The Digital-Safety Risks of Financial Technologies for Survivors of Intimate Partner Violence

Rosanna Bellini[‡], Kevin Lee[*], Megan A. Brown[ϕ], Jeremy Shaffer[‡],
Rasika Bhalerao[γ], Thomas Ristenpart[α]

[‡]*Cornell University,* [*]*Princeton University,* [ϕ]*New York University,* [γ]*Northeastern University,* [α]*Cornell Tech*

Abstract

Digital technologies play a growing role in exacerbating financial abuse for survivors of intimate partner violence (IPV). While abusers of IPV rarely employ advanced technological attacks that go beyond interacting via standard user interfaces, scant research has examined how consumer-facing financial technologies can facilitate or obstruct IPV-related attacks on a survivor's financial well-being. Through an audit of 13 mobile banking and 17 peer-to-peer payment smartphone applications and their associated usage policies, we simulated both close-range and remote attacks commonly used by IPV adversaries. We discover that mobile banking and peer-to-peer payment applications are generally ill-equipped to deal with user-interface bound (UI-bound) adversaries, permitting unauthorized access to logins, surreptitious surveillance, and, harassing messages and system prompts.

To assess our discoveries, we interviewed 12 financial professionals who offer or oversee frontline services for vulnerable customers. While professionals expressed an interest in implementing mitigation strategies, they also highlight barriers to institutional approaches to intimate threats, and question professional responsibilities for digital safety. We conclude by providing recommendations for how digital financial service providers may better address UI-bound threats, and offer broader considerations for professional auditing and evaluation approaches to technology-facilitated abuse.

1 Introduction

Survivors of intimate partner violence (IPV) face considerable risks to their digital safety [16, 30]. Technology-enabled financial abuse — the exploitation, surveillance, restriction, or sabotage of a survivor's financial well-being [2] — can make it particularly challenging for a survivor to leave an abusive relationship, and maintain control over their own lives [23]. Abusers may gain unauthorized access to the survivor's financial accounts, manipulate or control their financial transactions, and limit their access to financial resources [2]. While the majority of IPV adversaries are constrained by the existing functionality of user-interfaces, or are 'UI-bound', to conduct such attacks [16], abusive and legitimate interactions with digital financial systems are often indistinguishable [2]. Thus, new methodological approaches are needed to uncover common pathways to tech abuse that go beyond vulnerability discovery [18] or bug hunting [59].

Our study presents the first empirical evaluation of consumer-facing financial technologies from the UI-bound adversarial threat model commonly used by abusers of IPV. First, we identify the most predominant financially-orientated sociotechnical harms associated with IPV technologies through a scoping review of academic literature. Then, through in-depth audits of 30 consumer-facing financial smartphone applications, we simulate and analyze both close-range and remote UI-bound attacks. We discover that several applications fail to notify users of changes in biometric authentication upon device compromise, facilitate financial surveillance by not requiring authentication when re-entering an app, and do not prevent users from receiving abusive or harassing content via payment memos or direct messages. To evaluate our findings, we conducted a series of 13 semi-structured interviews with 12 financial professionals. Doing so helped us to identify novel contextual risks factors for IPV survivors subject to financial abuse, and barriers to effective UI-bound adversary prevention in consumer-facing financial technologies.

To summarize, our paper makes three contributions:

- An audit on the resilience of consumer-facing technologies to UI-bound adversarial attacks in IPV contexts.
- Insights from experts on the opportunities for and the barriers to mitigating UI-bound adversaries in consumer-facing technologies.
- Research directions for UI-bound adversaries for other populations with significant digital-safety concerns.

Our research findings are already having a beneficial impact for survivors of IPV. All financial service providers in our audit received a copy of our results with one consumer security team sharing that it would incorporate the UI-bound adversarial threat model in an annual review of their consumer-facing smartphone and web applications.

2 Background and Related Work

Intimate partner violence (IPV) is a pattern of abusive behaviors, aggression, or violence between current or former partners in an intimate relationship [5]. Approximately one in three women, one in six men, and one in two people from non-binary and transgender communities will be subject to IPV across their lifetime [13]. Technology-enabled abuse ('tech abuse') of readily available UI-based systems has been well documented in IPV contexts, such as doxxing a survivor's home address online [17], surreptitiously stalking a survivor's physical location via GPS [3, 55, 58], or simply destroying a survivor's digital devices to restrict access [16].

While UI-bound adversaries have been reported to use advanced technical attacks against survivors, (e.g., manipulating internet on home Wi-Fi routers [55]), there is a tendency to over-emphasize their technical ability [17] and access to malicious hardware [6]. The reality is that simpler routes to harm can satisfy adversarial goals [3, 26, 55], are widespread, and cause immense damage.

Financial technologies and intimate threats. Mobile banking (MB) applications are smartphone-based apps that allow customers to conduct financial transactions remotely in lieu of visiting a physical branch. A branchless banking application, a subset of MB applications, only offers transactions online and does not have a branch network. With peer-to-peer payment applications (P2PP), consumers use a third-party website or app to send money to another person's bank account. Applications based on MB have traditionally used weak authentication schemes which operate entirely on a single device, creating a single point of failure [12, 19]. For instance, Reaves et al. [40] discovered serious vulnerabilities related to homemade cryptography, certificate validation, and information in MB applications. Smartphone-based vulnerabilities also percolate to other software storing financial information, such as unified payment interfaces (UPIs) [24], e-shopping websites [22], and e-wallet applications [33].

Such valuable works help to highlight software vulnerabilities, however, we have yet to discover works that focus on close-range adversaries whom are often already equipped with authentication information [15, 17], and may not be acting on 'for-profit' motives [53]. For instance, *intimate threats* [29], describe a class of common threats to a person's privacy and security, who can leverage their physical and psychological proximity to a person to cause harm. Financial products interface have been analyzed their potential to deceive or mislead users [11, 40], yet we believe we are the first to investigate how such applications may fail to prevent abuse to survivors of IPV. In so much, financial abuse — the control of access, use, or maintenance of financial resources — is rarely accommodated for in security analysis, despite its prevalence for vulnerable customers [14, 37].

The intersection of technology and financial abuse poses significant challenges for survivors of IPV [2, 10, 44]. As financial service providers promote digital or online banking for daily interactions, abusers have exploited this shift to take control of survivors' finances [23, 37]. For instance, abusers may use dual-use applications — legitimate applications repurposed for harm — including social surveillance apps to monitor and control access to bank accounts, credit cards, and other financial resources [2]. Such tactics can extend into the areas of social engineering and social deception, such as identity theft (specifically 'catfishing') [2, 51] to target a survivor, their children, and family. The complexity of technology-facilitated financial abuse experienced by IPV survivors has led many to emphasize the need for comprehensive policies and support services [13, 23].

Audits for system abuse. Consumer-facing software may go through multiple stages of testing before launch. A product may commonly undergo user acceptance testing (UAT) during which hired subjects are given predetermined objectives and scripted test cases as they interact with it. A company may also use bug bounty programs to incentivize ethical security hackers to audit its released products, and these have been economically beneficial in fixing additional software bugs [59]. Nevertheless, such audits overestimate the barriers to entry for most real-world attacks [49]. Furthermore, user testing may only consider the 'average user' of a product against a highly sophisticated adversary [21], overlooking users at risk of digital-safety concerns that emerge out of complex social contexts, such as natural disasters, forced displacement, or interpersonal harm. While these quality assurance measures may help catch most software bugs, their fixed nature may fail to consider harm of these systems in the wild.

As Narayanan and Lee argue [35], unsophisticated attacks may do the greatest damage, since anyone, no matter their technical skill set, could become an adversary. In spite of calls for their creation and wider use, few methods exist for eliciting consumers' concerns about digital security [9, 46, 48, 50]. Several calls for 'considering' [30] or 'centering' [28, 47, 50] the perspectives of marginalized or at-risk users do not provide guidance on how to analyze risk [18], or on how to balance or triage multiple perspectives [41, 57]. Freed et al. [16] offer the closest suggestion for how to pragmatically evaluate system design for their potential to cause harm by means of *safety reviews*. As a specialized form of penetration testing, these could be conducted prior to product launch through cognitive walkthroughs. Inspired by these prior works, we make transparent what a methodological approach to eliciting digital-safety concerns might look like, in the context of consumer-based smartphone applications.

3 Methodological Approach

Our high-level goal is to identify digital-safety concerns in consumer-facing financial technologies and to do so, ideally, before survivors need to come forward to report such abuse. We used a variety of complementary methods to achieve this

Method	Description	
Scoping review	Literature search for sociotechnical harms and adversarial tactics in financial contexts.	§4
UI stepthroughs	Identification of key application features, and manual stepthrough via simulated UI-bound adversarial attacks of 30 consumer-facing financial smartphone applications	§5
Policy analysis	Analysis of ToS and AU policy documents on publicly-accessible P2PP applications	§6
Abuse scenarios	Creation of three abuse scenarios to synthesize audit findings to engage non-stakeholders	§7
Expert interviews	Conduct a series of semi-structured interviews with financial experts for evaluation and guidance	§8

Figure 1: Our methodological approach to elicit digital-safety concerns for IPV survivors in consumer-facing financial applications.

goal; relying on a structured sequence of auditing steps to design a threat model audit, analyze our results, and evaluate our discoveries with financial experts. In this section, we state the UI-bound threat model, data collection methods (summarized in Figure 1), our resulting analysis, and cover research team ethics and expertise.

Threat model. We presume a common characteristic of adversaries that target survivors of IPV ('abusers') is that they know a large amount of confidential information about their target, such as their routines and authentication information. We also presume that an adversary has access to their information, devices, or may be able to easily gain access to this through coercion or surveillance. Other threats, such as adults to minor children [44], adult children to elderly parents [25], caregivers to dependents [45], and housemate to housemate [29], all have similar threat model characteristics that significantly overlap with this threat model. Thus, we presume that some of our discoveries may be generalizable to groups exposed to similar threats outside of IPV contexts.

Scoping review. We hypothesized that grounding our audit in the context of situations involving IPV could help surface more damaging cases of abuse, and having the most extreme trust, safety, and privacy violations come to light could enhance the experience of all users [30, 57]. As survivors of IPV experience a severe, immediate threat, and, receive a lack of attention from financial services, we also hypothesized our results would be timely to such individuals. To identify adversarial attacks and goals, we conducted a scoping review [34] of tactics known to be typical of adversaries of the population (Section 4). We also reviewed relevant academic articles on other at-risk groups, media stories, or other secondary data sources. Using *adversarial thinking* (characterizing aspects of an adversary's mindset [43]) helped us to conceptualize timelines and contextual factors for attack vectors.

UI stepthrough. We conducted a methodical investigation into the UI features of the technology being audited (Section 5). We aimed to understand the set of features offered, as well as how they they might aid or inhibit a UI-bound adversary intent on causing harm to IPV survivors. Using the *UI-bound adversary* model as an intimate threat established that an adversary often knows, or can gain access to, authentication details, so a focus on stepping through authentication flows was important. Alternatively, if adversaries are likely to cause harm by sending emotionally abusive messages, then auditors might pay attention to communication features. We refer to a sequence of UI actions an abuser can take to cause harm as an *abuse vector*.

Policy analysis. In addition to exploring the abuse of technical mechanisms in our UI audit, we explore the permissibility of these abuses in publicly-accessible technical policy documents. Tech abuse cannot simply be 'designed out' [50], thus we needed to investigate what legal recourse survivors may have to the potential harms surfaced in our stepthrough. By analyzing Terms of Service (ToS) and Acceptable Use (AU) documents, this can help to situate these vectors in the wider technical ecosystem. We incorporate a policy review as a distinctive step to identify harm and abuse to evaluate abuse mitigation by measuring: acceptable and unacceptable user behavior; a system's acknowledgement of a (high-level) attack vector; and potential sanctions for an adversary. None of the applications we analyze overlap with Reaves et al.'s [40] study of seven branchless banking ToS (Airtel Money, GCash, mCoin, Oxigen Wallet, MoneyOnMobile, and Zuum), but our results may complement their findings.

We acknowledge that how policies are implemented in practice does not always reflect in how they are written [26]; however, they can provide a high-level insight into how applications can prevent or exacerbate abuse.

Abuse scenarios. We synthesize information collected via our audit and policy analysis to create three abuse scenarios, describing a series of events with a digital system that lead to abuse. Each scenario described a set of hypothetical events conducted through a consumer-facing technology in relation to intimate threat contexts. Transforming research findings into a story-like format has been shown to facilitate observational learning about security [39], are more likely to be remembered [36], and focus on harm done to an end user rather than a system [48].

Interviews. We evaluate the findings of our search, audit, and analysis, via in-depth interviews with a panel of financial experts. Interviews were conducted in a semi-structured manner, which allowed us to balance standardized questions with flexibility to explore additional topics raised by experts (see Section 8 for protocol). This method enabled us to delve deeply into their opinions, experiences, and recommendations related to the research findings.

Research team. Our auditing team brought together expertise on security, research methods, and insight into survivors

of IPV. As abuse is highly contextual, the research team includes members with extensive experience researching other at-risk groups, including IPV survivors, young adults, and sex workers. All team members also have experience in delivering frontline services to survivors of technology abuse, thus ensuring a correct amount of focus is paid to problem devices or services [17], rather than identifying flaws which are novel for an academic audience [26]. We complement this knowledge with other experts on consumer-facing policy agreements, methodological approaches to auditing, and threat modelling. Two team members are also working with a major financial institution to maximize the positive impact of this research on improving the financial safety of survivors.

Ethics. Our study, consisting of desk-based analysis, application stepthroughs, and interviews with financial professionals all underwent review by our institutional review board (IRB), and received approval prior to commencement. The audit analysis required no reverse engineering of software code, access to application stores outside of our study area, or any deceptive interaction with personnel at the financial services we audited (i.e., mystery shopper methods) [27]. Each team member was only asked to share the names of banks and financial products they held; no personally identifiable information (PII) was shared.

Since financial abuse is an emotionally charged topic, and most of our interview subjects had access to at-risk users, we took great care to protect their privacy. Each interview participant received an information sheet and a consent form that permitted participants to choose between the first author audio recording or taking non-identifiable notes of the session. We collected a reduced amount of demographic information (as reported in Table 3), and requested that interviewees not disclose any customer or service user PII.

Participants who consented to audio transcription were notified of, and agreed to have their responses transcribed by a trusted third-party transcriber service. The service has extensive experience transcribing research data for other projects, including at-risk groups (including IPV) for researchers, and redacts all identifiable information before returning the data for analysis. Data were then uploaded to a secure server accessible only to research team members and audio files were deleted following transcription. To further protect the identities of those involved, we use pseudonyms to distinguish interviewee accounts (P1—P12), and have lightly edited quotes to remove idiosyncratic words or phrases.

Responsible disclosure. Sharing the application names we tested may provide adversaries with new insights on harming users. In accordance with emergent best practices (e.g., see [16, 55]), we do not provide step-by-step instructions for replicating possible attacks. Furthermore, adversaries are already using consumer-based financial technology in UI-bound attacks [2, 40]. As such, we argue that safety concerns need to be highlighted to reduce risks for at-risk groups.

Harm category	**Financial sociotechnical harms**
Denial of service	Account and/or device control Account and/or device lockout Closure of account Denial of account creation (‘pre-hijacking’)
Harmful content	False abuse reporting Notification bombardment Private information exposure (‘doxing’) Profane/offensive content Spamming
Misrepresentation	False data and/or evidence Identity theft Impersonation (‘catfishing’)
Surveillance	Account and/or device monitoring Location tracking
Theft	Fraudulent payments Steal personal data

Table 1: Summary of the 16 sociotechnical harms identified via our scoping review, organized into five high-level categories of harm.

A responsible disclosure scheme was used to notify all organizations of named applications of UI-bound attacks. We included basic details of accepted mitigation practices for each finding. We noted that all organizations did not have a designated area for reporting digital-safety concerns outside of vulnerability or bug reports.

4 Scoping sociotechnical harms

As technology-facilitated abuse is the interplay of technical systems and social factors [31, 42], we focus on *sociotechnical* harms—harms that are technical in method but having social outcomes. We define sociotechnical harm as actions that subject a group or a single individual(s), to experience physical, psychological (mental, emotional), social, financial, sexual and legal damage or injury. We did this to identify typical adversarial goals with respect to harms to survivors of IPV, striving to look beyond the presumed for-profit (economic) mindset of many threat models [2, 53].

To identify sociotechnical harms specific to survivors of IPV, we conducted a rapid literature review [34] of known attack descriptions involving technology-enabled abuse (‘tech abuse’). We conducted a keyword search in April 2022 of search terms associated with technology-enabled abuse in IPV contexts [15, 16, 20, 60] using the ACM Digital Library, IEEE Xplore, and USENIX Paper Proceedings. We re-performed this search in November 2022 to identify missing papers.

Our initial search elicited 81 papers. We chose to include full-length works, where abuse of consumer-based technologies were the primary focus, were conducted in an IPV context, and were supported by empirical data. This resulted in 10 works from which to extract data (Appendix A, Table 5).

Application Type	Application Name
Mobile Banking (MB)	Amex, Bank of America Mobile Banking, Betterment, Capital One Mobile, Chase Mobile, Discover Mobile, Marcus, Monzo, PNC Mobile Banking, Revolut, Starling, TD Bank, U.S Bank
Peer-to-Peer Payment (P2PP)	Apple Cash (via Apple Pay), Azimo, Cash App, MoneyGram Money Transfers, Paypal, Remitly, Ria, Strike: Bitcoin & Payments, TransferGo: Money Transfer, Venmo, Western Union: Money Transfer, Wise, WorldRemit, Xoom Money Transfer, Zelle

Table 2: Complete list of all mobile banking (MB) and peer to peer payment (P2PP) applications tested.

We then extracted and pooled the sociotechnical attacks and resulting harms of each paper through analyzing attack taxonomies and qualitative findings. Next, the lead author systematically evaluated each type of harm and associated attack description against our area of study. For instance, *"impersonate victim using their accounts to cause them harm"* [16] was deemed in scope as an adversary could 'catfish' a survivor through P2PP application. However, outsourcing attacks for surveillance, such as *"hiring a private investigator"* [55] was judged to be out of scope. The sorting approach was validated by a second author through structured dialogue. This review resulted in identifying 16 sociotechnical harms (Table 1).

5 UI stepthroughs

Following our synthesis of sociotechnical attacks and harms sourced from the literature, we conducted a UI stepthrough analysis of 30 consumer-facing financial technology smartphone-based applications ('applications' or 'apps' hereinafter) displayed in Table 2.

App selection. Many MB applications require significant amounts of PII to set up an account, such as nation-issued identification (e.g., social security number (SSN)) in the United States (US). Our research team used a convenience sample of MB applications to avoid leaving a permanent, and potentially detrimental record of opening a bank account on any of their financial records. To do this, we chose to only review mobile accounts that were owned, and actively used, by the research team. In contrast, P2PP applications required less PII, did not report open accounts to credit bureaus, and facilitated relatively speedy account closures. These factors minimize the detrimental risk to research team members' financial well-being. As such, we selectively sampled beyond our convenience sample of P2PP applications with 10 more applications sourced from the *Top 10 Most Downloaded* (downloads per/cal month) applications in the Finance categories of the North America-regional App Store and Google Play store.

We conducted an in-depth analysis of 13 MB applications and 17 peer-to-peer payment applications (Figure 2). Our 13 MB include applications from six of the ten largest consumer banks by number of customers in the United States (U.S.) [1]. Collectively, these 30 applications serve millions of users across the U.S. and beyond. Our goal was not to obtain an exhaustive survey of all relevant financial applications (e.g., see [40]), or to conduct an evaluation of specific authentication approaches, but to provide a reasonable cross-section of the financial applications marketplace in the US.

Feature scoping: UI-analysis process. We present a subset of a larger feature scoping study in this work, which focuses on each of the following functionality: *account creation*; *authentication (login and re-access)*; *payment*; *account activity screens*; *user-to-user communication*; and *contacting customer service*. These areas were selected in accordance with our enumerated harms we identified in the previous literature and are common specific attack surfaces that were consistently targeted by adversaries (Section 4). As abusers of IPV use relatively technically unsophisticated attacks of standard consumer-facing technologies (Section 3), we did not manually analyze code for software vulnerabilities (unlike [8, 40]) or attempt to escalate access privileges [19] (see Section 3).

Using our research team's iOS and Android-based smartphone devices, we conducted our UI stepthrough analysis in three rounds between February 2022 to January 2023; first, examining P2PP applications, then examining MB—note that account creation was skipped for the MB applications only. Each team member followed a structured protocol that required text-based descriptions, screenshots, and occasional demonstrations of the applications to record the functionality of each app. Each member was required to present their findings—along with screenshots—at regularly-scheduled team meetings during this time period.

Stepthrough protocol. First, each researcher downloaded an up-to-date version of the application from the Play Store or App Store. To combat familiarization effects and encourage investigation, researchers were assigned P2PP applications if they did not already have an account. After installing an up-to-date version of the application, we registered for an account (for P2PP applications) using our personal information, noting the amount of PII needed, unique identifier (UID) associated with the account, and relative password strength suggested. For all applications, we recorded if the user was prompted with the option to change their method of authentication (e.g., to biometrics, PIN, pattern), and *'Remember this device'* (e.g., trusted device to skip 2FA) for convenience.

We examined the privacy settings on the application's social feed (if P2PP), such as default visibility for transactions and the option to change this. Payment protections such as limits for sending, receiving, cashout (cash withdrawal) were also recorded, paying particular note to limits imposed if the user is verified, alongside remotely freezing cards, viewing card information, and viewing or changing PINs. We also explored the transmission of abusive or offensive phrases in the memo field of test transactions, noting the minimum transaction amount required to do this. To conclude, we looked

for anti-harassment controls in the app, such as controlling requests for payment, the abilities to report or block an abuser, and the ease of contacting customer support.

5.1 UI stepthrough analysis findings

According to our UI stepthrough analysis, most MBs and P2PPs are vulnerable to some forms of access-based and remote attacks in IPV contexts. These harms are further compounded by a notable lack of customer support or guidance that directly addresses financial abuse to assist a survivor further if abuse were to occur.

We report our findings based on two primary UI-bound threats that IPV survivors report experiencing [16]: an adversary who can leverage **physical proximity** to a survivor's device to compromise a survivor's account; and, an adversary who uses legitimate access to **remotely attack** a survivor. In each instance, we used adversarial thinking and documented behavior of adversaries in IPV [3, 55] contexts to simulate both forms of threats. A comparative table of all our results can be found in our Appendix, Table 10, and Table 11.

5.1.1 Physical proximity, compromised access

Adversaries commonly leverage physical access to a survivor's personal devices [16, 30] and may add their own biometrics (e.g., face, fingerprint) to authenticate as a survivor [2]. For this threat model, we simulated an adversary who had *physical* access to a survivor's trusted smartphone device, and could authenticate as the survivor to achieve *compromised* account access.

Adding adversarial biometrics. Adversaries can add biometric information to a device surreptitiously while a survivor may be distracted [2, 16], for example, while a survivor is asleep or has left their phone unattended [3]. We trialled if adding a new fingerprint belonging to the adversary to TouchID on iOS and Fingerprint Unlock on Android would result in a visible, noticeable alert to the user next time a MB or P2PP app was first launched or accessed.

None of the P2PP applications (0 of 17) we trialled alerted the user of a change in biometrics—either on iOS or Android, nor forced users to sign out when these biometrics were changed. All MB applications we tested forced a sign out to users when biometric changes are detected, prevented the use of biometrics for re-entry, and displayed an operating system (OS)-based security alert. However, there were inconsistencies in how users were notified of these changes. TD Bank, Chase, and Amex do not notify a user when changes were made to TouchID or FaceID, such as when an adversary added a fingerprint or an alternative look (another face for FaceID). In such instances, while each user was forcibily logged out, the reason for the action was unclear—an alert is merely displayed that biometrics are currently unavailable as a login method. This threat is more acute when considering that we identified that a minority of P2PP (7 of 17) and MB (2 of 13) apps prompted users to add biometrics — so as to bypassing the knowledge of a username or password — for future login attempts.

Unauthorized entry on login. In line with prior work [19], we find that most P2PP applications (8 of 17) still prefer to use one app authorization (1AA) for login via a trusted device—a username and password pairing alone. Conversely, two-factor authentication (2FA) is now present by default in nearly all of the MB we trialled (12 of 13), and we discovered only a single MB application—Monzo—that requires users to log in to their bank account via a one-time-use link (a 'magic email') to a user's email account, with no option for a user to change this setting. As account and device compromise are common in contexts involving IPV [15, 20], this makes this form of authentication highly susceptible to unauthorized entry into a financial application.

All P2PP applications we tested were vulnerable to ongoing intimate surveillance. Users were not asked to input biometrics to re-access the application once they had been successfully authenticated via username and password.

Theft of financial information. Most applications required an additional step of authentication prior to sending payment on the account; traditionally by the use of biometrics or 2FA depending on the configuration of the settings. As such, if an adversary was interested in tampering with a survivor's account — for instance, making a fraudulent payment — they could only do so if they had previously added their biometrics to a survivor's device. Once authorized, we discovered several applications that permitted the user to view and change a PIN number associated with an account without additional authentication challenges.

Many MBs and P2PPs also provided users with physical debit or credit cards that were visually represented in the application. Viewing personal identifiable numbers (PINs) associated with the cards was possible on four MBs (Amex, Monzo, Revolut, and Starling) and on all three P2PP which also had physical cards associated with the accounts (Cash App, Venmo, Wise). We also identified that 11 MB apps and the same three P2PP applications permitted users to freeze associated cards instantaneously without additional challenges as an 'anti-theft' mechanism. Opting to freeze a card could enable an abuser to block or restrict a survivor from using the physical card associated with the account.

5.1.2 No physical access or compromised account access

As is common in many situations involving IPV, access to a survivors' account can be lost if a survivor is no longer cohabiting with an abuser [30]. For this threat model, we simulated an adversary who does not have physical access to a survivors' account or device, and may not require authentication information to pose as them.

Pre-hijacking and impersonation. Most P2PP applications requested a first and last name (7 of 17), three applications requested a full address, while four applications re-

quested a date of birth for account creation. Formal governmental identification such as visual scans of driver's licence, passport, or SSN were not requested by any of the P2PP trialled. As account creation took relatively little effort on behalf of an adversary, and with minimal amounts of PII shared, it is reasonable to presume that an adversary could prevent a survivor from signing up for an account in the future, what is called a pre-hijacking attack [52]. Such minimal amounts of formal identification also leaves a lack of a transparent paper trail, also potentially resulting in account impersonation ('catfishing'). This has the potential to damage a survivor's reputation or leverage a survivor's social capital to fraudulently coax friends and family for financial gain.

Remote surveillance. A variety of mechanisms can be used to surveill an intimate partner without their knowledge [55]. A sizeable number of P2PP applications (5 of 17) had the visibility of high-level descriptions of financial transactions set to public; two of which meant visibility to any user either signed up to use of the app (2 of 17), and three to whomever possessed the uniform resource locator (URL) to a survivor's account (3 of 17). This can permit remote adversaries to view details about a survivor's financial history, including the payment amount, the receiver, a date, and (where possible) short text and emoji-based messages. In collation, an adversary could use this information to learn about a survivor's movements to stalk, or surveil their financial wellbeing. None of the MB applications permitted any external parties to view transaction data — an unsurprising result considering the restrictions on the visibility of customer data at a federal level.

Text-based harassment via payment. Alongside testing the visibility of existing transactions, we simulated an adversary that harasses a survivor remotely through interacting with them in-app, such as via a legitimate payment, continuously sending requests for money, or adding them as a friend. First, through interacting with the memo or reference field (a text-based box that allows the initiator of a transaction to add a tag for future reference), we trialed the use of crude language, English-based expletives, and suggestive emojis (e.g., emojis associated with genitalia). Our trial revealed that none of the MB (0 of 13) nor P2PP applications (0 of 17) prevented the user to send any of these categories of harassment that could accompany a transaction to a survivor. Most (17 of 30) apps employed some form of content moderation — Wise, for instance, prevented special characters from being included in memos — but this moderation was not geared towards stemming hateful messages.

Twenty two of the total 30 applications we trialled have minimum spend requirements of less than $1.00 to send financial payments to another user. Adversaries could potentially repeatedly exploit this in their direct interactions with survivors in these apps, while also pairing this with abusive messages in micro-payment transactions.

Lack of anti-harassment measures. UI-bound adversaries are often successful in abusing survivors as many interactions are not identified as necessitating customer support. Only 2 of 13 MB in our audit — Monzo and Starling — deployed explicitly anti-harassment measures; functions that permitted a user to limit, report, or block users or accounts from sending or requesting money. These low numbers were also reflected in P2PP applications, of which only 4 of 17 allowed the user to block other users by selecting an option on a payee's profile. A mere 3 applications had reporting functions that allowed users to isolate a transaction or a user interaction for misconduct. Just 6 of 17 allowed users to directly contact customer support from the application without being redirected to a website or a pre-written set of FAQs — none of which addressed harassment or IPV. If survivors are financially harmed through these applications, we found that they encounter many pages that do not display help and support information; potentially prolonging abuse from a persistent, remote adversary.

6 Policy review

While our UI-stepthrough aimed to identify possible areas for tech abuse mitigation, we acknowledge that motivated adversaries will still find ways to harm survivors. We conducted a content analysis of the digital Terms of Service (ToS) and acceptable use (AU) policy documents of 16 P2PP apps to identify policies which create or mitigate vulnerabilities for financial abuse for survivors using the application. *Azimo* was deprecated between stage one and stage two, thus this analysis covers the policy documents of 16 applications (Section 5).

We analyzed the policy documents for the P2PP applications only, as the ToS and AU policies represent the full agreement between a user and the application. MB organizations also require a user to sign additional contracts with users that are not publicly available, therefore replicating any content which appears in the policy documents (i.e. quoting their text here) is a violation of the agreement to not disclose private customer information for responsible disclosure (Section 3).

Two members of the research team identified the policy agreements for each application by searching the website of each application for the ToS (also known as Terms of Use, ToU), and for the AU policies if one existed. A full list of the ToS and AU policy documents covered in this audit can be found in Appendix 7. To focus on technology abuse, we then manually examined the five policy documents of each application that could be exploited by intimate threats (Section 5.1). To do this, we focused on exploring if the policy documents state that: (a) one must only act on their own behalf when creating an account or using the service; (b) an authorized user can act on behalf of the account owner; (c) the account owner is solely responsible for maintaining the security of their username, password, or other authentication credentials; (d) the platform cannot be used for fraudulent purposes, and (e) the platform cannot be used for harassment. Each of these clauses address the issues of compromised

access and remote harassment to determine if an account owner (e.g., a survivor) is responsible for another's (e.g., an adversary) actions.

6.1 Terms of use findings

Out of the 15 apps we analyzed, eleven clearly stated that the responsibility for another person using one's account credentials belongs to the account owner. We identified three applications (3 of 16) that clearly stated an authorized user — a user that receives authorization from another to act on their behalf — as an account owner. Of the 16 apps, seven stated that one must only act on behalf of oneself in their interactions through the application. The policy documents of four applications (4 of 16) used language that did not state 'act on behalf of oneself' explicitly, and used unclear language to result in loopholes such as: (1) stating that 'one cannot impersonate another person', and (2) 'one cannot use an account that does not belong to them.' Both of these loopholes ensure that an adversary can claim that they were not actively impersonating a user when using their account or device. In addition, if an adversary themself does not have an account, then this could be a way to avoid sanctions. A twelfth app's policy stated that the account owner is not permitted to allow anybody else to access their credentials.

Of the policy documents for the 16 apps, only five (5 of 16) included a policy against using the platform for harassment — therefore actively acknowledging that their application could be used as such. Perhaps unsurprisingly, applications that possessed a memo or personalized message feature (Paypal, Venmo, CashApp) associated with payments more often had rules against harassment. Eleven apps contained policies explicitly declaring that the app could not be used for fraud, and four more apps stated that the app could not be used for carrying out "unlawful actions" but did not specify fraud as one of the actions.

Taken together, these findings show that often, ToS may limit the extent to which survivors can access remedies when they have been harmed by abusers via P2PP applications. As we shall outline in the following section (Scenarios A, B), adversaries rely on normal account authentication practices, in which case survivors may not be protected by terms of service regarding unauthorized use.

7 Crafting abuse scenarios

To gain a deeper understanding of an IPV adversary's capabilities (to complement our threat model in Section 3), as well as to develop a holistic view of security threats, we created *abuse scenarios*. To design our abuse scenarios that covered a broad range of financial abuse pathways through our chosen applications, two authors with direct experience of working with survivors of IPV constructed textual descriptions of action sequences. This required utilizing a combination of deductive reasoning, adversarial thinking, and professional experience to theorize how an adversary could use a system to harm a survivor which we explicate here.

Transforming findings into scenarios. We first collated our findings from our two simulated intimate threat attack models (Section 5.1) and policy analysis (Section 6.1). In our analysis, we chose to prioritize adequate coverage of the range of technical attacks over specificity to be platform-agnostic and ensure that participants would not disengage if they did not provide a service.

Through this approach we identifed **three preconditions** and **two presumed goals** of the adversary that enabled such attacks through the P2PP and MB applications. We identified that an adversary needed to: have device-based access, have compromised account-based access, or interact with a survivor's public profile to conduct the full range of the 16 sociotechnical attacks identified. We categorized attacks based on whether the adversary was motivated by financial goals, or non-financial or social goals.

Two versions of each scenario were made; one initial, *extensive* abuse scenario that had a full description of basic pathways, alternative pathways, triggers, mitigation points, and an in-depth adversary profile[1], and one *distilled* abuse story that provided a high-level overview for stakeholders. Two security professionals clarified our scenarios by offering suggestions on how to represent other characteristics of at-risk groups [41], so as to not portray the 'average' user [18, 53]. As such, we chose to construct three scenarios (depicted as Scenarios A, B, and C in Figure 2), each representing different at-risk characteristics as they intersect with IPV; young adults (A), stigmatized sexualities (e.g. lesbian, gay, bisexual, asexual individuals, etc.) (B), and genders (e.g. trans, intersex, non-binary individuals, etc.) (C).

8 Interviews with financial professionals

To validate our findings on UI-bound intimate threats and to evaluate our methodological approach, we conducted 13 semi-structured interviews with 12 financial professionals. Such individuals had experience of working with, or overseeing the delivery of services for survivors of financial abuse.

Our 12 participants came from ten different organizations. Eight participants (N=8) came from specialist non-profit organizations for survivor assistance and advocacy, financial counselling, low-income support, and legal guidance. For readabililty purposes, we refer to this set of interviewees as *financial support workers* (FSWs). In contrast, four participants were employed at *financial service providers* (FSPs), including two banks, an insurance company, and an investment house (see Table 3).

Recruitment. Participants were contacted via professional mailing lists and were required to have direct frontline or management experience with survivors, and possess a minimum of

[1] A copy of an extended abuse scenario can be found at this link.

Scenario A.
Daphne$^{\alpha}$ and Jonas$^{\alpha}$ have been together for several months and both attend the same college. Using her mobile banking app, Daphne has linked all of her bank accounts to her main bank account's data visualization screen. She secures her banking application with her fingerprint. After accusing Daphne of sexual infidelity, Jonas adds his thumbprint to her iPhone surreptitiously to unlock it. Daphne is not alerted that her biometrics have changed, so she is unaware that Jonas accesses her account while she sleeps to set up monitoring alerts to his number. The first thing he does is inform Daphne which spending categories are too high, in order to motivate her to adhere to his frugal attitude to spending and finance.

Scenario B.
Venture capital funding has led Mark$^{\alpha}$ and Hendrick$^{\alpha}$, a long-distance couple, to open up a joint business venue together. To transfer money to his own personal bank account, Hendrick regularly logs into Mark's business account remotely via his own smartphone, which was authorized previously by Mark. While Mark is aware of Hendrick's behavior, knowing Hendrick has been in considerable debt for some time, he fears that Hendrick will follow through with his threat to report Mark for misuse of funds. His belief is based on the fact that he attempted to contest the claim of fraud with the bank, but the bank said he would be held liable for any lost income. All transactions are in Mark's name with his authorized devices.

Scenario C.
Shaquille$^{\alpha}$ and Aisha$^{\alpha}$ have been legally divorced for several years and share three teenage children of whom they both financially provide for. Shaquille's new family members are regularly harassed by Aisha, who has old photos of his identification cards and passport which she uses to create numerous fake accounts in his name. In many mobile banking payments, Aisha uses the reference box to write abusive messages when any sort of financial reimbursement is required at family gatherings with the children. Shaquille can block Aisha, but he still needs to stay in touch with her for parental contact. When he complaints to the application's customer service they are unhelpful and take several days to take down fake accounts.

Figure 2: UI-bound abuse scenarios A, B, and C. *Scenario A* describes a non-financially-motivated adversary with device access; *Scenario B* describes a financially-motivated adversary with compromised access; and *Scenario C* describes a non-financially motivated adversary with standard account access. $^{\alpha}$ denotes the use of a pseudonym.

12 months of experience at their current organization. Participants (N=7) who were recruited via professional mailing lists then recommended five others (N=5) in their sector to help elicit further insight. Our attempts to recruit further FSPs was unsuccessful, with many individuals declining the invitation citing concerns around sharing proprietary information.

All participants were offered complementary technology abuse training in-lieu of payment due to many organizations barring financial compensation for participation in research. This training was taken up by four participants and delivered by two members of the research team.

Interview protocol. Interviews were conducted by two members of the authorship team, either by video-conferencing (N=9) or in-person (N=3) at a neutral location chosen by participants. Due to a conflict in their schedule, one participant requested a two-part interview. Each interview lasted between 35–75 minutes (M: 42, SD: 6).

Participants were first asked about their knowledge of technology and financial abuse (particularly the intersection of), and how this occurred in client cases. Afterwards, we asked about emerging patterns in client cases and how they responded to actual or theorized UI-bound adversaries in their organizations. We did this through presenting our three distilled abuse scenarios, which we theorized would have the added benefit of mitigating the risk of private information being disclosed about real cases and help us evaluate the benefits and drawbacks of performing our audit. Two question protocols were used to match the professional background of the interviewee (see Appendix A), where FSPs were asked about the security tools for customers, while support seeking behaviors in greater depth with FSWs.

Nine participants agreed to be audio recorded while three participants (all FSPs) consented to detailed notes being taken in the interview. Recorded interviews were then transcribed by a professional transcription service and resulted in 96 K words or 192 pages (500 words/page) of data for analysis.

Qualitative data analysis. We used open inductive coding in accordance with Lewis and Ritchie's framework analysis [38] to qualitatively analyse our interviews. Two members of the authorship team reviewed the transcripts in full before coding a sample of four transcripts to generate an initial set of codes of 52 codes (*digital red flags*, *poor financial practice*, *weak biometric authentication*). The authors then jointly coded the remaining transcripts, meeting up over the space of three months to reconcile coding differences. Synthesizing our codes led to the development of six themes.

Our final codebook (see Appendix A, Table 4) consisted of 46 codes (*repairing financial harm*, *financial forensic investigation*, *customer activity endpoints*). Inter-rater reliability (IRR) was calculated by a random sample of 30 lines of transcripts across the 12 participants showing coding agreement in 26 of 30 lines (Cohen's kappa of 0.89 [32]).

8.1 Interview Findings

We present our findings from our interviews in two complementary parts: professional responses to our audit findings (Section 8.1.1) and identified barriers to customer protections against UI-bound adversaries (Section 8.1.2). We elicited insight from financial professionals about *contextual risk factors*, information on *other at-risk groups* (e.g., elder financial abuse), and the *limitations* of our abuse scenario exercise (Figure 2) to combat a UI-bound threat. Our participants also reflected on the barriers to preventing further harm to IPV survivors, including the risk of watering down *policy that could prevent other harms*, the desire to *re-purpose existing safety systems*, and *the need for professional tooling* for UI-bound threat detection.

Note that *client* is often used to refer to survivors in advocacy settings, while *offender* or *fraudster* are common placeholders for adversaries.

ID	Gender	Experience (Y)	Job Title	Job Role
P1	W	16-20	Support Service Management	FSW
P2	W	11-15	Support Service Management	FSW
P3	W	1-5	Policy Researcher	FSW
P4	W	11-15	Policy Researcher	FSW
P5	W	1-5	Financial Planner	FSW
P6	M	1-5	Customer Security Contractor	FSP
P7	W	11-15	Financial Planner	FSP
P8	M	21-25	Financial Advocate	FSW
P9	M	6-10	Customer Security Contractor	FSP
P10	W	26-30	Consumer Lawyer	FSW
P11	W	1-5	Financial Planner	FSW
P12	M	6-10	Branch Manager	FSP

Table 3: Participant demographics including participant number, self-identified gender, years of experience in financial services or support, and current job profession as a financial support worker (FSW) or financial service provider (FSP).

8.1.1 Evaluating audit findings

The use of our abuse scenarios elicited further understandings about UI-bound adversaries; namely contextual risk factors and lessons for other intimate targets. At the same time, interviewees felt limited in preventing such threats, because the narratives were unable to demonstrate the prevalence of UI-bound adversaries. In this theme, we share the lessons learned about MB and P2PPs in IPV contexts, and the drawbacks of using fictional accounts of financial abuse for engagement.

Surface contextual risk factors. Most professionals (n=9) were unfamiliar with our findings on P2PPs on their use of weak authentication methods (e.g., 1AA), but a few (n=3) had heard reports of account takeovers via smartphones (c.f. [60]). Scenarios A and B seemed to resonate with most professionals, each reporting several cases of account compromises that affected their clients. For instance, after learning about a hidden financial account through shouldersurfing, an interviewee reported that a survivor's personal device was compromised in a similar manner to Scenario A (device compromise):

> *"... he saw that she had [P2PP] installed on her phone ... the offender had already added his fingerprint is on there so ... he transferred all the money out ... and that was the end of that"* (P11)

A number of participants (n=4) agreed that setting up an alternative form of income without the use of P2PP was difficult. Prior works suggest that P2PP applications are mostly used for casual, social situations [11], but professionals shared that these services can serve as way to hide money, especially from an adversary who controls a main bank account. When survivors were under the control of a perpetrator, they often lacked the official government identification they needed to open another bank account. The use of images of formal identification could, however, be used for setting up P2PP accounts discreetly. As most P2PP applications do not require a debit card or bank account to join (Section 5), professionals such as a manager of a financial support service (P2) noted that a lack of a digital footprint could be traced back to a survivor by an adversary:

> *"We're hearing things ... like survivors storing money in their [P2PP] account ... their family sends them money, then they leave it there ... it's allowing survivors to squirrel away an escape fund"* (P2)

In a few cases, case workers and managers (n=2) described mapping out a survivor's financial history by asking specific questions about how they used P2PP and MB to identify areas where a survivor may be inadvertently monitored by an adversary. Nevertheless, the majority of professionals (n=7) were cautious when recommending or encouraging the use of such protective strategies, noting: *"if they're using them [Venmo, CashApp], great, if they're not well ... we don't recommend them"* (P9). Due to the lack of authentication and security, P2PP applications were considered more likely to be subject to account takeovers by an adversary with devastating effects.

Inform knowledge of other intimate targets. Several professionals (n=8) used our abuse scenarios to provide further insight into adversaries and survivors outside of IPV settings. Participants were reportedly deeply moved by some abuse stories (validating [39]'s findings), so much so that several (n=5) disclosed personal experiences of such attacks, either directly or through a relative. These disclosures included reports of other intimate threats in close relationships [29], such as abuse between parents and children (familial) and fraud against elders (elder financial abuse). Upon the discussion of Scenario A, a physical device compromise, a financial abuse advocate shared a personal annecdote about elder abuse:

> *"my own relative was targeted ... a fraudster gained access to her bank accounts through her tablet and phone ... it wasn't just the financial loss that hurt her, it was that she was a smart woman who had 'let' someone into her bank account ... she stopped using mobile banking after that."* (P3)

Some respondents (n=3) noted that many applications, despite the trend towards socializing transactions, were not well-equipped to handle non-financial attacks such as harassment (Scenario C). Specifically, in a case involving teen dating violence, an interviewee reflected how they also believed this threat model was 'invisible' to others:

> *"I was assigned to a person and I tried to counsel them. According to the scenario that was just described, [the case] pretty much went like that ... I was trying to help but so many people don't have this threat in their head yet"* (P2)

Provide limited means for service change. A number of participants (n=10) expressed a desire to know more about the issues inherent to financial abuse before they became problems, such as the triggers and exacerbating factors. Some managers (n=3) were optimistic that categorizing financial abuse as an issue that security, safety, and usability teams needed to work together on might help resolve the separation of professional teams in their organization:

> *"I see potential in getting multiple teams around the table on these issues; especially because the user flow makes it too easy for apps to facilitate harassment like that – fraud, ux [user experience], customer service ... yeah financial safety is about security, but it's so much more than that."* (P9)

In particular, the interviewees (n=11) expressed appreciation for the fictive elements of each scenario, as they reported being able to reflect on their own systems and determine if the attacks described in such scenarios could be performed. However, to make a business case for a change in policy or practice, many financial professionals (n=5) required a quantitative measure of the prevalence of such attacks or the severity of the security breach. According to one researcher (P4), there also had to be a critical mass of complaints from customers for this to occur:

> *"having an aspiration to protect customers is one thing, but if it's not backed up by official policy, it's just seen by some as empty talk ... that's where things get tough ... customers are left hanging in the balance. I mean, ... how are they supposed to get in touch with these companies if there's no customer service to handle their issues?"* (P4)

Without reliable prevalence data, most professionals (n=7) shared that their company may struggle to grasp the scope and severity of a specific threat, leading to complacency or underestimation of the associated risks. A lack of tangible evidence could also lead a threat being perceived as speculative, resulting in a lack of urgency in addressing the issue.

8.1.2 Understanding barriers to UI-bound protections

All interviewees (n=12) highlighted that removing the barriers to UI-bound protections was crucial to address the vulnerabilities faced by IPV survivors subject to financial abuse. We identified that these barriers encompassed a reluctance to change authorized use policies, a desire to repurpose but not redesign existing customer safety mechanisms, as well as an absence of professional tools to detect UI-bound threats.

Non-consensual use policy prevents other harms. Many participants (n=8) positioned the ToS and AU of several firms, banks, and financial institutions as flawed but necessary elements to using a service. Such documents were described to help to protect customers from data breaches, cyberattacks, and other legal liabilities, but also to conduct practical day-to-day account management. As one participant described, a ToS helped *"to ensure we know you are the authorized party acting"* (P5). We found most conversations around these documents focus on the drawbacks for the organizations, rather than the consumers, with many reinforcing that customers credentials *"should not be shared with anyone"* (P3).

In focusing on Scenario B, whereby a survivor is coerced to share their login credentials, interviewees (n=7) were reluctant to state the client was entirely at fault, but some affirmed (n=2) that the financial abuse had occurred through poor security decisions. When reflecting on new changes to their training and product advertising in their organization, one financial service provider (P6) shared:

> *"we always tell customers to protect themselves, best get that established early ... otherwise sharing credentials is just kinda handing the keys to your Ferrari to somebody else, sort of like what Mark did here"* (P6)

In response to our abuse stories where adversaries were able to circumnavigate additional protections, such as two-factor authentication (Scenario B) and device fingerprinting (Scenario A), some interviewees (n=3) stated that individuals should be responsible for resolving these security concerns:

> *"it's a two-way street - customers still need to take ownership of their account security, and we need to maintain a solid security policy to protect our customers and our own interests."* (P12)

Repurpose existing safety mechanisms. Instead of developing and deploying new financial safety tools to protect against UI-bound adversaries, most of our interviewees (n=7) suggested repurposing existing financial safety measures for IPV survivors. A financial service provider's (P7) response to a question about how to protect IPV survivors from situations such as Scenario B, for example, recommended using a preexisting financial safety feature for elders:

> *"We ask every client when they open a new account here to add a trusted contact. ... we then go back and ask them on occasion 'hey you haven't added one yet do you want to add a trusted contact?' That's a really critical thing that I would like to see more clients add."* (P7)

An emergency financial contact is someone who can step in and protect an account holder from financial abuse. Through such a service, consumers may be informed that specific institutions are working to protect their assets and prevent scams. Even though alerts were used abusively in Scenario A, most

participants (n=10) suggested that further monitoring and notification systems would be necessary to prevent financial abuse. As one financial manager shared (P8): *"If it's not blaring on your phone in front of you, it's kind of lost in the shuffle of things."* Advocates were cautious about recommending more technology for the survivor to be responsible for, especially if survivors were in a situation where MBs or P2PPs were the one of the primary sources of harm:

> *"Intimate partner violence is about control ... survivors rarely have a trusted contact that is not also under the influence of an offender and they will likely not want to be contacted by the bank that risks their safety"* (P10)

Lack of UI-bound auditing tools or outcomes. Most participants (n=10) were in agreement that that changes to industry standards should improve recognition of unauthorized access by UI-bound adversaries, such as those shown in our scenarios. However, some professionals (n=4) also shared how the absence of professional auditing tools specifically designed to address emerging intimate threats posed significant challenges for their organizations. For instance, an interviewee who managed a team of front-line workers argued that even their managerial position did not allow them to *"know what was going on ... on the other side of the screen"* (P12).

Several interviewees (n=5), particularly lawyers and advocates, raised the possibility that our audit results could lead to a public ranking system, whereby specific applications that were vulnerable to intimate threats could be *"named and shamed"* (P2). Many interviewees (n=4), who acknowledged that the data could be made public, however, were cautious to recommend it immediately. For instance, a lawyer (P10) argued that such information could have inadvertent negative consequences:

> *"say I have a client who chooses to bank with [P2PP-application], they get scammed, Aisha's lawyer is going to use that as evidence aren't they? They'll go 'well why did you use [P2PP-application] if everyone knows it's so flawed from the scale'? ... I can see the case notes now ..."* (P10)

Other interviewees (n=2) also indicated that companies without high rankings on a theoretical digital safety scale of our MB and P2PP applications could *"breathe easy"* (P3) and avoid being singled out for criticism and attention. In spite of this, most interviewees (n=9) agreed that the audit results should be made public and used to further change, either as guides for online safety or as evidence in primary legislation. For instance, a financial planner (P5) suggested that irrespective of the complexity of the financial attacks that such information could be a catalyst for change:

> *"yeah I see the potential for motivating companies to act ... once these results could be made public ... why not try it? I'll always try something once"* (P5)

9 Discussion

Our work extends evaluatory approaches to sociotechnical harms [16, 41, 46, 50], as well as understandings of intimate threats to at-risk groups [4, 57] and of the insecurities present in digital financial applications [2, 19, 40]. In this section, we first outline concrete considerations for digital financial service providers for both *in-app processes* and broader *system ecosystems*. We then consider *other at-risk groups* whom are subject to financial abuse, before concluding with implications for *professionalizing auditing for digital-safety risks*.

Building systems resilience to UI-bound adversaries. Our findings add to the growing body of work that identifies the risks that oversights in security design and implementation may incur to survivors of IPV [16, 48, 53]. We also complement and extend prior work [2, 19, 40] to show that P2PP applications still lag in their protections for user safety from device and account compromise. As technology-enabled financial abuse may rise in prevalence due to the rapid adoption of digitized financial services [2], we outline a few, immediate steps that consumer-facing financial service providers can take towards protecting vulnerable customers.

Changes to in-app processes. MBs often disable biometrics as a login method (Section 5.1.1), but such alerts to users are often inadequate, and may lead users to conflate this with system errors or scheduled maintenance. Customers need to be clearly notified of any changes to biometrics that may have occurred on their device, and how the ToS may define interactions with the device following these changes.

In situations such as theft or loss of property, in-app card freezes that are quick to execute are clearly designed with the end-user in mind (Section 5.1.1). We found that a compromised device could also lead to a remote attack on physical cards to control a survivor's spending by freezing their card at important moments (c.f., [2]). Customers may need to receive an additional knowledge-based challenge to slow down the ease of this attack in cases of account or device compromise.

Finally, all MB and P2PP that we tested are already conducting some forms of content moderation, such as the prevention of special characters in reference boxes (Section 5.1.2). We suggest that financial organizations can do more to protect any free-text boxes from being used to send abusive messages (as represented in Figure 2) to payees.

Changes to system ecosystems. As highlighted by Reaves et al. [40], the liability model for many MB apps must be revisited in light of fraud, and we argue specifically in light of UI-bound adversaries. Financial providers should not refuse responsibility toward at-risk customers whom are often unable to protect authentication information or prevent account and device takeovers. Providers should consider adding caveats to their policy documentation to void any customer responsibility if performed under coercion or without consent.

Our audit and interviewee findings showed that survivors

are often at a loss as to how to get in touch with customer service, or describe their experiences. As financial abuse is present in a substantial amount of cases of IPV and elder abuse [13, 23], service providers should look to how they may become better equipped to respond to vulnerable customers whom reach out. If there is customer support available in-app, and a variety of ways to contact the service, survivors can carefully navigate help-seeking pathways, even on compromised devices. If IPV survivors reaching out choose to speak to a person, Zou et al. [60] provide concrete recommendations for how agents may respond to such cases.

Research directions for other at-risk groups. Survivors of IPV represent a wide heterogeneous group, yet they do not represent a substantial number of other at-risk groups (c.f. [57]) who also face financial risks. Despite our focus on survivors, several of our interviewees provided valuable insight into other at-risk groups (Section 8.1.1), such as on elders and children. In these examples, we see that using one group, subject to substantial safety threats, may uncover other, otherwise unknown at-risk groups during the process of investigation. Nevertheless, using a single at-risk group alone can cause its own issues; namely, how our interviewees looked to re-purpose pre-existing safety mechanisms for financial elder abuse, such as the 'trusted contact' (Section 8.1.2). Recommending a 'trusted contact' option in the context of a coercive and controlling relationship may inadvertantly entail deepening the level of control an adversary has over an individual, particularly if the contact is an adversary or an enabler. While using a common threat model for at-risk groups can address the concerns surrounding scalability of our audits, there is a risk that it may be used to cut corners and conflate disparate vulnerabilities and contextual factors together [18].

A way to combat this could be through investigating other related, at-risk users that have counterfactual contextual factors that augment their risk of financial abuse space. Doing so may reinforce these differences to help combat the tendency of 'one size fits all'. For instance, journalists with access to sensitive resources [56], and how the use of attack vectors on social media platforms (e.g., brigading, dogpiling, doxxing etc.) may damage their financial wellbeing could inspire new feature designs for financial services. Conversely, for older adults with cognitive impairments who may face allocative harms (a system withholding goods and services) on e-shopping websites could elicit broader reflections by a service provider on their distribution of services.

Professionalize auditing for digital-safety risks. The question of who should establish and legitimize an appropriate team to elicit digital-safety concerns remains open. This question is further compounded by the scarcity of the unique skillset required to conduct an appropriate evaluation of consumer-facing technologies. After all, the skills and knowledge required to conduct an audit to elicit digital-safety concerns intimidated several financial experts (Section 8.1.2), crossing computational, financial, and social skill-sets. While such professionals exist (e.g., as highlighted by recent security literature [50, 54]), these individuals may be concentrated in research or advocacy, seemingly distant from the digital services that may generate such abuse. While this distance may help to ensure auditors have no financial conflict in their recommendations, it may also limit their ability to persuade those who may view changes to design as an unnecessary financial cost to an otherwise functioning service (Section 8.1.2). For instance, our findings on the ease of adding adversarial biometrics may warrant complex changes to system authentication (Section 5.1), or adapting ToS statements to allow survivors of IPV recourse for account takeovers may require substantial re-writes of several policies — neither suggestions being low-cost or low-effort. We see the potential for professional auditors, paid by an independent entity to act on behalf of user groups to be a promising direction for professionalizing the practice of auditing for digital-safety concerns.

Technology abuse is impossible to 'design out' entirely [50], entailing the development of robust approaches to encourage seemingly disparate groups to work together in an organization. Bringing together security and usability teams [48], which are often framed as adversarial relationships, held particular promise for our participants; identifying a potentially unmet need in consumer-facing companies. Our multi-method approach and easily accessible abuse scenarios [39], however, could help to explain our participants' enthusiasm in bringing together a range of teams to address user and non-user safety (Section 8.1.1). Reports of potential abusive outcomes, while short of the actual statistics on prevalence or severity of attacks (Section 8.1.2), could equip motivated individuals to push for change in customer service responses [60] or interface design [7]. In the near-term, service providers could position a digital-safety audit, such as an approach we describe in this work, of their products and services from both an ethically and financially beneficial standpoint. By preventing product abuse, companies may also reduce the number of complaints by at-risk consumers and the damage to their reputations if such concerns become public. Internally, organizations may gain an understanding of the problems of the software and applications they offer to consumers as a result of bug bounty programs and responsible disclosure of software vulnerabilities [59].

Acknowledgements

We thank all our participants who graciously shared their experiences to advance safer technology development. We are deeply grateful to our shepherd and anonymous reviewers for their efforts to help improve this manuscript. This work was funded in part by NSF Award #1916096, as well as gifts from JPMorgan Chase.

References

[1] *25 Largest and Most Popular Banks in the U.S. - MagnifyMoney*. URL: https://www.magnifymoney.com/news/largest-banks-in-the-us/ (visited on 02/04/2023).

[2] Rosanna Bellini. "Paying the Price: When Intimate Partners Use Technology for Financial Harm". In: *Proceedings of the 2023 CHI Conference on Human Factors in Computing Systems*. CHI '23. event-place: Hamburg, Germany Canada. New York, NY, USA, 2023. DOI: https://doi.org/10.1145/3544548.3581101.

[3] Rosanna Bellini et al. ""So-Called Privacy Breeds Evil": Narrative Justifications for Intimate Partner Surveillance in Online Forums". In: *Proceedings of the ACM on Human-Computer Interaction* 4.CSCW3 (Jan. 2021). DOI: 10.1145/3432909.

[4] Rasika Bhalerao et al. "Ethical Practices for Security Research with At-Risk Populations". In: *2022 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)*. ISSN: 2768-0657. June 2022. DOI: 10.1109/EuroSPW55150.2022.00065.

[5] Centers for Disease Control and Prevention. *Fast Facts: Preventing Intimate Partner Violence*. 2022. URL: https://www.cdc.gov/violenceprevention/intimatepartnerviolence/fastfact.html (visited on 06/09/2023).

[6] Rahul Chatterjee et al. "The Spyware Used in Intimate Partner Violence". In: *2018 IEEE Symposium on Security and Privacy (SP)*. ISSN: 2375-1207. May 2018. DOI: 10.1109/SP.2018.00061.

[7] Janet X. Chen et al. "Trauma-Informed Computing: Towards Safer Technology Experiences for All". In: *Proceedings of the 2022 CHI Conference on Human Factors in Computing Systems*. CHI '22. New York, NY, USA, Apr. 2022. DOI: 10.1145/3491102.3517475.

[8] Tom Chothia et al. "Why banker Bob (still) can't get TLS right: A Security Analysis of TLS in Leading UK Banking Apps: 21st International Conference on Financial Cryptography and Data Security (FC 2017)". In: *Financial Cryptography and Data Security*. Lecture Notes in Computer Science (Dec. 2017). Publisher: Springer. DOI: 10.1007/978-3-319-70972-7_33.

[9] Yi Ting Chua et al. "Identifying Unintended Harms of Cybersecurity Countermeasures". In: *2019 APWG Symposium on Electronic Crime Research (eCrime)*. ISSN: 2159-1245. Nov. 2019. DOI: 10.1109/eCrime47957.2019.9037589.

[10] Shelly Clevenger, Jordana N. Navarro, and Thomas J. Holt. "The Financial Leash: Cyberfinancial Abuse within Intimate Relationships". In: *Victims & Offenders* 17.5 (2022). DOI: 10.1080/15564886.2022.2065714.

[11] Jay L. Cunningham et al. "The Cost of Culture: An Analysis of Cash App and the Financial Inclusion of Black American Communities". In: *Designing Interactive Systems Conference*. DIS '22. New York, NY, USA, June 2022. DOI: 10.1145/3532106.3533569.

[12] Hesham Darvish and Mohammad Husain. "Security Analysis of Mobile Money Applications on Android". In: *2018 IEEE International Conference on Big Data (Big Data)*. Dec. 2018. DOI: 10.1109/BigData.2018.8622115.

[13] *Domestic and sexual violence fact sheet - NNEDV*. July 2022. URL: https://nnedv.org/wp-content/uploads/2022/07/DVSA-Fact-Sheet-Updated-71222.pdf.

[14] Marie Eriksson and Rickard Ulmestig. ""It's Not All About Money": Toward a More Comprehensive Understanding of Financial Abuse in the Context of VAW". In: *Journal of Interpersonal Violence* 36.3-4 (2021). DOI: 10.1177/0886260517743547.

[15] Diana Freed et al. ""Is my phone hacked?" Analyzing Clinical Computer Security Interventions with Survivors of Intimate Partner Violence". In: *Proceedings of the ACM on Human-Computer Interaction* 3.CSCW (Nov. 2019). DOI: 10.1145/3359304.

[16] Diana Freed et al. ""A Stalker's Paradise": How Intimate Partner Abusers Exploit Technology". In: *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems*. CHI '18. event-place: Montreal QC, Canada. New York, NY, USA, 2018. DOI: 10.1145/3173574.3174241.

[17] Diana Freed et al. "Digital Technologies and Intimate Partner Violence: A Qualitative Analysis with Multiple Stakeholders". In: *Proceedings of the ACM on Human-Computer Interaction* 1.CSCW (Dec. 2017). DOI: 10.1145/3134681.

[18] K. R. Fulton et al. "Vulnerability Discovery for All: Experiences of Marginalization in Vulnerability Discovery". In: *Proceedings of the 2023 IEEE Symposium on Security and Privacy (SP)*. Los Alamitos, CA, USA, May 2023. DOI: 10.1109/SP46215.2023.00017.

[19] Vincent Haupert, Dominik Maier, and Tilo Müller. "Paying the Price for Disruption: How a FinTech Allowed Account Takeover". In: *Proceedings of the 1st Reversing and Offensive-oriented Trends Symposium*. ROOTS. New York, NY, USA, Nov. 2017. DOI: 10.1145/3150376.3150383.

[20] Sam Havron et al. "Clinical Computer Security for Victims of Intimate Partner Violence". en. In: 2019. URL: https://www.usenix.org/conference/usenixsecurity19/presentation/havron.

[21] P. Hope, G. McGraw, and A.I. Anton. "Misuse and abuse cases: getting past the positive". In: *IEEE Security & Privacy* 2.3 (May 2004). Conference Name: IEEE Security & Privacy. DOI: 10.1109/MSP.2004.17.

[22] Haochen Huang et al. "PYLIVE: On-the-Fly Code Change for Python-based Online Services". In: 2021 USENIX Annual Technical Conference (USENIX ATC 21). 2021. URL: https://www.usenix.org/conference/atc21/presentation/huang-haochen.

[23] Laura Johnson et al. "Examining the impact of economic abuse on survivors of intimate partner violence: a scoping review". In: *BMC Public Health* (2022). URL: https://doi.org/10.1186/s12889-022-13297-4.

[24] Renuka Kumar et al. "Security Analysis of Unified Payments Interface and Payment Apps in India". In: *Proceedings of the 29th USENIX Conference on Security Symposium*. SEC'20. USA, Aug. 2020. URL: https://www.usenix.org/conference/usenixsecurity20/presentation/kumar.

[25] Celine Latulipe, Ronnie Dsouza, and Murray Cumbers. "Unofficial Proxies: How Close Others Help Older Adults with Banking". In: *Proceedings of the 2022 CHI Conference on Human Factors in Computing Systems*. CHI '22. New York, NY, USA, Apr. 2022. DOI: 10.1145/3491102.3501845.

[26] Kevin Lee and Arvind Narayanan. "Security and Privacy Risks of Number Recycling at Mobile Carriers in the United States". In: *Proceedings of the 2021 APWG Symposium on Electronic Crime Research (eCrime)*. 2021. DOI: 10.1109/eCrime54498.2021.9738792.

[27] Kevin Lee et al. "An Empirical Study of Wireless Carrier Authentication for SIM Swaps". In: *Sixteenth Symposium on Usable Privacy and Security (SOUPS 2020)*. Aug. 2020. URL: https://www.usenix.org/conference/soups2020/presentation/lee.

[28] Roxanne Leitão. "Anticipating Smart Home Security and Privacy Threats with Survivors of Intimate Partner Abuse". In: *Proceedings of the 2019 on Designing Interactive Systems Conference*. DIS '19. New York, NY, USA, June 2019. DOI: 10.1145/3322276.3322366.

[29] Karen Levy and Bruce Schneier. "Privacy threats in intimate relationships". In: *Journal of Cybersecurity* 6.1 (Jan. 2020). DOI: 10.1093/cybsec/tyaa006.

[30] Tara Matthews et al. “Stories from Survivors: Privacy & Security Practices when Coping with Intimate Partner Abuse”. In: *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems*. CHI ’17. event-place: Denver, Colorado, USA. New York, NY, USA, 2017. DOI: 10.1145/3025453.3025875.

[31] Allison McDonald et al. “" It’s stressful having all these phones": Investigating Sex Workers’ Safety Goals, Risks, and Practices Online”. In: *30th USENIX Security Symposium*. 2021. URL: https://www.usenix.org/conference/usenixsecurity21/presentation/mcdonald.

[32] Mary L. McHugh. “Interrater reliability: the kappa statistic”. In: *Biochemia Medica* 22.3 (Oct. 2012). URL: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC3900052/ (visited on 01/29/2023).

[33] Iffath Tanjim Moon et al. “Towards the Advancement of Cashless Transaction: A Security Analysis of Electronic Payment Systems”. In: *Journal of Computer and Communications* 10.7 (July 29, 2022). Num Pages: 27 Number: 07. DOI: 10.4236/jcc.2022.107007.

[34] Philip Moons, Eva Goossens, and David R. Thompson. “Rapid reviews: the pros and cons of an accelerated review process”. In: *European Journal of Cardiovascular Nursing* 20.5 (June 2021). DOI: 10.1093/eurjcn/zvab041.

[35] Arvind Narayanan and Kevin Lee. “Security Policy Audits: Why and How”. In: *IEEE Security & Privacy* 21.2 (2023). DOI: 10.1109/MSEC.2023.3236540.

[36] Kim Peters, Yoshihisa Kashima, and Anna Clark. “Talking about others: Emotionality and the dissemination of social information”. en. In: *European Journal of Social Psychology* 39.2 (2009). DOI: 10.1002/ejsp.523.

[37] Judy L. Postmus et al. “Economic Abuse as an Invisible Form of Domestic Violence: A Multicountry Review”. In: *Trauma, Violence, & Abuse* 21.2 (2020). PMID: 29587598. DOI: 10.1177/1524838018764160.

[38] *Qualitative Research Practice: A Guide for Social Science Students and Researchers*. English. Second edition. Los Angeles, Calif., Dec. 2013.

[39] Emilee Rader, Rick Wash, and Brandon Brooks. “Stories as informal lessons about security”. In: *Proceedings of the Eighth Symposium on Usable Privacy and Security*. SOUPS ’12. New York, NY, USA, July 2012. DOI: 10.1145/2335356.2335364.

[40] Bradley Reaves et al. “Mo(bile) Money, Mo(bile) Problems: Analysis of Branchless Banking Applications”. In: *ACM Transactions on Privacy and Security* 20.3 (Aug. 2017). DOI: 10.1145/3092368.

[41] Shruti Sannon and Andrea Forte. *Privacy Research with Marginalized Groups: What We Know, What’s Needed, and What’s Next*. arXiv:2206.15037 [cs]. June 2022. DOI: 10.48550/arXiv.2206.15037.

[42] Morgan Klaus Scheuerman et al. “A Framework of Severity for Harmful Content Online”. In: *Proceedings of the ACM on Human-Computer Interaction* 5.CSCW2 (Oct. 2021). arXiv:2108.04401 [cs]. DOI: 10.1145/3479512.

[43] Fred B Schneider. “Cybersecurity education in universities”. In: *IEEE Security & Privacy* 11.4 (2013). DOI: https://doi.org/10.1109/MSP.2013.84.

[44] Nicola Sharp-Jeffs. “Understanding the economics of abuse: an assessment of the economic abuse definition within the Domestic Abuse Bill”. en. In: *Journal of Gender-Based Violence* 5.1 (Feb. 2021). DOI: 10.1332/239788220X16076181041680.

[45] Debra Sinclair. “Romance Fraud: Taking a Lack of Ethics to a New Low”. In: *Ethics & Critical Thinking Journal* 2013 (June 2013).

[46] Julia Slupska and Leonie Maria Tanczer. “Threat modeling intimate partner violence: tech abuse as a cybersecurity challenge in the Internet of Things”. In: *The Emerald International Handbook of Technology-Facilitated Violence and Abuse*. 2021.

[47] Julia Slupska et al. “"They Look at Vulnerability and Use That to Abuse You": Participatory Threat Modelling with Migrant Domestic Workers”. en. In: 2022. URL: https://www.usenix.org/conference/usenixsecurity22/presentation/slupska-vulnerability.

[48] Ashkan Soltani. *Abusability Testing: Considering the Ways Your Technology Might Be Used*. Feb. 2019. URL: https://www.usenix.org/node/226468.

[49] Alex Stamos. “Tackling the Trust and Safety Crisis”. In: *28th USENIX Security Symposium (USENIX Security 19)*. Santa Clara, CA, Aug. 2019. URL: https://www.usenix.org/conference/usenixsecurity19/presentation/stamos.

[50] Angelika Strohmayer, Rosanna Bellini, and Julia Slupska. “Safety as a Grand Challenge in Pervasive Computing: Using Feminist Epistemologies to Shift the Paradigm From Security to Safety”. In: *IEEE Pervasive Computing* (2022). Conference Name: IEEE Pervasive Computing. DOI: 10.1109/MPRV.2022.3182222.

[51] Michael J Strube and Linda S. Barbour. “The Decision to Leave an Abusive Relationship: Economic Dependence and Psychological Commitment”. In: *Journal of Marriage and Family* 45.4 (1983). URL: http://www.jstor.org/stable/351791 (visited on 12/15/2022).

[52] Avinash Sudhodanan and Andrew Paverd. “Pre-hijacked accounts: An Empirical Study of Security Failures in User Account Creation on the Web”. In: *31st USENIX Security Symposium (USENIX Security 22)*. Boston, MA, Aug. 2022. URL: https://www.usenix.org/conference/usenixsecurity22/presentation/sudhodanan.

[53] Kurt Thomas et al. “SoK: Hate, Harassment, and the Changing Landscape of Online Abuse”. In: *2021 IEEE Symposium on Security and Privacy (SP)*. ISSN: 2375-1207. May 2021. DOI: 10.1109/SP40001.2021.00028.

[54] Emily Tseng et al. “Care Infrastructures for Digital Security in Intimate Partner Violence”. en. In: *CHI Conference on Human Factors in Computing Systems*. New Orleans LA USA, Apr. 2022. DOI: 10.1145/3491102.3502038.

[55] Emily Tseng et al. “The tools and tactics used in intimate partner surveillance: an analysis of online infidelity forums”. In: *Proceedings of the 29th USENIX Conference on Security Symposium*. SEC’20. USA, Aug. 2020. URL: https://www.usenix.org/conference/usenixsecurity20/presentation/tseng.

[56] N. Warford et al. “Strategies and Perceived Risks of Sending Sensitive Documents”. In: May 2021. URL: https://www.semanticscholar.org/paper/Strategies-and-Perceived-Risks-of-Sending-Sensitive-Warford-Munyendo/5cc1e7d8708f8b76fe3465739a109c343ed0478d (visited on 01/22/2023).

[57] Noel Warford et al. “SoK: A Framework for Unifying At-Risk User Research”. In: *2022 IEEE Symposium on Security and Privacy (SP)*. ISSN: 2375-1207. May 2022. DOI: 10.1109/SP46214.2022.9833643.

[58] Miranda Wei et al. “Anti-Privacy and Anti-Security Advice on TikTok: Case Studies of Technology-Enabled Surveillance and Control in Intimate Partner and Parent-Child Relationships”. In: *Eighteenth Symposium on Usable Privacy and Security (SOUPS 2022)*. Boston, MA, Aug. 2022. URL: https://www.usenix.org/conference/soups2022/presentation/wei.

[59] Jiali Zhou and Kai-Lung Hui. “Bug Bounty Programs, Security Investment and Law Enforcement: A Security Game Perspective”. In: *Proceedings of the 2019 Workshop on the Economics of Information Security (WEIS)*. 2019. URL: https://weis2019.econinfosec.org/wp-content/uploads/sites/6/2019/05/WEIS_2019_paper_36.pdf.

[60] Yixin Zou et al. "The Role of Computer Security Customer Support in Helping Survivors of Intimate Partner Violence". en. In: *USENIX Security Symposium* (Aug. 2021). URL: https://www.usenix.org/conference/usenixsecurity21/presentation/zou.

A Appendix

A.1 Interview Protocols

Author note: We include here our interview protocols that were used with financial support workers (FSWs) or financial service providers (FSPs). All participants were asked the same questions, unless otherwise stated.

Introduction. We are currently engaged in a research study investigating the intersection of technology, financial, and intimate partner abuse. Our focus is on how financial service providers or support organizations can provide assistance to survivors of intimate partner violence (IPV) through their customer support services or through the re-design of their services. Following our discussion today, we want to analyze your responses and utilize them to formulate recommendations to the wider security community. We would be happy to offer you the opportunity to access and benefit from this work once it is complete, and any training that you identify may be required after our conversation.

Part 1: General knowledge

- Can you tell me what you know about financial abuse/financial control? In elderly contexts? In cases of strangers?
- How about in intimate partner relationships
- Can you give me an example of a recent case, without disclosing any identifiable details where financial abuse and/or financial control between intimate partners was present?
- Was technology present, if so how? How did you respond to it?
- Were there any challenges?

Part 2: Patterns in Cases

- Have you been able to identify any patterns in the cases that arise? Prominent attack approaches?
- Age of client/customer?
- How do you become aware that a customer/client has a problem related to financial abuse/financial control?
- How do they share this concern with you? Prompt: Email, Customer Service?
- Do you intervene before they reach out?

Part 3: Specific examples You are going to be presented with a series of attacks we identified from our analysis, and I would like you to describe what the process would be for resolving the issue. It may be helpful to describe how the initial steps might be taken, the extent to which other departments would be involved, and what kind of support you might be able to offer the client or customer.

- Daphne and Jonas; Mark and Henrick; Shaquille and Aisha

Part 4: Understanding responses.

- Our investigation has looked into customer-facing applications and found lots of ways that they can be abused, how might you image you could report these problems in your organization? (FSPs)
- If someone in your organisation suspects financial abuse, do they report it to local law enforcement, adult protective services or attempt to manage it internally? (FSPs, FSWs)
- Could you walk me through what they do? (FSPs, FSWs)
- What digital tools do you make available to account holders and financial caregivers to enable them to: Detect suspicious account activity? (E.g. alerting system, dashboard overview) Signal to you that there is a problem? (FSPs)
- How might researchers be better equipped to evaluate these issues? (FSWs)

Conclusion. Are there any questions that you feel we haven't covered? Is there anything that you would like to ask me?

Codebook	
abuse risk factor	"keep up with" technology
abuse tactics	make services accessible
alert attorney or law enforcement	manipulated by scammer
assisting financial abuse services	money theft lead to isolation
bank security protocols	neglect
cannot stay ahead of abuse tactics	personal information sold
cannot stay ahead of technology	physical access to device
checklists	practical tactics
confiding in family member	social isolation
co-signing	stalking prevention
creating distrust	social support
debt	suspicious activity report
develop training materials	suspicious phone call
discovery by chance	tech toolkit
elder abuse	train service providers
fake tools that look real	training conference
financial exploitation most-mortem	training tactics
financial abuse questions to ask	trusts and funding
financial exploitation vs. elder abuse	trusted relationship
financial surveillance	try not to shame victim

Table 4: Codebook for qualitative interviews.

Paper Title	**Venue**	**Year**	**Authors**
Digital Technologies and Intimate Partner Violence: A Qualitative Analysis with Multiple Stakeholders	CSCW	2017	Diana Freed et. al.
Stories from survivors: Privacy & security practices when coping with intimate partner abuse	CHI	2017	Tara Matthews et al.
A Digital Safety Dilemma: Analysis of Computer-Mediated Computer Security Interventions for Intimate Partner Violence During COVID-19	CHI	2018	Diana Freed et al.
Usability analysis of shared device ecosystem security: informing support for survivors of IoT-facilitated tech-abuse	NSPW	2019	Simon Parkin et al.
Anticipating Smart Home Security and Privacy Threats with Survivors of Intimate Partner Abuse	DIS	2019	Roxanne Leitão
Clinical Computer Security for Victims of Intimate Partner Violence	USENIX	2019	Sam Havron et al.
Standing in the Way of Control: A Call to Action to Prevent Abuse through Better Design of Smart Technologies	CHI	2021	Dana McKay et al.
"So-called privacy breeds evil": Narrative Justifications for Intimate Partner Surveillance in Online Forums	CSCW	2021	Rosanna Bellini et al.
Networks of Care: Tech Abuse Advocates' Digital Security Practices	USENIX	2022	Julia Slupska et al.
Being Hacked: Understanding Victims' Experiences of IoT Hacking	SOUPS	2022	Asreen Rostami et al.

Table 5: List of included papers

P2PP Application Name	App Store Link	Google Play Store Link
Apple Cash (via Apple Pay)	https://www.apple.com/apple-cash/	N/A
Azimo	https://apps.apple.com/us/app/azimo-global-money-transfers/id543921619	https://play.google.com/store/apps/details?id=com.azimo.sendmoney
Cash App	https://apps.apple.com/us/app/cash-app/id711923939	https://play.google.com/store/apps/details?id=com.squareup.cash&hl=en_US&gl=US
MoneyGram Money Transfers	https://apps.apple.com/us/app/moneygram-money-transfers-app/id867619606	https://play.google.com/store/apps/details?id=com.mgi.moneygram
Paypal	https://apps.apple.com/us/app/paypal-send-shop-manage/id283646709	https://play.google.com/store/apps/details?id=com.paypal.android.p2pmobile
Paysend	https://apps.apple.com/us/app/money-transfer-app-paysend/id1140130413	https://play.google.com/store/apps/details?id=com.paysend.app&hl=en_US&gl=US
Remitly	https://apps.apple.com/us/app/remitly-send-money-overseas/id674258465	https://play.google.com/store/apps/details?id=com.remitly.androidapp
Revolut	https://apps.apple.com/us/app/revolut/id932493382	https://play.google.com/store/apps/details?id=com.revolut.revolut
Ria	https://apps.apple.com/us/app/ria-money-transfer/id1065921908	https://play.google.com/store/apps/details?id=com.ria.moneytransfer
Strike: Bitcoin & Payments	https://apps.apple.com/us/app/strike-bitcoin-payments/id1488724463	https://play.google.com/store/apps/details?id=zapsolutions.strike
TransferGo: Money Transfer	https://apps.apple.com/us/app/transfergo-money-transfer/id1110641576	https://play.google.com/store/apps/details?id=com.transfergo.android&hl=en_US&gl=US
Venmo	https://apps.apple.com/us/app/venmo/id351727428	https://play.google.com/store/apps/details?id=com.venmo&hl=en_US&gl=US
Western Union: Money Transfer	https://apps.apple.com/us/app/western-union-money-transfer/id424716908	https://play.google.com/store/apps/details?id=com.westernunion.moneytransferr3app.eu
Wise	https://apps.apple.com/us/app/wise-ex-transferwise/id612261027	https://play.google.com/store/apps/details?id=com.transferwise.android&hl=en_US&gl=US
WorldRemit	https://apps.apple.com/us/app/worldremit-money-transfer/id875855935	https://play.google.com/store/apps/details?id=com.worldremit.android
Xoom Money Transfer	https://apps.apple.com/us/app/xoom-money-transfer/id529615515	https://play.google.com/store/apps/details?id=com.xoom.android.app&hl=en_US&gl=US
Zelle	https://apps.apple.com/us/app/zelle/id1260755201	https://play.google.com/store/apps/details?id=com.zellepay.zelle&hl=en_US&gl=US

Table 6: Complete list of all peer-to-peer payment applications (P2PP) tested.

P2PP Application Name	Terms of Service	Acceptable Use Policy
Apple Cash (via Apple Pay)	https://www.apple.com/legal/applepayments/direct-payments/	N/A
Azimo	N/A	N/A
Cash App	https://cash.app/legal/us/en-us/tos#cash-account	https://cash.app/legal/us/en-us/acceptable-use-policy#bullying
MoneyGram Money Transfers	https://www.moneygram.com/mgo/us/en/m/terms-and-conditions/	N/A
Paypal	https://www.paypal.com/us/webapps/mpp/ua/useragreement-full?locale.x=en_US	https://www.paypal.com/us/legalhub/acceptableuse-full?locale.x=en_US
Paysend	https://paysend.com/ga/terms	N/A
Remitly	https://www.remitly.com/us/en/home/agreement	N/A
Revolut	https://www.revolut.com/legal/terms/	N/A
Ria	https://corporate.riafinancial.com/terms-and-conditions	N/A
Strike: Bitcoin & Payments	https://strike.me/legal/tos/	https://strike.me/legal/acceptable-use/
TransferGo: Money Transfer	https://www.transfergo.com/terms-conditions/transfergo-ltd	N/A
Venmo	https://venmo.com/legal/us-user-agreement/	https://www.paypal.com/us/legalhub/acceptableuse-full
Western Union: Money Transfer	https://www.westernunion.com/us/en/legal/terms-conditions.html	N/A
WorldRemit	https://www.worldremit.com/en/about-us/terms-and-conditions	N/A
Xoom Money Transfer	https://www.xoom.com/user-agreement	N/A
Zelle	https://www.zellepay.com/legal/user-service-agreement	N/A

Table 7: Complete list of peer-to-peer payment (P2PP) Terms of Service and Acceptable Use Policy documents analyzed

	Only act on behalf of yourself	Only act on behalf of yourself or an authorized user	Responsibility for other person using your credentials	Policy against using the platform for harassment	Policy against using the platform for fraud
Apple Cash (via Apple Pay)		X	X		X
Azimo					
Cash App		X	X	X	X
MoneyGram Money Transfers	X		X		L
Paypal	X		X	X	L
Paysend	X		X	X	X
Remitly	X				X
Revolut	U		X	X	X
Ria	U	U	X	X	
Strike: Bitcoin & Payments	I		X	X	L
TransferGo: Money Transfer		X	X	X	X
Venmo	O		X		L
Western Union: Money Transfer					X
Wise	X		X	X	X
WorldRemit	X		A		X
Xoom Money Transfer	X		X		X
Zelle		C			X

Table 8: Terms of service and acceptable use policy document analysis. X: holds true and explicitly stated, U: condition is unclear, I: holds true under identity impersonation only, O: holds true if user cannot open account in another person's name, C: holds true under authorization of credit/bank card, A: holds true if user permits access to their account, L: unlawful content banned, but fraud not explicitly listed.

Banking Applications	iOS	Android	Online Only
American Express	https://apps.apple.com/us/app/amex/id362348516	https://play.google.com/store/apps/details?id=com.americanexpress.android.acctsvcs.us&hl=en_US&gl=US	•
Bank of America Mobile Banking	https://apps.apple.com/us/app/bank-of-america-mobile-banking/id284847138	https://play.google.com/store/apps/details?id=com.ustrust.mobileapps.accountaccessandroid&hl=en_US&gl=US	
Betterment	https://apps.apple.com/us/app/betterment-invest-save-money/id393156562	https://play.google.com/store/apps/details?id=com.betterment&hl=en_US&gl=US	•
Capital One Mobile	https://apps.apple.com/us/app/capital-one-mobile/id407558537	https://play.google.com/store/apps/details?id=com.konylabs.capitalone&hl=en_US&gl=US	
Chase Mobile	https://apps.apple.com/us/app/chase-mobile-bank-invest/id298867247	https://play.google.com/store/apps/details?id=com.chase.sig.android&hl=en_US&gl=US	
Discover Mobile	https://apps.apple.com/us/app/discover-mobile/id338010821	https://play.google.com/store/apps/details?id=com.discoverfinancial.mobile&hl=en_US&gl=US	•
Marcus	https://apps.apple.com/us/app/marcus-by-goldman-sachs/id1489511701	https://play.google.com/store/apps/details?id=com.marcus.android&hl=en_US&gl=US	•
Monzo	https://apps.apple.com/us/app/monzo-mobile-banking/id1052238659	https://play.google.com/store/apps/details?id=com.getmondo&hl=en_US&gl=US	•
PNC Mobile Banking	https://apps.apple.com/us/app/pnc-mobile-banking/id303113127	https://play.google.com/store/apps/details?id=com.pnc.ecommerce.mobile&hl=en_US&gl=US	
Revolut	https://apps.apple.com/us/app/revolut-spend-save-trade/id932493382	https://play.google.com/store/apps/details?id=com.revolut.revolut&hl=en_US&gl=US	•
Starling	https://apps.apple.com/gb/app/starling-bank-mobile-banking/id956806430	https://play.google.com/store/apps/details?id=com.starlingbank.android&hl=en_US&gl=US	•
TD Bank	https://apps.apple.com/us/app/td-bank-us/id382107453	https://play.google.com/store/apps/details?id=com.tdbank&hl=en_US&gl=US	
U.S. Bank	https://apps.apple.com/us/app/u-s-bank-mobile-banking/id458734623	https://play.google.com/store/apps/details?id=com.usbank.mobilebanking&hl=en_US&gl=US	

Table 9: Complete list of all mobile banking (MB) applications tested.

	Default authentication			Biometrics			Min send ($)			Max send per ($)			Static limits	Theft / Fraud protection			Handle			In-app safety measures			Tx visibility	Required PII for signup						
	None	1AA	2FA	Prompt	Auto logout on change	Notify of change	0.01	1	>1	Tx	Week	Month	Yes	Freeze card	View PIN	Change PIN	None	Username	Other	Block	Report	Support	Default public	Name	Email	Phone	Address	DOB	Additional
Apple Cash (via Apple Pay)	•				•	•		•			10,000^		•						AppleID	•		•				•			AppleID
Azimo			•						•	12,000			•				•							•	•				
Cash App			•	•				•			2,500		•	•	•	•		•		•	•		•	•	•	•			
MoneyGram	•			•				•		15,000			•				•							•	•	•	•	•	Birth country
Paypal			•	•			•			10,000			•				•			•		•			•	•			Nationality; residency
Paysend		•							•			≤999	•				•												
Remitly		•							•		10,000		•				•								•				
Revolut		•		•					•	250,000			•	•	•	•	•				•	•	•			•			Residency
Ria		•		•				•			7,999		•				•								•				Nationality
Strike			•	•													•						•		•	•			
TransferGo		•							•				•						Auto-assigned					•	•	•	•		
Venmo		•					•			299.99*			•	•	•	•		•		•	•	•	•	•	•			•	Nationality; SSN
Western Union: Money Transfer	•			•				•		5,000			•					•							•				
Wise			•	•	•	•	•			15,000			•	•	•	•	•					•		•	•	•	•	•	Residency
WorldRemit		•					•			5,000			•				•								•				Nationality
Xoom		•		•					•	6,000			•						•						•	•			Nationality
Zelle		•		•	•	•		•		2,000		12,000	•				•						•	•	•	•	•		

Table 10: Our UI stepthrough analysis findings for P2PP apps.

	Default authentication			Biometrics			Min transfer ($)			Max transfer per ($)			Static limits	Theft / Fraud protection			Alerting				Anti-harassment measures	
	None	1AA	2FA	Prompt	Auto logout on change	Notify of change	0.01	1	>1	Tx	Day	Month	Yes	Freeze card	View PIN	Change PIN	History	Security alerts	Balance & txs	Delivery	Block user	Report user
American Express			•	•	•				•	10,000			•	•	•			•	•	App / Email / SMS		
Bank of America			•	•						10,000			•	•				•	•	App / Email / SMS		
Betterment			•								10,000		•					•	•	App / Email		
Capital One			•	•	•	•	•			10,000	10,000	25,000	•	•		•		•	•	App / Email / SMS		
Chase			•	•	•	•	•			10,000	25,000			•			•	•	•	App / Email / SMS		
Discover			•	•	•				•			250,000	•	•		•		•	•	App / Email / SMS		
Marcus			•	•	•					10,000	10,000		•						•	App / Email / SMS		
Monzo		•		•				•			10,000			•	•			•	•	App / Email	•	•
PNC			•		•	•					2,000	5,000		•					•	App / Email / SMS		
Starling			•	•				•		25,000			•	•	•				•	App / Email	•	•
TD Bank			•	•	•						3,000	5,000		•				•	•	Email / SMS		
U.S. Bank			•	•	•	•					2,500			•			•	•	•	App / Email		

Table 11: Our UI stepthrough analysis findings for mobile banking apps.