-crossing logistics and administrative processes; for example, descriptions of Thai immigration procedures such as *"Mae Sot Immigration Bureau, detention 20–30 days, 55,000 baht for expedited processing"* suggest insider or experiential knowledge (P-3jU). They actively post advice by warning against contacting local police in compromised jurisdictions and warn *"locals get $3000 rewards for returning escaped victims to compounds"* (P-m6R, P-D2Y) and instead recommend hiding first, then coordinated outreach to embassies and vetted rescue teams.

Family responses to grassroots teams are mixed. While some treated them as vital lifelines, others rejected their help outright. In one case (P-UU2), a volunteer recounted contacting a mother about her son in Cambodia who refused to provide help because they viewed the victim as a burden or as unfilial, saying he had *"spent a lot of the family's resources [money]... and thrown the household into complete disorder,"* and concluded, *"there is no more money left to save him, so we will just stop caring about him."* Finally, not all grassroots rescues succeed. Failed rescues were thwarted by armed perpetrators, with the rescue team saying *"We did all we could... unless something unexpected happened, the person is already [back] inside the mountain compound"* (P-yY6).

Legal proceedings. RedNote posts show how official narratives frame (voluntary surrender) as the only path to leniency under an expanding legal crackdown. Users actively relayed such warnings that *"from May 1 onwards, all individuals engaged in overseas telecom fraud—whether voluntary or coerced—will be punished under the new law. Only those who surrender to public security may receive mitigation or exemption"* (P-3fm). These announcements were reinforced by posts citing state media reports that *"44,000 suspects have been transferred back, including 171 ringleaders"* (P-x9a). The user also recounted stories of returnees who, after being rescued through family payments, later chose to turn themselves in out of conscience. These accounts suggest that survivors and families view the legal environment as highly punitive and are unsure whether coerced participants will be treated as offenders or as victims, shaping their decisions about escape, reporting, and surrender.

4.3.1 Reintegration. Survivors experience trauma when recovering from trafficking experiences, however, some still face family and social pressure.

Trauma and prolonged recovery. Our analysis of reintegration challenges reveals how trafficking survivors face long-term complex recovery. Medical supervision becomes necessary for many victims, as documented in one case where a 17-year-old survivor *"had been tortured to mental breakdown, even his basic walking posture was abnormal ... Every morning when he woke up, he would lie down with his buttocks raised in preparation for being beaten"* (P-YP8). This example showcases how trafficking trauma manifests through conditioned behavioral responses that require extensive psychological intervention. Compulsory rehabilitation becomes necessary for victims forced into drug dependency during captivity. One account describes how a victim was *"forced to consume drugs 'K powder' ... She will face compulsory drug rehabilitation and psychiatric treatment"* (P-c0o), where the control mechanisms imposed during trafficking create long-term barriers to recovery.

Family roles in reintegration and social expectation. Survivors who returned home may face intensive and compulsory treatments. In one case (P-c0o), the survivor required compulsory drug rehabilitation and psychiatric care after months of violence and forced drug use in Cambodia. Recovery depended heavily on *"requires her family's ongoing care and support."* Some families implemented strict surveillance of rescued victims as they are *"constantly watched by parents, confined at home and not allowed to go out"* (P-th4), reflecting deep mistrust after what the victim has been through. Beyond immediate family dynamics, survivors also needed to deal with judgment from the wider social circles and online communities. As one user commented on a successful rescue (P-wy1): *"I hope she learns her lesson and goes on to live smoothly in the future,"* reintegration is often framed not only as recovery but also as a moral correction.

4.4 RQ4: Protective Strategies

RedNote users have developed protective strategies that emerge from collective trauma and transformed individual experiences into community wisdom. Our analysis identifies four main themes in users' proposed protective strategies, ranging from self-defense to navigating institutional responses and support.

4.4.1 Self-defense. RedNote users have recognized several opportunities and the critical intervention windows to defend themselves and avoid subsequent harms, especially in the early stages of scamming and recruitment.

Early assessment and trusted contact for different demographics. RedNote users offered tips for people from different backgrounds to self-assess the risks in a potential scam. For individuals seeking overseas employment opportunities, users noticed several red flags in job ads, including *"high pay for minimal work," "all-expenses-paid round-trip tickets," "only reveal location after you arrive,"* and *"boast extensively but won't show you company videos or photos"* (P-1Jy), *"temporary flight adjustments"* (P-5XF), movements through specific high-risk routes that bypasses official checkpoints such as *"Mae Sot and Tak in Thailand toward Myawaddy in Myanmar"* (P-3jU), and requirements to *"bring China-issued bank cards abroad"* (P-Y9s). Rather than suggesting turning down all potential opportunities, users highlighted actionable verification steps, including confirming company legal registration, demanding authentic labor contracts and proper work visas, and rejecting offers requiring *"tourist visas"* or vague *"training/team-building"* arrangements (P-5XF).

When users posted warnings to raise awareness, we observed different strategies depending on the target audience's gender. Posts targeting women commonly use hashtags such as #girlsmustsee, #femalesafety, and #GirlsTalk, creating dedicated channels for delivering warnings to female users (P-F2d). Users shared specific suggestions for female users against grooming or romantic scams, which may gradually steer victims towards sex trafficking and forced participation in *"client services"* on scam campuses such as Myawaddy. Protective strategies for women emphasize maintaining communication independence: retaining phone access and location services, as well as avoiding *"solo meetings"* and *"free trips."* By contrast, warnings involving men rarely employ demographic-specific hashtags, instead relying on generic employment-fraud warnings or highlighting extreme physical torture, forced labor, and organ trade (P-OI6).

International students are highlighted as another vulnerable group. RedNote users emphasized protective strategies specific to the student context, including maintaining skepticism toward unsolicited contact from strangers, avoiding any money transfer requests regardless of the claimed authority source, and ensuring regular communication with family members. The community particularly warned against schemes involving *"embassy, online shopping, relatives borrowing money, online gambling, online pornography"* (P-0gV) as common tactics used to target international students who may be more vulnerable due to their distance from family support systems. All these early intervention strategies highlight the need to build a reliable support network which may involve family members and friends, with whom one can share detailed itineraries and emergency contacts: *"report your itinerary to family and friends, letting them know your whereabouts"* prior to a job visit (P-E3U); or trusted college staff who can help verify the legitimacy of international financial transactions. Additionally, it is crucial to maintain stable communication channels and regular check-ins, even using *"code words"* such as *"My brother died in northern Myanmar"* which, as noted in P-9og, *"some rescue teams can recognize."*

Self-preparation for escape and rescue. Although the ideal timing to mitigate further human trafficking risks is prior to a foreign travel, RedNote users still identified several opportunities that increase the chances of escaping or being rescued by collecting evidence and establishing communication channels. First, the *"waystations"* such as farms, barracks, or private houses where survivors are detained during transportation present chances for survivors to (P-L8z) *"record vehicle license plates and driver details upon boarding"*. This information may serve as evidence that enables upstream arrests and facilitates negotiated release. Additionally, users also emphasized the practical considerations of installing Google Maps for location tracking as *"domestic Chinese navigation services become unreliable abroad"* (P-Y9s).

For individuals already trapped within trafficking compounds, RedNote users provided detailed intelligence-gathering protocols to facilitate rescue operations. Critical information includes *"compound names, company operational codes, specific building and room numbers, identification documentation, precise geolocation coordinates, and recent photographs"* (P-H1K). Users also documented creative escape strategies from successful escape experiences, including exploiting *"medical emergencies excuse"* (P-T1T) as opportunities to leave compounds under supervision. However, community guidance strongly advises against pre-payment and recommends insisting on *"simultaneous person-for-payment exchanges"* when negotiation becomes unavoidable. This reflects hard-learned lessons from cases where advance payments resulted in continued captivity or transfer to additional criminal networks.

4.4.2 Institutional support. Although RedNote users recognized the complication in receiving institutional support internationally, they expressed their expectation for more precise accountability measures.

Complexity in cross-border cooperation. RedNote users recounted experiences with multiple institutional stakeholders in rescues, highlighting both their contributions and the difficulties of cross-border coordination. Chinese embassies play a key role in victim verification and arranging rescues, often credited with *"coordinating with local police to take my brother safely across the border"* (P-L1M), or with Thai immigration police in joint rescues of Chinese victims (P-v3S). P-U6m demonstrates how families were advised to *"contact the embassy immediately — embassy staff will arrange personnel to help find and confirm victim safety."* Embassy personnel coordinate complex rescue operations across multiple jurisdictions, as described in one case where embassy staff *"arranged a contact to visit my brother [victim] and allowed me to video call him, confirming their location was safe"* (P-U6m). However, the diplomatic process requires navigating complex international relationships and local corruption challenges.

Thai immigration authorities manage detention and processing systems that differentiate based on victims' documentation status. P-3jU details how victims with valid passports are *"transferred to Thailand's Mae Sot Immigration Bureau, detained 20–30 days (can pay 55,000 baht for expedited processing), then transferred to the Bangkok Immigration Bureau"* and extended detention periods for victims without valid passports. The immigration system offers expedited processing options, but at substantial financial cost, including *"1,200 baht for family contact, ticket money, prison hygiene fees, escort fees, and expedited fees (20,000 baht)."* Police agencies provide the formal reporting mechanism and coordinate with international partners. However, their effectiveness varies significantly

across jurisdictions. A victim's relative recounted that domestic police often have limited authority in cross-border cases, with officers stating *"we have no law enforcement or investigative authority"* and advised to contact the Wa State police in Myanmar (P-u9F). The Wa State police then required a formal request letter from the Chinese public security authorities before taking any action. Families are required to navigate multiple institutions with overlapping but constrained responsibilities.

Calls for more precise accountability measures. User attitudes reveal growing frustrations with genuine victim authenticity. P-Z2A claims that *"about 90% are not real victims but participate in overseas fraud activities."* This skepticism has led to calls for preventative accountability measures, with users demanding *"passport blacklisting for rescued survivors for at least three years as a lesson to prevent recurrence"* (P-Z2A). Such proposals reflect the community's desire for stricter enforcement mechanisms that would deter voluntary participation in overseas fraud operations. Institutional support relies on coordination between embassies, police, immigration authorities, and legal advocates, each offering essential but limited services within their jurisdictions. While these institutions enable successful rescues and legal protections, the multi-stakeholder system creates bureaucratic delays and mixed rescue outcomes. At the same time, community debates over victim authenticity advocate for stronger preventative measures. Nevertheless, P-VL5 illustrates a contrasting view from a defense lawyer that many survivors should be *"treated with leniency"* in lawsuits, because they *"had no malicious intent, and did no substantial work there."* They also noted unclarities and challenges in such lawsuits as *"many witnesses' testimonies were fake."*

4.4.3 Public exposure. We find that RedNote serves as a channel for people who have experienced scam-driven human trafficking, including self-proclaimed survivors or scam workers, to raise public awareness by exposing details in the ecosystem.

Survivor self-perception and exposure. Self-identified survivors revealed contested understandings of their roles in scam operations. Their self-perception is shaped by both evolving awareness through engagement in scam work and public moral judgment. Many initially viewed their work as legitimate employment and only realized the deception later. One post recounted that *"only then did she realize that the so-called high-paying job was actually a telecom fraud scheme"* (P-Gy2). Others knew from the outset that they were entering illicit work. One described themselves as a *"volunteer for this scam"* (P-uY1). To warn others, survivors strategically exposed recruitment tactics by sharing scammers' private communications. P-BN3 includes messages from *"a Cambodian scam company boss who wanted me to help recruit."* They positioned their testimony as cautionary advice to *"make those who want to pursue gold-digging or high-salary jobs abroad give up their dreams."* Under violence and surveillance, survivors adopted survival-focused mindsets. One stated *"Since I'm already here, I might as well just do the job"* (P-0gV) while observing coworkers becoming *"inhuman and ghostlike"* (P-uY1). At the same time, survivors recognized they are participating in fraud. One admitted *"If I say that those of us who depend on this industry are all not good people, I really have no way to refute that"* (P-uY1). Their voices include those who were deceived and now *"hate [themselves] for being too naive."* They also include those who *"voluntarily participated in fraud."*

Public reactions toward survivors' disclosure alternate between sympathy and condemnation. Some view survivors as purely coerced, while others view them as greedy or complicit. Some insisted *"No one can force you [survivors] to go if you don't want to."* Posts invoke *"perfect victim"* expectations and debate *"whether they [survivors] should be condemned."* This judgment produces self-censorship among survivors. One testimony preemptively requests *"hoping for no malicious criticism"* (P-3BQ). Survivors' self-understanding thus remains unstable. Altogether, survivors also view themselves as a hybrid of victims of coercion and perpetrators of fraud in response to public judgment.

Collective live updates. Victims, survivors, and rescue teams leverage RedNote to share live updates regarding individual status and the progress of rescue campaigns, extending beyond simple awareness posts. Victims trapped in scam compounds provide ongoing status reports about their situations to maintain a connection with the outside world and create digital evidence trails of their experiences. In one example, one self-identified victim said (P-tK4): *"if I don't post updates for a long while, that means I am close to death."* Beyond personal survival communications, victims and insiders provide detailed updates about compound activities such as enforcement deadlines, organizational changes, victim transfer patterns, punishment and location of execution. For example, a post shared that a local armed force will *"hand over a batch of around 3,000 dog pushers back to China through the Chinese and Thai cap uncles [the police] this year."* These updates serve both as warnings and as informal reporting channels, which enable families and rescue groups to verify compound activities, locate victims, and coordinate interventions. Taken together, RedNote users transform individual experiences into collective protective strategies, ranging from self-defense and escape preparation to survivor testimony and collective live updates. These practices strengthen vigilance, expand support networks, and serve as cautionary signals that help others avoid victimization.

5 Discussion

Here we present our key takeaways while situating our findings in the broader literature. Informed by our observations, we further discuss the tensions and opportunities for individuals, online platforms, and regulatory bodies to improve users' safety against scam-driven human trafficking.

5.1 Key Insights

In the following, we summarize how our key insights extend prior work. In particular, we discover four aspects that influence users' safety and the use of RedNote for exchanging support across multiple phases of scam and human-trafficking.

5.1.1 Exploited cultural obligations undermine survivors' safety and well-being from recruitment through reintegration. Although Chinese kinship ties motivate some family members of the trafficking victims to seek help online (§4.3), our analysis shows that these same cultural obligations based on kinship ties were exploited at every stage of the trafficking lifecycle—from recruitment to control

and reintegration—contrasting prior work that primarily highlights their positive roles in digital bounding and online safety [18, 53]. During recruitment, traffickers weaponize kinship ties as a recruitment channel and frame refusal as cultural betrayal (§4.1.1), extending beyond the generic social-tie recruitment strategies documented in prior research [52, 63]. These obligations thus become intentional vectors of exploitation. The exploitation continues during captivity, where cultural expectations reinforce power imbalances and enable psychological control within scam compounds (§4.2.1). Reintegration of survivors is further complicated by family rejection (§4.3.1), as families often interpret survivors' return as a need for moral correction rather than trauma recovery, akin to the "victim-offender" identity dynamics described in criminology research on scammers involved in human trafficking [116].

5.1.2 Targeted digital skills in recruitment for exploitation. We found that digital skills simultaneously increased vulnerability during recruitment and enabled exploitation within scam operations, yet also facilitated survivors' communication during captivity (§4.3). This aligns with prior observations [44, 63] that traffickers target digitally skilled workers, then repurpose those skills into forced cybercriminal labor [34, 41] (§4.2.1). Beyond individual-level vulnerabilities highlighted in prior work [52, 63, 64], our analysis reveals structural vulnerabilities: weak social safety nets, labor precarity, and mobility-driven instability, particularly for left-behind youth and other mobile populations, which create conditions traffickers exploit (§5.1.1). These findings suggest that technical skills alone do not guarantee online or offline safety awareness.

5.1.3 Community-based support in light of institutional gaps. Prior work on trafficking responses has largely emphasized institutional interventions [77, 111], while our findings reveal how RedNote users assemble bottom-up support systems in response to inadequacies in institutional governance. Coordinated interventions succeed sometimes, but they are often slowed by bureaucracy [28] or undermined when victims are uncertain whether they will face legal punishment or be recognized as victims (§4.3). This gap has pushed families toward RedNote for informal information channels and grassroots networks for rescue coordination and ransom verification—channels that offer rapid response times but lack institutional verification mechanisms (§4.4.2).

Beyond expanding recruitment reach across multiple platforms [52, 77], RedNote users raised awareness of how traffickers exploit blind spots in cross-border governance by moving victims between multiple Chinese and foreign platforms, making single-platform interventions insufficient (§4.1.2). They also recognized the inefficacy of Chinese communication apps in rescue coordination (§4.4.2). While prior research has examined testimonies of individual survivors [52], we showed how diverse RedNote users can collectively develop prevention strategies grounded in lived experiences (§4.4). Survivors shared firsthand accounts and "confession" as warnings to the community, and the community generated red-flag lists with hashtags tailored to specific demographics—especially women and younger adults, reflecting RedNote's dominant demographics [115]—and highlighted relevant self-defense strategies (§4.4.1).

5.1.4 Online visibility as double-edged sword in contested victimhood. Platform visibility enables crisis coordination but simultaneously exposes survivors to public judgment about their complicity in fraud. There are cases where users debated whether the survivor knowingly entered the scam work (§4.1.2), perceiving them as "victim-offenders" [64, 116]. Survivors must therefore reconcile their own victimization with the harm they caused under coercion, leading many to self-censor preemptively out of fear of judgment. This dynamic contrasts sharply with online community support for unambiguous victims, such as sexual-assault survivors [84], where disclosure is more likely to evoke empathy than accusations of criminality.

At the same time, survivors depend on visibility to seek help, posting distress signals and urgent pleas on RedNote. However, the shifting discourse among RedNote users—including slang repurposed from historically discriminatory terms for Chinese immigrant workers [99]—can re-traumatize survivors (§4.2.1). Platform visibility also amplifies government warnings by framing voluntary surrender as the only path to leniency (§4.3), potentially deterring escape efforts. Our analysis confirms that escape carries severe risks, including abandonment, re-trafficking, or even death [52, 64, 94, 109] (§4.3), and survivors often face long-term trauma treatment. Fear of judgment and uncertainty about legal consequences thus prevents many from seeking help, compounding the harms they have already endured.

5.2 Implications

Based on our findings, we present the key implications of our work, including tensions that hinder the systematic resolution of scam-driven human trafficking as well as potential venues to mediate these tensions.

5.2.1 Structural vulnerability in the labor market. The recruitment targets of scam-driven trafficking reflect broader structural vulnerabilities that extend beyond individual risk factors. China's rapid economic development and high penetration rate of Internet services have fostered a massive population of digitally literate people, while widespread digital platform adoption has outpaced safety awareness and protective literacy [16]. Furthermore, geo-political tensions and the COVID-19 pandemic slowed down economic growth and introduced risks in global trade, exacerbating financial pressure and labor surplus on individuals, including skilled workers since 2018 [2, 68]. Some populations, including left-behind children and unemployed youth identified in our findings (§4.1.1), still lack access to appropriate support networks and social protections due to urban-rural disparities [43]. Meanwhile, geopolitical shifts in Southeast Asia and the transformation of traditional criminal and drug economies have created new opportunities for traffickers [44], creating a vacuum that pulls individuals into recruitment scams. Despite joint efforts between the Chinese government and several affected Southeast Asia countries [36], the threats posed by scam-driven human trafficking are challenging to eradicate due to the complicated economic and geopolitical factors. Rather than relying on technical solutions, which often fall short in the face of such a significant sociotechnical challenge, our recommendations focus on how to better mitigate scams, provide support to survivors, and minimize harms during recovery.

5.2.2 Building culturally and socially informed digital safenets. Our findings reveal the tensions arising from the Chinese social codes and values, which make survivors' families and close contacts a primary coordinator of rescue operations (§4.3.1), but it can also be leveraged as a vulnerability in spreading recruitment scams and manipulating survivors (§4.1.1) or slow down survivor reintegration (§4.3.1). These tensions highlight the need to build a safe and trustworthy support network against scam-driven human trafficking, leveraging the Chinese cultural values positively and accommodating the diverse backgrounds of Internet users. One opportunity is to align online safety literacy and education with China's recent push for "digital technology-empowered grassroots governance" [57], which mobilizes local resources and personnel to provide timely digital support, including in rural communities. We argue for strengthening "grassroots governance" for online safety by engaging trusted community figures in awareness campaigns and family counseling [117]. Grassroots initiatives could also adapt proven models such as tech clinics for intimate partner violence survivors in the Western context [29, 32] and anonymous legal helplines [37] that help victims and families navigate the legal complications. To support people in remote regions and those working abroad, social media platforms could facilitate the promotion of relevant clinical and counseling services.

Furthermore, we hypothesize that individuals vulnerable to scam-driven human trafficking, such as left-behind children, are digitally connected yet remain isolated from positive emotional bonds (§4.1.1). Such bonds are critical for both preventing recruitment scams and supporting reintegration. Future research could therefore examine the role of culturally informed AI personas as a key component in the safenet, which have shown strong potential for strengthening the digital connections of Chinese users [53, 114]. In particular, personified AI agents that highlight social connection and integration beyond individual agency preferred by Chinese users [25, 104] may be capable of providing timely emotional support, safety guidance, and other resources tailored to under-resourced communities. More importantly, we argue that such agents should contribute to mediating kinship relationships within Chinese families rather than merely regulating users' unsafe behaviors. Overemphasis on discipline risks reinforcing power imbalances grounded in filial piety [18], escalating family tensions, provoking rebellious unsafe online behaviors against Confucian values [87], and ultimately increasing susceptibility to scam and human trafficking risks (§5.1.1). Nevertheless, deploying AI agents with vulnerable populations requires careful mitigation of potential harm, including privacy risks, over-reliance on AI for critical safety decisions and exploitation by malicious actors [121].

5.2.3 Improving content recommendation and moderation for safety protection on social media. RedNote hosts a complex ecosystem where warnings, survivor testimonies, grassroots rescue operations, and potentially fraudulent services coexist. Despite considerable efforts to detect and moderate online fraud with law enforcement [82], our findings show that support information still requires verification to mitigate misinformation and re-traumatization risks. This calls for advances in the application of trauma-informed computing [9] for content recommendation and moderation systems, by incorporating the cultural and social contexts of scam-driven human-trafficking with foregrounded safety, trust, and survivor agency. First, a key challenge concerns verifying grassroots rescue teams (§4.3), which requires collaboration with law enforcement. Second, the success of RedNote's AI-driven scam detection, which intercepted 94.3% of scam behaviors using over 100 recognition models and reduced user scam reports by 60% [82], suggests a pathway to extending these tools for scrutinizing support information moderation.

Nevertheless, like many other social media platforms, RedNote's recommendation and moderation systems remain opaque [91]. This opacity and often "over-sensitive" moderation lead marginalized users to develop their folk theories [65, 115] and adopt coded phrases and repurpose hashtags to evade detection, conceptualized as "algorithmic resistance" [22] (§4.2.2). Moreover, moderation tools risk being weaponized by malicious actors [92] and adding pressure on survivors who are already navigating moral debates (§4.4.2). Trafficking-related content poses further moderation challenges due to the contested victimhood. Unlike hate speech, which can often be addressed through standard moderation policies [131], harmful discourses questioning survivors' deservingness may go unreported and unmoderated because of self-censorship and moral conflict (§4.4.3). We argue that platforms should shift from passive hosting to active support. They could, for instance, provide tailored, explainable feedback to post authors to improve transparency while maintaining content quality [45]. Platforms could also deepen collaboration with community experts and leverage existing anti-scam campaigns and volunteer networks [27]. These efforts could enhance the precision of moderation, better leveraging human insights with automated moderation tools, and improve the inclusivity and timeliness of online safety content, for example, by highlighting contributions from certified grassroots advocates (§4.3) and by offering users dedicated categorization and persistent archives for useful posts (§4.4.1).

5.2.4 Overcoming technical barriers in overseas rescue. The current preventive technologies that the Chinese law enforcement deploys focus on domestic network traffic monitoring, blacklisting suspicious applications, and client-side detection and reporting through the *"National Anti-Fraud Center"* app [39]. The app was launched in March 2021 by the Ministry of Public Security (China) and is used to detect suspicious calls, messages, and apps, issue warnings, allow users to report fraud, and push prevention content. However, the installation of the "National Anti-Fraud Center" app is voluntary [135], and it sees a lack of motivation for potential targets to install it. Additionally, the anti-fraud app, along with other domestic Chinese digital services (e.g., navigation apps), falls short in integrating localized knowledge overseas that is useful in early awareness as well as rescue [17]. Law enforcement could consider leveraging trusted local third parties, such as the overseas business associations [66], in efforts to build and manage online platforms and communication channels, balancing timeliness of responses and trustworthiness of support.

5.3 Future Work

This study points to several directions for future research. First, while our analysis centers on user narratives on RedNote, future work can examine the *recruitment platforms* themselves. We did not

find substantial active evidence that human-trafficking recruitment scams occur through RedNote posts; instead, users primarily use the platform to exchange support. This likely reflects RedNote's strict moderation policies and anti-scam campaigns [10]. However, RedNote users reported encountering scam activities on short-video platforms such as Kuaishou and Douyin (§4.1.2) or via messaging channels (§4.1.2). These observations motivate future investigations into the real-world effectiveness of content moderation and anti-scam interventions across platforms.

Second, future research could evaluate and strengthen *automated detection methods* for scam content to mitigate human trafficking risks, including LLM-based approaches, with particular attention to multi-modal scam contents, evolving scam tactics, and cross-platform scam operations (§4.1.2). Such work must address technical challenges including human–LLM collaboration for scam prevention and reporting [38], the loss of contextual information during platform transitions (§4.1.2), and privacy-preserving detection techniques such as on-device models [118] or homomorphic encryption [46].

Third, future work could track how the *global landscape of scam-driven trafficking* shifts geographically and adapts to anti-scam campaigns and regulatory changes. Cross-platform analyses (e.g., Weibo, Douyin, Facebook, and Telegram) would show how recruitment strategies and resistance narratives unfold under different platform affordances and governance structures. Comparative work across Western, Southeast Asian, and Chinese contexts would further clarify how social, cultural, and technical factors shape the scam and human-trafficking ecosystem, particularly as cross-border scam-driven trafficking expands into Western regions.

Finally, future work could examine how *responsibility is distributed among stakeholders*, including social media platforms, international organizations, and governments, and develop models that support cross-border, multi-stakeholder collaboration. While RedNote's close cooperation with Chinese law enforcement is notable, such frameworks may not generalize to other national contexts. Research should therefore explore alternative support infrastructures (e.g., anti-scam apps, NGO portals, platform reporting tools) tailored to different governance and deployment settings.

6 Conclusion

This study represents the first systematic analysis of scam-driven human trafficking discourse on Chinese social media, examining 158 RedNote posts to understand how users collectively interpret and respond to this emerging form of exploitation. Through qualitative content analysis of recruitment tactics, exploitation mechanisms, reintegration challenges, and protective strategies, we demonstrate how digital communities serve as critical sites for trafficking knowledge construction, survivor testimony, and grassroots resistance efforts. The research reveals important tensions between cultural dynamics that both enable trafficking and complicate survivor support, highlighting opportunities for culturally informed interventions in prevention, platform governance, and cross-border coordination. This research establishes a foundational understanding of how digital communities respond to emerging trafficking forms and identifies opportunities for culturally informed interventions that strengthen prevention efforts, survivor support networks, and cross-border institutional coordination building on existing anti-trafficking frameworks.

Acknowledgments

We thank Tj Elmas and anonymous reviewers for their helpful feedback. We acknowledge support from the Centre for Doctoral Training in Machine Learning Systems at the University of Edinburgh. The research is partially funded by the Deutsche Forschungsgemeinschaft (DFG, German Research Foundation) under Germany's Excellence Strategy – EXC 2092 CASA – 390781972 and by Google through the Google Academic Research Award on Trust and Safety (2024; ID 00029925). We used a generative AI service, ChatGPT, to assist with light language and style polishing.

References

[1] Carmen Aguilar García, Sarah Marsh, and Philip McMahon. 2024. Chinese Network Behind One of World's 'Largest Online Scams'. News reports, The Guardian. https://www.theguardian.com/money/article/2024/may/08/chinese-network-behind-one-of-worlds-largest-online-scams

[2] George Alessandria, Shafaat Yar Khan, Armen Khederlarian, Kim J Ruhl, and Joseph B Steinberg. 2025. Trade war and peace: US-China trade and tariff risk from 2015–2050. *Journal of International Economics* 155 (2025), 104066. doi:10.1016/j.jinteco.2025.104066

[3] Mutahar Ali, Arjun Arunasalam, and Habiba Farrukh. 2025. Understanding Users' Security and Privacy Concerns and Attitudes Towards Conversational AI Platforms. In *Proceedings of the 2025 IEEE Symposium on Security and Privacy*. IEEE, 298–316. doi:10.1109/SP61157.2025.00241

[4] Shiza Ali, Afsaneh Razi, Seunghyun Kim, Ashwaq Alsoubai, Joshua Gracie, Munmun De Choudhury, Pamela J. Wisniewski, and Gianluca Stringhini. 2022. Understanding the Digital Lives of Youth: Analyzing Media Shared within Safe versus Unsafe Private Conversations on Instagram. In *Proceedings of the 2022 CHI Conference on Human Factors in Computing Systems*. ACM, Article 148, 14 pages. doi:10.1145/3491102.3501969

[5] BBC News 中文. 2025. 中国演员经泰国落入缅甸诈骗窝点获救后：网民促当局展开更多救援 / After Chinese actor being rescued who fell into hands of Cambodian defraudsters via Thailand: Netizens urged the authorities to rescue more. https://www.bbc.com/zhongwen/articles/c9d51p355jdo/simp

[6] Rosanna Bellini, Emily Tseng, Nora McDonald, Rachel Greenstadt, Damon McCoy, Thomas Ristenpart, and Nicola Dell. 2021. "So-called privacy breeds evil": Narrative Justifications for Intimate Partner Surveillance in Online Forums. *Proceedings of the ACM on Human-Computer Interaction* 4, CSCW3, Article 210 (2021), 27 pages. doi:10.1145/3432909

[7] Virginia Braun and Victoria Clarke. 2019. Reflecting on reflexive thematic analysis. *Qualitative Research in Sport, Exercise and Health* 11, 4 (2019), 589–597. doi:10.1080/2159676X.2019.1628806

[8] Ann Cao. 2025. Alibaba teams up with social media platform RedNote in fresh e-commerce push — scmp.com. News. https://www.scmp.com/tech/big-tech/article/3309414/alibaba-collaborates-social-media-platform-rednote-fresh-domestic-e-commerce-push

[9] Janet X. Chen, Allison McDonald, Yixin Zou, Emily Tseng, Kevin A. Roundy, Acar Tamersoy, Florian Schaub, Thomas Ristenpart, and Nicola Dell. 2022. Trauma-Informed Computing: Towards Safer Technology Experiences for All. In *Proceedings of the 2022 CHI Conference on Human Factors in Computing Systems*. ACM, Article 544, 20 pages. doi:10.1145/3491102.3517475

[10] Wenyue Chen. 2025. The Impact of Evolving Regulatory Policies on Content Strategies: A Case Study of Xiaohongshu (Red Note) Bloggers. *Academic Journal of Management and Social Sciences* 11, 3 (2025), 60–63. https://drpress.org/ojs/index.php/ajmss/article/view/31250/30601

[11] Xiao-Ping Chen and Chao C. Chen. 2004. On the Intricacies of the Chinese Guanxi: A Process Model of Guanxi Development. *Asia Pacific Journal of Management* 21, 3 (2004), 305–324. doi:10.1023/B:APJM.0000036465.19102.d5

[12] Yanyu Chen. 2024. Moving Bricks: Money-Laundering Practices in the Online Scam Industry. *Global China Pulse* 3, 1 (2024), 105–114. https://globalchinapulse.net/moving-bricks-money-laundering-practices-in-the-online-scam-industry

[13] Allen Chun, John Clammer, Patricia Ebrey, David Faure, Stephan Feuchtwang, Ying-Kuei Huang, P. Steven Sangren, and Mayfair Yang. 1996. The Lineage-Village Complex in Southeastern China: A Long Footnote in the Anthropology of Kinship [and Comments and Reply]. *Current Anthropology* 37, 3 (1996), 429–450. https://www.jstor.org/stable/2744542

[14] Eleanor Cockbain and Kate Bowers. 2019. Human trafficking for sex, labour and domestic servitude: how do key trafficking types compare and what are their

predictors? *Crime, Law and Social Change* 72, 1 (2019), 9–34. doi:10.1007/s10611-019-09836-7

[15] Juliet Corbin and Anselm Strauss. 2008. *Basics of Qualitative Research (3rd ed.): Techniques and Procedures for Developing Grounded Theory.* Sage Publications. doi:10.4135/9781452230153

[16] Rogier Creemers. 2022. China's emerging data protection framework. *Journal of Cybersecurity* 8, 1, Article tyac011 (2022), 12 pages. doi:10.1093/cybsec/tyac011

[17] Zhang De-tian, Wang Jia-ao, and Chen Fei. 2017. A comprehensive study of mapping services in China. *Journal of East China Normal University (Natural Science)* 2017, 6 (2017), 85. doi:10.3969/j.issn.1000-5641.2017.06.008

[18] Yue Deng, Changyang He, Yixin Zou, and Bo Li. 2025. "Auntie, Please Don't Fall for Those Smooth Talkers": How Chinese Younger Family Members Safeguard Seniors from Online Fraud. In *Proceedings of the 2025 CHI Conference on Human Factors in Computing Systems*. ACM, Article 864, 17 pages. doi:10.1145/3706598.3714137

[19] Rachna Dhamija, J. Doug Tygar, and Marti Hearst. 2006. Why Phishing Works. In *Proceedings of the 2006 SIGCHI Conference on Human Factors in Computing Systems*. ACM, 581–590. doi:10.1145/1124772.1124861

[20] Julie S Downs, Mandy Holbrook, and Lorrie Faith Cranor. 2007. Behavioral Response to Phishing Risk. In *Proceedings of the Anti-Phishing Working Groups 2nd Annual eCrime Researchers Summit*. ACM, 37–44. doi:10.1145/1299015.1299019

[21] Serge Egelman, Lorrie Faith Cranor, and Jason Hong. 2008. You've Been Warned: An Empirical Study of the Effectiveness of Web Browser Phishing Warnings. In *Proceedings of the 2008 SIGCHI Conference on Human Factors in Computing Systems*. ACM, 1065–1074. doi:10.1145/1357054.1357219

[22] Houda Elmimouni, Sarah Rüller, Konstantin Aal, Yarden Skop, Norah Abokhodair, Volker Wulf, and Peter Tolmie. 2025. Exploring Algorithmic Resistance: Responses to Social Media Censorship in Activism. *Proceedings of the ACM on Human-Computer Interaction* 9, CSCW2, Article CSCW072 (2025), 24 pages. doi:10.1145/3710970

[23] Hannah Feeney, Samantha Charm, and Jennifer Hardison Walters. 2024. *Evaluation of the National Human Trafficking Hotline: Evaluation Findings and Considerations for Future Practice.* Technical Report OPRE Brief 2024-106. Office of Planning, Research, and Evaluation, Administration for Children and Families, U.S. Department of Health and Human Services. https://acf.gov/opre/report/evaluation-national-human-trafficking-hotline-evaluation-findings-and-summary

[24] Ivan Franceschini, Ling Li, and Mark Bo. 2023. Compound Capitalism: A Political Economy of Southeast Asia's Online Scam Operations. *Critical Asian Studies* 55, 4 (2023), 575–603. doi:10.1080/14672715.2023.2268104

[25] Xiao Ge, Chunchen Xu, Daigo Misaki, Hazel Rose Markus, and Jeanne L. Tsai. 2024. How Culture Shapes What People Want From AI. In *Proceedings of the 2024 CHI Conference on Human Factors in Computing Systems*. ACM, Article 95, 15 pages. doi:10.1145/3613904.3642660

[26] General Office of the State Council of the People's Republic of China. 2021. 国务院办公厅关于印发中国反对拐卖人口行动计划（2021–2030年）的通知 / Notice of the General Office of the State Council on Issuing the China Action Plan Against Human Trafficking (2021–2030). State Council Gazette, Document No. 13 [2021] of the General Office. https://www.gov.cn/gongbao/content/2021/content_5609081.htm

[27] Global Anti-Scam Organization. 2022. Scam Victims Help | Global Anti Scam. https://www.globalantiscam.org/

[28] Laura Gómez-Mera. 2016. Regime complexity and global governance: The case of trafficking in persons. *European Journal of International Relations* 22, 3 (2016), 566–595. doi:10.1177/1354066115600226

[29] Naman Gupta, Kate Walsh, Sanchari Das, and Rahul Chatterjee. 2024. "I really just leaned on my community for support": Barriers, Challenges, and Coping Mechanisms Used by Survivors of Technology-Facilitated Abuse to Seek Social Support. In *Proceedings of the 33rd USENIX Security Symposium*. USENIX Association, 4981–4998. https://www.usenix.org/conference/usenixsecurity24/presentation/gupta

[30] Ling Han. 2019. New Technologies in Combating Child Trafficking in China: Opportunities and Challenges for Children's Rights. *Peace Human Rights Governance* 3, 3 (2019), 389–414. doi:10.14658/pupj-phrg-2019-3-5

[31] Heidi Hartikainen, Netta Iivari, and Marianne Kinnula. 2016. Should We Design for Control, Trust or Involvement? A Discourses Survey about Children's Online Safety. In *Proceedings of the 15th International Conference on Interaction Design and Children*. ACM, 367–378. doi:10.1145/2930674.2930680

[32] Sam Havron, Diana Freed, Rahul Chatterjee, Damon McCoy, Nicola Dell, and Thomas Ristenpart. 2019. Clinical Computer Security for Victims of Intimate Partner Violence. In *28th USENIX Security Symposium (USENIX Security 19)*. USENIX Association, 105–122. https://www.usenix.org/conference/usenixsecurity19/presentation/havron

[33] Shijing He, Chenkai Ma, Chi Zhang, Ruba Abu-Salma, and Jose Such. 2025. "Living-Alone Girls' Lives Matter": Exploring the Security and Safety Perceptions and Practices of Young Women Living Alone in China. In *Proceedings of the Extended Abstracts of the 2025 CHI Conference on Human Factors in Computing Systems*. ACM, Article 23, 8 pages. doi:10.1145/3706599.3719961

[34] Angie C. Henderson and Shea M. Rhodes. 2022. "Got Sold a Dream and It Turned into a Nightmare": The Victim-Offender Overlap in Commercial Sexual Exploitation. *Journal of Human Trafficking* 8, 1 (2022), 33–48. doi:10.1080/23322705.2021.2019530

[35] Claudine Anita Hingston and Danita Hingston. 2023. Human Trafficking: A Dark Side of the Cyberspace. In *Cybercrime and Challenges in South Africa*. Palgrave Macmillan, 177–192. doi:10.1007/978-981-99-3057-9_8

[36] Selina Ho, Xue Gong, and Carla P. Freeman. 2025. China's Interventions in 'Gray Special Economic Zones' in Southeast Asia's Borderlands. *Journal of Contemporary China* (2025), 17 pages. doi:10.1080/10670564.2025.2484205

[37] Joan Van Horn, Mara Eisenberg, Carol McNaughton Nicholls, Jules Mulder, Stephen Webster, Caroline Paskell, Ashley Brown, Jeantine Stam, Jane Kerr, and Natalie Jago. 2015. Stop It Now! A Pilot Study Into the Limits and Benefits of a Free Helpline Preventing Child Sexual Abuse. *Journal of Child Sexual Abuse* 24, 8 (2015), 853–872. doi:10.1080/10538712.2015.1088914

[38] Ismail Hossain, Sai Puppala, Md Jahangir Alam, and Sajedul Talukder. 2025. AI-in-the-Loop: Privacy Preserving Real-Time Scam Detection and Conversational Scambaiting by Leveraging LLMs and Federated Learning. Preprint, arXiv:2509.05362 [cs.CR]. doi:10.48550/arXiv.2509.05362

[39] Elles Houweling. 2021. Chinese 'anti-fraud centre' becomes most downloaded app. News report, Verdict. https://www.verdict.co.uk/news/chinese-anti-fraud-centre-becomes-most-downloaded-app/

[40] Ying Huang and Weishan Miao. 2024. Domesticating algorithms through data reflectivity and user reflexivity: The metaphor of Yanghao on Xiaohongshu (RED). *Convergence* 30, 6 (2024), 1959–1973. doi:10.1177/13548565241301146

[41] Humanity Research Consultancy. 2022. *HRC Briefing: Cyber Slavery in the Scamming Compounds.* Technical Report. Humanity Research Consultancy. https://www.humanity-consultancy.com/publications/hrc-briefing-cyber-slavery-in-the-scamming-compounds

[42] Humanity Research Consultancy. 2023. *HRC Briefing: Guidance on Responding to Victims in Forced Scam Labour.* Technical Report. Humanity Research Consultancy. https://www.humanity-consultancy.com/publications/hrc-briefing-guidance-on-responding-to-victims-in-forced-scam-labour

[43] Jason Hung, Jingying Chen, and O. Chen. 2025. The practice of social protection policies in China: a systematic review on how left-behind children's mental health can be optimised. *Perspectives in Public Health* 145, 4 (2025), 220–229. doi:10.1177/17579139231205491

[44] Sasha Jesperson, Henrik Alffram, Lisa Denney, and Pilar Domingo. 2023. *Trafficking for Forced Criminality: The Rise of Exploitation in Scam Centres in Southeast Asia.* ODI Thematic Brief. Overseas Development Institute (ODI), London, UK. https://odi.org/documents/8832/The_rise_of_exploitation_in_scam_centres_in_southeast_asia.pdf Produced in partnership with ASEAN-ACT and supported by the Australian Government Department of Foreign Affairs and Trade.

[45] Jialun Aaron Jiang, Peipei Nie, Jed R. Brubaker, and Casey Fiesler. 2023. A Trade-off-centered Framework of Content Moderation. *ACM Transactions on Computer-Human Interaction* 30, 1, Article 3 (2023), 34 pages. doi:10.1145/3534929

[46] Weizhao Jin, Yuhang Yao, Shanshan Han, Jiajun Gu, Carlee Joe-Wong, Srivatsan Ravi, Salman Avestimehr, and Chaoyang He. 2023. FedML-HE: An Efficient Homomorphic-Encryption-Based Privacy-Preserving Federated Learning System. Preprint, arXiv:2303.10837 [cs.LG]. doi:10.48550/arXiv.2303.10837

[47] Ye Jingzhong. 2011. Left-behind children: the social price of China's economic boom. *Journal of Peasant Studies* 38, 3 (2011), 613–650. doi:10.1080/03066150.2011.582946

[48] Kathleen Kim. 2010. The Coercion of Trafficked Workers. *Iowa Law Review* 96 (2010), 409–474. https://traffickingroundtable.org/wp-content/uploads/2013/09/The-Coercion-of-Trafficked-Workers.pdf

[49] Edward R. Kleemans and Monika Smit. 2014. Human Smuggling, Human Trafficking, and Exploitation in the Sex Industry. In *The Oxford Handbook of Organized Crime*, Letizia Paoli (Ed.). Oxford University Press, Oxford, 381–401. doi:10.1093/oxfordhb/9780199730445.013.011

[50] Yubo Kou, Xinning Gui, Yunan Chen, and Kathleen Pine. 2017. Conspiracy Talk on Social Media: Collective Sensemaking during a Public Health Crisis. *Proceedings of the ACM on Human-Computer Interaction* 1, CSCW, Article 61 (2017), 21 pages. doi:10.1145/3134696

[51] Mark Latonero. 2012. Technology and Human Trafficking: The Rise of Mobile and the Diffusion of Technology-Facilitated Trafficking. Preprint, SSRN 2177556. doi:10.2139/ssrn.2177556

[52] Suleman Lazarus, Mina Chiang, and Mark Button. 2025. Assessing Human Trafficking and Cybercrime Intersections Through Survivor Narratives. *Deviant Behavior* (2025), 18 pages. doi:10.1080/01639625.2025.2470402

[53] Ying Lei, Shuai Ma, Yuling Sun, and Xiaojuan Ma. 2025. "AI Afterlife" as Digital Legacy: Perceptions, Expectations, and Concerns. In *Proceedings of the 2025 CHI Conference on Human Factors in Computing Systems*. ACM, Article 981, 18 pages. doi:10.1145/3706598.3713933

[54] Jingjie Li, Kaiwen Sun, Brittany Skye Huff, Anna Marie Bierley, Younghyun Kim, Florian Schaub, and Kassem Fawaz. 2023. "It's up to the Consumer to be Smart": Understanding the Security and Privacy Attitudes of Smart Home Users on Reddit. In *Proceedings of the 2023 IEEE Symposium on Security and Privacy*. IEEE, 2850–2866. doi:10.1109/SP46215.2023.10179344

[55] Na Li, Chuhao Wu, Hongyang Zhou, Huiran Yi, Jie Cai, and John Carroll. 2025. Challenges of Providing Social Support on a Women-Centric Platform: Insights from REDnote. In *Companion Publication of the 2025 Conference on Computer-Supported Cooperative Work and Social Computing*. ACM, 465–470. doi:10.1145/3715070.3749271

[56] Tianshi Li, Elizabeth Louie, Laura Dabbish, and Jason I. Hong. 2021. How Developers Talk About Personal Data and What It Means for User Privacy: A Case Study of a Developer Forum on Reddit. *Proceedings of the ACM on Human-Computer Interaction* 4, CSCW3, Article 220 (2021), 28 pages. doi:10.1145/3432919

[57] Yi Liang, Haohao Zhang, and Zejiong Zhou. 2022. Research on the Digital Technology Enabling Grass-Roots Government Governance: Based on the Case of the Yingzhou District Government in Fuyang. *Frontiers in Humanities and Social Sciences* 2, 12 (2022), 35–43. doi:10.54691/fhss.v2i12.3129

[58] Stephanie A. Limoncelli. 2009. Human Trafficking: Globalization, Exploitation, and Transnational Sociology. *Sociology Compass* 3, 1 (2009), 72–91. doi:10.1111/j.1751-9020.2008.00178.x

[59] Leo S. F. Lin. 2025. Business As Usual? Chinese Organised Crime in Southeast Asia. Blog article, Australian Outlook, Australian Institute of International Affairs. https://www.internationalaffairs.org.au/australianoutlook/business-as-usual-chinese-organised-crime-in-southeast-asia/

[60] Joyce C. H. Liu. 2023. Cyber Slavery, Port Cities and Systemic Cruelty: Logistics of Labor Extraction in the 21st Century. *Innovation in the Social Sciences* 1, 2 (2023), 211–233. doi:10.1163/27730611-bja10014

[61] Neil Loughlin. 2024. Transnational Crime Meets Embedded Corruption in Cambodia. *Global China Pulse* 3, 1 (2024), 27–33. https://globalchinapulse.net/transnational-crime-meets-embedded-corruption-in-cambodia

[62] Zhicong Lu, Yue Jiang, Chenxinran Shen, Margaret C. Jack, Daniel Wigdor, and Mor Naaman. 2021. "Positive Energy" Perceptions and Attitudes Towards COVID-19 Information on Social Media in China. *Proceedings of the ACM on Human-Computer Interaction* 5, CSCW1 (2021), 25 pages. doi:10.1145/3449251

[63] Hai Thanh Luong. 2025. "Simple job, high salary": unveiling the complexity of scam-forced criminality in Southeast Asia. *Humanities and Social Sciences Communications* 12, Article 1305 (2025), 11 pages. doi:10.1057/s41599-025-05605-1

[64] Hai Thanh Luong and Hieu Minh Ngo. 2024. Understanding the Nature of the Transnational Scam-Related Fraud: Challenges and Solutions from Vietnam's Perspective. *Laws* 13, 6, Article 70 (2024), 15 pages. doi:10.3390/laws13060070

[65] Samuel Mayworm, Michael Ann DeVito, Daniel Delmonaco, Hibby Thach, and Oliver L. Haimson. 2024. Content Moderation Folk Theories and Perceptions of Platform Spirit among Marginalized Social Media Users. *ACM Transactions on Social Computing* 7, 1–4, Article 1 (2024), 27 pages. doi:10.1145/3632741

[66] Lorraine Mazerolle. 2023. Partnership approaches in policing: An analysis of different types of partnerships and how they work to reduce crime and disorder. *Policing: A Journal of Policy and Practice* 17, Article paad075 (2023), 11 pages. doi:10.1093/police/paad075

[67] Nora McDonald, Sarita Schoenebeck, and Andrea Forte. 2019. Reliability and Inter-rater Reliability in Qualitative Research: Norms and Guidelines for CSCW and HCI Practice. *Proceedings of the ACM on Human-Computer Interaction* 3, CSCW, Article 72 (2019), 23 pages. doi:10.1145/3359174

[68] Warwick McKibbin and Roshen Fernando. 2023. The global economic impacts of the COVID-19 pandemic. *Economic Modelling* 129, Article 106551 (2023), 18 pages. doi:10.1016/j.econmod.2023.106551

[69] Poppy McPherson. 2025. Amnesty says Cambodia is enabling brutal scam industry. News report, Reuters. https://www.reuters.com/sustainability/society-equity/amnesty-says-cambodia-is-enabling-brutal-scam-industry-2025-06-26/

[70] Guiomar Merodio, Elena Duque, and Juan Carlos Peña Axt. 2020. They Are Not Romeo Pimps, They Are Traffickers: Overcoming the Socially Dominant Discourse to Prevent the Sex Trafficking of Youth. *Qualitative Inquiry* 26, 8-9 (2020), 1010–1018. doi:10.1177/1077800420938881

[71] Nurul Nabilah Huda Mohamad Shukri, Nolila Mohd Nawi, Amin Mahir Abdullah, and Norsida Man. 2018. Consumer's perception on the quality of controversial contents in edible bird's nest products. *Pertanika Journal of Scholarly Research Reviews* 4, 1 (2018), 1–9. https://files01.core.ac.uk/download/pdf/234560172.pdf

[72] Yiftach Nagar. 2012. What Do You Think? The Structuring of an Online Community as a Collective-Sensemaking Process. In *Proceedings of the ACM 2012 Conference on Computer Supported Cooperative Work*. ACM, 393–402. doi:10.1145/2145204.2145266

[73] NanmiCoder. 2025. MediaCrawler - 自媒体平台爬虫 / Crawler of self-media platforms. GitHub repository. https://github.com/NanmiCoder/MediaCrawler

[74] Nathalie Nthala and Rick Wash. 2021. How Non-Experts Try to Detect Phishing Scam Emails. In *Proceedings of the Workshop on Technology and Consumer Protection (ConPro 2021), IEEE Symposium on Security and Privacy Workshops*. IEEE, 7 pages. https://www.ieee-security.org/TC/SPW2021/ConPro/papers/nthala-conpro21.pdf

[75] Rajvardhan Oak and Zubair Shafiq. 2025. "Hello, is this Anna?": Unpacking the Lifecycle of Pig-Butchering Scams. In *Proceedings of the Twenty-First Symposium on Usable Privacy and Security*. USENIX Association, Article 1, 18 pages. https://www.usenix.org/system/files/soups2025-oak-butchering.pdf

[76] Rajvardhan Oak and Zubair Shafiq. 2025. Victims, Vigilantes, and Advice Givers: An Analysis of Scam-Related Discourse on Reddit. In *Proceedings of the Twenty-First Symposium on Usable Privacy and Security*. USENIX Association. https://www.usenix.org/conference/soups2025/presentation/oak-discourse

[77] OHCHR Regional Office for South-East Asia. 2023. *Online Scam Operations and Trafficking into Forced Criminality in Southeast Asia: Recommendations for a Human Rights Response*. Technical Report. Office of the United Nations High Commissioner for Human Rights (OHCHR), Bangkok. https://bangkok.ohchr.org/sites/default/files/wp_files/2023/08/ONLINE-SCAM-OPERATIONS-2582023.pdf

[78] Natalia Ollus. 2015. Regulating forced labour and combating human trafficking: The relevance of historical definitions in a contemporary perspective. *Crime, Law and Social Change* 63, 5 (2015), 221–246. doi:10.1007/s10611-015-9566-6

[79] Livia Ottisova, Sarah Hemmings, Louise M. Howard, Cathy Zimmerman, and Sian Oram. 2016. Prevalence and risk of violence and the mental, physical and sexual health problems associated with human trafficking: an updated systematic review. *Epidemiology and Psychiatric Sciences* 25, 4 (Aug. 2016), 317–341. doi:10.1017/S2045796016000135

[80] Jessica A. Pater, Moon K. Kim, Elizabeth D. Mynatt, and Casey Fiesler. 2016. Characterizations of Online Harassment: Comparing Policies Across Social Media Platforms. In *Proceedings of the 2016 ACM International Conference on Supporting Group Work*. ACM, 369–374. doi:10.1145/2957276.2957297

[81] Wang Pei. 2024. Confucian filiality revisited: The case of contemporary China. *Philosophy & Social Criticism*, Article 01914537241288471 (2024), 22 pages. doi:10.1177/01914537241288471

[82] People's Daily Online. 2025. RedNote Proactively Blocked 94.3% of Fraud Attempts in 2024. https://finance.people.com.cn/BIG5/n1/2025/0312/c1004-40437651.html Reposted by China Economic Net: https://www.ce.cn/xwzx/shgj/gdxw/202503/12/t20250312_39317706.shtml.

[83] Steve Peterson, Keri K. Stephens, Hemant Purohit, and Amanda Lee Hughes. 2019. When Official Systems Overload: A Framework for Finding Social Media Calls for Help during Evacuations. In *Proceedings of the 16th International Conference on Information Systems for Crisis Response and Management (ISCRAM)*. València, Spain. http://idl.iscram.org/files/stevepeterson/2019/1928_StevePeterson_etal2019.pdf

[84] Mikayla Pevac. 2022. Online Safe (Enough) Spaces: Internet Support Groups for Survivors of Sexual Assault. In *Handbook of Research on Communication Strategies for Taboo Topics*. IGI Global, 285–301. doi:10.4018/978-1-7998-9125-3.ch014

[85] Carlotta Preiss. 2022. Digital Migration Infrastructures. In *Introduction to Migration Studies: An Interactive Guide to the Literatures on Migration and Diversity*. Springer, 99–110. doi:10.1007/978-3-030-92377-8_5

[86] Casey Randazzo and Tawfiq Ammari. 2023. "If Someone Downvoted My Posts—That'd Be the End of the World": Designing Safer Online Spaces for Trauma Survivors. In *Proceedings of the 2023 CHI Conference on Human Factors in Computing Systems*. ACM, Article 481, 18 pages. doi:10.1145/3544548.3581453

[87] Yichen Rao. 2019. From Confucianism to psychology: Rebooting Internet addicts in China. *History of Psychology* 22, 4 (2019), 328–350. doi:10.1037/hop0000111

[88] Rebecca Ratcliffe. 2025. Revealed: the huge growth of Myanmar scam centres that may hold 100,000 trafficked people. News report, The Guardian. https://www.theguardian.com/global-development/2025/sep/08/myanmar-military-junta-scam-centres-trafficking-crime-syndicates-kk-park

[89] Lubna Razaq, Tallal Ahmad, Samia Ibtasam, Muhammad Umer Ramzan, and Shrirang Mare. 2021. "We Even Borrowed Money From Our Neighbor": Understanding Mobile-based Frauds Through Victims' Experiences. *Proceedings of the ACM on Human-Computer Interaction* 5, CSCW1, Article 41 (2021), 30 pages. doi:10.1145/3449115

[90] Afsaneh Razi, Ashwaq AlSoubai, Seunghyun Kim, Shiza Ali, Gianluca Stringhini, Munmun Choudhury, and Pamela J. Wisniewski. 2023. Sliding into My DMs: Detecting Uncomfortable or Unsafe Sexual Risk Experiences within Instagram Direct Messages Grounded in the Perspective of Youth. *Proceedings of the ACM on Human-Computer Interaction* 7, CSCW1, Article 89 (2023), 29 pages. doi:10.1145/3579522

[91] Christian Ryan. 2025. *RedNote: A Threat Assessment*. Research Report. 2430 Group, Pittsburgh, PA, USA. https://static1.squarespace.com/static/6572026973c5981bbe67fcc5/t/688baa22b923616fd50318eb/1753983522324/Red+Note_+A+Threat+Assessment.pdf

[92] Nazanin Sabri, Bella Chen, Annabelle Teoh, Steven P. Dow, Kristen Vaccaro, and Mai Elsherief. 2023. Challenges of Moderating Social Virtual Reality. In *Proceedings of the 2023 CHI Conference on Human Factors in Computing Systems*. ACM, Article 384, 1–20 pages. doi:10.1145/3544548.3581329

[93] Gargi Sarkar and Sandeep K. Shukla. 2024. Bi-Directional Exploitation of Human Trafficking Victims: Both Targets and Perpetrators in Cybercrime. *Journal of Human Trafficking* (2024), 22 pages. doi:10.1080/23322705.2024.2353015

[94] Gargi Sarkar and Sandeep Kumar Shukla. 2025. Cyber Slavery Infrastructures: A Socio-Technical Study of Forced Criminality in Transnational Cybercrime. Preprint, arXiv:2510.12814 [cs.CY]. doi:10.48550/arXiv.2510.12814

[95] Muhammad Saud, Musta'in Mashud, and Rachmah Ida. 2020. Usage of social media during the pandemic: Seeking support and awareness about COVID-19 through social media platforms. *Journal of Public Affairs* 20, 4, Article e2417 (2020), 9 pages. doi:10.1002/pa.2417

[96] Benjamin Saunders, Julius Sim, Tom Kingstone, Shula Baker, Jackie Waterfield, Bernadette Bartlam, Heather Burroughs, and Clare Jinks. 2018. Saturation in qualitative research: exploring its conceptualization and operationalization. *Quality & Quantity* 52, 4 (2018), 1893–1907. doi:10.1007/s11135-017-0574-8

[97] Steve Sheng, Mandy Holbrook, Ponnurangam Kumaraguru, Lorrie Faith Cranor, and Jason Hong. 2010. Who Falls for Phish? A Demographic Analysis of Phishing Susceptibility. In *Proceedings of the 2010 SIGCHI Conference on Human Factors in Computing Systems*. ACM, 373–382. doi:10.1145/1753326.1753383

[98] Dean A. Shepherd, Vinit Parida, Trent Williams, and Joakim Wincent. 2022. Organizing the exploitation of vulnerable people: A qualitative assessment of human trafficking. *Journal of Management* 48, 8 (2022), 2421–2457. doi:10.1177/01492063211046908

[99] Mitsuru Shimpo, Ong Jin Hui, Steven Vertovec, Ravinder K. Thiara, Darshan Singh Tatla, and Michael Twaddle. 1995. Asian Indentured and Colonial Migration. In *The Cambridge Survey of World Migration*, Robin Cohen (Ed.). Cambridge University Press, 45–76. doi:10.1017/CBO9780511598289.003

[100] Kate Starbird and Leysia Palen. 2011. "Voluntweeters": Self-Organizing by Digital Volunteers in Times of Crisis. In *Proceedings of the 2011 SIGCHI Conference on Human Factors in Computing Systems*. ACM, 1071–1080. doi:10.1145/1978942.1979102

[101] Sophie Stephenson, Lana Ramjit, Thomas Ristenpart, and Nicola Dell. 2025. Digital Technologies and Human Trafficking: Combating Coercive Control and Navigating Digital Autonomy. In *Proceedings of the 2025 CHI Conference on Human Factors in Computing Systems*. ACM, Article 832, 21 pages. doi:10.1145/3706598.3713544

[102] Heidi Stöckl, Camilla Fabbri, Harry Cook, Claire Galez-Davis, Naomi Grant, Yuki Lo, Ligia Kiss, and Cathy Zimmerman. 2021. Human trafficking and violence: Findings from the largest global dataset of trafficking survivors. *Journal of Migration and Health* 4, Article 100073 (2021), 6 pages. doi:10.1016/j.jmh.2021.100073

[103] Natalie Jomini Stroud. 2008. Media use and political predispositions: Revisiting the concept of selective exposure. *Political behavior* 30, 3 (2008), 341–366. doi:10.1007/s11109-007-9050-9

[104] Yuling Sun, Sam Addison Ankenbauer, Zhifan Guo, Yuchen Chen, Xiaojuan Ma, and Liang He. 2025. Rethinking Technological Solutions for Community-Based Older Adult Care: Insights from 'Older Partners' in China. *Proceedings of the ACM on Human-Computer Interaction* 9, 2, Article CSCW160 (2025), 36 pages. doi:10.1145/3711058

[105] Yijia Sun and Tuan Phong Ly. 2023. The Influence of Word-of-web on Customers' Purchasing Process: The Case of Xiaohongshu. *Journal of China Tourism Research* 19, 2 (2023), 221–244. doi:10.1080/19388160.2022.2057378

[106] Joshua Sunshine, Serge Egelman, Hazim Almuhimedi, Neha Atri, and Lorrie Faith Cranor. 2009. Crying Wolf: An Empirical Study of SSL Warning Effectiveness. In *Proceedings of the 18th USENIX Security Symposium*. USENIX Association, 399–416. https://www.usenix.org/legacy/event/sec09/tech/full_papers/sunshine.pdf

[107] Mohammad Tahaei, Kami Vaniea, and Naomi Saphra. 2020. Understanding Privacy-Related Questions on Stack Overflow. In *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems*. ACM, Article 639, 14 pages. doi:10.1145/3313831.3376768

[108] Hannah Tam, Karthik S Bhat, Priyanka Mohindra, and Neha Kumar. 2023. Learning to Navigate Health Taboos through Online Safe Spaces. In *Proceedings of the 2023 CHI Conference on Human Factors in Computing Systems*. ACM, Article 295, 15 pages. doi:10.1145/3544548.3580708

[109] United Nations Human Rights Office of the High Commissioner. 2023. *Online Scam Operations and Trafficking into Forced Criminality in Southern Asia: Recommendations for a Human Rights Response*. Technical Report. United Nations Human Rights Office of the High Commissioner. https://bangkok.ohchr.org/sites/default/files/wp_files/2023/08/ONLINE-SCAM-OPERATIONS-2582023.pdf

[110] United Nations Office on Drugs and Crime. 2024. Human Trafficking. Web page. https://www.unodc.org/unodc/en/human-trafficking/human-trafficking.html

[111] USIP Senior Study Group. 2024. *Transnational Crime in Southeast Asia: A Growing Threat to Global Peace and Security*. Technical Report. United States Institute of Peace, Washington, DC. https://www.usip.org/publications/2024/05/transnational-crime-southeast-asia-growing-threat-global-peace-and-security

[112] Elham Pourabbas Vafa, Mohit Singhal, Poojitha Thota, and Sayak Saha Roy. 2025. Learning from Censored Experiences: Social Media Discussions around Censorship Circumvention Technologies. In *Proceedings of the 2025 IEEE Symposium on Security and Privacy*. IEEE, 1325–1343. doi:10.1109/SP61157.2025.00062

[113] Sylvia Walby, Birgit Apitzsch, Joanne Elisabeth Armstrong, Susan Balderston, Karolina Szmagalska-Follis, Brian Joseph Francis, Liz Kelly, Corinne Anne May-Chahal, Awais Rashid, Karen Shire, Jude Towers, and Markus Tunte. 2016. *Study on the gender dimension of trafficking in human beings*. Technical Report. Publications Office of the European Union. doi:10.2837/462884

[114] Qian Wan and Zhicong Lu. 2024. Investigating vTubing as a Reconstruction of Streamer Self-Presentation: Identity, Performance, and Gender. *Proceedings of the ACM on Human-Computer Interaction* 8, CSCW1, Article 80 (2024), 22 pages. doi:10.1145/3637357

[115] Ruyuan Wan, Lingbo Tong, Tiffany Knearem, Toby Jia-Jun Li, Ting-Hao'Kenneth' Huang, and Qunfang Wu. 2025. Hashtag Re-Appropriation for Audience Control on Recommendation-Driven Social Media Xiaohongshu (rednote). In *Proceedings of the 2025 CHI Conference on Human Factors in Computing Systems*. ACM, Article 895, 25 pages. doi:10.1145/3706598.3713379

[116] Fangzhou Wang. 2024. Victim-Offender Overlap: The Identity Transformations Experienced by Trafficked Chinese Workers Escaping from Pig-Butchering Scam Syndicates. *Trends in Organized Crime* (2024). doi:10.1007/s12117-024-09525-5

[117] Shuna Wang and Yang Yao. 2007. Grassroots Democracy and Local Governance: Evidence from Rural China. *World Development* 35, 10 (2007), 1635–1649. doi:10.1016/j.worlddev.2006.10.014

[118] Xubin Wang, Zhiqing Tang, Jianxiong Guo, Tianhui Meng, Chenhao Wang, Tian Wang, and Weijia Jia. 2025. Empowering Edge Intelligence: A Comprehensive Survey on On-Device AI Models. *Comput. Surveys* 57, 9, Article 228 (2025), 39 pages. doi:10.1145/3724420

[119] Rick Wash. 2020. How Experts Detect Phishing Scam Emails. *Proceedings of the ACM on Human-Computer Interaction* 4, CSCW2, Article 160 (2020), 28 pages. doi:10.1145/3415231

[120] Miranda Wei, Sunny Consolvo, Patrick Gage Kelley, Tadayoshi Kohno, Tara Matthews, Sarah Meiklejohn, Franziska Roesner, Renee Shelby, Kurt Thomas, and Rebecca Umbach. 2024. Understanding Help-Seeking and Help-Giving on Social Media for Image-Based Sexual Abuse. In *Proceedings of the 33rd USENIX Security Symposium*. USENIX Association, 4391–4408. https://www.usenix.org/conference/usenixsecurity24/presentation/wei-miranda-understanding

[121] Laura Weidinger, Jonathan Uesato, Maribeth Rauh, Conor Griffin, Po-Sen Huang, John Mellor, Amelia Glaese, Myra Cheng, Borja Balle, Atoosa Kasirzadeh, Julia Haas, Courtney Biles, Sasha Brown, Zac Kenton, Will Hawkins, Tom Stepleton, Abeba Birhane, Lisa Anne Hendricks, Laura Rimell, William Isaac, Sean Legassick, Geoffrey Irving, and Iason Gabriel. 2022. Taxonomy of Risks Posed by Language Models. In *Proceedings of the 2022 ACM Conference on Fairness, Accountability, and Transparency*. ACM, 214–229. doi:10.1145/3531146.3533088

[122] Jason B. Whiting, Rachael Dansby Olufuwote, Jaclyn D. Cravens-Pickens, and Alyssa Banford Witting. 2019. Online Blaming and Intimate Partner Violence: A Content Analysis of Social Media Comments. *The Qualitative Report* 24, 1 (2019), 78–94. doi:10.46743/2160-3715/2019.3486

[123] Monica T. Whitty and Tom Buchanan. 2012. The online romance scam: a serious cybercrime. *CyberPsychology, Behavior, and Social Networking* 15, 3 (2012), 181–183. doi:10.1089/cyber.2011.0352

[124] Xiaoping Wu and Richard Fitzgerald. 2021. 'Hidden in plain sight': Expressing political criticism on Chinese social media. *Discourse Studies* 23, 3 (2021), 365–385. doi:10.1177/1461445620916365

[125] Xinhua News Agency. 2023. Hundreds of thousands trafficked to work as online scammers in SE Asia: UN report. Retrieved November 28, 2025 from https://english.news.cn/20230829/502ce4d385e84d0dad18f475734fd96d/c.html

[126] Xinhua News Agency. 2025. Thailand receives 61 foreign victims of human trafficking from Myanmar. Retrieved November 28, 2025 from https://english.news.cn/20250207/3765271300f94b0c909905d5d324a3eb/c.html

[127] Qihang Xue, Huimin Wang, and Jian Wei. 2023. Internet technology and regional financial fraud: evidence from Broadband expansion in China. *Journal of Applied Economics* 26, 1 (2023), 2281167. doi:10.1080/15140326.2023.2281167

[128] Ying Yin, Mudiarasan Kuppusamy, and Benjamin Chan Yin Fah. 2023. Acceptance of Xiaohongshu APP of Overseas Chinese Users. *International Journal of Advanced Business Studies* 2, 2 (2023), 28–36. doi:10.59857/MTAO4047

[129] Kangyu Yuan, Li Zhang, Hanfang Lyu, Ziqi Pan, Yuanhao Zhang, Junze Li, Bingcan Guo, Jiaxiong Hu, Qingyu Guo, and Xiaojuan Ma. 2025. "I Love the Internet Again": Exploring the Interaction Inception of "TikTok Refugees" Flocking into RedNote. In *Proceedings of the Extended Abstracts of the 2025 CHI Conference on Human Factors in Computing Systems*. ACM, Article 12, 8 pages. doi:10.1145/3706599.3719738

[130] Renwen Zhang, Jordan Eschler, and Madhu Reddy. 2018. Online Support Groups for Depression in China: Culturally Shaped Interactions and Motivations. *Computer Supported Cooperative Work (CSCW)* 27, 3 (2018), 327–354. doi:10.1007/s10606-018-9322-4

[131] Jiangrui Zheng, Xueqing Liu, Mirazul Haque, Xing Qian, Guanqun Yang, and Wei Yang. 2024. HateModerate: Testing Hate Speech Detectors against Content

Moderation Policies. In *Findings of the Association for Computational Linguistics: NAACL 2024*. ACL, 2691–2710. doi:10.18653/v1/2024.findings-naacl.172

[132] Rui Zhou, Jasmine Hentschel, and Neha Kumar. 2017. Goodbye Text, Hello Emoji: Mobile Communication on WeChat in China. In *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems*. ACM, 748–759. doi:10.1145/3025453.3025800

[133] Tao Zhu, David Phipps, Adam Pridgen, Jedidiah R Crandall, and Dan S. Wallach. 2012. Tracking and Quantifying Censorship on a Chinese Microblogging Site. Preprint, arXiv:1211.6166 [cs.IR]. doi:10.48550/arXiv.1211.6166

[134] Tao Zhu, David Phipps, Adam Pridgen, Jedidiah R. Crandall, and Dan S. Wallach. 2013. The Velocity of Censorship: High-Fidelity Detection of Microblog Post Deletions. In *Proceedings of the 22nd USENIX Security Symposium*. USENIX Association, 227–240. https://www.usenix.org/conference/usenixsecurity13/technical-sessions/paper/zhu

[135] 英国小队长 / LeaderUK. 2023. 中国留学生在小红书上被骗钱！大使馆提醒：在英留学生近期被罪犯盯上了 / Chinese students were scammed on Xiaohongshu! The Embassy warned: Chinese students in the UK have recently been targeted by criminals. News report. https://www.sohu.com/a/649035623_100147587

A Keyword Set Used for Crawling

We list the English translations of key terms used to search and crawl data:

Cambodian scam, Experience of abduction, Experience of trafficked labor, Forced labor, Golden Triangle human trafficking, High-paying jobs in Cambodia, High-paying labor, Human smuggling, Human trafficking, Human trafficking experience, Human trafficking gang, Human trafficking hotspot, Human trafficking survivor, Labor trafficking, Myawaddy compound/zone, Myawaddy escape experience, Northern Myanmar, Online and offline human trafficking, kidney cutting (organ harvesting), Overseas job scam, Recruitment at the Myanmar border, Sharing lessons from overseas, Trafficked and trapped overseas, Wage fraud against workers, Working in Southeast Asia, Yunnan border defense.

B Excluded Tags

We list the English translations of the excluded tags:

Classic films and TV, Daily drama-watching, Documentary, Drama chasing, Drama check-in, Drama shortage, Food and fun, Good drama recommendations, Good Korean drama recommendations, Gourmet / food, Korean drama, Korean drama commentary, Korean drama fan, Korean drama recommendation, Korean drama sharing, Local specialties, Movie, Movie recommendation, Net worth, New drama updates, No More Bets (film), Original work, Popular short drama, Popular TV series, Short drama, Show recommendations (when out of ideas), Stress-relief video, TV series, TV series recommendation, TV series updates, The drama I'm following, Travel recommendation, Trending Korean drama guide, Variety show, Watching dramas at home, Web drama.

C Prompt for LLM-based Binary Relevance Filtering

```
You are Qwen, created by Alibaba Cloud. You are a helpful assistant.
You will receive a social media post. Please classify the post and
output 0 for Irrelevant or 1 for Relevant as defined below.

[Topic Definitions]
[0] Irrelevant: The post does not contain specific information about
scam and human trafficking or cross-border human trafficking (e.g.,
vague and general crime discussions and unrelated lifestyle posts).

[1] Relevant: The post contains specific information about both scam
and human trafficking or cross-border, particularly in China and
Southeast Asia, human trafficking (e.g., reports and awareness
materials about rescue and anti-fraud campaigns, survivors or close
contacts sharing direct experiences of recruitment scams and
exploitation, requests for help regarding scams and suspected
trafficking cases, and prevention strategies, scam awareness tips,
or warnings against scams or human-trafficking).

Example 1:
我前两天去了泰国，然后被人接上了车，在泰国边境的哒府离妙瓦底还
有20分钟的车程...到了缅甸妙瓦底器官移植园区...
Assignment: 1

Example 2:
最近听到网上说泰国旅游很危险，大家最好别去。我朋友说有些地方不
安全。
Assignment: 0
```

D Codebook

Table 1: Codebook: Recruitment – Targeting

Recruitment: Targeting			
Code	**Definition**	**Sub-code**	**Sub-code definition**
Lack of awareness	A general gap in knowledge or inattentiveness to the current situation, including geographical understanding and legal awareness.	**Lack of geographical understanding**	Individual is unfamiliar with their geographical surroundings. They are unable to identify trafficking hotspots.
		Lack of legal awareness	Individual is unfamiliar or unaware of the legality of an activity. This may be a factor in how the individuals are deceived.
Physical limitation and differences	The difference in physical strength or ability to escape captivity between the victim and the trafficker.	**Physical differences**	Physical characteristics that may limit a person's ability to escape or resist a trafficker. These can include age, strength, or mobility issues that limit escape or resistance.
		Disability and health conditions	Pre-existing health conditions or a disability that hinder escape.
Over-reliance and overtrust	Individuals are targeted due to their reliance and trust in a third-party.	**Authority**	Individual is reliant on support from authorities.
		Family and personal relation	Individual is reliant on support from trusted familiar family member or close contacts.
Financial instability	The urgency for money in low-income individuals or families.	**Debt**	Urgency to repay outstanding debts.
		Urgent expenses	Urgency to cover expenses, e.g., bills or living costs.
		Uncertain financial income	Financial instability due to lack of stable income.
		Ransom	Financial instability caused by ransom payments.
Age	Age of the individuals, e.g., targeting children (young age).	**Children**	Includes babies and children, depicted with lack of lived experience.
		Teenagers	Includes minors between the ages of 13 to 18, depicted with lack of lived experience.
		Adults	Includes individuals aged 18+.
Gender	Targeting individuals based on gender. This may include women, men, girls, boys, depending on the traffickers' strategies and the type of exploitation involved.	**Male**	Individuals who identify as male.
		Female	Individuals who identify as female.
Language	The language skills an individual possesses and how it factors into the trafficking process.	**Multilingual**	Individual is targeted due to their ability to speak multiple languages. They are exploited and forced into deceiving others who speak different languages.
		Inability to understand local language	Individual's inability to understand the local language increases susceptibility to deception.
Employment status	Job status of the individual.	**Unemployed**	Individual is unemployed or in the process of seeking a job.
		Student	Individual is a student.
		Employed	Individual is in secure employment or self-employed.
Marital status	Marital status of individuals.	**Married**	Individual is legally married.
		Unmarried	Individual is not considered married.
Education level	Individual's educational background.	**Little to no education**	Individual has received little to no education.
		Secondary education	Individual has received up to secondary school level education.
		Higher education	Individual has received up to college/university level education.
Ethnicity	Targeting individuals based on ethnic identity, minority status, or ethnic belonging. This can involve discrimination, social exclusion, language barriers, or stereotypes that traffickers exploit to increase vulnerability.	**Ethnic minority status**	Individuals from ethnic groups who face discrimination, limited resources, or reduced protection.
		Migrant or cross-border ethnic ties	Individuals with cross-border ties prone to migrating through risky channels.

Table 2: Codebook: Recruitment – Recruitment Channels

Recruitment: Recruitment Channels			
Code	**Definition**	**Sub-code**	**Sub-code definition**
Gambling	Online or in-person gambling centers where individuals are defrauded and pose a risk of being trafficked.	N/A	N/A
Trading and investment platforms	Trading platforms where individuals invest money and are scammed.	N/A	N/A
Social media platforms	Platforms that have chat functions where individuals can communicate with perpetrators.	N/A	N/A
Public spaces	Perpetrators who deceive people in public spaces, e.g., on the street.	N/A	N/A
Telephone calls	Fraudulent schemes conducted via phone calls that exploit trust or urgent situations.	N/A	N/A

Table 3: Codebook: Recruitment – Recruitment Approaches

Recruitment: Recruitment Approaches			
Code	**Definition**	**Sub-code**	**Sub-code definition**
Impersonation	Deceptive use of false or stolen identities to mislead individuals.	**Authority**	Impersonating authority to gain trust and deceive individuals.
		Service worker	Posing as everyday service staff.
		Romantic partner	Faking romantic relationships for manipulation.
		Business and service scam	Fraud workers who pretend to be clients or company representatives to approach the individual's company or services.
		Fake family and friends	Impersonating family or friends online.
Direct referral	Individuals are referred to recruitment channels or trafficked by a trusted familiar person.	N/A	N/A
Emotional manipulation	Exploiting empathy through fabricated distress.	**Distress**	Creating fake emergencies to pressure decisions.
		Family/blood-tie appeals	Exploiting strong Chinese norms of filial duty, kinship, and family trust.
		Disability deception	Feigning physical/age-related vulnerability.
Fake promises	Offering illusory opportunities to gain the individual's interest.	**Foreign and cross-border work opportunity**	Offering an enticing overseas job.
		High-paying job and contracts	Unrealistic or misleading job advertisements promising large salaries and perks, often masking illicit work in scam compounds.
		Travel or studying abroad	Luring people abroad under the pretext of traveling or studying overseas.
		High return	Promises of guaranteed high profits, luxury rewards, or lifestyle benefits through gaming, gambling, or trading platforms.
Upfront rewards	Acts of apparent goodwill used by perpetrators to build trust with the victim.	**Expense coverage**	Paying for expenses upfront to gain individual's trust.
		Trial opportunity	Offering probationary work periods with illusory choice to leave.
		Advance payment	Providing preliminary earnings or upfront payment as an act of good will.
Travel	Recruitment through movement or transportation. Traffickers persuade victims to travel under false pretenses or control their transport to trafficker-controlled locations.	**Voluntary but misled travel**	Victim travels towards a high-risk/trafficker-controlled location willingly due to deception.
		Arranged transportation	Perpetrators organize transport to controlled locations. Can use pre-paid tickets, staging deceptive pick-ups, or through illegal border routes.

Table 4: Codebook: Control Mechanisms

Control Mechanisms			
Code	**Definition**	**Sub-code**	**Sub-code definition**
Seized documentation and personal possessions	Withholding documents or personal belongings to enforce control.	N/A	N/A
Psychological abuse	The use of psychological methods to control, intimidate, or break the victim. Including threats, isolation, humiliation, and inducing trauma.	**Threats against family**	Victims are controlled by threats to harm family members.
		Verbal humiliation	Victims are insulted, degraded, or ridiculed to break their morale.
		Shame, responsibility manipulation, and dependency on abuser	Victims are subject to threats and psychological manipulation. Victims are pressured into compliance by being made to feel personally responsible for debts and willingly pay perpetrator.
		Brainwashing	Victims are brainwashed to maintain control and break morale.
		Fear induction and threat to life	Victims are manipulated by fear through staged violence, fake police threats, stories of punishment, observing other's cruel punishments, and death.
Drugs	The victim is forced to take drugs to disorientate and subdue, taking away autonomy.	N/A	N/A
Physical abuse and violence	Victim is subjected to harsh beatings or torture as punishment.	**Beaten**	Beatings used to punish or intimidate.
		Torture	Various forms of physical abuse as punishment.
		Death	Victims die as a result of the harsh punishments or are killed when no longer useful.
		Rape	Sexual violence for non-compliance.
		Electrocution	Electrocution used to punish or intimidate.
Long work hours	Victims suffer physical fatigue and psychological burnout due to long hours and oppressive quotas.	N/A	N/A
Confinement	Victims are intentionally isolated or restricted through physical barriers, resource deprivation, or controlled living conditions, making escape or access to help nearly impossible.	**Locked up**	Physically restraining victims in rooms or in handcuffs for days.
		Poor compound living conditions	Victim is confined within a trafficker-controlled compound with deliberately poor living standards, including unsafe or insufficient food, unsanitary facilities, and restricted access to basic services to maintain control and dependency.
		No access to help	Blocking access to funds or support.
Monitoring	The victim is constantly monitored to ensure compliance and control.	**Assigned fraud worker**	A handler monitors the victim and punishes resistance.
		Forced searches	Victims are subjected to strip searches and property checks.
		Surveillance	24/7 surveillance that discourages victims from escaping due to lack of privacy.
		Hunters	Fraud workers will search for victims' escape attempts. They are stationed at borders and will apprehend and torture those who are caught.

Table 5: Codebook: Exploitation

Exploitation			
Code	**Definition**	**Sub-code**	**Sub-code definition**
Fraud-working scheme	The victim is forced into deceiving other people into the fraud parks. This can include online and in-person activity.	**Telecom fraud and phone scam**	Victims are forced into making fraudulent phone calls to scam others.
		Romantic fraud	Victims are forced to adopt romantic personas to deceive others.
		Online fraud	Victims are forced to create, operate, and maintain online fraud channels to deceive others. Such as creating fraudulent websites, gambling, social media posts, using fake identities.
Sex exploitation	The victim is forced to perform sexual acts, into prostitution, or is raped.	N/A	N/A
Financial exploitation	The perpetrator fines the victim for money, or collects ransom from the victim's family. Victims could also be resold for money.	**Debt bondage**	Inflated recruitment or release fees used to justify exploitation.
		Ransom	Demanding money from the family for the victim's release.
Organ harvesting	The victim has organs forcefully removed to be sold.	N/A	N/A
Reselling	Selling the victim to another party. This generates money for the trafficker, but the exploitation of the victim continues elsewhere.	**Reselling to scam parks**	Victims are resold between scam compounds for profits or for exchange.
Child exploitation	Children under 18 are coerced into exploitative work, criminal activity, or trafficking operations.	N/A	N/A

Table 6: Codebook: Post-Trafficking – Outcomes and Risks

Post-Trafficking: Outcomes and Risks			
Code	**Definition**	**Sub-code**	**Sub-code definition**
Escape	The survivor initiates and successfully carries out an act that leads to physical separation from traffickers or makes first contact with the outside world without assistance from authorities or third parties.	**Contacting for help**	The survivor (or someone acting on their behalf) is able to communicate with an external person, organization, or authority for help.
		Self-escape attempts	The survivor independently tries to escape, such as fleeing a compound or evading guards. These attempts may succeed or result in partial or failed escapes if intercepted by traffickers.
Rescue	Rescue operation carried out by authorities or family members. Survivors contact others for help in order to plan escape.	**State and international intervention**	Rescue led by law enforcement or embassies through police raids, cross-border operations, and assistance with legal documents or safe return.
		Local authorities intervention	Survivors or relatives contact local-level officials for help. This includes community police stations, municipal officers, or local government branches.
		Family and friends	Rescue or ransom payment made by relatives or friends.
		Grassroots and advocates	Grassroots groups, online volunteers, or influencers help raise awareness or guide victims to escape.
		Failed rescue attempts	Rescue attempts that are blocked or intercepted. For example, armed local forces at borders to recapture escapees.
Abandoned	Survivors are abandoned due to inability to conduct scam work.	N/A	N/A
Retrafficked	The survivor is resold for money and further exploitation to other parks.	**Scam park transfers**	Victims are moved from one scam compound to another for continued exploitation.
		Bounty	Fraud parks issues bounties for escaped survivors to convince them to return.
		Sold for other exploitation	Victims are resold for non-scam exploitation (e.g., forced labor, sexual exploitation, or marriage).

Table 7: Codebook: Post-Trafficking – Support and Reintegration

Post-Trafficking: Support and Reintegration			
Code	**Definition**	**Sub-code**	**Sub-code definition**
Medical and psychological support	Victims are provided with healthcare, trauma counseling, or rehabilitation.	N/A	N/A
Legal procedure	Victims are engaged in legal process or receive legal aid to pursue justice, claim rights, or prevent deportation.	**Immigration and residency protection**	Legal help or processes provided to secure lawful immigration status, avoid deportation, or obtain safe repatriation.
		Criminal cases	Victims/survivors receive legal representation or participate in prosecutions.
		Identity and documentation support	Assistance in recovering or reissuing passports, IDs, or residency documents confiscated by traffickers.
Social reintegration	Victims attempt to rebuild their lives, reconnect with communities, and reintegrate into society.	**Family reunification**	Victims are reunited with relatives and work to rebuild trust and repair relationships affected by trauma or deception.
		Experience sharing	Victim shares their experiences with media networks, news, others in order to draw attention to the matter or to give information.
		Community support networks	Survivors connect with NGOs, peer support groups, or local communities for recovery.

Table 8: Codebook: Protective Strategies – Prevention and Response

Protection Strategies: Prevention and Response			
Code	**Definition**	**Sub-code**	**Sub-code definition**
Female safety tips	Empower women with situational awareness, self-defense knowledge, and clear steps for seeking help when needed, particularly in grooming or romance-related scams.	N/A	N/A
Legal and labor protection	Promoting access to legal aid, labor rights education, and official employment resources to reduce exploitation risks.	**Access legal aid and labor info**	Use official hotlines, labor bureaus, and vetted NGOs for rights and redress.
		Avoid illegal travel	Advises legal cross-border travel.
Caution	Encouraging careful evaluation of opportunities and interactions, including verifying job offers, staying vigilant online, and maintaining realistic expectations about overseas prospects and personal assets.	N/A	N/A
Indicators of scams	Spreads information on how to identify a scam or trafficking attempt.	**Withholding information**	Purposeful withholding of important information to delude or deceive an individual. They will try to waive suspicion.
		Third-party apps and messaging platforms	Use of unregulated platforms to avoid detection or track payments.
Rescue and emergency actions	Guidance on immediate actions, coordination, and information sharing to facilitate safe rescue from trafficking or fraudulent captivity scenarios.	**Emergency exit strategies**	Advice on safe escape routes from dangerous areas (e.g., KK compound) without triggering retaliation.
		Cooperation	Victims are encouraged to stay calm during rescue and provide accurate information to authorities, helping ensure safety and support effective investigations.
		Seek help	Advises victims to seek help immediately from relatives or local authority. Encouraged to give important details such as name, location, and condition.
		Contact trusted rescue teams	Encourages victims or families to work with trusted, legitimate rescue groups or authorities instead of unverified intermediaries.
Institutional support	Support from governments, embassies, NGOs, and digital systems. These range from anti-scam apps, awareness campaigns to legal protections, cross-border cooperation, and embassy assistance. Aims to prevent recruitment, aid rescue, and reduce re-trafficking.	N/A	N/A

Table 9: Codebook: Post Types

Post Types			
Code	**Definition**	**Sub-code**	**Sub-code definition**
News and awareness	The post shares a piece of news, summaries, or opinions to raise awareness about scam-fuelled human trafficking; may include brief commentary or discussion prompts.	N/A	N/A
First-person experience	The author of the post shares their first-person account of being a victim of scams that led to or might have led to human trafficking or as a previous fraud worker.	N/A	N/A
Asking for information or support	Poster is requesting for information or support regarding an incident or person related to scam-fuelled human trafficking.	N/A	N/A
Tactics against human trafficking	Poster gives advice against scam-fuelled human trafficking or posts about what tactics are used.	N/A	N/A