Paying the Price: When Intimate Partners Use Technology for Financial Harm

Rosanna Bellini
rbellini@cornell.edu
Cornell University
New York, New York, USA

ABSTRACT

Financial abuse — the control of a survivor's access to and use of financial resources — is highly prevalent in intimate partner violence (IPV) cases. Based on the reports of 158 survivors of IPV and 16 financial advocates, we present a comprehensive investigation into how abusers exploit technologies to harm survivors financially through various technical attacks and deceptive strategies. In doing so, we identify four motivations for abusers who use these harmful attacks and how these acts exploit, monitor, restrict, and sabotage a survivor's financial well-being and independence. As each dimension of these financial harms warrants a tailored approach, we highlight potential directions for practice and research to protect survivors from technology-enabled financial harms. Broadly, we call for the financial technology sector to consider designing for intimate threats through adversarial thinking, recommend strategies for detecting financially abusive activity and provide guidance for how customer service agents may be financially abuse aware.

CCS CONCEPTS

• **Human-centered computing** → *Empirical studies in HCI*.

KEYWORDS

financial abuse, intimate partner violence, technology-enabled abuse

ACM Reference Format:
Rosanna Bellini. 2023. 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), April 23–28, 2023, Hamburg, Germany.* ACM, New York, NY, USA, 17 pages. https://doi.org/10.1145/3544548.3581101

1 INTRODUCTION

Technologies play a growing role in connecting people with their finances: by providing new ways to bank [25, 47], earn [55], pay [21, 62], send gifts [73], and track expenditure [43, 49, 86]. However, many survivors of intimate partner violence (IPV) — who may also experience technology-facilitated abuse [12, 22] — are especially vulnerable to financial services' "turn to digital" [27]. IPV is a severe societal problem which affects one in four women and one in six men in the United States across their lifetime[13]. Financial abuse is a highly prevalent yet over looked component of IPV [81], that includes harmful behaviors that target a survivors' financial independence [44, 68], making it hard for a survivor to leave [75, 77], seek help [74], or resist further harm [24, 63]. While many works have explored how digital technologies exacerbate financially-motivated offenses (e.g., fraud, identity-related crime [16, 39, 57], elder financial abuse [7, 31, 47]), we have yet to identify such work in IPV contexts.

We provide an in-depth analysis into how abusers of IPV use, and may even be motivated by, technology to financially harm survivors and their dependents. We do this by conducting a retrospective case review of a technology clinic based in a major metropolitan area in the United States (U.S.) to analyze the clinical records of 158 IPV survivors who have experienced technological and financial abuse. These research efforts identified that abusers use various technical, non-technical and deceptive strategies to harm a survivor's financial stability and well-being, which we organize into an attack taxonomy. We discuss how abusers specifically target a survivor's password managers and activate a fraudulent password recovery process to gain access to a survivor's financial information and accounts. Following this, abusers may compromise survivors' accounts to make non-consensual purchases, alter existing orders or subscriptions, and sell a survivor's digital assets (e.g., stocks and cryptocurrencies). In extreme cases, abusers leveraged their authority as owners or authorized users of a survivor's accounts to rack up coerced debt or deplete a survivor's service allowance. Abusers did not require compromised access to a survivor to harm them, such as maliciously targeting a survivor's online business or making multiple credit card applications in a survivor's name to damage their credit score.

To help us retain focus on those responsible for causing such harm [8], we also conducted 16 interviews with financial advocates to illuminate abusers' potential motivations for abuse, and the consequences for survivors. We characterize these attacks by discussing the four motivations that underpin each attack, which include how abusers use technology to *exploit*, *monitor*, *restrict* and *sabotage* a survivor's ability to establish financial stability and freedom. We discuss how an abuser did not require physical access to a survivor's devices, knowledge of confidential financial information, or even the need to interact directly with a survivor (online or offline) to cause financial harm. Perhaps most concernedly, most attacks identified either aimed to *restrict* a survivor's expenditure or directly *sabotage* their finances, which do not require an abuser to benefit from such behavior financially. Such findings around financial restriction and sabotage differentiate such attacks from identity-related crimes (e.g., such as 'identity theft') due to their persistent, targeted nature on a target, and the complex social goals of the offender.

CHI '23, April 23–28, 2023, Hamburg, Germany

ACM ISBN 978-1-4503-9421-5/23/04.
https://doi.org/10.1145/3544548.3581101

As different methods and motivations for attack require tailored approaches to combat, we conclude with a discussion for how our discoveries have implications: for survivors at acute risk of being targeted; for designers of financial systems to respond to intimate threats who are *not* primarily motivated financially; and for research around where technology and financial abuse research goes from here.

Our paper makes three contributions to the Human-Computer Interaction (HCI) and computer security community. First, we directly extend and refactor Freed et al.'s [29] comprehensive *attack taxonomy* to evidence how IPV abusers leverage financial technologies, non-financial technologies, and social engineering attacks to inflict financial harm on survivors and their dependents. Second, we identify *four motivations* that underpin and characterize these abusive attacks and link these to protective strategies for how survivors attempt to defend their financial accounts and information. Finally, we contribute concrete design approaches by *adversarial thinking* about intimate threats and *consentful interactions* to guide how existing financial systems can be re-designed to address some of the challenges survivors report facing upon attempting to rebuild their financial stability. Broadly, our work calls on the financial sector to address the pressing concern of financial abuse in intimate contexts by adequate customer service training and taking on the challenge of detecting financially abusive interactions.

2 BACKGROUND AND RELATED WORK

Intimate partner violence (IPV) — also known as domestic violence (United Kingdom) or family violence (Australia) — is a significant and devastating problem for individuals, communities, and society. IPV is characterized by a pattern of abusive behavior, or aggression in a current or former intimate relationship that gains or maintains power and control over someone through physical, sexual, emotional, economic or psychological means [13, 72, 74]. *Financial abuse*, the primary focus of this work, addresses money, finances, and the use of finances which is a subcategory of economic abuse — the control of economic resources more broadly, such as education and housing [60]. For this work, we refer to people who use patterns of abusive behaviour as *abusers*, and people who are subject to them as *survivors*.

Financial abuse has recently been recognised as a distinct form of abuse [26, 60], rather than solely a consequence of IPV [21], and is present in the majority of cases of IPV [68]. Such abuse includes behaviors used to coerce and control a survivor's ability to acquire, use and maintain financial resources, such as bank accounts, credit cards, and loans [2, 78], directly damaging their financial security and independence from their abuser. Any behaviours that target a survivor's financial freedom represent a significant barrier for a survivor to leave the relationship [77], use protective strategies if leaving is unfeasible [63], or refrain from returning to an abuser [68]. However, the aftermath of financial abuse can be life-long and continue after a relationship has ended, such as exposing survivors to homelessness, job loss, poverty, and poor health outcomes [41, 67]. Abusers, in a similar vein to identity thieves [39], may saddle survivors with large debts through stealing their income, damage their financial reputation, and leave few savings or assets in their name to rebuild their financial lives [3, 44, 67]. Survivors who occupy low socio-economic statuses (e.g., be on fixed income [90]), be financially dependent on their abuser (e.g., be disabled [4, 50, 64]), or be financially responsible for other individuals (e.g., children, elderly parents [37, 44]) are acutely vulnerable to this devastating form of abuse.

Recent work in HCI has demonstrated that digital technologies play a significant role in IPV contexts by providing an abuser with the ability to surpass geographic and spatial boundaries to exacerbate their abuse [14, 22, 33, 61, 91]. For instance, Freed et al. [29] offer an invaluably comprehensive attack taxonomy that demonstrates how abusers may gain access to a survivor's accounts through owning devices or services, compromising a survivor's accounts, posting harmful messages about them, or disclosing private information. Recent work has also indicated that abusers may use surveillance and spyware to track a survivor's location and control their behavior [9, 82]. However, technology-enabled financial harms in intimate relationships – which scholars argue can be easily overlooked by service providers and researchers [20, 34, 92] – have yet to be scrutinized in significant depth. Although several lessons can be drawn from identity-related crimes [39, 46] and elder financial abuse [47], evaluating their suitability for IPV contexts are still in their infancy.

A small number of survivor-focused studies describe a few accounts of how abusers may have tampered with online bank accounts remotely [92], withheld finances from joint accounts [20], and sent harassing messages through payment transfers [34]. Nevertheless, such findings do not illuminate *how* abusers gain access, theorize *why* they do so, and investigate how abusers may cause financial harm beyond online banking. Indeed, as many survivors of IPV lack a bank account entirely [32] and with more financial services becoming digitized each year, it is essential to explore how *all* areas of their financial activity may be affected. Arguably, in line with calls from fraud and identity theft scholars [3, 59], an important way to prevent financial abuse is to mitigate its occurrence in the first place. As such, building a solid picture of when and how technology mediates financial abuse in IPV contexts is the first step in designing policy and practice that protects survivors' financial stability and supports their attempts to regain financial independence.

Investigating the role that digital financial systems play in IPV contexts also responds to recent calls in HCI for more insight into financial household management [86], family settings [32], and personal financial tracking [5, 43, 49]. Indeed, valuable work has already shown how inflexible financial infrastructure can lead to specific complications people who are unbanked or underbanked [10, 32, 38], cash- or cheque-reliant [85], people who face historical exclusion based on race [21], and people who may be targeted due to lack of technical knowledge [16, 47]. Such complications may directly threaten affirmative and informed consent [40, 76, 96] — the gold standards for sensitive design that respect privacy, trust, and autonomy of the user — it is thereby vital to scrutinise how consent to financial services can, and is, being undermined by adversaries. Arguably, any lessons learned for consentful design in financial services for specific population groups, such as survivors of financial abuse, can not only work toward improved outcomes in IPV contexts, but for the broader population as well.

Recent work on digitized financial banking [19, 23], e-wallets [42], and payment systems [17], also call for greater transparency in how they could be used abusively in more intimate contexts. For instance, scholars have consistently shown that mobile money or branchless banking applications use weak authentication and fail to secure authentication data in transit [65]. With terms and conditions that hold the customer responsible for fraudulent activity, consumers are left with no recourse to dispute fraudulent transactions, even if conducted abusively by a malicious insider [65, 68] such as an abuser with direct access to a device.

3 METHODOLOGY

Retrospective case series studies [36] are descriptive studies that use existing participant data collected in connection with an intervention to help guide areas for future research where little is known already [1]. We adapted this approach to investigate how abusers had used technology to inflict financial abuse on IPV survivors who received direct services from a technology clinic in the U.S. between 2018 and 2022. To clarify our findings, we also spoke to 16 professionals who work directly with survivors (all 16 professionals) and abusers (5 of 16 professionals) of financial abuse to help us contextualize the motives behind such attacks and the relative harms survivors may experience to their financial health.

3.1 Research Context and Access to Data

We conducted this investigation in a technology clinic (*clinic* hereafter) — the Clinic to End Tech Abuse (CETA) — in the major U.S. metropolitan area of New York City that provides front-line services to IPV survivors (*clients* hereafter) who are also subject to technology abuse. The clinic (est. 2018) consists of a team of 40 volunteers (*consultants* hereafter) and has served over 450 clients to help them address their security, privacy and digital safety concerns. CETA was created as a research initiative run out of Cornell University and is regularly reviewed and monitored by an Internal Review Board (IRB) to protect the rights and welfare of research subjects. The clinic manages a large evidence base on technology abuse in IPV contexts. It uses this data to improve survivors' outcomes by publishing research findings [28, 35, 83, 84], delivering advocate training [58], and lobbying for primary legislation change in consumer law.

The author of this work has been an active consultant at the clinic since 2021 and works as part of a five-person leadership team to coordinate the quality of care services for clients and volunteers. She approached the leadership team to propose an investigation into financial abuse and explore how this harm intersected with clients' existing technology concerns. CETA leadership discussed this pitch and recommended that the research project use existing client case notes before making any new attempts to collect data from clients. As clients may experience trauma when recounting their abuse histories [15, 18], the research chose to use a retrospective case series analysis on existing client records.

3.2 Clinic Protocol and Case Notes

Caseworkers that make up a broader IPV support ecosystem (composed of legal assistance, housing, and counseling) refer a client to CETA once they have identified a technology-related concern. Following this referral, a set of trained consultants work with the clients across a series of appointments (*consultations* hereafter) that aim to: understand their technology concerns, investigate areas of potential compromise, and provide guidance on steps related to digital safety [35]. Each consultation lasts between 60 – 90 minutes and is conducted through encrypted videotelephony software, in-person at a secure location or a combination of both [83]. Clients are mainly English or Spanish-speaking and have either already left (post-separation) or are in the process of leaving an abusive relationship to mitigate risks to their digital safety. All clients referred to the clinic are offered the ability to contribute their anonymized and de-identified data to research; however, clients receive the same quality of service irrespective of their decision. Accordingly, our data set comprises clients who have given explicit written or verbal consent for researchers to use their data in projects on technology abuse in IPV contexts. As the clinic prioritizes data minimization to protect clients from any risks of de-anonymization by a data breach, it does not collect detailed demographic data; therefore, we do not report participant demographics in this study.

Client case files that were the data analyzed for this work consist of consultant-taken consultation notes, transcripts of audio-recorded consultations and referral forms. These case files are stored in a strictly access-controlled secure content management system (CMS) that the author has access to as part of her leadership role in CETA. All analyses took place inside a separate, access-controlled secure cloud system hosted by Cornell University, regularly used for sensitive data to mitigate the risk of data leaks.

3.3 Search Strategy and Interviews

We first conducted a trial using the CMS search function using a small set of terms and phrases associated with finance ("bank", "money", and "account") and financial abuse ("controlled spending", "stole money") [26, 60] to identify cases that contained descriptions of financial abuse. We evaluated positive match cases against our definition of financial abuse (Section 2), and we determined this was an effective strategy to determine the relevancy of cases.

While slightly outside of the strict definition of financial abuse, we chose to be inclusive of cases that contained descriptions of how technology was: a) directly interfering with employment (included in *economic* abuse definitions [60]) if survivors *also* described how this had an impact on accessing their salary; and b) deliberately damaged so that survivors would incur financial costs of repair (included in *consequences of abuse* definitions [44]). In these cases, clients described how technology-facilitated abuse directly led to loss of finances and how these behaviors directly impacted their financial well-being.

As our search queries would return irrelevant cases, we manually coded the search results for relevancy, using a broader set of keywords (listed in full in Appendix A) that included inflected forms of each word and leveraged truncation wildcards. We performed our search strategy three times, first in October 2021, then repeated in February 2022 and August 2022, as more client data were added.

Our search strategy identified 174 consultations with 158 tech abuse survivors who reported experiencing financial abuse. Some clients required multiple consultations, resulting in a discrepancy between the number of consultations

and the number of clients. Our final data set consists of 158 client cases composed of case notes, transcripts from recorded conversations, and referral forms that make up approximately 45,000 words of survivor descriptions of financial abuse.

Alongside our search, we also conducted 16 interviews with financial advocates which would help contextualize our discoveries through their familiarity with financial systems. In this work, we refer to practitioners who directly assist or oversee services for access to financial products and services for clients at greater risk of financial harm as *financial advocates*. Advocates often act as proxies for IPV survivors in prior studies [30, 70] and can speak about the consequences of financially harmful behavior without requiring survivors to continuously recount what can be traumatising experiences in their lives [11, 89, 93]. Many advocates are responsible for creating survivor-centered safety plans that require analyzing survivor descriptions and other information sources to understand abuser motives and anticipate potential future harm [64, 74]. As eliciting firsthand descriptions of abusive behavior can be extremely challenging [9], we chose to leverage advocates' professional experience to speak about many potential motivators for financially abusive behavior. We discuss the limitations of this approach in greater depth later in our work (Section 3.5).

A recruitment call was shared across professional networks of institutions that provided consumer finance, banking, and insurance services to consumers in the United States. Business-to-business and business-to-consumer organizations were excluded. A round of selective sampling was also used to recruit specialist financial organizations that are often underrepresented in broad recruitment calls (e.g., minoritized and racialized groups). Sixteen participants responded to the call and included victim support workers, family lawyers, financial therapists, financial planners, insurance agents, and customer support agents.

Each interview lasted between 35 and 65 minutes and was conducted over video-conferencing software (13 participants) or in-person (3 participants). Participants were asked to share their experiences working with people affected by financial abuse in IPV contexts; help us contextualize our financial attacks (Table 1) according to an abuser's motive; and theorize the role that third-party agents (e.g., financial institutions, law enforcement) could play in responding to these attacks. All advocates possessed firsthand experiences in working directly with clients who described use of (five participants) or being subject to (sixteen participants) financially abusive behavior in intimate relationships. The resulting data was incorporated into the study's analysis. As financial compensation was disallowed by the majority of our participant organizations, we distributed an executive summary of our findings to participants as thanks for their time and contributions.

3.4 Data Analysis

The study used an adapted version of *Glaserian Grounded Theory* (GGT) [66] to iteratively move between data sampling and analysis. This approach allowed for the identification of actionable changes to practice (as detailed in Section 3.5) and potential areas for further research. We familiarized themselves with the data through reading and conducted two rounds of open coding to generate an initial taxonomy of financial attacks (Section 1). Upon the completion of the second round of coding, we invited financial advocates to provide feedback on our findings and sought their experiences on working with cases of financial abuse. This data was incorporated into the final theoretical coding effort [54] and the researchers took memos throughout this stage to record the complex socio-technical factors that influence financial and technology abuse [52].

3.5 Ethics

We received approval from the Institutional Review Board (IRB) at Cornell University for all study procedures and data security practices. However, emotionally-charged research on topics such as IPV creates specific concerns for the well-being of all involved [53], and continuous exposure to narratives of abuse incurs a heightened risk of experiencing vicarious trauma [15]. Special care was taken to protect client identities and safeguard the well-being of the research team. After the author performed an initial pass of the work to remove identifying information, the work was reviewed by two privacy experts and updated accordingly.

In line with the ethical practice that recommends survivors see a direct benefit from participating in research, [45, 89, 93], the survivors in our study received tailored services via the clinic, that helped them navigate their privacy and security concerns. Motivated to immediately improve client outcomes, the author of this work was assigned to clients who described experiences of financial abuse due to her familiarity with navigating vulnerabilities in financial systems and providing bespoke advice.

Finally, the author has experience working with groups impacted by IPV and has established safe practices to mitigate compassion fatigue and burn out such as self-care plans and spending regular time away from transcript-based research [15, 89]. To protect the identity of our participants, we use S1 — S158 to denote survivor cases and A1 — A16 to denote financial advocate cases. We have lightly edited our quotes to remove idiosyncratic tools, phrases, and locations.

3.6 Study Limitations

Our study has several limitations, including sampling concerns, reliance on keywords for case relevancy, and the use of indirect data. This study uses a non-representative sample of survivors and professionals who live in a major metropolitan environment in the U.S. While financial abuse can impact people of any socioeconomic status, gender or relationship status, the survivors in this work were predominantly women, English-speaking, post-separation from their abuser and currently receiving IPV services. Even so, our research may serve as a useful resource for scholars who wish to explore the impact of financial abuse on post-separated survivors of abuse [75].

Next, our strategy relied on sourcing client cases via keyword search terms or phrases. While our search process and analysis have been methodologically systematic and rigorous in scope, this may result in missing cases. Third, our findings draw from indirect sources of information – tech abuse case studies and advocate perspectives on abuser motivations – which may lack detailed descriptions of potential technical vulnerabilities and attacks. As this research draws on survivor and professional

recollection of events, it is possible that they were affected by observer bias and a small number of cases lacked direct observation of an abuser conducting such an attack. However, a large number of survivors reported being notified of system-side indicators, such as security alerts via email or text, and social indicators, such as a post-attack taunt by an abuser which helps to validate their experiences. We see promise in using our study as the groundwork for studies that elicit abuser perspectives on technology-enabled abuse, either in-person or online [8, 82, 88].

4 TECH-ENABLED FINANCIAL ATTACKS

We identify that technology already plays a significant role in facilitating new paths to control access to a survivor's financial resources, which we explicate in two complementary sections. Firstly, we demonstrate how abusers of IPV use a combination of non-financial and financial services to inflict financial harm on survivors, which we present through *five categories*. Second, with the help of financial advocates, we categorize these attacks according to *four motivations* that underpin financially abusive behaviors.

In our analysis, we discovered that abusers use a combination of social engineering techniques, non-financial technologies, and financial technologies to target a survivor's resources, assets and data. We organize these attacks into five high-level *attack categories* shown in Table 1 and directly extend the invaluable taxonomy as offered by [29] to financial contexts. Abusers may be the *(1) owner or an authorized user* of a survivor's financial account or exploit a survivor's authentication mechanisms to conduct an *(2) account compromise*. Abusers could construct *(3) harmful posts or reports*, or use *(4) deception and identity theft* to manipulate a survivor psychologically. Finally, abusers *(5) bypass physical defences* to destroy property such as financial records or work devices. In our study, we identified abusers who use technology to carry out abuse do so via categories previously identified by HCI communities (account/device compromise, harmful messages, and ownership-based attacks as identified in [29]), however, we provide a novel, comprehensive analysis of how technology abuse *also* directly leads to financial harms.

4.1 Ownership-/Authorized-user-Based

Survivors may often use devices or accounts that abusers have bought, allowing an abuser to have *privileged* access and perform actions that may be unable to standard users (e.g., viewing service usage statistics). However, we identified situations where survivors described being convinced by an abuser to add them as an *authorized user* on their online financial accounts and credit card plans, allowing an abuser to make purchases on a survivor's credit account and card. Authorized users differ from being added to a family plan as the account holder (often a survivor in our dataset) is legally responsible for any expenditure accrued, while an authorized user is not. If an abuser deliberately abuses their authorized user privileges, this hurts the account holder's credit score.

Ownership-based. Survivors shared that an abuser was often the primary (and sometimes the sole) owner of an online financial account in their relationship, which abusers used to digitally and physically restrict their access to banking infrastructure. A few survivors shared how survivors were not permitted to own a smartphone and so were physically unable able to access mobile banking or peer-to-peer payments:

> *"He made sure that I don't get anywhere near finances ... everything, every single thing, all accounts, all bank accounts, any accounts, everything is 100% under his name ... I was invisible to the banks and utility providers."* (S21)

Survivors also disclosed that abusers could also digitally restrict access to a financial account, such as ensuring that a survivor was not registered or named on any online accounts. As transfers and changes often have to be done by the account holder or as an authorized user, survivors shared they had been unable to make savings or transfer money to their children. When an abuser did list a survivor on their bank or credit account, we found survivors described they would still receive verbal threats to remove them from using a financial account. For instance, a survivor (S51) shared that she was an authorized user on her ex-husband's credit account, allowing her access to finances when she could not work. However, her ex-husband continuously threatened her with removal from his account should she do something that upset him.

Abusers leveraged physical or digital control of the household financial accounts to their advantage, and a few survivors shared cases where the only income they received was through their abuser, which they referred to as *"an allowance"* (S128). Abusers could provide this 'allowance' through cash handouts, cheques, or even top-up cards where a partner would allocate a fixed amount each month to their survivor to spend yet refuse to provide more money when requested.

Some survivors also shared how they used devices that were purchased by — and therefore legally owned — by an abuser, which facilitated their everyday interactions with money, such as making mobile payments, tracking their expenditures, and cash cheques remotely. However, we saw descriptions of attacks where abusers leveraged third parties to remove or seize these devices from a survivor, often following the end of a relationship or moving out of a shared domestic environment:

> *"he brought the cops [police] around to where I lived, he showed them the receipts and since we were the legal owner ... and he took all my devices ... phones, tablet, laptop ... everything ... even the kids' devices"* (S157)

These attacks often required the use of law enforcement or the use of repossession agents to enforce the seizure. In all cases in our dataset, the abuser provided devices as financial gifts to a survivor, which had the added impact of causing psychological distress to a survivor and their dependents.

Authorized User-based. Many survivors described how they maintained a range of online subscriptions, including services for work (e.g., cloud storage) or entertainment (e.g., music, film streaming). As many of these services are now explicitly designed to serve families or couples, survivors shared stories of how they added partners and family members to their accounts, generally at their partner's request. However, abusers were reported to abuse these privileges, such as refusing to pay *"their fair share"* (S45) by financial contributions, despite formerly agreeing to.

		Authorization					Dependencies				Motivations			
Category	**Attacks that Target Survivor**	Authorization: Abuser	Authorization: Survivor	Access: Privileged	Access: Compromised	Access: Physical	Confidential Info	Additional Software	Survivor Interaction	Involve Third-party	Exploit Finances	Monitor Finances	Restrict Finances	Sabotage Finances
Authorized User & Ownership-based	Deplete survivor's digital resources (e.g., credit limits)	●		●							●		○	
	Digitally control access (e.g., survivor as authorized user)$^{\alpha}$	●		●									●	
	Make fraudulent purchases (e.g,. by online shopping)	●		●			◖				●		○	
	Physically prevent use of device/account (e.g., for banking)$^{\alpha}$					●			○				●	●
	Provide an 'allowance' via bank/mobile transfer	●				○							●	
	Seize devices (e.g., through law enforcement)	●		○		○			◖	●			●	○
	Withhold payment from survivor for subscriptions, bills	●					●		○		●		○	
Account Compromise	Cancel/change survivor's purchases, subscriptions		●	●	●		●	●					○	●
	Close survivor's online credit and bank accounts		●	●	●		●					○	●	●
	Delete/sell survivor's digital purchases (e.g., stocks)		●	●	●	◖	●	○		○	○		●	
	Edit survivor's info (e.g., changing address)$^{\alpha}$		●	●	●								○	●
	Lock survivor out (e.g., changing password)$^{\alpha}$		●	●	●		●	●		○	●			
	Make fraudulent transfers, purchases		●	●	●	●	◖	○			●		○	○
	Monitor survivor's expenditure (e.g., transactions)$^{\alpha}$		●	●	●	◖	◖	◖			○	●	○	
	Steal survivor's info (e.g., contact numbers, bank accounts)$^{\alpha}$		●	●	●							●		
Harmful Posts or Reports	Fraudulently report survivor of financial misconduct					○				●			●	●
	Post non-financial harmful content (e.g., negative review)$^{\alpha}$						○	○	○					●
	Post financial information on survivor$^{\alpha}$						●	○	●					●
	Report survivor's online business/fundraising-campaign						●		○	●			○	●
Deception & Identity Theft	Apply for financial loans/benefits in survivor's name						●	●		●	○		○	●
	Coerce survivor to share financial info (e.g., catfishing)						◖		●			●	○	
	Delete/hide evidence of online accounts/expenditure							○	○				●	
	Dupe agency to re-direct salary (e.g., payroll)	○	○	○	○		●			●	●		○	
	Falsify/fabricate evidence of online accounts/expenditure								○				●	
	Recruit third-parties to coerce secret financial info						○			●				
	Request credit report on survivor (e.g., credit agencies)						●			●		●		
	Track survivor's financial activity through legitimate apps						●	●				●	○	●
	Surveil survivor via financial profiles (e.g., peer-to-peer)						◖					●		
Bypass Physical Defences	Break into survivor's house to steal financial information				●	●						●		
	Damage/destroy survivor's device(s)$^{\alpha}$					●			○				●	●
	Damage/destroy device(s) of survivor's friends and family					●			○	●			○	●
	Physically withhold survivor's device(s)$^{\alpha}$					●			○				●	●
	Steal survivor's financial information by dumpster diving				●	●						●		
	Use mail theft to intercept financial information				●	●						●		

Table 1: A taxonomy of how abusers use technology to conduct attacks on a survivor's financial accounts and information, organized into five categories [Left]. We analyze each attack by examining the *Authorization* required for the attack, any *Dependencies* required for an attack to work, and the abuser *Motives* behind this action. A ● indicates that this criterion is necessary for an attack, and a ◖ indicates that this criterion is necessary to set up but not maintain an attack. A ○ indicates that this criterion is not necessary for an attack but was common in our data set. A blank space indicates a criterion does not hold or is not necessary for an attack. $^{\alpha}$ indicates an attack previously identified by Freed et al. [29]

Some survivors described how an abuser used this privilege to deplete their paid-for service allowance, such as the number of downloads or call minutes:

> *"he would spend all day online gaming ... so we would always run out [of the Internet] ... the kids would then have to use school's WiFi."* (S55)

Many survivors also reported cases where abusers deliberately depleted their online services to build debts in their names. For instance, one survivor shared how their partner had continuously rang up charges to expensive numbers, which depleted their phone credit, ensuring they could not use their phone contract to call family members. In using their *authorized user* access, abusers also made several non-consensual purchases online or in-person using a survivor's account and financial details. In online contexts, abusers made expensive purchases from popular online shopping sites, organize holidays, and also made decisions to participate in high-risk activities such as gambling or purchasing drugs. A

few survivors acknowledged that most couples do not ultimately oversee the other's spending; however, spending by an abuser was excessive and frequently drove the survivor into debt.

Survivors described how abusers would also leverage their physical access to take their financial card details and add them to their own digital wallet ('e-wallet'). Adding a survivor's financial information to their phone ensured that abusers did not need to take or withhold a survivor's physical credit or debit card, but still had the benefit of using the details:

> *"I knew he had been spending ... I received an email from the store, it was a receipt from an area of the city I do not visit ... and it was for hundreds of dollars that I definitely would not have agreed to spend."* (S11)

4.2 Account Compromise

In this category of attacks, abusers did not have legitimate or authorized access to a survivor's financial assets or accounts. Many survivors shared descriptions of how abusers compromised their authorization information to do so, such as physically accessing their devices. Alternatively, abusers accessed their information while they were distracted, occupied, or by compelling them to disclose their details by the threat of violence (discussed in-depth in Section 4.4). Prior studies have identified these compromises in IPV [29, 82, 91] and identity theft [3, 39], however, survivors revealed two new approaches: compromising a *password manager* and exploiting a *password recovery process*.

Preventing Survivor Re-Access. A few survivors described how they used standalone password managers to store their financial information, including card numbers, security card codes, bank customer numbers, and even personal identification numbers (PINs) for debit and credit cards. However, as many modern browsers or operating systems have built-in password managers (e.g., KeyChain, Google Password Manager), some survivors had not realized that they had inadvertently agreed for the browser to save these authentication details for a later session. One survivor (S92) expressed embarrassment at using a password manager in an insecure manner, including using a weak master password, a guessable PIN, or turning the automatic locking system off due to frustration at being asked to re-enter the password consciously when needed.

If an abuser compromised access to this password manager — through physical access, they could gain access to all their financial information, including emergency password reset codes. Abusers who were unable to guess a password could then use *request a password recovery or reset link* to intercept for system access.

We identified that peer-to-peer payment applications (P2PPs) and branchless banking applications proved especially vulnerable to this form of intimate attack as some prominent brands do not require passwords or secret answers for authentication (in line with [65]). A few survivors shared how abusers only needed to know a their phone number and were able to receive a two-factor authentication notification to access their financial account. Once authorized as a survivor, abusers could lock them out of their bank, credit, peer-to-peer payment applications, or investment accounts to prevent re-access. Some survivors were then forced by an abuser to try to continuously restore access to a financial account, being unable to abandon the services (without taking a significant financial loss [3]) with service agents who were unaware of the dynamics of a financially abusive relationship:

> *"I am either on the phone to the fraud team or customer service ... I was bounced around, and no one wanted to take ownership of this problem"* (S115)

In extreme cases, preventing re-access to financial accounts included using compromised access to submit a cancellation request of a survivor's credit card or online financial account. Survivors shared that if this cancellation is successful, a credit issuer shared that they were under no legal obligation to reinstate the account, leaving a permanent mark on a survivor's credit report:

> *"he closed out my credit card, and the company refused to reinstate it ... it screwed up my credit [score] as it was my oldest account"* (S5)

Making Changes to Purchases or Transfers. Many survivors also described how abusers would use their compromised access to purchase new items or services directly, frequently using their account or card to do so. Survivors described how abusers felt a sense of entitlement following this non-consensual authorized access to transfer any of a survivor's income into their own accounts on a regular basis. For instance, when one survivor challenged an abuser about why they had authorized a transfer from their account, they had responded that they did not *"feel like spending their own money"* (S85). As abusers had made purchases or transfers through a survivor's account, sometimes using their devices, customer service representatives struggled to recommend the next steps as the fraudulent charges appeared to be 'authorized':

> *"Then it showed that on my shopping account I bought a piece of furniture, I did not buy that! ... when I called to complain the company said it looked 'fine', but it was not as I did had not made that purchase. He had with my card information ..."* (S131)

A few survivors shared cases where abusers had used compromised access to their accounts to make alterations to existing orders or purchases, predominantly on online shopping websites. These included *"cancelling grocery shopping orders"* (S62), changing delivery slots when such purchases would arrive, and a survivor's delivery information. One survivor (S131) shared these actions which they perceived as annoying had undermined their ability to purchase items for themselves, their children and their friends. A small number of survivors identified cases where an abuser, posing as a survivor, would make non-consensual upgrades to subscription tiers to luxury or premium versions that cost more money. As subscription services charges are subtle, with auto-renew on by default, survivors who were subject to this attack were unaware of these changes until months afterwards.

Some abusers also used their ability to compromise survivor accounts to delete digital assets that survivors purchased through subscription sites or shopping services. These included deleting *"entire libraries"* (S73) of music, digital photo albums, games, and digital art, all of which had been purchased or commissioned by the survivor. One survivor shared that they cultivated these digital collections for years; this also represented a feeling of loss at having to start from scratch:

> *"he sold that artwork that I had commissioned for my family members, it meant so much for me to pass that on to them when the time was right ... and he sold it to some nobody online ..."* (S16)

In some cases, these changes included removing the assets by selling them through online investment accounts such as stocks and shares and brand-new digital assets, such as cryptocurrencies or non-fungible tokens (NFTs). Sales of stocks or shares were incredibly challenging for survivors as such sales are heavily regulated via federal and national regulations, making them difficult, if not impossible, to revoke. Likewise, as cryptocurrencies are built on digital currency protocols of immutable hash codes, transactions cannot be altered or cancelled once initiated.

4.3 Harmful Messages or Reports

Abusers did not require access to conduct harmful attacks on a survivor's finances and well-being or even choose to directly interact with a survivor to control their behavior financially. Digital technologies made many of these financial attacks possible due to their ability to provide an abuser with anonymity, such as creating a fake profile online, or submitting an anonymous tip-off to a financial agency over the phone.

Some survivors described how an abuser knew confidential financial information about them to tailor their attacks. However, survivors shared accounts where abusers used this information in attacks that were motivated to *harm* or *damage* their finances, indicating abusers may be also motivated by complex social goals that go beyond financial exploitation as often found in cases of identity theft.

False Reviews and Fraudulent Reports. To recuperate finances lost during their time with an abuser, many survivors shared that they had started their own online business, frequently hosted on social media sites. However, a small number of survivors shared that abusers had crafted multiple fake profiles to leave significant amounts of negative feedback known as 'review bombing' on survivor's public storefronts:

> *"I run a niche business; there are not many online providers who do what I do in my area. When he continuously leaves negative reviews to bring my rating down ... it makes my business look bad and existing customers bring it up."* (S40)

As many online businesses rely on good ratings and reviews to invite new customers or show on new search results, a few survivors described how any unwarranted negative feedback could directly affect their financial earnings. One survivor (S68) disclosed they had attempted to report the abuser, only for an abuser to make more accounts, many of which the platform never removed. Disputing fake negative reviews and building an online business proved costly, where another survivor shared that it would take them away from being able to *"engage with their real customers"* (S10) and set up new images of stock and services.

In many cases, survivors described how their abuser had fraudulently reported their businesses, and public fundraising attempts to the platform hosters for fraudulently *"misleading donors"* (S83) or customers. As several survivors often used fake names online to help them keep a low profile from their abuser, this could result in the temporary takedown of the page by the website host or platform before re-established due to a mismatch between stated identities. We also saw reports of abusers who made several anonymous fraudulent reports on survivors who received financial support through state institutions, including the social security administration, a financial benefit provider in the U.S. for low-income households:

> *"He made a report about how I was spending my benefits as if it is not restrictive enough as it is ... it stopped money coming into the house, I had to ask friends for cash ... it was humiliating".* (S117)

These actions inevitably deprived the survivor of the cash benefits that they could use for groceries and rent and impacted any children under the survivor's care.

Outsourcing Financial Attacks. Survivors shared how abusers would disclose and distribute known financial data, such as authentication details, social security numbers, bank passwords or full card numbers, with others, such as on public forums. While the breach of personal information can occur at a business-wide level (e.g., the Experian leak of 2015), some cases described abusers posting financial information on online forums and would also pair these posts with personal messages that contained links to the forum posts to the survivor:

> *"whatever I do with my bank accounts, they [abuser and new partner] still find ways around the changes I make to protect myself ... one time they posted my new bank account and password on a classified ads site"* (S11).

These actions indicated to survivors that their abusers were directly behind the attacks; however, as survivors were not the original content posters, they could not easily take the information down. As an abuser had outsourced these attacks, one survivor (S108) described that it was hard to know if an abuser was behind an attack that directly used their information or if another user online used it as an opportunity to take advantage.

Unfortunately, we also saw banks begin to be exploited as third parties in an abuser's attempt to harass and intimate their survivor. For instance, some accounts described how abusers would bombard a survivor with security alerts (e.g., "someone has tried accessing your account", "log in an attempt") that survivors had in place on their accounts as a way around contacting them directly. The frequency and wording of many alerts proved alarming to many survivors who experienced this and had a cumulative impact on their mental well-being.

4.4 Deception and Identity Theft

As per Eriksson and Ulmestig [26], we identified that survivors' experiences of financial abuse came with other forms of abuse, notably psychological and emotional abuse. Survivors described abusers as using deception to convince them to disclose information, limit their knowledge of existing financial accounts, or use strategies that would make survivors question their sanity [71] or 'gaslighting'.

Controlling access to a survivor's financial information is a core part of financial abuse [2], and we saw a disturbing manifestation of

this where many survivors could not control access to their *privacy* of this financial information. Survivors were acutely aware of the level of authority an abuser had with new knowledge about them (e.g., attacks in Section 4.3).

Deceiving Survivors. Some survivors stated that abusers regularly used psychological manipulation and gaslighting to control the oversight survivors had over their personal and household finances. Deceptive behavior included deliberately hiding, destroying or deleting digital evidence of an abuser's financial products, such as debts, bank statements or receipts, that kept the survivor in the dark about their finances. We saw examples where an abuser had reassured a survivor that they had *"paid a utility bill online"* (S31) only for the survivor to discover that this had gone unpaid through a reminder email. One survivor explained that their ex-partner even went through the process of printing false receipts of a plane ticket she was unable to afford on her own:

> *"He would print out something that said he had a plane ticket on hold for me to go back home, but it never really happened, there was no plane ticket ... It was just a game to him".* (S13)

Many survivors shared instances where their abusers would attempt to socially manipulate them into sharing private financial details across a range of different contexts, such as posing as *"genuine customers interested in making a purchase"* (S39) through their online business. In one case, a survivor shared that their abuser had created a new, fraudulent business to elicit financial information:

> *"I noticed a business profile on social media, so I was interested in following them as they looked cool ... then questions about my outgoing costs started ... then he replied from his account by mistake and then I realised it was him".* (S6)

In a similar case (S111), one survivor felt isolated as they could not determine legitimate customers from their abuser and took protective privacy measures that directly damaged their earnings.

Deceiving Others Connected to Survivors. In our data set, we read descriptions of how financial institutions and banks rarely had additional levels of verification that necessitated properly authenticating new applicants for a credit or debit card. Many survivors disclosed how abusers exploited this lack of online security by using a their personal financial information to apply for multiple credit cards online in their name fraudulently. Applications for credit cards and loans necessitated a creditor looking at a survivor's credit file to determine how much risk they posed as a borrower, known often as a *hard pull* or *hard credit inquiry*:

> *"She set up various credit cards from a variety of different banks without my permission, using my social security, prepaid cards, you name it, my score tanked".* (S32)

These requests acted as permanent marks on a survivor's credit history, and nearly all accounts disclosed that this directly negatively impacted their credit scores for at least two years following the application. These documents contained further confidential information about a survivor that they did not want to be made public, including public records (e.g., files for bankruptcy), and account information (e.g., missed payments). Although credit bureaus can prevent requests for new credit reports and accounts through credit freezes, consumer uptake of these tools is low due to a lack of awareness, a conflation with tools on other financial products, and usability concerns [95]. In two cases survivors described considering freezes, but hesitated to disclose their status as a survivor of IPV out of concern of being stigmatized and thereby receiving negative financial marks on their accounts. These concerns illustrate a common misconception on freezes—that customers need to disclose a reason for a freeze request (as found by Zou et. al. [95]).

Survivors described situations where abusers would also interfere with their ability to earn through socially manipulating financial coordinators at their workplace to redirect salary and benefits. If successful, this attack was challenging for survivors to manage as employers were resistant to re-compensating the survivor of lost income, and due to short time restrictions for withdrawals of transfers for online transfers:

> *"My husband called up my work to share the 'correct' details for an account he described as 'our' joint account ... My work didn't confirm it with me ... when I returned I discovered he had stolen two weeks' worth of my salary".* (S133)

4.5 Bypass Physical Security

Finally, survivors described how abusers pursued their physical possessions and property. Abusers used tactics to repeatedly invade a survivor's sense of privacy around finances through destroying, damaging, or withholding their digital devices and bypassing home security systems to steal financial documents and authentication information.

These attacks were motivated to destroy and steal physical representations of information and devices to control their interactions with finances and their financial institutions. While some of these strategies mirror dumpster diving and mail interception found in cases of targeted identity theft [39], the post-attack taunt that abusers used against survivors appeared to be a distinctively psychologically harmful variant of these attacks.

Targeting Devices. Abusers may destroy devices that they legally own [29]; however, our accounts show how abusers also destroy other people's devices to control them. These devices included phones, cameras, speakers, laptops, tablets, external hard drives and physical cryptocurrency wallets that survivors had to insure repeatedly to protect them from damage.

A few survivors shared how they were subject to *"lengthy claims processes"* (C69) through customer service to report a device damaged or stolen, only to discover that they needed to pay off the amount in full before getting a new device. However, some abusers withheld their devices for a particular period to control their ability to coordinate work arrangements. When abusers did this, it had a uniquely harmful impact on survivors who conducted business online or needed digital devices for their jobs in the creative industry:

> *"... he would take my phone away and keep it for a day or two. I would panic because this is where my money*

comes through. That is the number my customers call me on, and I need this phone." (S12)

During this time, a few survivors described how abusers prevented from receiving emergency money from friends and family, including money sent via text messages such as Apple Cash or through peer-to-peer payment applications (e.g., Venmo and Cash App). Withholding rather than stealing a device meant survivors faced barriers to submitting an official report to try and legally reclaim the item. One survivor (S20) shared that law enforcement would eventually dispute the phone as stolen if it was physically back in their possession. As personal devices play a significant role in authentication approaches, such as through the use of authenticator apps and two-factor authentication (2FA), we saw a significant overlap of this attack with locking a survivor out of their financial accounts (discussed in Section 4.2).

Targeting Physical Copies of Financial Data. Abusers also demonstrated significant dedication to the gathering, collecting and stealing financial information related to a survivor's online accounts, typically targeting from their home and places of work (akin to intimate partner surveillance [9, 82, 88] and social engineering [46]). Several shared how their abusers had targeted physical copies of bank statements, medical or utility bills, account details, card details and mail containing cards or PIN codes:

"I failed to receive papers from the bank ... important ones with card details and PINs. On another occasion, some letters had been opened and placed back in the mailbox ... to send a message" (S9).

A few survivors shared that these attacks also targeted the addresses of the survivors' trusted family members, who were used as a *"safe place to visit"* (S58) following the relationship. These physical violations of a survivor's privacy also extended to abusers accessing their trash, such as dumpster diving for information. Several survivors shared that they had considered that someone else other than an abuser could have also performed this attack. However, in each case, their abusers had paired these attacks with conversations with survivors that contained references to accounts that would have otherwise been unknown:

"I do not even throw out a scrap of paper without shredding it because I am just constantly frightened that he will have insight into what is happening in my life." (S6).

5 CONTEXTUALIZING ABUSIVE BEHAVIORS

In this section, we report *why* abusers might conduct these attacks by identifying *four motivations* for financial harm from interviews with 16 financial advocates. While only five financial advocates shared second-hand accounts of how client had disclosed use of financially coercive and controlling behavior against a partner, all 16 advocates spoke to numerous examples of the devastating impact such behaviors had on survivors which we report here.

We identified that advocates argue that abusers predominantly use four main approaches to cause financial harm with technology; actions that would *exploit*, *monitor*, *restrict* and *sabotage* a survivor's financial well-being and independence (Figure 1). As financial abuse is a constellation of controlling behaviors [68, 69], several actions could belong to two or more motives. We note that some categories directly validate some previously identified conceptual categories of measurements of economic abuse (e.g., Postmus et al.'s [60] economic exploitation, employment sabotage), suggesting that our findings reflect survivors' experiences.

5.1 To Exploit a Survivor's Finances

Advocates shared with us several instances where abusers would use financially coercive and controlling behaviors to *exploit* their current or former partners. In these contexts, advocates shared cases where an abuser would be motivated to financially extract income or resources without sharing this benefit. Advocates identified that exploitative behaviors could also use a survivor's good credit score:

"so abusers might be motivated to apply for loans in the survivor's name as there is no chance that they will get that approved if they apply in their own [name]. Abusers instead piggyback off a survivor's good reputation and then use up the finances too ..." (A6).

Advocates shared that this behavior was pervasive when a survivor was in a stronger financial position than an abuser, such as possessing a higher salary, a more prestigious job, or having healthier financial behaviors such as budgeting. In some interviews, advocates who had worked closely with survivors through several leave-stay cycles [75] identified that the risk of exploitation was more acute when an abuser suspected a survivor would leave them.

In this context, advocates shared that survivors attempted to avoid being exploited by actively restricting their behaviors and deliberately avoiding signing up to, or using existing digital financial services. These cases proved distressing for advocates who described survivors who did this as *"representing a new form of digital divide"* (A1) — users who did have access to digital services but felt unable to use them out of fear of being taken advantage of.

5.2 To Restrict a Survivor's Access

Advocates highlighted that the most common behavior across our taxonomy were behaviors to *restrict* and limit what survivors could do. Some of our interviewees shared that these behaviors were especially manipulative (possibly explaining its saturation in Section 4.4) as abusers framed these actions as acts of care to a survivor, which may be misinterpreted as generosity to 'manage' responsibilities for household finances by others:

"abusers are really good at framing what they do as in the victim's interest ... 'don't worry, I'll get that bill, receipt or I'll handle it ... people don't see how that victim doesn't have a say in whether that bill gets paid!" (A14).

When abusers were motivated to restrict a survivor's finances, advocates shared that this could allow them to have total control over any financial decisions made online or offline regarding shared finances. These restrictive behaviors could also be motivated by a desire to restrict how much a survivor was mentally aware of financial setbacks or how much money a partner had saved. However, advocates shared that they had noticed an uptick in the number of survivors that had found ways around an abuser attempting to

restrict access to an online bank account or a device that supported one:

> *"we have seen people at all stages ... you know traditional bank account gone, so they use Venmo, or Paypal accounts ... we try to encourage two-factor [authentication] but yeah the logins on those aren't super secure ... and to state the obvious ... they are not bank accounts"* (A2).

In some situations, survivors navigated this restriction with care, using friends' and family members' devices or peer-to-peer payment applications and online payment services. These services were a 'secret store' for finances that may be required for an escape; however, advocates felt uncomfortable recommending these practices without careful consideration as *"stashing money can be harmful ... it's the exact opposite of what a healthy relationship is!"* (S16).

5.3 To Monitor a Survivor's Activity

Mirroring prior findings in intimate partner surveillance [9, 14, 82], advocates shared that several financial abusers were motivated to monitor or surveil what a survivor was doing across all of their financial accounts. These motives were subtle, and advocates shared that they could be tough to prove as being directly harmful, as these actions had the *potential* to lead to something more harmful in the future. Advocates identified that having an active criminal or legal case with a survivor was a common occurrence for abusers who were motivated to watch their partner remotely continuously:

> *"it's a consistent dedication to ensure that their partner has no privacy, no right to privacy on anything you do ... it's a need to know what someone is doing, every transaction, every restaurant they go to..."* (A8).

Advocates shared that tackling cases of extreme intimate surveillance could be difficult. Many banks had now directly designed surveillance tools into personal and shared spending accounts through financial interfaces, such as 'track your expenditure' screens. When a survivor felt that an abuser was monitoring their finances, advocates shared that some survivors had consciously started to *"pay for services with cash"* (A7) to ensure that an abuser could infer no financial, location or time data. Advocates cautiously suggested that the inability to lead a private life concerning financial transactions could also be a trigger for survivors to leave their abuser:

> *"I had a client who told their abuser, 'I wanted to separate, he thought being the husband meant giving me no right to privacy ... I did not want to live like that ...' so it can work both ways, both as a cage and realizing the client needs to break free"* (A4).

5.4 To Sabotage a Survivor's Independence

Finally, advocates discussed that abusers could be motivated by a desire to sabotage their survivor's financial life through behaviors that could severely harm or destroy their financial reputation. Advocates highlighted that the social dynamics of IPV made financial abuse especially attractive to abusers due to its ability to serve two purposes of controlling the person in the short-term and sabotaging them in the long run:

> *"It's the power and control and hurting the person, ruining their credit so they cannot do anything, right? It is easy to do so online, like ... sinking a credit score with another card application ... a simple action has a long-lasting impact ..."* (A14).

Abusers who wanted to destroy someone's finances were particularly hard to discuss with financial institutions. Most customer service representatives were equipped to deal with identity thieves who are overwhelmingly financially motivated [3, 59], rather than financial abusers. These motives sometimes appeared to run directly contrary to *exploiting* a survivor, which may require an abuser to rely on a survivor's good credit or lack of debt to ensure access to more money. Once more, some advocates identified that abusers used these behaviors after a survivor had left a relationship and after any legal proceedings had happened. Advocates suggested that many survivors shared the struggle of wanting to rebuild an online identity, such as having an online business, but that this left them directly exposed to an abuser finding them:

> *"a survivor might have an online business ... it is a constant visual target ... you can be hundreds of miles away, and your abuser will still be able to get you somehow. They [abusers] will still find a way to damage you financially online with no cost to them"* (A2).

6 DISCUSSION

Our descriptive study from the reports of 158 survivors of IPV and 16 financial advocates sheds light on how technology directly enables abusers to harm survivors financially. The range of attacks used by abusers expands well beyond traditional online banking infrastructure [20, 34, 92], including employers, benefits providers, online shopping sites, credit bureaus, investment managers, and more. Indeed, many of these harmful attacks identified in our study reinforce the plethora of deceptive tactics, bypassing physical security and methods for account compromise so often identified in cases of identity theft [39]. However, the facets of financial harm that specifically targeting a survivor's identity online, such as damaging a survivor's business reputation is more in line with hate and harassment identity campaigns than theft alone [80]. We suggest such findings warrant novel preventative approaches from those in elder financial abuse [6, 31, 47], whereby sabotage would seemingly work counter to most fraudsters aspirations for financial gain.

Providing advocates who work with survivors of intimate partner violence with a better understanding of the dynamics between technology, finances, and coercive control could lead to improved outcomes for survivors [56]. However, many advocates lack confidence in their ability to respond to technology-facilitated harms [28, 30, 69], and may struggle to secure funding for survivors in need of protection when other legal avenues are inaccessible [22, 44, 89]. Our findings lead us to call for broader agendas in scholarly research, computer security, and financial sectors to address *intimate threats* and financial abuse in technologies that use, store, or facilitate financial information – areas of work often neither struggle for funding or resources [5, 27].

6.1 Detecting Financially Abusive Interactions

Our findings add to the growing number of works that show how common authentication approaches on consumer technologies fail [29, 30, 90] to differentiate between legitimate and authorized-but-adversarial users. In our data-set, several abusers were able to surpass knowledge, possession and inherence-based identity challenges to pose as the survivor (e.g., fraudulent transfers), or obstruct a survivor from being authorized (e.g., to block access) [46]. However, *detecting* fraudulent interactions also seemingly slipped under the radar as these interactions did not fall outside of the range of a consumer's 'normal' behaviour that may trigger rule-based queries (e.g., expenditure in an atypical country). For instance, online transactions or upgrades to subscription tiers (as shown in Section 4.2) are *legitimate* uses of a system, but can act as another lever of control in an abuser's *"constellation of abuse"* [24].

We suggest that the expertise of advocates could be useful here, many of whom identified several life changes to an escalation in technology and financial abuse (Section 4.5) which may complement known risk factors in areas of financial elder abuse. These included leaving a shared domestic environment, being engaged in court or criminal legal against an abuser (e.g., divorce proceedings, stay-away orders) or starting an online business. Financial service providers, or even e-commerce providers, may be able to infer these life changes through address changes, legal fees, or changes in income. Although identity-based crime prevention professionals warn platforms against *"empty technological promises"* that both fail to adequately respond to emerging sources of risk for victimization [59], we believe there is far more to be done to protect survivors and deter abusers. Such shifts in a survivor's financial journey may warrant different privacy and security considerations for different stages of relationships involving financial abuse which may be recommended by a system[51].

While many online business owners also experience hate and harassment (e.g., content creators [80]), platform and web-hosters could also expand their guidance to include survivors of IPV who have recently left – or are in the process of leaving – a relationship. For instance, guides could be explicitly tailored to the unique coercive and controlling dynamics of IPV and recommend fine-tuned control options for business owners with a persistent problem customer who could well be an abuser.

6.2 Modelling Threats and Consent

For many survivors of IPV, traditional banking and payment infrastructure were implicated in directly facilitating and motivating an abuser's harmful behaviors (e.g., bypassing physical security attempts Section 4.5) and permitted them to exploit, restrict, sabotage, and monitor a survivor's financial activity. As financial services have predominantly focused on protecting consumers from external threats [71], often at the expense of considering attacks closer to home [46], such as intimate partners or family members, this is a potentially unsurprising result [48]. While such assumptions are clearly baked into existing financial infrastructure, we discuss two complementary approaches to mitigate harm from intimate threats and augment consentful interactions with personal finance.

6.2.1 Designing for Intimate Threats. Despite often being designed into the fabric of many financial products (e.g., joint, family accounts), users who have a close intimate relationship with another user are rarely considered as adversarial or a potential intimate threat toward users whom they share an account with [48, 89]. Indeed, our findings support what scholars have long sought to challenge the stereotype of the faceless stranger that plagues perceptions of identity theft; more-often than not being a relative, family friend, colleague, or a commercial service provider to the survivor. [87]. We as such posit that building on promising work in HCI that has drawn attention to the acute risk of harmful third-parties [5, 47], designers of financial infrastructure might synthesize two valuable concepts of *intimate threats* and *adversarial thinking* where 'thinking like an attacker' is informed by intimate *knowledge about* and *access to* a target [29, 48].

Adopting this approach could enable anticipating some of these attacks before they occur, such as those primarily motivated by *sabotaging* a survivor's finances or simply *restrict* their ability to access financial accounts. For instance, making multiple credit card applications in a survivor's name for the sole purpose of negatively impacting their credit score (Section 4.4) may be able to be caught early. Likewise, benefit providers could anticipate how abusers could use deceptive strategies (Section 4.3) to manipulate anti-fraud mechanisms [95], such as triggering a freeze on an existing benefits account. We see great promise in legal advocacy and design justice groups lobby for changes in the consumer credit model through demonstrating how existing infrastructure leaves vast expenditures from authorized *but adversarial* users as legally responsible for paying off.

6.2.2 Designing for Consentful Interactions. Survivors incurred significant harms when financial actions were performed without their consent by their abuser; from taking actions they disagreed to to exposing private information to a wider audience. Akin to other scholars critiques of other technical systems [76, 96], other interactions with financial services (e.g., confirming payment details, playing an order) were taken to infer rather than confirm consent through informed, affirmative or enthusiastic approaches [40]. Such inflexible consent systems were perceived so poorly that advocates reported cases where survivors consciously chose to abandon systems out of concern of being "taken advantage of" (Section 5.2) mirroring emergent work on racialized identities [21].

We acknowledge it is no easy feat for digital services to obtain consent for financial interactions that is voluntarily provided by an informed user in a manner that is unburdensome and reversible. Nevertheless, without working toward these gold standards, it is hard to anticipate how systems may bridge the socio-technical gap that may interpret consent performed under the coercion of financial abuse. An immediate starting point could be understanding consent to financial interactions as specific and contextually situated (akin to [96]) where new or changes to financial activity requires specific and informed approval from the user. We look to authentication and scholars on identity-related crimes for how such requests might be done so sensitively, and even be delivered through non-technical means for survivors who do not have access to their devices or accounts.

6.3 Financial Abuse Aware Customer Service

The survivors and advocates in our work described several instances where survivors met inadequate responses to financial harm when reaching out to an e-commerce site or their financial institution for help. When making reports of non-consensual purchases, survivors shared how online banking and e-commerce support staff stated that the purchases *"looked fine"*. Reports of customer service representatives focusing on *technical* faults over other *social* influences such as abuse reinforces previous findings in the security software space [94]. Our findings point out that representatives would benefit from adequate training to understand financial abuse and the range of ways customers can experience it.

Representative training could start with incorporating social indicators for financial abuse or 'red flag' descriptions from customers, such as survivors who share that they have *"no privacy"* (A7) with spending, or *"not being allowed near finances"* (S21). If customer representatives suspect cases of financial abuse, *conversation toolkits* [79] that provide structured conversation prompts for representatives who may wish to gather further information and reassure a survivor what help their institution could offer. Reaching out to query unusual activity on a survivor's account should also be done with great care.

Financial institutions could consider delivering customer alerts that do not deliberately escalate the risk of physical abuse to a survivor under surveillance [83] or exacerbate trauma, by being potentially guided by Chen et al.'s *trauma-informed computing* [18]. Such a framework requests that designers, among others, both anticipate traumatic stress reactions, such as security indicators that could prove to be scary (e.g., using harsh colors, security jargon), and encouraging enablement where survivors can have greater control over their financial decisions and well-being. While conversations around financial abuse can be daunting, detecting a relatively 'hidden' harm could ensure that an organization can sanction a financial abuser before further and potentially irreparable damage is done to a survivor and their financial stability. As a relatively small per cent of IPV survivors reach out to support organizations for assistance [13, 93], consumer representatives need to be prepared to encounter disclosures and reports of financial harm across their career.

7 CONCLUSION

This paper reports the findings from a qualitative, descriptive study with 158 survivors of IPV and 16 financial advocates on how abusers use technologies to inflict financial harm on survivors. From an analysis of 174 consultations with survivors of tech abuse, we show that abusers use a range of familiar and unreported technological attacks, including leveraging their ability to own or act as authorized users on a survivor's accounts. Through deception and bypassing a survivor's physical security, abusers gain access to a wide range of financial information that abusers use to compromise their accounts, post harmful messages about them or apply for assets in a survivor's name.

Second, drawing from our discoveries, we spoke to advocates who were able to further characterize the motivations behind these attacks and highlight ways that survivors attempted to mitigate this impact on their financial well-being. We conclude this work with a call to action in the financial technologies sector and platforms that support survivor-led businesses to protect vulnerable users better as they attempt to secure their financial stability and independence from harm.

8 ACKNOWLEDGEMENTS.

Thank you to all our participants who graciously shared their experiences to benefit research for safer technology development. We would like to thank Jeremy Shaffer for his contribution to the data collection stage of our study, as well as Professor Nicola Dell and Professor Thomas Ristenpart for their feedback. In addition, we would like to thank our associate chairs and reviewers, whose comments helped improve this manuscript. This work was funded in part by NSF Award #1916096, as well as gifts from J.P.Morgan Chase.

REFERENCES

[1] Katherine Verdolini Abbott, Franca Benedicty Barton, Lauren Terhorst, and Adrianna Shembel. 2016. Retrospective Studies: A Fresh Look. *American Journal of Speech-Language Pathology* 25, 2 (May 2016), 157–163. https://doi.org/10.1044/2016_AJSLP-16-0025 Publisher: American Speech-Language-Hearing Association.

[2] Adrienne E. Adams, Cris M. Sullivan, Deborah Bybee, and Megan R. Greeson. 2008. Development of the Scale of Economic Abuse. *Violence Against Women* 14, 5 (May 2008), 563–588. https://doi.org/10.1177/1077801208315529 Publisher: SAGE Publications Inc.

[3] Chad Albrecht, Conan Albrecht, and Shay Tzafrir. 2011. How to protect and minimize consumer risk to identity theft. *Journal of Financial Crime* 18, 4 (Jan. 2011), 405–414. https://doi.org/10.1108/13590791111173722 Publisher: Emerald Group Publishing Limited.

[4] Michelle S. Ballan and Molly Freyer. 2019. Intimate Partner Violence and Women With Disabilities: The Role of Speech-Language Pathologists. *American Journal of Speech-Language Pathology* 28, 4 (Nov. 2019), 1692–1697. https://doi.org/10.1044/2019_AJSLP-18-0259 Publisher: American Speech-Language-Hearing Association.

[5] Belen Barros Pena. 2021. *Understanding and designing technologies for everyday financial collaboration.* doctoral. Northumbria University. https://nrl.northumbria.ac.uk/id/eprint/47849/

[6] Belén Barros Barros Pena, Bailey Kursar, Rachel E Clarke, Katie Alpin, Merlyn Holkar, and John Vines. 2021. Financial Technologies in the Cycle of Poor Mental Health and Financial Hardship: Towards Financial Citizenship. In *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems (CHI '21)*. Association for Computing Machinery, New York, NY, USA, 1–16. https://doi.org/10.1145/3411764.3445251

[7] Scott R. Beach. 2017. The Role of Technology in Elder Abuse Research. In *Elder Abuse: Research, Practice and Policy*, XinQi Dong (Ed.). Springer International Publishing, Cham, 201–214. https://doi.org/10.1007/978-3-319-47504-2_10

[8] Rosanna Bellini, Simon Forrest, Nicole Westmarland, and Jan David Smeddinck. 2020. Mechanisms of Moral Responsibility: Rethinking Technologies for Domestic Violence Prevention Work. In *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems (CHI '20)*. Association for Computing Machinery, New York, NY, USA, 1–13. https://doi.org/10.1145/3313831.3376693

[9] Rosanna Bellini, Emily Tseng, Nora McDonald, Rachel Greenstadt, Damon McCoy, Thomas Ristenpart, and Nicola Dell. 2021. "So-called privacy breeds evil": Narrative Justifications for Intimate Partner Surveillance in Online Forums. *Proceedings of the ACM on Human-Computer Interaction* 4, CSCW3 (Jan. 2021), 210:1–210:27. https://doi.org/10.1145/3432909

[10] Elinor Benami and Michael R. Carter. 2021. Can digital technologies reshape rural microfinance? Implications for savings, credit, & insurance. *Applied Economic Perspectives and Policy* 43, 4 (2021), 1196–1220. https://doi.org/10.1002/aepp.13151 _eprint: https://onlinelibrary.wiley.com/doi/pdf/10.1002/aepp.13151.

[11] Rasika Bhalerao, Vaughn Hamilton, Allison McDonald, Elissa M. Redmiles, and Angelika Strohmayer. 2022. Ethical Practices for Security Research with At-Risk Populations. In *2022 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)*. IEEE, Genoa, Italy, 546–553. https://doi.org/10.1109/EuroSPW55150.2022.00065

[12] Susanne Boethius, Malin Åkerström, and Margareta Hydén. 2022. The double-edged sword – abused women's experiences of digital technology. *European Journal of Social Work* 0, 0 (Feb. 2022), 1–13. https://doi.org/10.1080/13691457.2022.2040437 Publisher: Routledge _eprint: https://doi.org/10.1080/13691457.2022.2040437.

[13] Matthew Breiding, Kathleen C. Basile, Sharon G. Smith, Michele C. Black, and Reshma R. Mahendra. 2015. Intimate partner violence surveillance : uniform definitions and recommended data elements. Version 2.0. https://stacks.cdc.gov/view/cdc/31292 Place: Atlanta, GA.

[14] Megan Lindsay Brown, Lauren A. Reed, and Jill Theresa Messing. 2018. Technology-Based Abuse: Intimate Partner Violence and the Use of Information Communication Technologies. In *Mediating Misogyny: Gender, Technology, and Harassment*, Jacqueline Ryan Vickery and Tracy Everbach (Eds.). Springer International Publishing, Cham, 209–227. https://doi.org/10.1007/978-3-319-72917-6_11

[15] Rebecca Campbell. 2001. *Emotionally Involved: The Impact of Researching Rape*. Routledge, New York.

[16] Serena Caria, Fabio Paternò, and Carmen Santoro. 2019. Understanding ASD individuals' difficulties with managing money: an interactive study. In *Proceedings of the 13th Biannual Conference of the Italian SIGCHI Chapter: Designing the next interaction (CHItaly '19)*. Association for Computing Machinery, New York, NY, USA, 1–5. https://doi.org/10.1145/3351995.3352038

[17] Sam Castle, Fahad Pervaiz, Galen Weld, Franziska Roesner, and Richard Anderson. 2016. Let's Talk Money: Evaluating the Security Challenges of Mobile Money in the Developing World. In *Proceedings of the 7th Annual Symposium on Computing for Development (ACM DEV '16)*. Association for Computing Machinery, New York, NY, USA, 1–10. https://doi.org/10.1145/3001913.3001919

[18] Janet X. Chen, Allison McDonald, Yixin Zou, Emily Tseng, Kevin A Roundy, Acar Tamersoy, Florian Schaub, Thomas Ristenpart, and Nicola Dell. 2022. Trauma-Informed Computing: Towards Safer Technology Experiences for All. In *Proceedings of the 2022 CHI Conference on Human Factors in Computing Systems (CHI '22)*. Association for Computing Machinery, New York, NY, USA, 1–20. https://doi.org/10.1145/3491102.3517475

[19] Sen Chen, Ting Su, Lingling Fan, Guozhu Meng, Minhui Xue, Yang Liu, and Lihua Xu. 2018. Are mobile banking apps secure? what can be improved?. In *Proceedings of the 2018 26th ACM Joint Meeting on European Software Engineering Conference and Symposium on the Foundations of Software Engineering (ESEC/FSE 2018)*. Association for Computing Machinery, New York, NY, USA, 797–802. https://doi.org/10.1145/3236024.3275523

[20] Shelly Clevenger, Jordana N. Navarro, and Thomas J. Holt. 2022. The Financial Leash: Cyberfinancial Abuse within Intimate Relationships. *Victims & Offenders* 17, 5 (July 2022), 781–793. https://doi.org/10.1080/15564886.2022.2065714 Publisher: Routledge _eprint: https://doi.org/10.1080/15564886.2022.2065714.

[21] Jay L. Cunningham, Sydney T. Nguyen, Julie A. Kientz, and Daniela Rosner. 2022. The Cost of Culture: An Analysis of Cash App and the Financial Inclusion of Black American Communities. In *Designing Interactive Systems Conference (DIS '22)*. Association for Computing Machinery, New York, NY, USA, 612–628. https://doi.org/10.1145/3532106.3533569

[22] Dana Cuomo and Natalie Dolci. 2021. New tools, old abuse: Technology-Enabled Coercive Control (TECC). *Geoforum* 126 (Nov. 2021), 224–232. https://doi.org/10.1016/j.geoforum.2021.08.002

[23] Hesham Darvish and Mohammad Husain. 2018. Security Analysis of Mobile Money Applications on Android. In *2018 IEEE International Conference on Big Data (Big Data)*. IEEE, Seattle, WA, USA, 3072–3078. https://doi.org/10.1109/BigData.2018.8622115

[24] Rebecca Emerson Dobash and Russell P. Dobash. 1998. Violent men and violent contexts. In *Rethinking violence against women*. Sage Publications, Inc, Thousand Oaks, CA, US, 141–168. https://doi.org/10.4135/9781452243306.n6

[25] Chris Elsden, Tom Feltwell, Belén Barros Pena, Bettina Nissen, Inte Gloerich, Chris Speed, and John Vines. 2020. Designing Futures of Money and FinTech. In *Companion Publication of the 2020 ACM Designing Interactive Systems Conference (DIS' 20 Companion)*. Association for Computing Machinery, New York, NY, USA, 429–432. https://doi.org/10.1145/3393914.3395904

[26] Marie Eriksson and Rickard Ulmestig. 2021. "It's Not All About Money": Toward a More Comprehensive Understanding of Financial Abuse in the Context of VAW. *Journal of Interpersonal Violence* 36, 3-4 (Feb. 2021), NP1625–1651NP. https://doi.org/10.1177/0886260517743547 Publisher: SAGE Publications Inc.

[27] Jean Feingold. 2015. Meeting Customers Where They Are. *American Bankers Association. ABA Banking Journal* 107, 3 (Oct. 2015), 28–30. https://www.proquest.com/docview/1705092514/abstract/F07BA74BAB1F4ED4PQ/1 Num Pages: 3 Place: New York, Canada Publisher: Naylor Communications Ltd. Section: FEATURE: MARKETING TRENDS.

[28] Diana Freed, Sam Havron, Emily Tseng, Andrea Gallardo, Rahul Chatterjee, Thomas Ristenpart, and Nicola Dell. 2019. "Is my phone hacked?" Analyzing Clinical Computer Security Interventions with Survivors of Intimate Partner Violence. *Proceedings of the ACM on Human-Computer Interaction* 3, CSCW (Nov. 2019), 202:1–202:24. https://doi.org/10.1145/3359304

[29] Diana Freed, Jackeline Palmer, Diana Minchala, Karen Levy, Thomas Ristenpart, and Nicola Dell. 2018. "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)*. ACM, New York, NY, USA, 667:1–667:13. https://doi.org/10.1145/3173574.3174241 event-place: Montreal QC, Canada.

[30] Diana Freed, Jackeline Palmer, Diana Elizabeth Minchala, Karen Levy, Thomas Ristenpart, and Nicola Dell. 2017. Digital Technologies and Intimate Partner Violence: A Qualitative Analysis with Multiple Stakeholders. *Proceedings of the ACM on Human-Computer Interaction* 1, CSCW (Dec. 2017), 46:1–46:22. https://doi.org/10.1145/3134681

[31] Aaron J. Greene. 2021. Elder Financial Abuse and Electronic Financial Instruments: Present and Future Considerations for Financial Capacity Assessments. *The American Journal of Geriatric Psychiatry* 30 (March 2021), 90–106. Issue 1. https://doi.org/10.1016/j.jagp.2021.02.045

[32] Thilina Halloluwa, Pradeepa Bandara, Hakim Usoof, and Dhaval Vyas. 2018. Value for money: co-designing with underbanked women from rural Sri Lanka. In *Proceedings of the 30th Australian Conference on Computer-Human Interaction (OzCHI '18)*. Association for Computing Machinery, New York, NY, USA, 63–73. https://doi.org/10.1145/3292147.3292157

[33] Bridget Harris. 2018. Spacelessness, spatiality and intimate partner violence: Technology-facilitated abuse, stalking and justice administration. In *Intimate Partner Violence, Risk and Security*. Routledge, Melborne, AU. Num Pages: 19.

[34] Tirion Havard and Michelle Lefevre. 2020. Beyond the Power and Control Wheel: how abusive men manipulate mobile phone technologies to facilitate coercive control. *Journal of Gender-Based Violence* 4, 2 (June 2020), 2–18. https://doi.org/10.1332/239868020X15850131608789

[35] Sam Havron, Diana Freed, Rahul Chatterjee, Damon McCoy, Nicola Dell, and Thomas Ristenpart. 2019. Clinical Computer Security for Victims of Intimate Partner Violence. In *Proceedings of the 29th USENIX Conference on Security Symposium*. USENIX Association, USA, 105–122. https://www.usenix.org/conference/usenixsecurity19/presentation/havron

[36] Dean R. Hess. 2004. Retrospective studies and chart reviews. *Respiratory Care* 49, 10 (Oct. 2004), 1171–1174.

[37] Gretchen L. Hoge, Amanda M. Stylianou, Judy L. Postmus, and Laura Johnson. 2019. Domestic Violence/Intimate Partner Violence and Issues of Financial Abuse and Control: What Does Financial Empowerment Look Like? In *The Routledge Handbook on Financial Social Work*. Routledge, London, UK. Num Pages: 11.

[38] Samia Ibtasam, Hamid Mehmood, Lubna Razaq, Jennifer Webster, Sarah Yu, and Richard Anderson. 2017. An Exploration of Smartphone Based Mobile Money Applications in Pakistan. In *Proceedings of the Ninth International Conference on Information and Communication Technologies and Development (ICTD '17)*. Association for Computing Machinery, New York, NY, USA, 1–11. https://doi.org/10.1145/3136560.3136571

[39] Identity Theft Resource Center. 2021. *Consumer Aftermath Report: How Identity Crimes Impact Victims, their Families, Friends and Workplaces*. Technical Report. Identity Theft Resource Center. https://www.idtheftcenter.org/publication/identity-theft-the-aftermath-study/

[40] Jane Im, Jill Dimond, Melody Berton, Una Lee, Katherine Mustelier, Mark S. Ackerman, and Eric Gilbert. 2021. Yes: Affirmative Consent as a Theoretical Framework for Understanding and Imagining Social Platforms. In *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems (CHI '21)*. Association for Computing Machinery, New York, NY, USA, 1–18. https://doi.org/10.1145/3411764.3445778

[41] Laura Johnson, Yafan Chen, Amanda Stylianou, and Alexandra Arnold. 2022. Examining the impact of economic abuse on survivors of intimate partner violence: a scoping review. *BMC Public Health* 22, 1 (May 2022), 1014. https://doi.org/10.1186/s12889-022-13297-4

[42] Ratinder Kaur, Yan Li, Junaid Iqbal, Hugo Gonzalez, and Natalia Stakhanova. 2018. A Security Assessment of HCE-NFC Enabled E-Wallet Banking Android Apps. In *2018 IEEE 42nd Annual Computer Software and Applications Conference (COMPSAC)*, Vol. 02. IEEE, Tokyo, Japan, 492–497. https://doi.org/10.1109/COMPSAC.2018.10282 ISSN: 0730-3157.

[43] Joseph Jofish Kaye, Mary McCuistion, Rebecca Gulotta, and David A. Shamma. 2014. Money talks: tracking personal finances. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI '14)*. Association for Computing Machinery, New York, NY, USA, 521–530. https://doi.org/10.1145/2556288.2556975

[44] Kelly King, Christine E. Murray, Allison Crowe, Gwen Hunnicutt, Kristine Lundgren, and Loreen Olson. 2017. The Costs of Recovery: Intimate Partner Violence Survivors' Experiences of Financial Recovery From Abuse. *The Family Journal* 25, 3 (July 2017), 230–238. https://doi.org/10.1177/1066480717710656 Publisher: SAGE Publications Inc.

[45] Nikki Kiyimba and Michelle O'Reilly. 2016. The risk of secondary traumatic stress in the qualitative transcription process: a research note. *Qualitative Research* 16, 4 (Aug. 2016), 468–476. https://doi.org/10.1177/1468794115577013 Publisher: SAGE Publications.

[46] Bert-Jaap Koops, Ronald Leenes, Martin Meints, Nicole van der Meulen, and David-Olivier Jaquet-Chiffelle. 2009. A Typology of Identity-Related Crime. *Information, Communication & Society* 12, 1 (Feb. 2009), 1–24. https://doi.org/10.1080/13691180802158516 Publisher: Routledge _eprint: https://doi.org/10.1080/13691180802158516.

[47] Celine Latulipe, Ronnie Dsouza, and Murray Cumbers. 2022. 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)*. Association for Computing Machinery, New York, NY, USA, 1–13. https://doi.org/10.1145/

3491102.3501845
[48] Karen Levy and Bruce Schneier. 2020. Privacy Threats in Intimate Relationships. https://papers.ssrn.com/abstract=3620883
[49] Makayla Lewis and Mark Perry. 2019. Follow the Money: Managing Personal Finance Digitally. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems (CHI '19)*. Association for Computing Machinery, New York, NY, USA, 1–14. https://doi.org/10.1145/3290605.3300620
[50] Emily M. Lund. 2020. Interpersonal violence against people with disabilities: Additional concerns and considerations in the COVID-19 pandemic. *Rehabilitation Psychology* 65, 3 (2020), 199–205. https://doi.org/10.1037/rep0000347 Place: US Publisher: American Psychological Association.
[51] Tara Matthews, Kathleen O'Leary, Anna Turner, Manya Sleeper, Jill Palzkill Woelfer, Martin Shelton, Cori Manthorne, Elizabeth F. Churchill, and Sunny Consolvo. 2017. 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)*. Association for Computing Machinery, New York, NY, USA, 2189–2201. https://doi.org/10.1145/3025453.3025875
[52] Kath M. Melia. 1996. Rediscovering Glaser. *Qualitative Health Research* 6, 3 (Aug. 1996), 368–378. https://doi.org/10.1177/104973239600600305 Publisher: SAGE Publications Inc.
[53] Wendy Moncur. 2013. The Emotional Wellbeing of Researchers: Considerations for Practice. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI '13)*. ACM, New York, NY, USA, 1883–1890. https://doi.org/10.1145/2470654.2466248 event-place: Paris, France.
[54] Janice M. Morse, Barbara J. Bowers, Kathy Charmaz, Juliet Corbin, Adele E. Clarke, and Phyllis Noerager Stern. 2016. *Developing Grounded Theory: The Second Generation*. Routledge, London, UK. Google-Books-ID: jGyTDAAAQBAJ.
[55] Maryam Mustafa, Noor Mazhar, Ayesha Asghar, Maryem Zafar Usmani, Lubna Razaq, and Richard Anderson. 2019. Digital Financial Needs of Micro-entrepreneur Women in Pakistan: Is Mobile Money The Answer?. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems (CHI '19)*. Association for Computing Machinery, New York, NY, USA, 1–12. https://doi.org/10.1145/3290605.3300490
[56] Andy Myhill and Kelly Johnson. 2016. Police use of discretion in response to domestic violence. *Criminology & Criminal Justice* 16, 1 (Feb. 2016), 3–20. https://doi.org/10.1177/1748895815590202 Publisher: SAGE Publications.
[57] Arvind Narayanan and Kevin Lee. 2022. Security policy audits: why and how. https://doi.org/10.48550/arXiv.2207.11306 arXiv:2207.11306 [cs].
[58] National Network to End Domestic Violence. 2022. 10th Annual Technology Summit. https://nnedv.org/content/virtual-technology-summit-2022/
[59] Nicole Leeper Piquero, Alex R. Piquero, Stephen Gies, Brandn Green, Amanda Bobnis, and Eva Velasquez. 2021. Preventing Identity Theft: Perspectives on Technological Solutions from Industry Insiders. *Victims & Offenders* 16, 3 (April 2021), 444–463. https://doi.org/10.1080/15564886.2020.1826023
[60] Judy L. Postmus, Gretchen L. Hoge, Jan Breckenridge, Nicola Sharp-Jeffs, and Donna Chung. 2020. Economic Abuse as an Invisible Form of Domestic Violence: A Multicountry Review. *Trauma, Violence, & Abuse* 21, 2 (April 2020), 261–283. https://doi.org/10.1177/1524838018764160 Publisher: SAGE Publications.
[61] Anastasia Powell. 2021. 'Intimate Intrusions': Technology Facilitated Dating and Intimate Partner Violence. In *The Palgrave Handbook of Gendered Violence and Technology*, Anastasia Powell, Asher Flynn, and Lisa Sugiura (Eds.). Springer International Publishing, Cham, 157–179. https://doi.org/10.1007/978-3-030-83734-1_9
[62] Freya Probst, Hyosun Kwon, and Cees de Bont. 2021. Euros from the Heart: Exploring Digital Money Gifts in Intimate Relationships. In *HCI International 2021 - Late Breaking Papers: Design and User Experience (Lecture Notes in Computer Science)*, Constantine Stephanidis, Marcelo M. Soares, Elizabeth Rosenzweig, Aaron Marcus, Sakae Yamamoto, Hirohiko Mori, Pei-Luen Patrick Rau, Gabriele Meiselwitz, Xiaowen Fang, and Abbas Moallem (Eds.). Springer International Publishing, Cham, 342–356. https://doi.org/10.1007/978-3-030-90238-4_24
[63] Hawra Rabaan, Alyson L. Young, and Lynn Dombrowski. 2021. Daughters of men: Saudi women's sociotechnical agency practices in addressing domestic abuse. *Proceedings of the ACM on Human-Computer Interaction* 4, CSCW3 (2021), 1–31. Publisher: ACM New York, NY, USA.
[64] Maya I. Ragavan, Lauren Risser, Virginia Duplessis, Sarah DeGue, Andrés Villaveces, Tammy P. Hurley, Judy Chang, Elizabeth Miller, and Kimberly A. Randell. 2021. The Impact of the COVID-19 Pandemic on the Needs and Lived Experiences of Intimate Partner Violence Survivors in the United States: Advocate Perspectives. *Violence Against Women* December 3, 2021 (Dec. 2021), 10778012211054869. Issue 1. https://doi.org/10.1177/10778012211054869 Publisher: SAGE Publications Inc.
[65] Bradley Reaves, Jasmine Bowers, Nolen Scaife, Adam Bates, Arnav Bhartiya, Patrick Traynor, and Kevin R. B. Butler. 2017. Mo(bile) Money, Mo(bile) Problems: Analysis of Branchless Banking Applications. *ACM Transactions on Privacy and Security* 20, 3 (Aug. 2017), 11:1–11:31. https://doi.org/10.1145/3092368
[66] Phyllis Noerager Stern Example: P. N. Stern and J. Kerry: Restructuring 66. 2009. Glaserian Grounded Theory. In *Developing Grounded Theory*. Routledge, London, UK. Num Pages: 31.
[67] Elizabeth W. Sauber and Karen M. O'Brien. 2020. Multiple Losses: The Psychological and Economic Well-Being of Survivors of Intimate Partner Violence. *Journal of Interpersonal Violence* 35, 15-16 (Aug. 2020), 3054–3078. https://doi.org/10.1177/0886260517706760 Publisher: SAGE Publications Inc.
[68] Nicola Sharp-Jeffs. 2015. Money Matters : Research into the extent and nature of financial abuse within intimate relationships in the UK. http://repository.londonmet.ac.uk/1481/ Num Pages: 52 Place: London Publisher: London Metropolitan University.
[69] Nicola Sharp-Jeffs. 2021. Understanding the economics of abuse: an assessment of the economic abuse definition within the Domestic Abuse Bill. *Journal of Gender-Based Violence* 5, 1 (Feb. 2021), 163–173. https://doi.org/10.1332/239788220X16076181041680 Publisher: Policy Press Section: Journal of Gender-Based Violence.
[70] Julia Slupska and Angelika Strohmayer. 2022. Networks of Care: Tech Abuse Advocates' Digital Security Practices. In *Networks of Care: Tech Abuse Advocates' Digital Security Practices*. Advanced Computing Sytstems Association, Carlsbad, CA, USA, 341–358. https://www.usenix.org/conference/usenixsecurity22/presentation/slupska-networks
[71] Julia Slupska and Leonie Maria Tanczer. 2021. 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*. Emerald Publishing Limited, London, United Kingdom.
[72] Rachel Louise Louise Snyder. 2020. *No Visible Bruises* (reprint edition ed.). Bloomsbury Adult, New York, N.Y.
[73] Jocelyn Spence. 2019. Inalienability: Understanding Digital Gifts. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems - CHI '19*. ACM Press, Glasgow, Scotland Uk, 1–12. https://doi.org/10.1145/3290605.3300887
[74] Evan Stark. 2009. *Coercive Control: The Entrapment of Women in Personal Life*. Oxford University Press, Oxford, UK. Google-Books-ID: 8h0TDAAAQBAJ.
[75] Heather L. Storer, Maria Rodriguez, and Roxanne Franklin. 2021. "Leaving Was a Process, Not an Event": The Lived Experience of Dating and Domestic Violence in 140 Characters. *Journal of Interpersonal Violence* 36, 11-12 (June 2021), NP6553–NP6580. https://doi.org/10.1177/0886260518816325
[76] Yolande Strengers, Jathan Sadowski, Zhuying Li, Anna Shimshak, and Florian 'Floyd' Mueller. 2021. What Can HCI Learn from Sexual Consent? A Feminist Process of Embodied Consent for Interactions with Emerging Technologies. In *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems (CHI '21)*. Association for Computing Machinery, New York, NY, USA, 1–13. https://doi.org/10.1145/3411764.3445107
[77] Michael J. Strube and Linda S. Barbour. 1983. The decision to leave an abusive relationship: Economic dependence and psychological commitment. *Journal of Marriage and the Family* 45, 4 (1983), 785–793. https://doi.org/10.2307/351791 Place: US Publisher: National Council on Family Relations.
[78] Amanda Mathisen Stylianou, Judy L. Postmus, and Sarah McMahon. 2013. Measuring Abusive Behaviors: Is Economic Abuse a Unique Form of Abuse? *Journal of Interpersonal Violence* 28, 16 (Nov. 2013), 3186–3204. https://doi.org/10.1177/0886260513496904 Publisher: SAGE Publications Inc.
[79] Surviving Economic Abuse. 2021. Conversation Kits for Banks. https://survivingeconomicabuse.org/wp-content/uploads/2021/01/Conversation-kit-for-banks-v7-KB.pdf
[80] Kurt Thomas, Patrick Gage Kelley, Sunny Consolvo, Patrawat Samermit, and Elie Bursztein. 2022. "It's common and a part of being a content creator": Understanding How Creators Experience and Cope with Hate and Harassment Online. In *Proceedings of the 2022 CHI Conference on Human Factors in Computing Systems (CHI '22)*. Association for Computing Machinery, New York, NY, USA, 1–15. https://doi.org/10.1145/3491102.3501879
[81] National Network to End Domestic Violence. 2019. Financial Abuse and Empowerment. https://nnedv.org/spotlight_on/financial-abuse-empowerment/
[82] Emily Tseng, Rosanna Bellini, Nora McDonald, Matan Danos, Rachel Greenstadt, Damon McCoy, Nicola Dell, and Thomas Ristenpart. 2020. 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)*. USENIX Association, USA, 1893–1909.
[83] Emily Tseng, Diana Freed, Kristen Engel, Thomas Ristenpart, and Nicola Dell. 2021. A Digital Safety Dilemma: Analysis of Computer-Mediated Computer Security Interventions for Intimate Partner Violence During COVID-19. In *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems (CHI '21)*. Association for Computing Machinery, New York, NY, USA, 1–17. https://doi.org/10.1145/3411764.3445589
[84] Emily Tseng, Mehrnaz Sabet, Rosanna Bellini, Harkiran Kaur Sodhi, Thomas Ristenpart, and Nicola Dell. 2022. Care Infrastructures for Digital Security in Intimate Partner Violence. In *Proceedings of the 2022 CHI Conference on Human Factors in Computing Systems (CHI '22)*. Association for Computing Machinery, New York, NY, USA, 1–20. https://doi.org/10.1145/3491102.3502038
[85] John Vines, Paul Dunphy, Mark Blythe, Stephen Lindsay, Andrew Monk, and Patrick Olivier. 2012. The joy of cheques: trust, paper and eighty somethings. In *Proceedings of the ACM 2012 conference on Computer Supported Cooperative Work (CSCW '12)*. Association for Computing Machinery, New York, NY, USA,

147–156. https://doi.org/10.1145/2145204.2145229

[86] Dhaval Vyas, Stephen Snow, Paul Roe, and Margot Brereton. 2016. Social Organization of Household Finance: Understanding Artful Financial Systems in the Home. In *Proceedings of the 19th ACM Conference on Computer-Supported Cooperative Work & Social Computing (CSCW '16)*. Association for Computing Machinery, New York, NY, USA, 1777–1789. https://doi.org/10.1145/2818048.2819937

[87] WenJie Wang, Yufei Yuan, and N. Archer. 2006. A contextual framework for combating identity theft. *IEEE Security & Privacy* 4, 2 (March 2006), 30–38. https://doi.org/10.1109/MSP.2006.31 Conference Name: IEEE Security & Privacy.

[88] Miranda Wei, Eric Zeng, Tadayoshi Kohno, and Franziska Roesner. 2022. 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)*. USENIX Association, Boston, MA, USA, 447–462. https://www.usenix.org/conference/soups2022/presentation/wei

[89] Nicole Westmarland and Hannah Bows. 2018. *Researching Gender, Violence and Abuse: Theory, Methods, Action*. Routledge, London, England, UK. Google-Books-ID: YDZ7DwAAQBAJ.

[90] Leila Wood, Elizabeth Baumler, Rachel Voth Schrag, Shannon Guillot-Wright, Dixie Hairston, Jeff Temple, and Elizabeth Torres. 2022. "Don't Know where to Go for Help": Safety and Economic Needs among Violence Survivors during the COVID-19 Pandemic. *Journal of Family Violence* 37, 6 (Aug. 2022), 959–967. https://doi.org/10.1007/s10896-020-00240-7

[91] Delanie Woodlock. 2017. The Abuse of Technology in Domestic Violence and Stalking. *Violence Against Women* 23, 5 (April 2017), 584–602. https://doi.org/10.1177/1077801216646277 Publisher: SAGE Publications Inc.

[92] Delanie Woodlock, Karen Bentley, Darcee Schulze, Natasha Mahoney, Donna Chung, and Amy Pracillo. 2020. *Second National Survey of Technology Abuse and Domestic Violence in Australia*. Technical Report 2. University of New England, Australia, Australia. 1–72 pages. https://wesnet.org.au/wp-content/uploads/sites/3/2020/11/Wesnet-2020-2nd-National-Survey-Report-72pp-A4-FINAL.pdf

[93] World Health Organization. 2005. *Researching violence against women : practical guidelines for researchers and activists*. Technical Report. World Health Organization. https://apps.who.int/iris/handle/10665/42966 ISBN: 9789241546478 number-of-pages: 257.

[94] Yixin Zou, Allison McDonald, Julia Narakornpichit, Nicola Dell, Thomas Ristenpart, Kevin Roundy, Florian Schaub, and Acar Tamersoy. 2021. The Role of Computer Security Customer Support in Helping Survivors of Intimate Partner Violence. In *Proceedings of the 30th USENIX Conference on Security Symposium* (Virtual). USENIX Association, Virtual, 429–446. https://www.usenix.org/conference/usenixsecurity21/presentation/zou

[95] Yixin Zou, Abraham H. Mhaidli, Austin McCall, and Florian Schaub. 2018. "I've Got Nothing to Lose": Consumers' Risk Perceptions and Protective Actions after the Equifax Data Breach. In *SOUPS '18: Proceedings of the Fourteenth USENIX Conference on Usable Privacy and Security*. USENIX Association, Baltimore MD USA, 197–216. https://www.usenix.org/conference/soups2018/presentation/zou

[96] Douglas Zytko, Nicholas Furlo, Bailey Carlin, and Matthew Archer. 2021. Computer-Mediated Consent to Sex: The Context of Tinder. *Proceedings of the ACM on Human-Computer Interaction* 5, CSCW1 (April 2021), 189:1–189:26. https://doi.org/10.1145/3449288

A APPENDIX

A.1 Keywords

Type	Keywords
Actions	Finance, Budget, Retir* [e, ing, ment, ment plan], Purchase* [s], Buy^, Save^, Sell^, Steal^
Institutions	Bank, Business, IRS
Products	[Home, car, life] Insurance, Mortgage, Loan* [s], Invest* [ing, ment, ments] [s], Fund* [s], "[Joint, Checking] Account", Saving* [s, s Account], Debt* [s]
Security	PIN* [code, number], SSN, Social Security* [Number]
Item	Cash, Money, Dollar* [s], Purse, Wallet, Credit, Debit, Receipt*, [Debit, Credit] Card
Brand	Paypal, Venmo, "Cash App"

Table 2: List of keywords used to search client case notes