Shortchanged: Uncovering and Analyzing Intimate Partner Financial Abuse in Consumer Complaints

Arkaprabha Bhattacharya
JPMorgan Chase
New York, NY, USA

Kevin Lee
JPMorgan Chase
New York, NY, USA

Vineeth Ravi
JPMorgan Chase
New York, NY, USA

Jessica Staddon
JPMorgan Chase
Palo Alto, CA, USA

Rosanna Bellini
Cornell University
New York, NY, USA

ABSTRACT

Digital financial services can introduce new digital-safety risks for users, particularly survivors of intimate partner financial abuse (IPFA). To offer improved support for such users, a comprehensive understanding of their support needs and the barriers they face to redress by financial institutions is essential. Drawing from a dataset of 2.7 million customer complaints, we implement a bespoke workflow that utilizes language-modeling techniques and expert human review to identify complaints describing IPFA. Our mixed-method analysis provides insight into the most common digital financial products involved in these attacks, and the barriers consumers report encountering when doing so. Our contributions are twofold; we offer the first human-labeled dataset for this overlooked harm and provide practical implications for technical practice, research, and design for better supporting and protecting survivors of IPFA.

CCS CONCEPTS

• **Human-centered computing** → **Empirical studies in HCI**; • **Computing methodologies** → *Information extraction*; • **Security and privacy** → **Social aspects of security and privacy**.

KEYWORDS

financial abuse, intimate partner violence, technology-enabled abuse

1 INTRODUCTION

Financial abuse — the control of access to, and maintenance of, financial resources [90] — is a devastating form of intimate partner violence (IPV) that severely impacts the mental, physical, and spiritual wellbeing of those targeted. Such individuals are marginalized, highly vulnerable [80, 81, 90], and subject to substantive digital-safety risks from a targeted adversary [107]. An abuser may know confidential information about a survivor and possess complex social goals that go beyond financial gain. In these contexts, consumer-facing banking applications can facilitate the surveillance of a complainant's expenditure through online interfaces [14] or monitoring alerts [36], while coercive uses of authorized user status can enable an abuser to fraudulently make purchases or coerced debt [13].

Digital financial products and services can exacerbate existing harms [13, 14, 36], since they are rarely designed with digital-safety concerns in mind. While consumer-facing technologies play a growing role in these contexts [13, 36], identifying attacks is nevertheless fraught with difficulties [103]. Many technology-enabled attacks are reported retroactively, often requiring survivors to make inferences around how an attack was conducted or the vulnerabilities that made them possible [44]. It is also extremely difficult to reach survivors of financial abuse due to their marginalized and vulnerable status, necessitating extensive care and attention in research endeavors [104].

Financial institutions, including banks, credit bureaus, and insurance companies, have been recognized as crucial safeguarding environments for the financial well-being of survivors [9, 26, 89]. However, to do so, such institutions need to be equipped with an awareness of the challenges a survivor may face — particularly as more survivors may reach out to such organizations for complaints about consumer-facing products [113]. While prior work has described the attacks experienced by complainants currently receiving support via IPV services [43, 109], and how abusers may craft such attacks online [15, 102], we present a detailed view of how these concerns about digital products may be presented to financial institutions firsthand. This study examines how consumer-authored narratives on intimate partner-perpetrated financial abuse can provide insights into:

RQ1: How might computational text analysis help to identify financial abuse between intimate partners in online consumer complaints?

RQ2: Which digital consumer-facing financial products and technology-enabled financial attacks are prominently represented in such complaints?

RQ3: What barriers to service do consumers report encountering when attempting to resolve concerns around technology-enabled financial abuse?

We collaborated with industry and academic experts on IPV and customer safety to create a tailored workflow for collecting relevant complaints. Our workflow combines pre-trained language models with careful human review to identify instances of financial abuse in text-based consumer complaints. Using the vast Consumer Financial Protection Bureau (CFPB) Consumer Complaint Database — totaling over 2.7 million entries — and our workflow, we generated a specialized dataset of 513 consumer accounts reporting financial abuse to financial institutions. Utilizing Framework Analysis [85] and Critical Discourse Analysis [17, 37, 64], we characterize when survivors reach out to the CFPB for help, which digital products they cite as a cause for concern, what barriers they encounter while doing so, and how much they report losing financially. Their path through the complaint process at the financial institution is lengthy and complex, with reported challenges in policy design, the need for digital evidence collection, and considerable digital-safety risks.

Our findings offer insight into how to improve the safety of digital financial products for survivors of financial abuse. To mitigate financial attacks, we offer suggestions for how to implement safety checkups and regular system audits in financial products as promising strategies in this area. Our work also highlights the importance of considering new approaches to evidence gathering and reporting approaches when reaching out to institutions for help, and better align with the needs of vulnerable customers. We conclude by highlighting new research directions in technology-enabled financial abuse that are especially poignant in light of the growing adoption of digital financial products.

2 BACKGROUND AND RELATED WORK

In this study, our focus is on targeted digital financial attacks in situations involving intimate partner violence. These attacks, carried out by an abuser, can result in the loss of wealth, property, or other financial benefits for a survivor [90, 98], for a range of social, or financial motives [13, 44]. We refer to these actions as *intimate partner financial abuse* (IPFA), which may also branch into elder financial abuse [40, 65] if involving older adults (see Appendix A for differentiation). To align with current best practice, we employ the term *survivor* to honor an individual's strength and resilience in the face of adversity, and use *abuser* to identify the direction of abuse [43, 44, 100].

Digital technologies play a substantive role in enabling abusers to coerce, control, harass and otherwise harm their current or former intimate survivors. Recent work has shown that these actions extend to financial and economic sectors, from surveillance of financial expenditure [25, 102], to permitting unauthorized entry into smartphone applications [14], to harassing messages sent in payment memos [36]. In their in-depth review of survivor accounts of tech-enabled abuse, Bellini [13] identified a range of technical attacks across a variety of technical products, including credit accounts, shared banking infrastructures, and online businesses. Thus, abusers defy the conventional threat models of consumer technologies by exerting physical control over a survivor's devices and exploiting use of private financial information. While some scholars have identified that flexible, proportionate, and consentful design could mitigate certain negative effects of some consumer technologies [9], these designs are unfortunately still in their early

stages and not widely embraced by mainstream services. Additionally, there is insufficient knowledge about which financial products or features are prone to targeting [13, 14], hindering the ability for financial service providers to make impactful changes for users.

Many human-computer interaction (HCI) and computer security researchers have investigated interventions that work to support survivors of technology-facilitated abuse. Approaches to clinical computer security that pair survivors with privacy and security experts have shown promise in protecting survivors' devices and preventing their digital footprints from being targeted [41, 56]. In such technology clinics, experts are able to provide in-depth insight into the types of digital technologies that incur unique risks to survivors [104], while also helping to professionalize such services. Zou et al. [113] also provide a welcome focus on customer support agents at computer security companies who may provide assistance to survivors during or in the immediate aftermath of a technical attack. There remains a paucity of research on how survivors of technology abuse, particularly in financial contexts, may reach out in ways beyond expected customer service channels [113], or direct referrals to specialized technology services [41, 56, 104]. This is in spite of the increasing recognition that financial institutions and similar organizations can serve as powerful social and political influencers due to their close connections with customers [9, 19, 61, 79, 89]. Thus, obtaining deeper insights into technology-enabled financial abuse could offer significant ways forward for intervention and technical implementation for financial institutions and designers [19, 60, 89].

Obtaining such first-hand insights into the financial actions of vulnerable service users to inform our gaps in knowledge about IPFA and digital systems is, understandably, challenging. For many consumers, the mere discussion of finances can be culturally taboo [10]; out of fear of manipulation by others [2], or by experiencing embarrassment or shame [106]. Financial institutions also go to great lengths to maintain customer confidentiality about information relating to their finances to both prevent fraud and protect against the disclosure of proprietary information.

Deep learning and natural language processing have been used to parse and analyze large datasets, which have enabled the inference of otherwise inaccessible characteristics [4, 83, 87]. Scholars have leveraged these approaches to elicit risk factors to vulnerable groups, contextualize taboo topic areas (e.g., end-of-life [111], climate change [38]), and identify under-recognized forms of sociotechnical harms [2, 53]. In the context of abuse and hate, Bidirectional Encoder Representations from Transformers (BERT)-based transformer models have been deployed to detect hate speech online [63, 110], identify descriptions of abuse in patient records [18], and detect abusive transactions [66]. However, at the time of writing, we have yet to locate research that has grappled with the challenges of applying such approaches to better contextualize technology-enabled abuse for survivors of IPFA.

3 STUDY AND WORKFLOW DESIGN

Technology-enabled financial abuse by intimate partners is an emergent area of research [13, 14, 36], involving the identification of subtle and complex factors that even human agents may struggle to

identify. While many HCI works have shown that machine learning may hold many benefits in addressing under-explored problem spaces, we acknowledge it *"has no clairvoyant abilities"* [7], thus requiring careful reasoning about data, workflow, and derived conclusions to resist negative knock-on-effects [23, 24, 68, 86]. We aim to address this challenge head-on through our exploration of **RQ1** by our study design, which involves synthesizing natural language processing with careful manual review with experts; a technique that has seen promise in other areas [54, 75, 82].

In this section, we describe our *study context*, and our approach to *data collection and cleaning*. We then describe the *workflow to identify IPFA complaints*, accompanied by an *assessment of its effectiveness* through techniques designed for explaining machine learning model decisions. We follow up to this with an overview of our dataset and analysis, before concluding with a reflection on *ethical considerations*.

Study context: public consumer complaints. We investigate IPFA in the context of unstructured complaints written by consumers and submitted to the Consumer Financial Protection Bureau (CFPB), a United States (U.S.) government agency responsible for consumer protection in the financial sector. Since the CFPB's inception in 2011 through the Dodd-Frank Act[1], the U.S. Congress has directed the bureau to collect and monitor complaints from consumers about financial products and services from over 6,100 financial companies in order to promote transparency and fairness for consumer-facing financial products and services (e.g., credit reporting and mortgage lending).[2]

The CFPB handles its primary duty to collect, investigate, and resolve consumer complaints via a toll-free hotline or through a secure online portal for companies. Consumers may submit complaints to the CFPB, either before or after contacting their financial institution(s), which includes financial service providers and credit bureaus. If a consumer disagrees with the financial institution's resolution to their concern, they can file a complaint with the CFPB. Complaints include free-text narratives (subject to a 10,000 character limit) and can categorize their concerns via selections from pre-populated menus. The CFPB forwards verified complaints to financial organizations, which must then respond per service level agreements and legal guidance [39].

Over 50% of complainants consent to making their complaint publicly available once personally identifiable information has been redacted [21]. The CFPB publishes over 10,000 complaints monthly that have undergone redaction [26]. Complaints in this dataset have been the center of past analyses, showcasing complaint trends, regional submissions, company response rates, and latent topics [8, 11], thus indicating the value of this source for understanding financial abuse.

Survivors' complaints about specific financial products with respect to privacy, security, and safety concerns, are generally inaccessible for external research purposes because they often require access to proprietary or sensitive information. Alternatively, existing studies that elicit such findings are performed after a survivor has received services — such as Bellini's [13] retroactive case study review of service users, which does not cover all survivors [90]. Our distinctive approach — that focuses on survivors as *consumers* thus entitled to consumer rights — affords us the opportunity to harness real-world data and scrutinize emerging trends and critical issues. Further, this approach hopes to enhance the existing body of knowledge in HCI on technology-enabled abuse [15, 43, 44] by concentrating on grievances specifically related to the digital financial products and services implicated by IPFA.

Data collection and cleaning. We downloaded a working dataset of 2,760,540 complaints (2.2 GB) from the CFPB website in June 2022. Each complaint is represented as a data entry of 18 data fields, including complaint date, product description, customer narratives, and company (Table 6, Appendix C). Our analysis is centered on the customer complaint narratives (CCNs), which are customer-authored free-form text without character limits. Complaints with CCNs averaged 1,043 words, with significant variability (SD 1,276 characters; Figure 8, Appendix C).

To focus on consumer-identified financial abuse complaints, we excluded 1,786,680 complaints without a CCN. We then identified and removed same-day, same-time duplicates (indicative of a technical error), while retaining duplicates that we judged to be customer-authored resubmissions (i.e., complaints of identical content sent to different financial institutions) As such, our total dataset contains 973,860 complaints. All tokenization, cleaning, and keyword searches in our workflow were performed with the use of the spacy library (version numbers for all tools are in Table 7, Appendix D). As we are unable to establish ground truth in the authorship of each complaint, we refer to the user who wrote the complaint as the *complainant*, and retain the terminology of abuser.

Survivors of financial abuse in IPV contexts are doubly marginalized; given that money is often a highly taboo discussion topic, and survivors face substantial stigmatization from wider society [107]. While survivors may feel empowered by sharing personal stories [103], it may also exhaust an individual already suffering from significant trauma, resulting in additional responsibility on them to share their experiences [13]. We are aware that despite our study motivation to reduce harm to at-risk groups, we did not directly engage survivors of financial abuse to share their personal stories which poses an ethical tension [16]. After speaking to several experts on both IPV and financial abuse, we were cautious to not directly engage survivors before we learned more about this area [16]. We plan to use the insights gained from this work to design a future study that engages with survivors directly.

IPFA identification workflow. To identify this subtle form of financial harm in consumer accounts [13, 14], and help to provide answers to **RQ1**, we designed a five-step (①—⑤) iterative workflow that synthesizes manual human expert review, natural language processing, and information retrieval techniques (Figure 1). First, we carefully designed our query for IPFA cases involving technology abuse ① via a range of different keywords from prior literature [13, 81, 90] to produce two lists of English-language keywords associated with intimate partners (*intimate partner keywords*)

---

[1]12 U.S. Code § 5491 - Establishment of the Bureau of Consumer Financial Protection
[2]CFPB supervisory powers cover banks, thrifts, and credit unions with assets over $10 billion, along with non-bank mortgage originators, payday lenders, and private student lenders. Recently, these powers expanded to include consumer reporting, student loan servicing, international money transfer, automobile finances, and consumer debt collection.
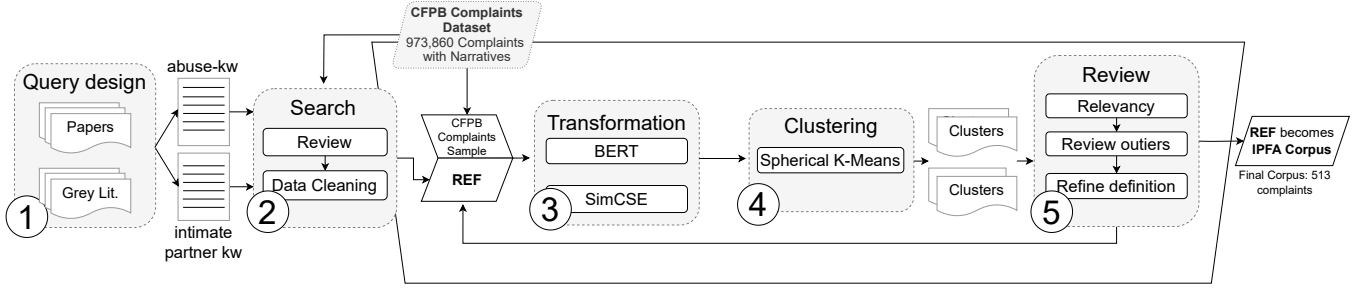
Figure 1: The IPFA complaint collection workflow involves a reference set (*ref*) of known IPFA examples and unlabelled CFPB complaints containing an intimate partner keyword. Text embeddings are created using a sentence transformer model, and these embeddings are then clustered. The clusters with the most reference set complaints are manually reviewed to identify additional IPFA examples, which are then added to the reference set. This process is iterated with new IP complaints. When the desired iterations are complete, *ref* becomes the final collected dataset.

and financial abuse (*financial abuse keywords*) (Appendix B). To evaluate the performance of using *intimate partner keywords* for identifying complaints mentioning intimate partners, two authors independently reviewed a sample of 100 CCNs that were flagged if a keyword from *intimate partner keywords* was present, to confirm if a flagged complaint mentioned an intimate partner. Both reviewers were able to resolve all disagreements, yielding a precision of 0.95 and recall of 0.93 for this set of keywords. We observed in a small sample of IPFA-relevant complaints (identified by random selection and manual review) that an abuse keyword often appeared in close proximity to a mention of an intimate partner. Using this finding, we then enacted a keyword search ② by searching all 973,860 complaints for cases containing at least one phrase from *intimate partner keywords* and at least one phrase from *financial abuse keywords* within a 10-word proximity to each other. We refer to this process as *keyword matching with proximity*, which resulted in 1,179 matches. To further verify the matched complaints and remove matches that did not pertain to IPFA, two human labellers reviewed the complaints to identify relevance, resulting in an initial reference set (*ref*) of 288 complaints.

We used text embeddings (③) — text represented as numerical vectors such that semantically similar text results in vectors that are nearby in the embedding space — to represent the identified IPFA complaints from ① (*ref*) and a sample of new complaint narratives from the original dataset. We instantiated these text embeddings from sentence transformer models, *bert-large-nli-stsb-mean-tokens* and *sup-simcse-roberta-base* [50, 84]. The models themselves were instantiated with the `sentence-transformers` and `simcse` libraries.

Once embeddings of a sample of new complaint narratives and *ref* were generated (③), they were clustered using *k*-means clustering ④, with the goal of grouping complaints that had semantically similar CCNs. We used the `sklearn` library's *k*-means algorithm to perform this. Upon first attempt, we discovered that outlier-sensitive clustering algorithms, such as HDBScan [71], tended to exclude a large proportion of complaint embeddings from clusters due to the high dimensionality of the vectors and semantic complexity of complaints. We thus relied on *k*-means clustering, a process which assigns complaints to the same cluster if they are close (by

distance metric) to a common cluster center [88]. The clusters containing the most complaints from the current reference set *ref* were then reviewed via their relative yield. For example, in one iteration, we proceeded with the top cluster (*Cluster-6*) which contained 49% of our *ref* complaints (Figure 3c), and cross-compared this with the second and third highest (22% in *Cluster-7* and 13% in *Cluster-3*).

These clusters were then sampled for complaints, and were manually reviewed for IPFA relevance (⑤) by five co-authors of this work, all with experience of IPV or at-risk populations in security contexts (see *Ethical Considerations*). Each researcher received 300 sampled complaints per round across eight rounds (2,400 complaints/researcher total), and each complaint had two researchers for determining relevance. Complaints that no researcher marked as relevant were removed, and disputes were then reviewed by the group. Determining relevance for reviewed complaints was challenging because of the need to understand IPFA's impact on the complainant and offender, as well to distinguish it from fraud and harassment (Appendix A).

We augmented *ref* with the reviewed complaints confirmed relevant and repeated the workflow (③–⑤). After six iterations, this resulted in a final set of *n* = 513 relevant complaints.

Workflow evaluation. Out of 513 IPFA complaints, 221 did not meet the keyword matching with proximity criteria (①), and 169 did not satisfy keyword matching without proximity. This suggests that our workflow augmented the initial reference set, resulting in a 43% increase in corpus size from ②. Our workflow did prove to require substantive time and effort on behalf of both expert and researcher reviewers, thus we look to supplement this method via other approaches to elevate this burden in future work (Section 5).

During the workflow, SHapley Additive exPlanations (SHAP) scores — a model feature explanation technique that reveals words or phrases that impact text classification — helped identify words influencing a complaint's cluster assignment. We calculated SHAP scores for *Cluster-6* (mentioned in ④) using a random forest classifier trained on *ref* (with the `sklearn` and `shap` libraries). Term Frequency - Inverse Document Frequency (TF-IDF) vectors of each complaint were input to this classifier, with the complaint's cluster assignment as its classification. Words like 'our,' 'we,' and 'us' negatively affected a complaint's classification in the target cluster.
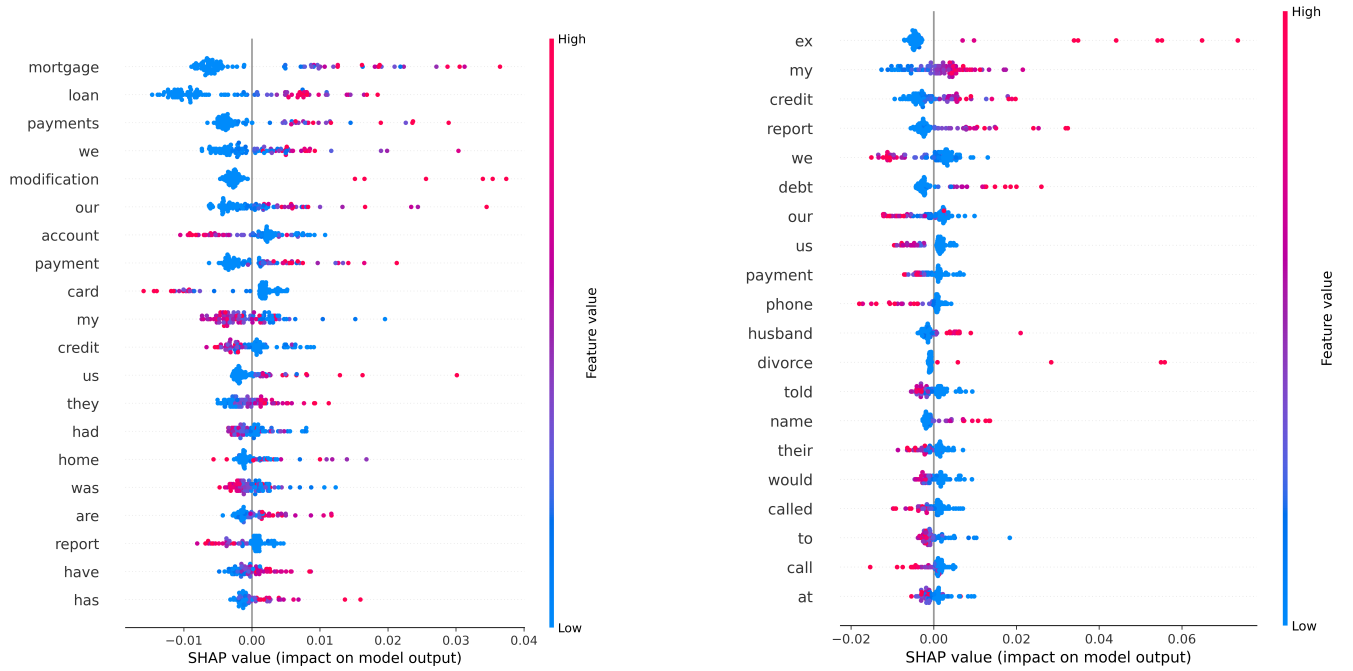
Figure 2: SHAP scores for K-Clusters 1 [Left], and 6 [Right]. The color bar corresponds to the raw values of the variables for each instance. If the variable for a particular word is high, it appears as a red dot, while low variable values appear as blue. Figure 7 in Appendix C shows SHAP scores for all clusters.

When complaints mentioned these words, it could indicate either that the complaint does not meet the definition of IPFA, or, it involves complex IPFA not easily identified due to shared financial harm. The results suggest that our workflow can distinguish how complainants describe harm, which is crucial for identifying IPFA.

The 513 complaints produced with this workflow represent a sample of possible IPFA within the CFPB dataset. Given the reliance on keywords in creating our reference set ((1)) and on our existing understanding of forms of financial abuse in manually reviewing clusters ((5)), we emphasize that this dataset and methodology are not intended as a means of finding a sample of complaints that represent the entire space of how IPFA is described in complaints. Rather, it represents a focused dataset that can be further analyzed to inform future study exploring this larger space.

Dataset and Framework Analysis. Following a manual review, a single author identified and removed a total of 49 complaints (2 duplicates, 47 re-submissions), associated with 37 unique identifiers. This resulted in a dataset of 464 narratives for further analysis. Our complaints span from 2015 — 2022, with the highest number submitted in 2020 (103), while the highest number of total complaints submitted to CFPB was in 2021 (Figure 3b) [26]. Most complaints in the corpus were short, containing 1K words or less (M:283.5, SD:333.8, Figure 3a), slightly longer than the average complaint length within the larger CFPB dataset (M:213.74, SD:259.06). Our shortest complaint contained a mere 15 words (*"My former spouse unlawfully used my personal information to create an account with [institution]"*) (C327), and the longest contained 4,863 words.

In our analysis of our final dataset of 464 complaints, we used a deductive approach of framework analysis [12] which is adaptable for specific questions [47], limited timeframes [62], pre-designed samples (e.g., customers of financial services) [34], and addressing a priori issues [48]. In framework analysis, data is sifted, charted, and sorted in accordance with key issues and themes through familiarization, identification of a thematic framework, indexing, charting, mapping, and interpretation. This method is optimal for datasets with a structured schema, like CFPB data categories, helping us summarize a complex dataset to answer our research questions.

To create an analytical *"structure for guiding research"* [35], we used deductive reasoning to identify four essential components for indexing the narratives to differentiate an IPFA case from other financial harms. These components included: complainant identity, relationship status, financial product or service, and types of financial abuse reported by the complainant (Table 8, Appendix E). For financial product or services, we obtained an initial list from the CFPB website that consists of a range of products that the consumer can identify in the metadata of the complaint.[3] To analyze the type of abuse, we relied on established taxonomies on technology abuse [43], surveillance [102], technology-enabled financial abuse [13], and economic abuse[20] as a set of starting labels for developing our written descriptions. By doing so, we were able to easily pinpoint instances of new types of technology-enabled abuse (discussed in Section 4.1). Following a close reading of a subset of complaints (*n* = 100), the research team regathered to determine how such abuse were discovered, the reported impact of such abuse, and what

---

[3]The Consumer Complaint Database lists 74 sub-products.

(a) The frequency distribution of complaint lengths (by number of tokens).

(b) The frequency distribution of the number of complaints submitted per year (2015–2022).

(c) The distribution of *ref* across clusters; where Clusters -3, -6, and -7 would be selected for review.
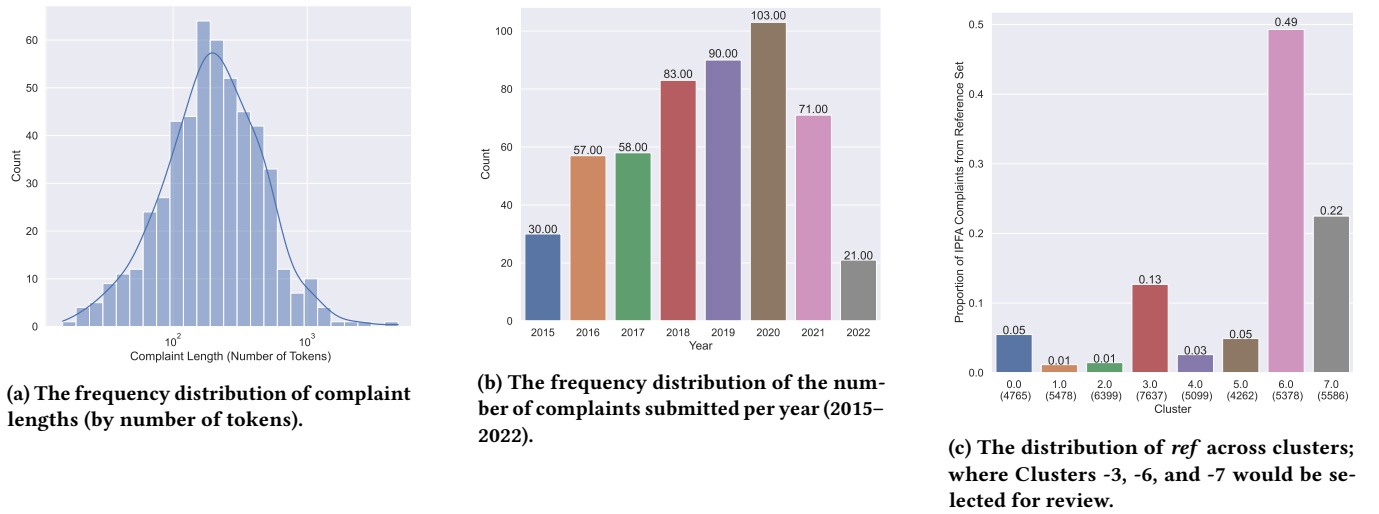
Figure 3: The graphs from our meta-data analysis: the complaint length, distribution over years, and identification of higher *ref* cases in clusters.

attempts (if any) that complainants made to resolve these concerns, were also poignant to capture.

Five coders (all co-authors) independently assessed and indexed data from these eight categories from each IPFA-related CCN in our dataset in three primary coding rounds over four weeks. First, each coder coded 20 cases each for consistency. Inter-rater reliability was calculated, showing near-perfect agreement (Fleiss's κ: Product 0.91, Abuse 0.92, Discovery 0.52, Resolution 0.91) [70]. Discrepancies in how abuse was discovered ("Discovery") were resolved in round two (0.84). Due to such a high inter-rater reliability, the remaining 444 CCNs were coded by a single researcher followed by a final consistency check. We then investigated how these variables intersected, by charting and interpreting any patterns or connections between categories via qualitative analysis software Atlas.ti to gain a clearer understanding and explanation of the 'bigger picture' [22].[4] Using a bespoke charting and summarization matrix (see [47, 62]), two authors identified higher level categories and typologies, which are presented in our findings (Section 4).

Critical Discourse Analysis. Understanding how survivors communicate about abuse is crucial for aiding survivors, as marginalized groups often avoid labeling their experiences [6]. To answer our RQs, we had to dig deeper than merely reporting the descriptions complainants shared.

Critical Discourse Analysis focuses on how texts aim to persuade or convey meaning beyond the obvious to a human reader[85], and we applied this approach to survivor's experiences of financial abuse, its consequences, and areas for financial service provider intervention. Thus, we applied Critical Discourse Analysis to scrutinize how complainants used language to convey what the financial

abuse meant to them, and how they chose to communicate it. For instance, in our analysis, we would frequently read how complainants were distressed at feeling *"unable to access finances"* or *"having their finances controlled"* by an intimate partner, but did not report such behaviors as explicitly abusive.

To do this, two authors performed a close reading of each narrative, asking about intended meanings and significance. This was done using the indexed framework analysis version of the dataset so relevant data could be easily located. Two authors also made note of what elements were noticeably absent from the narrative and how complainants attempted to appeal to the emotional sensitivities of the reader. Alongside identifying features, thematic elements and discursive fragments were also tagged and reviewed in a separate logging tool akin to analytical memoing. To consolidate all these memos together, we used Atlas.ti for a second time to map a cohesive narrative across all these memos until we were satisfied we had captured all linguistic nuances of the narratives. Framework Analysis and Critical Discourse Analysis are complementary [12], with Framework Analysis being epistemologically neutral [22], while Critical Discourse Analysis has been shown to surface underlying power relationships (a vital component of many IPV-related research projects) [55, 105].

Ethical considerations. As a cross academia-industry team, we obtained approval from our Institutional Review Board and internal legal group before starting this work. Like other HCI scholars before us, we were cognizant that the use of public data incurs unique ethical concerns (e.g., de-anonymization, adversarial learning, and misrepresentation [16, 24]), particularly for the discussion of at-risk groups and sensitive topics [107]. We thus took steps to protect the digital safety of both the complainants and the research team.

The CFPB data we used is publicly accessible for research purposes, and may be downloaded without user registration on the CFPB website. We chose to exclusively work with complaint data

---

[4]ATLAS.ti is a computer-assisted qualitative data analysis software that facilitates analysis of qualitative data for qualitative research, quantitative research, and mixed methods research, https://atlasti.com/.

I opened a <u>credit card</u> with <u>my bank</u> for rewards with an <u>online retailer</u>. My <u>ex-girlfriend</u> stole and used my card without permission and <u>then owned up to using it once I found hidden charges</u> ... I initially agreed to let my <u>ex-girlfriend</u> pay off the charges over time ... Later, I discovered that she had recorded my credit information and used it online without my knowledge ... I contacted my credit card company to report the fraudulent charges. Initially, they assured me that I was not liable for the charges and began the refund process. However, later on an investigator from <u>the bank</u> reversed this decision, claiming that the <u>ex-girlfriend</u> living in the same household <u>made me responsible for the charges</u>. This resulted in a <u>significant balance</u> on the <u>credit card</u> and my <u>credit company</u> reported a huge <u>negative impact to my credit score</u> as a result ... <u>I felt victimized</u> by both my <u>ex-girlfriend</u>'s actions and the actions of <u>my bank</u>.

Figure 4: Example, paraphrased complaint (C5) with indicators for the framework creation. Our analytical framework is built from identifying the <u>abuser</u>, <u>financial product</u>, <u>actors</u>, <u>attacks</u>, <u>point of discovery</u>, <u>steps toward resolution</u>, and <u>negative impact</u> on the complaint.

that was already redacted by the CFPB [26]. To ensure low risk of re-identification, each complaint was also manually checked for any uniquely identifiable details.

We made a conscious effort to avoid any bias towards complaints from a particular time period, considering the entire history of the complaints database.

We analyzed a one-year-old snapshot of the database (June 2022), which may allow complainants — including from the newest narratives — to have a greater chance to seek out safety resources. No effort was made to identify original posters. We made no attempt to attribute complaints with their original identifiers, and have abridged prominent quotes to remove a few idiosyncratic details, phrases, or terms while retaining the meaning of the data to prevent reverse search-engine lookup. Our approach involved human review and labeling by our research team, which built in discussions on distressing complaints during weekly meetings. Each team member has extensive experience on researching the digital-safety concerns of at-risk populations. Three team members have a professional background in personally supporting and overseeing the voluntary service provision for survivors of IPV in security contexts. Thus, each researcher has a self-care strategy that mitigate the impacts of vicarious trauma [73].

All work was conducted in secure, access-controlled cloud environments that were accessible to core research team members. Finally, we also engaged two security professionals external to the research team to review our work for the potential to teach adversaries new strategies or techniques to exacerbate their abuse. Both experts judged that this work did not contain novel techniques viable for adversarial feedback.

4 FINDINGS

In this section, we report the findings from two qualitative approaches (Framework Analysis, Critical Discourse Analysis), starting with an analysis of the profile of consumers who reach out to financial institutions with reports of technology-enabled financial abuse. We then attempt to answer what attacks and devices are implicated **RQ2** (Section 4.1) and what barriers survivors encounter while doing so **RQ3** (Section 4.2). Device and attack counts are provided for reference purposes, but should not be read as proportional attacks. Each example complaint has been lightly abridged and assigned an anonymous identifier (C1—C464). We report on the proportion of descriptive codes used to characterize our dataset

through percentages, as these codes were only used once per narrative and were mutually exclusive.

Complainant and abuser profiles. Our corpus gave us insight into the relationship between an abuser and complainant, their living situation, their roles in a family unit, and, the level of support the complainant was able to receive from financial institutions (Table 1). A small number of complainants reported more than one abuser, individuals often who were able to exploit their close physical and emotional relationships with the complainant, including extended family members, close friends, and business associates. While we cannot claim that pronoun identification is an effective method to determine gender, we can highlight that, akin to other HCI work in this area [15, 43], complainants predominantly reported incidents involving a sole former male partner [1], namely an ex-husband, and former non-married relationships, namely an ex-boyfriend.

Validating other identified risk factors as highlighted by HCI scholars [43, 103], we identify a significant proportion of complainants reported either seeking legal representation or were already engaged in legal proceedings, primarily related to divorce. This is perhaps to be expected, as complainants jointly described that divorce had been both the point of discovery for such abuse and a motivator to take action against such harms, often through hiring a legal advocate. Just one complainant labeled their experiences as 'financial abuse', validating our approach to alleviate the burden of relying on customers to self-report or self-identify financial abuse in their interactions with digital devices.

Complaint profile. Technology-enabled financial attacks by an intimate partner was costly to a complainant, which resulted in substantial negative impacts on a complainant's financial wellbeing. We separate this harm into four distinctive categories: money loss from *theft*, *debt* incurred by identity theft, *financial fees* (toil of IPV [80]), or *finances that were withheld* from them by an abuser.

Thirteen complaints reported direct financial losses due to theft, totaling $671,035 (M: $51,618, SD: $105,681), such as digital checks from a shared online business account ($10,000) and unauthorized access to peer-to-peer payment accounts ($6,000). Additionally, 101 cases involved complainants being unaware of accounts opened in their name by abusers, resulting in a total reported debt of $656,256 (M: $6,497, SD: $103,948), ranging from secured credit cards to substantial loans.

Relationship	Sample descriptors	Event	Sample descriptors
Ex-relationship, married	*ex-husband (32.3%), ex-wife (24.3%), ex[-]spouse (7.1%)*	Legal proceedings	divorce (45.7%), theft (23.2%), business disputes (9.4%)
Ex-relationship, not married	*ex[-]boyfriend (6.9%), ex[-]girlfriend (4.3%), ex (7.1%)*	Parental responsibilities	childcare provision, alimony payments, visitation rights
Family members	*father (3.7%), mother (3.1%), brother in-law (2.2%)*	Criminal activity	identity theft (26.2%), fraud (18.4%), physical theft (15.2%)
Other associates	*close friends (3.4%), ex-room-mate (2.2%), new partner (1.3%)*		

Table 1: Most frequently occurring personal and contextual descriptors contained in our complaints. Where possible we have worked to demonstrate the proportionality of complaints that contain these, or lexical variations, of these descriptors. Note that 'x gf', 'x girlfriend', 'x-girlfriend'. all count as 'ex-girlfriend'

Technology-enabled financial abuse can also result in indirect costs which 10 complainants immediately had to pay to pursue or cover, such as legal fees, overdraft fees, and digital forensics totaling $41,970 (M: $4,197, SD: $124,231). Furthermore, complainants reported $4,590,970 (M: $124,000; SD: $103,110) lost due to financial negligence, where abusers withheld money for services they were responsible for, such as child support and housing.

4.1 What areas of digital financial products do complainants report abusers targeting?

Our analysis elicited 14 independent forms of technology-enabled financial attacks across 24 different technical products, systems, and services. Among the 464 complaints, the most common attack types were the opening of a checking or credit account in a complainants' name (n=186), negligence on financial duties to a complainant (n=141), and the theft of the complainants' identity (n=53). Less frequently mentioned were an abuser conducting fraudulent chargebacks via a complainant's account (n=11), unauthorized request of their credit report (n=6), bankruptcy filing without a complainants' knowledge (n=6), and restricting a complainant from accessing their account (n=4). The attacks relied on named digital financial products (Figure 5) and roughly correlated with established technology abuse taxonomies in this space [13, 43, 102].

We identify three areas of significance that had variations on known technical attacks (e.g., unauthorized opening of accounts [43], identity theft [114, 115]) that we suggest indicate novel manifestations of technology abuse. We present these by their overarching behaviors, such as negligence, account takeover, and deception. Namely, we identify that *Access/account takeovers* for explicitly criminal activity, *Negligence* over asset/debt ownership, and *Deception and interference with customer-firm interactions* were particularly devastating to complainants.

Asset/account takeover for criminal activity. Malicious blocking has been reported in prior studies to be an effective way of denying someone access to their own or shared accounts [43], which may often be performed through repeated password requests or through triggering an investigation into an account [13]. However, our analysis shows that abusers may leverage a hijacked account for other criminal purposes, namely, to conduct other acts of identity theft, scams, and more. In these situations, an account takeover was not just performed to gain access and control over a complainant's data

or finances, but for abusers to leverage a complainant's consumer products as a layer of protection against their own being implicated in fraud cases. While some reports show that financial abusers use a survivor's account that are in better financial credit standing than their own [13, 98], we have yet to discover accounts in prior HCI literature such as these where abusers directly implicate them in a crime through this takeover:

> *"I have discovered I am now a victim of identity theft ... My ex husband was deported for using my identity as well as my son's ... please help me resolve these online accounts on my credit report ... it is fraudulent and was not opened by me." (C269)*

In some cases, this could mean engaging in reported money laundering, or using their complainant's account as a means to commit acts such as charge backs, romance scams, or extortion.

Complainants in our dataset expressed disappointment upon finding out that their hijacked account affected multiple other targets of a crime, especially since legitimate purchases could be falsely reported by the abuser. Complainants described a range of worrying channels for discovering previously unknown forms of financial abuse, such as discovering 'unknown accounts'.

> *"... my online bank account was compromised by my ex husband and fraudulent activities were done against my account. I notified my bank ... when several thousands of forged money orders were deposited into ATMs ... I haven't committed a crime nor have authorities pursued any charges to justify why this ban for me to open a bank account ..." (C28)*

Online sources of information on credit, such as a report (listing credit history), being contacted by a collections agency, and a credit score check history proved to be the most common discovery channels for such attacks, roughly co-aligning with how many complainants may discover instances of identity theft. Such findings suggest that despite prominent advice around identity theft [114], some complainants do not discover financial abuse through traditional information discovery methods entailing that "fraudulent activities" could continue without their knowledge. Complainants that described technology-enabled financial abuse, could, however already be aware of the existence of financial misconduct, or, were
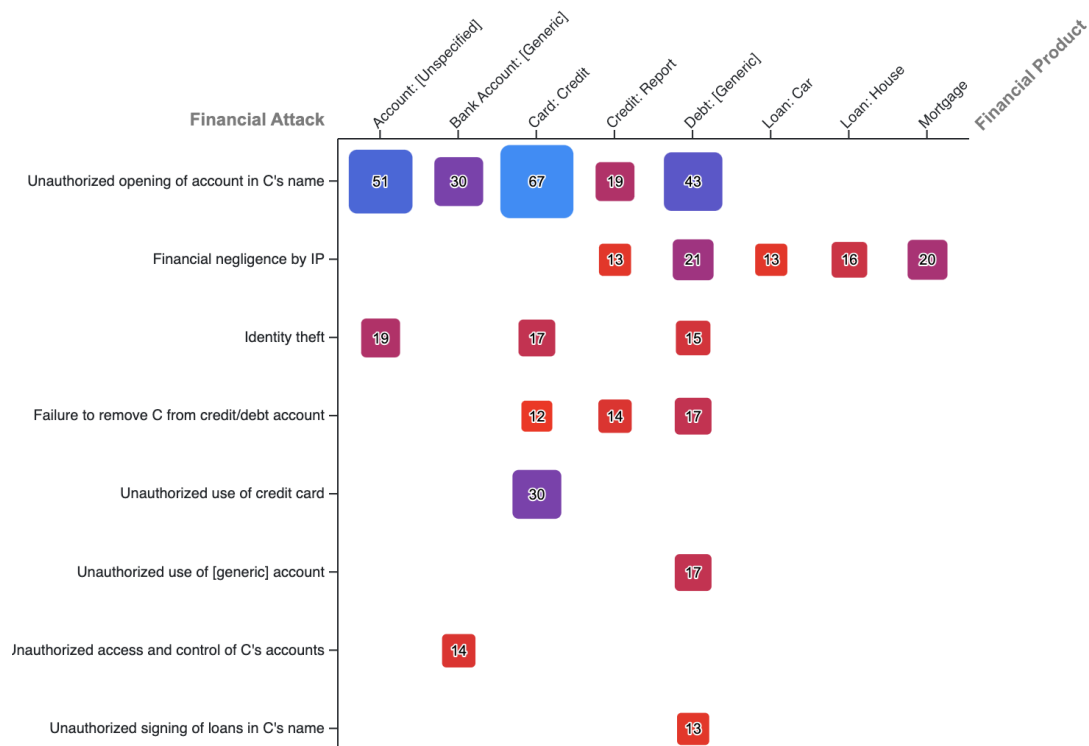
Figure 5: Top 20 products to financial attack mapping. Complainant (C), Intimate Partner (IP), [*Unspecified*] means unspecified product, [*Generic*] means a collective of consumer banking products.

not prompted to reflect on how such information came to light (e.g., upon complaint submission).

Negligence over digital asset/debt management. Financial negligence in connection to digital products stands out from other forms of technology-enabled harm (e.g., [13, 43, 103] as it involves an abuser deliberately breaching a previously established financial agreement. These agreements may vary in nature, being either legally binding, such as child support or debt division in a separation, or informal, like the refusal to contribute to rent or utility bills. Financial negligence could cover a wide range of actions, from refusing to negotiate an online agreement to breaking a digital asset arrangement. In one instance, a complainant shared being unable to coordinate in the repayment of an outstanding debt due to being unable to contact their former partner:

> *"I cannot submit any documents without my ex-husband of 14 years' signature ... This situation is extremely challenging. He harbors resentment, is uncooperative, and abusive. He is aware that this issue affects both our credit reports, yet he adamantly refuses to assist in resolving it"* (C17)

This could also extend to abusers reneging on a previously agreed-upon arrangement, most often through the court, which could be described by complainants as an avoidance to *"adhere to stipulations"* (C59). Many of these agreements, especially those stemming from legal separations, often include considerations of ownership related to specific assets or debts, such as being awarded

property. The processes surrounding asset and debt ownership became a clear area in which this type of abuse intersects with financial institutions' services. For instance, we identified that complainants often suffer harm from this type of attack precisely because they are still held accountable when they believe they should not be. When describing a challenge with respect to a shared online joint account, a complainant shared:

> *"my ex-husband and I maintained a shared account together. According to our divorce agreement, he assumed responsibility for both the account and the associated debt. Despite this clear arrangement, my bank has been uncooperative in removing my status as a joint online account holder, even though I am no longer legally liable for any debt accrued on that account since our date of separation ..."* (C222)

Deception and interference with customer-firm interactions. Our analysis uncovered several tactics employed by individuals engaging in financial abuse against their intimate partners that align with the concept of *'financial deception'*, or *'financial infidelity'* [33]. However, in this context, we discovered it exhibits a distinctive, darker nature. While many intimate partners might be driven by a desire to avoid upsetting their significant other or to evade confrontation [60], complainants explicitly characterize these actions as deliberate, explicitly harmful components of a broader pattern of abuse. For instance, when bank statements were sent electronically, complainants reported uncovering instances where an abuser had

Asset/Account Behavior	Asset/Debt Ownership and Management	Customer-Firm Interactions
• Challenging valid transactions to create unexpected debt • Deceptive handling of borrowed or stolen funds • Intercepting funds for coercion or personal gain • Unauthorized financial actions under the target's profile • Unauthorized use of financial assets for fraud	• Blocking/reversing payments on financial agreements • Failure to remove target from credit/debt account • Ignoring/reverting established financial agreements • Non-compliance with agreed financial obligations • Refusal to establish financial agreements • Tricking the target into signing financial obligations	• Exploiting financial hardship as leverage • Threatening legal action, including divorce • Using fear of other abuses as leverage

Table 2: Common attack types identified via complaints, organized by financial service it interacts with.

set up email redirects to intercept emails from financial institutions, effectively preventing the statements from reaching them. In joint accounts, abusers occasionally prevented information sharing by providing their personal phone number for both accounts, ensuring that only an abuser received notifications of any irregularities.

> *"... I reached out to my bank's fraud department for assistance, but they declined to take any action on my behalf ... I neither initiated the creation of this credit card nor possessed any knowledge of its existence, let alone ever receiving a single statement. It came to light that my wife had confessed to concealing these online statements from me. ... My legal counsel advised me that, given my wife's admission to defrauding me and concealing this fact for a duration of three years, I should request the credit card statements ..."* (C361)

In a few instances, complainants described instances in which abusers partially admitted to certain purchases, but complainants reported being misled about the actual cost of these purchases. Another tactic involved abusers secretly maintaining a bank account unbeknownst to their partner, thereby circumventing the need to share funds equitably. However, in most cases outlined in our complaints, these hidden accounts were primarily used for incurring debt and engaging in high-risk borrowing, often on short notice.

In extreme cases, we came across situations where a spouse had accumulated debts without the knowledge of the other spouse, and these debts only came to light following the debtor's death. In these scenarios, complainants expressed distress not only at having to cope with the loss of a spouse but also at having to address the joint debts in their name, debts of which they were previously unaware.

4.2 What barriers to resolving financial abuse do complainants report encountering?

A poignant reason for contacting the CFPB was that a complainant had received an unsatisfactory resolution from their financial institution, credit bureau, or consumer protection organization (17.9%) — a situation that CFPB's *Customer Complaints Initiative* was explicitly designed for [26, 31]. In the final phases of our analysis, we considered what *types* of unsatisfactory resolutions (or lack of) may trigger a complainant to reach out to such services, as this has significant implications for how digital services are designed to improve this access. Our analysis shows that a single complaint

journey has multiple stages, each necessitating substantive interaction with different financial entities (Figure 6), with complainants often having to repeat the elements of the same story of technology-enabled financial abuse multiple times, or having a lack of access to important information regarding their finances.

As addressing barriers to socio-technical systems for recourse from abuse has significant implications, our analyses identifies three sub-types that constitute barriers to addressing technology-enabled financial abuse; first, an *absent policy design to recognize financial abuse in intimate partnerships*, second, *barriers to evidencing the existence of technology abuse*, and, most concernedly, *a potential escalation of digital-safety risks through recommended resolutions by the financial institution*.

Policies that overlook the dynamics of technology-enabled financial abuse. Mirroring work in other areas of digital finances in HCI [27, 100], we identified that many complainants reported feeling that they were poorly served by company policy in managing financial abuse cases. We identify two commonly occurring challenges in the context of IPV: authorized transactions and consent-based concerns.

Identifying the difference between authorized and unauthorized online transactions was a common problem for many complainants; where receiving a judgement of unauthorized would trigger a fraud investigation, while authorized could result in a lack of action.

Although peer to peer payment services were a rare occurrence in our dataset (as many of those companies do not as of yet earn over $10B in assets, the minimum threshold to be tracked by the CFPB), we identified several complainants who cited previous legitimate interactions with an abuser where the financial service provider refused to label fraudulent transactions as fraudulent due to a previous history between the users. We noted a lack of consistency in how a complainant's experience was categorized in our dataset. For instance, one complainant shared the following after having a phone stolen:

> *"... there was a fraudulent transaction from my account issued to "[fake-name]" in the amount of $10,000.00. This "[fake name]" was an ex-boyfriend who had stolen my phone and sent the money to himself after turning off my notifications to my number. I immediately contacted [P2PP] and inform them of the fraudulent transaction ... I was able to get nothing resolved until far after the time to which they informed me that it*
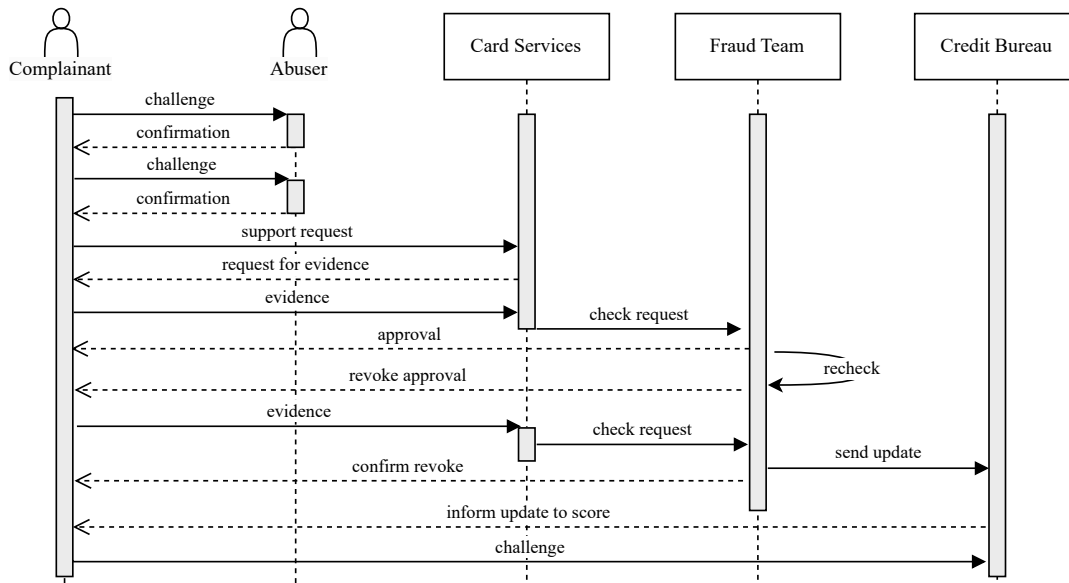
Figure 6: Example complexity of multiple interactions between financial services inherent in a single case of IPFA. This model was generated via the account in Figure 4, where a complainant challenges their abuser twice about the use of their credit card details online, and coordinates between card services, fraud teams, and credit bureaus.

> *was a non fraudulent transaction because said " [fake name] " and I had previous transactions"* (C97)

In this situation, the fact that a complainant had previously interacted with an intimate partner in this context — despite a clear description of device compromise — was enough to categorize this transaction as non-fraudulent; resulting in a substantive loss of money for a complainant.

In some cases, while complainants stated that employees of financial institutions were more sympathetic to their concerns, most reported an inability for policy to permit them to do so:

> *"My husband has 100% control of all of our money ... I attempted repeatedly to get into my account to get funds to hire an attorney ... I was then told I never had an account there ... I pleaded with the teller who quietly told me she believes me but she would lose her job if she tried to help me"* (C251)

Challenges to evidencing 'legitimate' financial abuse. Despite multiple adversities, some complainants attempted to take on the complexities of their specific financial case independently, but were met with a *lack of a response* from the financial organization (7.3%). We identified that the threshold for being able to demonstrate proof of financial abuse was considerably high, namely, that when complainants attempted to contest authorized opening of credit cards in their name, a financial organization would turn around and ask for 'proof':

> *"... My ex-wife has continued to obtain new credit in my name. I have disputed many accounts that appear on all 3 credit bureaus only to have them respond with "we need proof". ... nothing changes or helps ... I'm really just stuck ... This is insane."* (C48)

The quality of the evidence was also judged harshly; oftentimes, screenshots and transcripts were rarely taken into consideration, as they were judged to not meet the threshold expected to dispute such harms. Complainants sadly provided detailed descriptions of trauma as a consequence of collecting their own evidence (2.4%). Digital evidence gathering was distressing for many complainants who reported that they had already been affected by similiar requests during legal proceedings, such as for divorce or restraining orders. However, this reportedly trapped them in what a complainant described as a "vicious cycle" — that to get the digital proof they needed to ask the financial institution to send over the documentation, whom would then refuse to do so without first seeing 'proof' of abuse.

While some financial institutions aimed to assist complainants with the challenge in documenting their experiences, this also introduced entirely new barriers. Many complainants reported not receiving necessary documents or lacking the means to obtain them from financial institutions, or feeling pressured to share personal information they would rather keep private (e.g., salary, location history). In one scenario, a complainant received the requested statements relating to an abuser opening an account via an email from a financial institution, but encountered a further digital barrier, reporting they were *"unable to open the zipped attachment to see the contents"* (C89) as they required a password that the complainant reported the institution then refused to provide.

Suggested resolutions may elevate digital-safety risks. Many financial products we identified in our analysis were often co-shared or connected between a complainant and an offender, including bank accounts, house loans, car insurance, and utility bills. Relationships with offenders can present unique digital-safety risks [107], such as fraudulent purchases, identity theft, or social engineering to

elicit financial information through social engineering [43, 44, 108]. Our analysis revealed that financial support workers are broadly unaware of such a risk, and made multiple recommendations for a complainant to directly *challenge* an offender until the concern was resolved. In spite of explaining concerns about being unable to resolve the issue on their own, financial support workers and branch staff would recommend complainants *"take the issue up"* with an offender (C11). As one complainant described after reporting a card opened in their name:

> *"I called today to find out the status, and was told [by the financial support worker] that I benefited from this. I don't understand how I benefited from being the victim of domestic abuse. They said I had to file a police report, but, if I did that, my husband could possibly hurt me physically … "* (C82)

In general, complainants reported being afraid of physical retaliation after approaching the abuser, citing *"feeling fearful and scared"* of the person that they had been admonished for *"trusting them"* by a financial representative (C306). Namely, complainants were often encouraged by representatives at financial institutions to find another source of income, forgo claims for theft of financial assets, hire an attorney to pursue legal action, to *"find another bank"* (C408), or even to pay off the outstanding debt. In response of being recommended to modify a loan took out through coercion ('coerced debt') by a representative at a financial institution, one complainant exclaimed: *"I am not looking to modify this loan, I am looking to be free of this loan!"* (C288).

While financial support workers should not be expected to provide direct IPV support to complainants who describe this (as highlighted by Zou et al. [113]), such results point to the need for financial support workers to have training on how to handle such complaints without discrediting or putting a complainant at further risk.

5 DISCUSSION

Through a combination of natural language processing techniques and careful human review, we have taken the first step in what identifying consumer complaints linked to IPFA could look like in public datasets (**RQ1**). Our subsequent analyses provides a complementary approach to existing work in HCI on technology abuse [43, 44] by uncovering new insights into digital products (**RQ2**), and barriers to digital services (**RQ3**), from survivors who do not label their experiences as abuse, and thus, may not presently be receiving professional help.

Despite the challenges of complicated reporting pathways (Section 4.2) and navigating the design of digital products that do not accommodate their digital-safety needs (Section 4.1), survivors are nevertheless still reaching out to customer complaint services for help. In light of these findings, we recommend several strategies to bolster the digital-safety of individual financial products through improved security tooling (Section 5.1), enhance digital systems for evidence gathering (Section 5.2), and suggest ways to improve financial support systems to support clients (Section 5.3).

5.1 Safety Checkups for Digital Financial Accounts

Our research reveals that unclear account ownership and authorization approaches can create unique vulnerabilities to survivors of IPFA attacks in digital financial systems. These are common, complex challenges for any digital system [67], but the negative consequences of getting this wrong for survivors are severe. The unauthorized use of a complainant's accounts for criminal activity resulted in the complainant being held accountable for the repercussions (Section 4.1).

Similarly, when it comes to financial deception, the complainant is unfairly liable for a joint account they had no knowledge of. While prior HCI research has already highlighted the complications that may arise from close social relationships — be these unofficial proxies [65] (adults who assist older adults) or caretakers [72] — intimate partners may have to pool their financial resources to pay for specific assets or experiences [13, 69], which require shared account access and permissions [51, 77]. Revoking consent for shared access is not effectively indicated in most digital account or asset workflows, or notifications to users, making it difficult to identify attacks until much later. Thus, focusing on improved digital workflows could benefit the user's understanding of account ownership and where their information is being used elsewhere.

Safety checkups geared towards financial systems may be able to help survivors or other concerned users audit their mobile and desktop devices for signs of technology abuse. Such safety checkups are initiated by users and help them with actions such as checking and resetting app permissions, configuring privacy settings, and monitoring device logins [28]. The user interfaces for carrying out the above actions exist across different technology platforms [28], and was even observed by authors in existing financial mobile apps. However, a guided workflow for utilizing these interfaces is not always present.

A prominent example of such a guided workflow is Apple's Safety Check feature for the iPhone [5], which guides users through a review of: data (e.g. location, shared photo albums) users share with other users, app permissions, and devices logged into a user's Apple ID. This feature also provides users the option to reset permissions and sharing privileges, providing users with a description of the potential consequences of doing so (e.g. other users may be able to observe a loss of access). Based on our analysis, it is evident that digital financial workflows may benefit from similar guided mechanisms being implemented in financial institution applications that build on the actions that existing safety checks already employ.

Regularly auditing financial accounts with such a guided tool could help identify early signs of financial attacks, such as by looking for signs of unexpected account behavior or how personal financial data, credit cards, and other assets have been attributed elsewhere without permission. For instance, a financial safety check mechanism may expand on reviewing device logins by exposing more details about account accesses during in-branch or over the phone interactions. This could potentially reveal acts of financial deception where an offender attempts to impersonate the target while speaking to a relevant financial service provider. Further, if any suspicious activity is identified, users could receive trauma-informed

recommendations on their next actions [113], like notifying their financial institution or initiating the resolution process.

Financial institutions are already well-equipped to provide such support to other groups vulnerable to digital financial crimes, such as targets of identity theft or scams. Thus, it could be the case of adapting existing mechanisms to fit this specific use case, particularly during high-risk events such as during account openings or when fraud policies are triggered. We see particular promise in situations involving *deception and interference with customer-firm interactions* (Section 4.1). Thus, we are confident such functionality would also benefit other, inter-related financial harms, such as account compromise through device theft, or elder financial abuse [65].

5.2 Automated, intelligent approaches to technology-enabled financial abuse evidence

Insufficient clarity on what constitutes sufficient evidence and complicated resolution procedures can obstruct the evidence gathering and resolution process for possible IPFA cases (Section 4.2). Thus, digital evidence that validates a survivor's experience of abuse is crucial to address psychological harm [81, 90] and pursue a potential resolution [14, 44]. These challenges identified in our analysis, if left under-addressed, could directly increase consumer vulnerability, resulting in long-term financial costs in the hundreds of thousands (Section 4). As digital evidence gathering processes may be required by financial institutions or legal policies to take any step towards resolving actions, we pose two approaches that can augment existing evidence gathering and evidence reporting approaches.

Evidence gathering approaches. The process for gathering digital evidence for complainants can be difficult due to the dynamic nature of financial attacks. For instance, complainants reported losing digital documentation, unresponsive organizations, and cases where financial institutions provided the information in a format that was inaccessible (Section 4.2). These processes can make resolution to such attacks seem impossible due to complainants feeling overloaded by working with different stakeholders and unclear standards for sufficient evidence [44].

To mitigate these barriers to access, our results suggest that having a shared evidence log that adequately documents what is required to showcase different types of technical attacks, and the required standard that such digital evidence would need to meet could be useful. While similar concepts already exist in cases of identity theft [74], the majority of digital financial harms that are largely exempt from our work, such as fraud and scams, are usually addressed as individual incidents. Our approach underlines that this shared evidence store should emphasize the complex social dynamics of intimate partner violence and the associated risks.

For instance, Surviving Economic Abuse, a registered charity that supports women who have experienced economic abuse by a current or former partner, offers *The Economic Abuse Evidence Form* [99] as a tool for debt advisers to consolidate information about abuse in a single location about the abuse experienced by a survivor, and help a debt adviser support a survivor when communicating with creditors. While this digital form is designed solely with coerced debt in mind, we posit this could be augmented to cover more forms of technology enabled financial abuse, such as the types of financial attacks (see Table 2). Such an approach could also inspire new frameworks for conversations about financial abuse and training for staff, as hinted at by Bellini [13] to simultaneously build confidence in responding to reported cases.

Evidence reporting approaches. The emergence of technology-enabled IPFA brings many new challenges to HCI scholars who are interested in alleviating the harm caused by financial and monetary loss, such as through preventing access to technical products (Section 4.1), or the accumulation of fees or credit (Section 4). An obstacle that caused significant time burdens for complainants was that even when they had successfully collected evidence of suspected financial abuse, the reporting infrastructures introduced new barriers to sharing this with financial institutions, evidenced often by a lack of response by the institution to these efforts.

While there are many ways to approach the challenge of reporting abuse, a small design decision that could have an enormous impact on survivors [97], could be a closer look at the design of online complaint forms. Doing so could help to gather further insight into the fine-grained information that were regrettably absent from our results. The complaint form for the CFPB had a welcome large character limit for complainants to share experiences (10,000 words). Though improved complaint form design that asks for vital contextual information — potentially guided by the eight categories in our framework analysis — could elicit good indicators for when evidence may be absent, it could also stall a process of resolution.

Further, the form could ask optional questions about the complainant's relationship to the suspected offender, the impact of abuse, and their desired resolution, which could be encouraged by a natural language processing approach, akin to smart email suggestions, that could help the consumer identify what vital contextual information or digital documentation may be missing from their stories. Guiding complainants to provide details such as how they discovered such abuse may also be a valuable area of future study, with implications in identifying the appropriate means of support for a complainant, based on their unique circumstances. While this technical suggestion is especially useful in the context of IPFA, this could also be useful more broadly to any complainant reaching out about financial challenges.

5.3 Further insight into technology-enabled financial abuse

Existing computer security support infrastructure has been shown to fall short in cases of addressing the unique threat model of intimate partner technology abuse [28, 42, 43], resulting in the development of carefully designed security clinics [56, 104]. However, as raised by Zou et al. [113], sadly many survivors may never reach these clinics. Our work provides a first look into how survivors of IPFA describe their own experiences independently of professional services, while also not identifying as a survivor of abuse. We are encouraged by the many suggestions offered by the HCI community [13, 14, 113], that call for adequate training of financial support workers and frontline staff around technology abuse. As our findings show, the fact that complainants reach out to multiple institutions over time (Figure 6) while experiencing multiple attacks [43, 104], only reinforces this need. However, we believe

that further insight is still needed into IPFA to ensure that such interventions are effective.

Our dataset is the first example of a corpus demonstrating potential IPFA cases in digital financial products 'in the wild'. Despite this, we acknowledge shortcomings of this dataset, and encourage the augmentation of this resource by data from other consumer organizations and financial institutions alike. When studying or addressing IPFA, we suggest that a broad range of complainant language should be anticipated and a focus on the attributes of the complainant experience may prove to be key in identifying supportive services, whether that be through manual or automated methods. Specifically, merging our dataset with internal complaints from financial institutions can achieve a similar goal as monitoring tech-enabled IPV cases for computer security customer agents: capturing a detailed record of encountered attacks [13, 103], vulnerabilities in support systems [14], and the impact of trauma on targets and financial support workers [113].

Building and analyzing such a dataset at scale may benefit from triaging large complaints datasets at financial institutions, possibly with automated approaches. For instance, one could leverage complaints language and recent techniques that demonstrate performance gains in language modeling tasks with large language models, step-by-step reasoning, and rationales [57, 58, 112] to create a robust classifier of complaints. A cohesive set of IPFA examples across different consumer reporting sources can help researchers as well. Research characterizing the harms of IPFA over time may be improved by joining a survivor's complaints made to different organizations as abuse progresses. Similarly, non-profit organizations for survivor assistance and advocacy may better support survivors in their evidence gathering and reporting approaches with a unified evidence store. These use cases all call for thorough investigation prior to implementation, but we hope that they inspire stakeholders in HCI to enhance system safety for all.

Limitations. Our dataset is modest compared to some fraud datasets [45, 46], so our results should be interpreted cautiously by designers, developers, and fellow researchers. Namely, our study focus may not be representative of all survivors, as our dataset only examines a specific sample of IPFA cases where the complainant explicitly shows awareness of harm or abusive behavior through specific keywords. The subsequent use of our workflow intends to mitigate this issue, but still relies on the results of proximity-based keyword-based approaches as a reference set which may limit how new patterns of IPFA are discovered. Like other HCI studies based on self-reported data, complainants may overstate certain aspects of their financial history due to social desirability bias [91] or to elicit empathy and alleviate financial burdens [49]. People with negative experiences may be more inclined to write formal complaints [59], while others may fear repercussions or societal stigma [44, 90].

Our primary goal was nevertheless to understand what specific financial attacks and barriers complainants report experiencing to professional organizations. Thus, despite these limitations, our dataset still offers a substantial cross-section of survivor accounts to U.S.-based financial institutions, providing valuable insights for institutions dealing with financial abuse concerns, particularly via digital technologies. We look forward to further work that explores the different forms of harm and language used in self-reported instances of IPFA.

REFERENCES

[1] Nasreen Ali, Jabeer Butt, and Melanie Phillips. 2021. *Improving Responses to the Sexual Abuse of Black, Asian and Minority Ethnic Children.* Technical Report. Centre of Expertise on Child Sexual Abuse. https://www.csacentre.org.uk/app/uploads/2023/09/Responding-to-CSA-of-Black-Asian-minority-ethnic-children.pdf

[2] Ashwaq Alsoubai, Jihye Song, Afsaneh Razi, Nurun Naher, Munmun De Choudhury, and Pamela J. Wisniewski. 2022. From 'Friends with Benefits' to 'Sextortion:' A Nuanced Investigation of Adolescents' Online Sexual Risk Experiences. *Proceedings of the ACM on Human-Computer Interaction* 6, CSCW2, Article 411 (nov 2022), 32 pages. https://doi.org/10.1145/3555136

[3] Keith B Anderson. 2004. *Consumer Fraud in the United States: An FTC Survey.* Technical Report. https://www.ftc.gov/sites/default/files/documents/reports/consumer-fraud-united-states-ftc-survey/040805confraudrpt.pdf

[4] Maria Antoniak, Anjalie Field, Jimin Mun, Melanie Walsh, Lauren Klein, and Maarten Sap. 2023. Riveter: Measuring Power and Social Dynamics Between Entities. In *Proceedings of the 61st Annual Meeting of the Association for Computational Linguistics.* Association for Computational Linguistics, 377–388. https://doi.org/10.18653/v1/2023.acl-demo.36

[5] Apple. 2023. How Safety Check on iPhone Works to Keep You Safe. https://support.apple.com/en-euro/guide/personal-safety/ips2aad835e1/web

[6] Shirley Ardener. 2005. Ardener's "Muted Groups": The Genesis of an Idea and its Praxis. 28, 2 (2005), 50–54,72. https://search.proquest.com/openview/005729b56276e042142e34142afebcb9/1

[7] Daniel Arp, Erwin Quiring, Feargus Pendlebury, Alexander Warnecke, Fabio Pierazzi, Christian Wressnegger, Lorenzo Cavallaro, and Konrad Rieck. 2022. Dos and Don'ts of Machine Learning in Computer Security. In *Proceedings of the 31st USENIX Security Symposium (USENIX Security).* USENIX Association, 3971–3988. https://www.usenix.org/conference/usenixsecurity22/presentation/arp

[8] Ian Ayres, Jeff Lingwall, and Sonia Steinway. 2013. Skeletons in the Database: An Early Analysis of the CFPB's Consumer Complaints. *Fordham Journal of Corporate & Financial Law* 19 (2013), 343. https://ir.lawnet.fordham.edu/jcfl/vol19/iss2/2

[9] Belén Barros Pena, Bailey Kursar, Rachel E. Clarke, Katie Alpin, Merlyn Holkar, and John Vines. 2021. "Pick Someone Who Can Kick Your Ass" - Moneywork in Financial Third Party Access. *Proceedings of the ACM on Human-Computer Interaction* 4, CSCW3 (2021), 1–28. https://doi.org/10.1145/3432917

[10] 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* (2021-05-07) *(CHI '21).* Association for Computing Machinery, 1–16. https://doi.org/10.1145/3411764.3445251

[11] Kaveh Bastani, Hamed Namavari, and Jeffrey Shaffer. 2019. Latent Dirichlet Allocation (LDA) for Topic Modeling of the CFPB Consumer Complaints. *Expert*

Systems with Applications 127 (2019), 256–271. https://doi.org/10.1016/j.eswa.2019.03.001

[12] Jörg Becker and Björn Niehaves. 2007. Epistemological Perspectives on IS Research: A Framework for Analysing and Systematizing Epistemological Assumptions. 17, 2 (2007), 197–214. https://doi.org/10.1111/j.1365-2575.2007.00234.x

[13] Rosanna Bellini. 2023. Paying the Price: When Intimate Partners Use Technology for Financial Harm. In *Proceedings of the 2023 ACM SIGCHI Conference on Human Factors in Computing Systems (CHI)*. Association for Computing Machinery (ACM), 17 pages. https://doi.org/10.1145/3544548.3581101

[14] Rosanna Bellini, Kevin Lee, Megan A. Brown, Jeremy Shaffer, Rasika Bhalerao, and Thomas Ristenpart. 2023. The Digital-Safety Risks of Financial Technologies for Survivors of Intimate Partner Violence. In *Proceedings of the 32nd USENIX Security Symposium (USENIX Security)*. USENIX Association, 87–104. https://www.usenix.org/conference/usenixsecurity23/presentation/bellini

[15] 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 (2021), 1–27. https://doi.org/10.1145/3432909

[16] Rosanna Bellini, Emily Tseng, Noel Warford, Alaa Daffalla, Tara Matthews, Sunny Consolvo, Jill Palzkill Woelfer, Patrick Gage Kelley, Michelle L. Mazurek, Dana Cuomo, Nicola Dell, and Thomas Ristenpart. 2023. SoK: Safer Digital-Safety Research Involving At-Risk Users. (2023). arXiv:2309.00735

[17] Jan Blommaert and Chris Bulcaen. 2000. Critical Discourse Analysis. *Annual Review of Anthropology* 29, 1 (2000), 447–466. https://doi.org/10.1146/annurev.anthro.29.1.447

[18] Riley Botelle, Vishal Bhavsar, Giouliana Kadra-Scalzo, Aurelie Mascio, Marcus V. Williams, Angus Roberts, Sumithra Velupillai, and Robert Stewart. 2022. Can Natural Language Processing Models Extract and Classify Instances of Interpersonal Violence in Mental Healthcare Electronic Records: An Applied Evaluative Study. *BMJ Open* 12, 2 (2022), e052911. https://doi.org/10.1136/bmjopen-2021-052911 Publisher: British Medical Journal Publishing Group Section: Health informatics.

[19] Layla Branicki, Senia Kalfa, Alison Pullen, and Stephen Brammer. 2023. Corporate Responses to Intimate Partner Violence. *Journal of Business Ethics* (2023). https://doi.org/10.1007/s10551-023-05461-6

[20] Linnéa Bruno. 2022. Economic Abuse From Child and Youth Perspectives: A Review of the Literature. *Social Inclusion* 10, 4 (2022), 29–38. https://doi.org/10.17645/si.v10i4.5396

[21] Consumer Financial Protection Bureau. 2015. Narrative Scrubbing Standard. https://files.consumerfinance.gov/f/documents/201503_cfpb_Narrative-Scrubbing-Standard.pdf.

[22] 1994. *Analyzing Qualitative Data* (1994-01-05). Routledge. https://doi.org/10.4324/9780203413081

[23] Stevie Chancellor. 2023. Towards Practices for Human-Centered Machine Learning. *Commun. ACM* 66, 3 (2023). https://doi.org/10.1145/3530987

[24] Stevie Chancellor, Michael L. Birnbaum, Eric D. Caine, Vincent MB Silenzio, and Munmun De Choudhury. 2019. A Taxonomy of Ethical Tensions in Inferring Mental Health States from Social Media. In *Proceedings of the conference on fairness, accountability, and transparency*. 79–88. https://doi.org/10.1145/3287560.3287587

[25] Rahul Chatterjee, Periwinkle Doerfler, Hadas Orgad, Sam Havron, Jackeline Palmer, Diana Freed, Karen Levy, Nicola Dell, Damon McCoy, and Thomas Ristenpart. 2018. The Spyware Used in Intimate Partner Violence. In *2018 IEEE Symposium on Security and Privacy (SP)*. 441–458. https://doi.org/10.1109/SP.2018.00061 ISSN: 2375-1207.

[26] Consumer Financial Protection Bureau. 2023. Consumer Response Annual Report. https://s3.amazonaws.com/files.consumerfinance.gov/f/documents/cfpb_2022-consumer-response-annual-report_2023-03.pdf

[27] 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* (2022-06-13) (*DIS '22*). Association for Computing Machinery, 612–628. https://doi.org/10.1145/3532106.3533569

[28] Alaa Daffalla, Marina Bohuk, Nicola Dell, Rosanna Bellini, and Thomas Ristenpart. 2023. Account Security Interfaces: Important, Unintuitive, and Untrustworthy. In *Proceedings of the 32nd USENIX Security Symposium (USENIX Security)*. USENIX Association, 3601–3618. https://www.usenix.org/conference/usenixsecurity23/presentation/daffalla

[29] Peteris Darzins, Georgia Lowndes, Jo Wainer, K Owada, and Ms Tijana Mihaljcic. 2009. *Financial Abuse of Elders: A Review of the Evidence*. Technical Report. https://www.eapu.com.au/uploads/research_resources/VIC-Financial_Elder_Abuse_Evidence_Review_JUN_209-Monash.pdf

[30] Stephen Deane. 2018. Elder Financial Exploitation Why it is a Concern, What Regulators are Doing About it, and Looking Ahead. (2018). https://www.sec.gov/files/elder-financial-exploitation.pdf

[31] Nabamallika Dehingia, Arnab K Dey, Lotus McDougal, Julian McAuley, Abhishek Singh, and Anita Raj. 2022. Help Seeking Behavior by Women Experiencing Intimate Partner Violence in India: A Machine Learning Approach to Identifying

Risk Factors. *PloS one* 17, 2 (2022), e0262538. https://doi.org/10.1371/journal.pone.026253810.1371/journal.pone.0262538

[32] Marguerite DeLiema. 2018. Elder Fraud and Financial Exploitation: Application of Routine Activity Theory. *The Gerontologist* 58, 4 (2018), 706–718. https://doi.org/10.1093/geront/gnw258

[33] Department of Justice. 2023. Elder Abuse and Elder Financial Exploitation Statutes. https://www.justice.gov/elderjustice/prosecutors/statutes

[34] Mary Dixon-Woods. 2011. Using framework-based synthesis for conducting reviews of qualitative studies. *BMC Medicine* 9, 1 (2011), 39. https://doi.org/10.1186/1741-7015-9-39

[35] Margaret Eisenhart. 1991. Conceptual Frameworks for Research Circa 1991: Ideas from a Cultural Anthropologist; Implications for Mathematics Education Rese. (1991). https://nepc.colorado.edu/publication/conceptual-frameworks-research-circa-1991-ideas-a-cultural-anthropologist-implications-m

[36] Ellie Butt. 2020. Know Economic Abuse Report 2020. , 50 pages. https://refuge.org.uk/wp-content/uploads/2020/10/Know-Economic-Abuse-Report-2020.pdf

[37] Norman Fairclough. 2012. Critical Discourse Analysis. In *The Routledge Handbook of Discourse Analysis*. Routledge.

[38] Max Falkenberg, Alessandro Galeazzi, Maddalena Torricelli, Niccolò Di Marco, Francesca Larosa, Madalina Sas, Amin Mekacher, Warren Pearce, Fabiana Zollo, Walter Quattrociocchi, et al. 2022. Growing Polarization Around Climate change on Social Media. *Nature Climate Change* (2022), 1–8. https://doi.org/10.1038/s41558-022-01527-x

[39] Pamela Foohey. 2017. Calling on the CFPB for Help: Telling Stories and Consumer Protection. *Law and Contemporary Problems* 80, 3 (2017), 177.

[40] Silvia Fraga Dominguez, Bee Ozguler, Jennifer E Storey, and Michaela Rogers. 2022. Elder Abuse Vulnerability and Risk Factors: Is Financial Abuse Different from Other Subtypes? *Journal of applied gerontology* 41, 4 (2022), 928–939. https://doi.org/10.1177/07334648211036402

[41] 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

[42] 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 (2019), 1–24. https://doi.org/10.1145/3359304

[43] 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*. ACM, 1–13. https://doi.org/10.1145/3173574.3174241

[44] 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

[45] FTC Data 2013 2013. Data Sets. https://www.ftc.gov/policy-notices/open-government/data-sets

[46] FTC Explore Data 2019 2019. Explore Data. https://www.ftc.gov/news-events/data-visualizations/explore-data

[47] Christine Furber. 2010. Framework Analysis: A Method for Analysing Qualitative Data. *African Journal of Midwifery and Women's Health* 4, 2 (2010), 97–100. https://doi.org/10.12968/ajmw.2010.4.2.47612 Publisher: Mark Allen Group.

[48] Nicola K. Gale, Gemma Heath, Elaine Cameron, Sabina Rashid, and Sabi Redwood. 2013. Using the Framework Method for the Analysis of Qualitative Data in Multi-Disciplinary Health Research. *BMC Medical Research Methodology* 13, 1 (2013), 117. https://doi.org/10.1186/1471-2288-13-117

[49] Nicolás Gambetta, Ana Zorio-Grima, and María Antonia García-Benau. 2015. Complaints Management and Bank Risk Profile. *Journal of business research* 68, 7 (2015), 1599–1601. https://doi.org/10.1016/j.jbusres.2015.02.002

[50] Tianyu Gao, Xingcheng Yao, and Danqi Chen. 2021. SimCSE: Simple Contrastive Learning of Sentence Embeddings. In *Proceedings of the 2021 Conference on Empirical Methods in Natural Language Processing*. Association for Computational Linguistics, 6894–6910. https://doi.org/10.18653/v1/2021.emnlp-main.552

[51] Goodbudget. 2020. How can I share my budget with my partner? https://goodbudget.com/help/mobile-apps/share-budget-w-partner/

[52] S Duke Han, Patricia A Boyle, Bryan D James, Lei Yu, and David A Bennett. 2016. Mild Cognitive Impairment and Susceptibility to Scams in Old Age. *Journal of Alzheimer's Disease* 49, 3 (2016), 845–851. https://doi.org/10.3233/JAD-150442

[53] Hans WA Hanley, Deepak Kumar, and Zakir Durumeric. 2023. Happenstance: Utilizing Semantic Search to Track Russian State Media Narratives about the Russo-Ukrainian War On Reddit. *Proceedings of the International AAAI Conference on Web and Social Media* 17, 327–338. https://doi.org/10.1609/icwsm.v17i1.22149

[54] Hamza Harkous, Sai Teja Peddinti, Rishabh Khandelwal, Animesh Srivastava, and Nina Taft. 2022. Hark: A Deep Learning System for Navigating Privacy Feedback at Scale. In *2022 IEEE Symposium on Security and Privacy (SP)*. IEEE, IEEE, 2469–2486. https://doi.org/10.1109/SP46214.2022.9833729

[55] Kate Lockwood Harris, Kellie E Palazzolo, and Matthew W Savage. 2012. 'I'm Not Sexist, but . . .': How Ideological Dilemmas Reinforce Sexism in Talk About Intimate Partner Violence. *Discourse & Society* 23, 6 (2012), 643–656. https://doi.org/10.1177/0957926512455382 Publisher: SAGE Publications Ltd.

[56] Sam Havron, Diana Freed, Rahul Chatterjee, Damon McCoy, Nicola Dell, and Thomas Ristenpart. 2019. Clinical Computer Security for Victims of Intimate Partner Violence. 105–122. https://www.usenix.org/conference/usenixsecurity19/presentation/havron

[57] Cheng-Yu Hsieh, Chun-Liang Li, Chih-Kuan Yeh, Hootan Nakhost, Yasuhisa Fujii, Alexander Ratner, Ranjay Krishna, Chen-Yu Lee, and Tomas Pfister. 2023. Distilling Step-by-Step! Outperforming Larger Language Models with Less Training Data and Smaller Model Sizes. In *Findings of the Association for Computational Linguistics: ACL 2023*. Association for Computational Linguistics, 8003–8017. https://doi.org/10.18653/v1/2023.findings-acl.507

[58] Jiaxin Huang, Shixiang Shane Gu, Le Hou, Yuexin Wu, Xuezhi Wang, Hongkun Yu, and Jiawei Han. 2023. Large Language Models can Self-Improve. In *Proceedings of the 2023 Conference on Empirical Methods in Natural Language Processing*. Association for Computational Linguistics, 1051–1068. https://doi.org/10.18653/v1/2023.emnlp-main.67

[59] Hossein Joudaki, Arash Rashidian, Behrouz Minaei-Bidgoli, Mahmood Mahmoodi, Bijan Geraili, Mahdi Nasiri, and Mohammad Arab. 2015. Using Data Mining to Detect Health Care Fraud and Abuse: A Review of Literature. *Global Journal of Health Science* 7, 1 (2015), 194. https://doi.org/10.5539/gjhs.v7n1p194

[60] Charlotte M. Karam, Michelle Greenwood, Laura Kauzlarich, Anne O'Leary Kelly, and Tracy Wilcox. 2023. Intimate Partner Violence and Business: Exploring the Boundaries of Ethical Enquiry. *Journal of Business Ethics* (2023). https://doi.org/10.1007/s10551-023-05462-5

[61] Bryan J Kemp and Laura A Mosqueda. 2005. Elder Financial Abuse: An Evaluation Framework and Supporting Evidence. *Journal of the American Geriatrics Society* 53, 7 (2005), 1123–1127. https://doi.org/10.1111/j.1532-5415.2005.53353.x

[62] Matthew D. Kiernan and Mick Hill. 2018. Framework Analysis: A Whole Paradigm Approach. *Qualitative Research Journal* 18, 3 (2018), 248–261. https://doi.org/10.1108/QRJ-D-17-00008 Publisher: Emerald Publishing Limited.

[63] Anna Koufakou, Endang Wahyu Pamungkas, Valerio Basile, Viviana Patti, et al. 2020. HurtBERT: Incorporating Lexical Features with BERT for the Detection of Abusive Language. In *Proceedings of the Fourth Workshop on Online Abuse and Harms*. Association for Computational Linguistics, 34–43. https://doi.org/10.18653/v1/2020.alw-1.5

[64] Gunther Kress. 1990. Critical Discourse Analysis. 11 (1990), 84–99. https://doi.org/10.1017/S0267190500001975 Publisher: Cambridge University Press.

[65] 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* (2022-04-29) *(CHI '22)*. Association for Computing Machinery, 1–13. https://doi.org/10.1145/3491102.3501845

[66] Anna Leontjeva, Genevieve Richards, Kaavya Sriskandaraja, Jessica Perchman, and Luiz Pizzato. 2023. Detection of Abuse in Financial Transaction Descriptions Using Machine Learning. (2023). arXiv:2303.08016

[67] Karen Levy and Bruce Schneier. 2020. Privacy Threats in Intimate Relationships. *Journal of Cybersecurity* 6, 1 (05 2020). https://doi.org/10.1093/cybsec/tyaa006

[68] Varoon Mathur, Caitlin Lustig, and Elizabeth Kaziunas. 2022. Disordering Datasets: Sociotechnical Misalignments in AI-Mediated Behavioral Health. *Proceedings of the ACM on Human-Computer Interaction* 6, CSCW2 (Nov. 2022), 416:1–416:33. https://doi.org/10.1145/3555141

[69] Nora McDonald, Alison Larsen, Allison Battisti, Galina Madjaroff, Aaron Massey, and Helena Mentis. 2020. Realizing Choice: Online Safeguards for Couples Adapting to Cognitive Challenges. 99–110. https://www.usenix.org/conference/soups2020/presentation/mcdonald

[70] Mary L. McHugh. 2012. Interrater Reliability: The Kappa Statistic. 22, 3 (2012), 276–282. https://www.ncbi.nlm.nih.gov/pmc/articles/PMC3900052/

[71] Leland McInnes, John Healy, and Steve Astels. 2017. HDBScan: Hierarchical Density Based Clustering. *Journal of Open Source Software* 2, 11 (2017), 205. https://doi.org/10.21105/joss.00205

[72] Helena M. Mentis, Galina Madjaroff, and Aaron K. Massey. 2019. Upside and Downside Risk in Online Security for Older Adults with Mild Cognitive Impairment. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems* (2019-05-02) *(CHI '19)*. Association for Computing Machinery, 1–13. https://doi.org/10.1145/3290605.3300573

[73] Wendy Moncur, Lorna Gibson, and Daniel Herron. 2016. The Role of Digital Technologies During Relationship Breakdowns. In *Proceedings of the 19th ACM Conference on Computer-Supported Cooperative Work & Social Computing* (2016-02-27) *(CSCW '16)*. Association for Computing Machinery, 371–382. https://doi.org/10.1145/2818048.2819925

[74] Robert Moskovitch, Clint Feher, Arik Messerman, Niklas Kirschnick, Tarik Mustafic, Ahmet Camtepe, Bernhard Lohlein, Ulrich Heister, Sebastian Moller, Lior Rokach, et al. 2009. Identity Theft, Computers and Behavioral Biometrics. In *2009 IEEE International Conference on Intelligence and Security Informatics*. IEEE, 155–160. https://doi.org/10.1109/ISI.2009.5137288

[75] Preksha Nema, Pauline Anthonysamy, Nina Taft, and Sai Teja Peddinti. 2022. Analyzing User Perspectives on Mobile App Privacy at Scale. In *Proceedings of the 44th International Conference on Software Engineering*. 112–124. https://doi.org/10.1145/3510003.3510079

[76] Annie L Nguyen, Laura Mosqueda, Nikki Windisch, Gali Weissberger, Jenna Axelrod, and S Duke Han. 2021. Perceived Types, Causes, and Consequences of Financial Exploitation: Narratives from Older Adults. *The Journals of Gerontology: Series B* 76, 5 (2021), 996–1004. https://doi.org/10.1093/geronb/gbab010

[77] Hyanghee Park and Joonhwan Lee. 2020. Can a Conversational Agent Lower Sexual Violence Victims' Burden of Self-Disclosure?. In *Extended Abstracts of the 2020 CHI Conference on Human Factors in Computing Systems* (2020-04-25) *(CHI EA '20)*. Association for Computing Machinery, 1–8. https://doi.org/10.1145/3334480.3383050

[78] Christopher L Peterson. 2016. Consumer Financial Protection Bureau Law Enforcement: An Empirical Review. *Tulane Law Review* 90, 5, Article 1057 (2016). https://www.tulanelawreview.org/pub/vol90/consumer-financial-protection-bureau-law-enforcement-an-empirical-review

[79] Amanda Phelan, Deirdre O'Donnell, and Sandra McCarthy. 2021. Financial abuse of older people by third parties in banking institutions: a qualitative exploration. (2021), 1–22. https://doi.org/10.1017/S0144686X21001574 Publisher: Cambridge University Press.

[80] Judy L Postmus, Sara-Beth Plummer, Sarah McMahon, N Shaanta Murshid, and Mi Sung Kim. 2012. Understanding Economic Abuse in the Lives of Survivors. *Journal of Interpersonal Violence* 27, 3 (2012), 411–430. https://doi.org/10.1177/0886260511421669

[81] Judy L. Postmus and Amanda M. Stylianou. 2023. *Building Financial Empowerment for Survivors of Domestic Violence: A Path to Hope and Freedom*. Rutgers University Press. https://doi.org/10.36019/9781978804937

[82] Alexander Jason Ratner. 2019. *Accelerating machine learning with training data management*. Ph. D. Dissertation. Advisor(s) Ré, Christopher.

[83] Afsaneh Razi, Seunghyun Kim, Ashwaq Alsoubai, Gianluca Stringhini, Thamar Solorio, Munmun De Choudhury, and Pamela J. Wisniewski. 2021. A Human-Centered Systematic Literature Review of the Computational Approaches for Online Sexual Risk Detection. *Proceedings of the ACM on Human-Computer Interaction* 5, CSCW2 (Oct. 2021), 465:1–465:38. https://doi.org/10.1145/3479609

[84] Nils Reimers and Iryna Gurevych. 2019. "Sentence-BERT: Sentence Embeddings using Siamese BERT-Networks". In *Proceedings of the 2019 Conference on Empirical Methods in Natural Language Processing and the 9th International Joint Conference on Natural Language Processing (EMNLP-IJCNLP)*. Association for Computational Linguistics, 3982–3992. https://doi.org/10.18653/v1/D19-1410

[85] Jane Ritchie, Jane Lewis, Professor of Social Policy Jane Lewis, Carol McNaughton Nicholls, and Rachel Ormston. 2013. *Qualitative Research Practice: A Guide for Social Science Students and Researchers*. SAGE Publishing.

[86] Joni Salminen, Willemien Froneman, Soon-gyo Jung, Shammur Chowdhury, and Bernard J. Jansen. 2020. The Ethics of Data-Driven Personas. In *Extended Abstracts of the 2020 CHI Conference on Human Factors in Computing Systems (CHI EA '20)*. Association for Computing Machinery, New York, NY, USA, 1–9. https://doi.org/10.1145/3334480.3382790

[87] Devansh Saxena, Seh Young Moon, Dahlia Shehata, and Shion Guha. 2022. Unpacking Invisible Work Practices, Constraints, and Latent Power Relationships in Child Welfare through Casenote Analysis. In *CHI Conference on Human Factors in Computing Systems*. ACM, New Orleans LA USA, 1–22. https://doi.org/10.1145/3491102.3517742

[88] Hinrich Schütze, Christopher D Manning, and Prabhakar Raghavan. 2008. *Introduction to Information Retrieval*. Vol. 39. Cambridge University Press Cambridge.

[89] Ayesha Scott. 2023. Financial Abuse in a Banking Context: Why and How Financial Institutions can Respond. 50 (06 2023), 679–694. https://doi.org/10.1007/s10551-023-05460-7

[90] Nicola Sharp-Jeffs. 2015. *A Review of Research and Policy on Financial Abuse within Intimate Partner Relationships*. Technical Report. https://repository.londonmet.ac.uk/1482/1/Review-of-Research-and-Policy-on-Financial-Abuse.pdf

[91] Apoorva Singh, Rohan Bhatia, and Sriparna Saha. 2024. Complaint and Severity Identification From Online Financial Content. *IEEE Transactions on Computational Social Systems* 11, 1 (2024), 660–670. https://doi.org/10.1109/TCSS.2022.3215528

[92] Russell G Smith. 2000. Fraud and Financial Abuse of Older Persons. *Current Issues in Criminal Justice* 11, 3 (2000), 273–291. https://doi.org/10.1080/10345329.2000.12036165

[93] Eugene Soltes. 2018. *Fraud: An American History from Barnum to Madoff*. Princeton University Press, Princeton, NJ, USA.

[94] R Nathan Spreng, Jason Karlawish, and Daniel C Marson. 2016. Cognitive, Social, and Neural Determinants of Diminished Decision-making and Financial

Exploitation Risk in Aging and Dementia: A Review and New Model. *Journal of elder abuse & neglect* 28, 4-5 (2016), 320–344. https://doi.org/10.1080/08946566.2016.1237918

[95] Victoria Stace. 2021. Debt Collection in New Zealand: Considering the Case for Adoption of Guidelines, Modelled on Australian Debt Collection Guidelines, to Address Poor Conduct by Debt Collectors. *Victoria University of Wellington Legal Research Paper* 6 (2021). https://doi.org/10.2139/ssrn.3799718

[96] Jennifer E. Storey. 2020. Risk Factors for Elder Abuse and Neglect: A Review of the Literature. 50 (2020), 101339. https://doi.org/10.1016/j.avb.2019.101339

[97] Angelika Strohmayer, Julia Slupska, Rosanna Bellini, Lynne Coventry, Tara Hairston, and Adam Dodge. 2021. *Trust and Abusability Toolkit: Centering Safety in Human-Data Interactions*. Report. Northumbria University. https://nrl.northumbria.ac.uk/id/eprint/47508/ Num Pages: 60.

[98] Amanda M Stylianou. 2018. Economic Abuse Within Intimate Partner Violence: A Review of the Literature. *Violence and Victims* 33, 1 (2018), 3–22. https://doi.org/10.1891/0886-6708.VV-D-16-00112

[99] Surviving Economic Abuse. 2021. Economic Abuse Evidence Form. https://survivingeconomicabuse.org/what-we-do/economic-abuse-evidence-form/

[100] Surviving Economic Abuse. 2022. Conversation Kits for Banks. https://survivingeconomicabuse.org/wp-content/uploads/2021/01/Conversation-kit-for-banks-v7-KB.pdf

[101] The MetLife Mature Market Institute. 2011. The MetLife Study of Elder Financial Abuse Crimes of Occasion, Desperation, and Predation Against America's Elders. *Metlife Mature Market Institute* (June 2011). https://ltcombudsman.org/uploads/files/issues/mmi-elder-financial-abuse.pdf

[102] 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 Security Symposium (USENIX Security)* (Virtual Conference). USENIX Association, 1893–1909. https://www.usenix.org/conference/usenixsecurity20/presentation/tseng

[103] 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 ACM SIGCHI Conference on Human Factors in Computing Systems (CHI)*. Association for Computing Machinery (ACM), 1–17. https://doi.org/10.1145/3411764.3445589

[104] 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 2019 ACM SIGCHI Conference on Human Factors in Computing Systems (CHI)* (Glasgow, Scotland, UK, 2019-05). Association for Computing Machinery (ACM), 1–20. https://doi.org/10.1145/3491102.3502038

[105] Teun A. van Dijk. 1993. Principles of Critical Discourse Analysis. 4, 2 (1993), 249–283. https://doi.org/10.1177/0957926593004002006 Publisher: SAGE Publications Ltd.

[106] Jessica Vitak, Yuting Liao, Mega Subramaniam, and Priya Kumar. 2018. 'I Knew It Was Too Good to Be True": The Challenges Economically Disadvantaged Internet Users Face in Assessing Trustworthiness, Avoiding Scams, and Developing Self-Efficacy Online. 2 (2018), 176:1–176:25. Issue CSCW. https://doi.org/10.1145/3274445

[107] Noel Warford, Tara Matthews, Kaitlyn Yang, Omer Akgul, Sunny Consolvo, Patrick Gage Kelley, Nathan Malkin, Michelle L. Mazurek, Manya Sleeper, and Kurt Thomas. 2022. SoK: A Framework for Unifying At-Risk User Research. In *Proceedings of the 43rd IEEE Symposium on Security & Privacy (S&P)*. Institute of Electrical and Electronics Engineers (IEEE), 2344–2360. https://doi.org/10.1109/SP46214.2022.9833643

[108] Stacey Wood and Peter A. Lichtenberg. 2017. Financial Capacity and Financial Exploitation of Older Adults: Research Findings, Policy Recommendations and Clinical Implications. 40, 1 (2017), 3–13. https://doi.org/10.1080/07317115.2016.1203382

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

[110] Tomer Wullach, Amir Adler, and Einat Minkov. 2021. Fight Fire with Fire: Fine-tuning Hate Detectors using Large Samples of Generated Hate Speech. In *Findings of the Association for Computational Linguistics: EMNLP 2021*. Association for Computational Linguistics, 4699–4705. https://doi.org/10.18653/v1/2021.findings-emnlp.402

[111] Zheng Yao, Diyi Yang, John M. Levine, Carissa A. Low, Tenbroeck Smith, Haiyi Zhu, and Robert E. Kraut. 2021. Join, Stay or Go? A Closer Look at Members' Life Cycles in Online Health Communities. 5 (2021), 171:1–171:22. Issue CSCW1. https://doi.org/10.1145/3449245

[112] Zhuosheng Zhang, Aston Zhang, Mu Li, Hai Zhao, George Karypis, and Alex Smola. 2023. Multimodal Chain-of-Thought Reasoning in Language Models. (2023). arXiv:2302.00923

[113] 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 Security Symposium (USENIX Security)*. USENIX Association, 429–446. https://www.usenix.org/conference/usenixsecurity21/presentation/zou

[114] Yixin Zou, Kevin Roundy, Acar Tamersoy, Saurabh Shintre, Johann Roturier, and Florian Schaub. 2020. Examining the Adoption and Abandonment of Security, Privacy, and Identity Theft Protection Practices. In *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems* (2020-04-23) *(CHI '20)*. Association for Computing Machinery, 1–15. https://doi.org/10.1145/3313831.3376570

[115] Yixin Zou and Florian Schaub. 2018. Concern But No Action: Consumers' Reactions to the Equifax Data Breach. In *Extended Abstracts of the 2018 CHI Conference on Human Factors in Computing Systems* (2018-04-20) *(CHI EA '18)*. Association for Computing Machinery, 1–6. https://doi.org/10.1145/3170427.3188510

A DETERMINING INTIMATE PARTNER FINANCIAL ABUSE

	Intimate Partner Financial Abuse	Elder Financial Abuse	Financial Fraud	Financial Harassment
Adversary	An individual [13]	An individual [96]	An individual, group, or business entity [93]	A set of individuals (organization) [95]
Adversary goals	To financially benefit, to have power over the target, damage their reputation, or cause them harm [13, 81]	To financially benefit [33]	To gain financial advantage often via deception [26]	To financially benefit often via intimidation [78]
Pre-Existing Trust Relationship	Yes	Yes	No	No
Examples	A partner opens non-consensual financial accounts in a target's name	An adult child uses a target's credit cards without their permission	A stranger promises high returns for a target's investment, but instead steals it	A collection agency harasses a debt owners' families to collect debts

Table 3: Comparative matrix that characterizes each form of financial harm by the adversary involved, their goals, and the pre-existing trust between the adversary and target. The bottom row briefly describes examples of how financial assets and/or information are used in each form of harm.

As many different groups can experience financial harm, we first identify the specific socio-technical characteristics that differentiate financial abuse in IPV context from other predominant harms. IPV has specific socio-technical characteristics that differentiate it from other forms of financial harm, including fraud, harassment, and the abuse of older adults (elder financial abuse) [32, 72]. To begin with, IPV is characterized by a range of complex social behaviors that occur within intimate relationships, often by leveraging fine-grained details about the partner which may not occur across all forms of financial harms. Following an in-depth literature review, we delineate these via adversary type, adversarial goals, and the existence of trust in a relationship (Table 3).

Financial fraud is committed by an individual, or group of individuals (e.g., an organization) to extract funds from a target with whom they do not have a pre-existing interpersonal, trust relationship [3, 59, 92, 93]. Deception is often used to achieve the adversary's main goal, which is financial gain, such as selling a product under false pretenses (e.g., undisclosed interest rates). Conversely, *financial harassment* involves a group of individuals (organization) with whom the target does not have a pre-existing interpersonal, trusting relationship. Offender objectives are primarily financial, and deception may be used to achieve them, such as a debt collector making unsolicited calls to a debtor or their family and making unsubstantiated claims about the consequences of not paying the debt [95]. *Financial abuse* necessarily involves a single individual, the abuser, with whom the target has a pre-existing interpersonal, trust relationship. The abuser may seek to harm a target by exploiting, sabotaging, restricting, or monitoring a target's activity related to money. Two prevalent sub-types of this form of harm are the financial abuse of elders, and financial abuse of intimate partners. *Elder financial abuse* is a form of elder abuse targeting the financial assets of vulnerable elderly adults (often defined as aged 60 or higher), and is recognized at a federal level [33]. Elder financial abuse (EFA) is typically perpetrated by individuals with a pre-existing trust relationship with an elderly target (such as a caretaker-patient relationship friend, or family member [29, 32, 76, 101]). Elder financial abuse may not rely on deception, and often takes advantage of *cognitive decline* with age [30]. As cognitive decline and the accumulation of wealth and assets are both positively correlated with age [30, 52, 94], older adults are at an acute risk of being targeted by

financially-motivated adversaries. Finally, *intimate partner financial abuse* (IPFA) occurs in the context of a romantic partnership. An offender may have goals beyond financially benefiting themselves, such as a set of complex social aims around the misuse of power and control over a target [13, 44]. While IPFA can co-occur with EFA [96], we differentiate between these forms of abuse based on the adversary involved and the adversary's motivation to *harm* the target's financial health — a factor that would be counter-intuitive to the financial exploitation inherent to EFA [13].

B QUERY DESIGN AND KEYWORD SEARCH

intimate partner keywords
"spouse", "ex-spouse", "husband", "wife", "ex-husband", "ex-wife", "other half", "girlfriend", "boyfriend", "partner", "ex-boyfriend", "ex-girlfriend", "ex-partner", "fiance"

Table 4: Intimate partner keywords (*intimate partner keywords*) we used in our study.

financial abuse keywords
"Steal", "Stealing", "Stole", "Stolen", "Hid", "Hide", "Hidden", "Spy", "Spied", "Spying", "Surveil", "Surveilling", "Surveilled", "Control", "Controlled", "Controlling", "Harass", "Harassed", "Harassing", "Abuse", "Abusive", "Abusing", "Abused", "Exploit", "Exploitative", "Exploiting", "Exploited", "Harm", "Harmful", "Harmed", "Harming", "Hurt", "Hurting", "Upset", "Upsetting", "Sabotage", "Sabotaged", "Sabotaging", "domestic abuse", "fraudulent", "fraudulently", "abused", "abusive", "violence", "violent", "stole", "stolen", "stealing", "forced", "harassed", "unwanted", "coerced", "opened", "victim", "victims", "survivor", "survivors", "Batterer", "Batterers", "perpetrator", "perpetrators", "abuser", "abusers", "Batterer", "Batterers", "perpetrator", "perpetrators", "abuser", "abusers'

Table 5: A full list of financial abuse key words (*financial abuse keywords*) we used in our study.

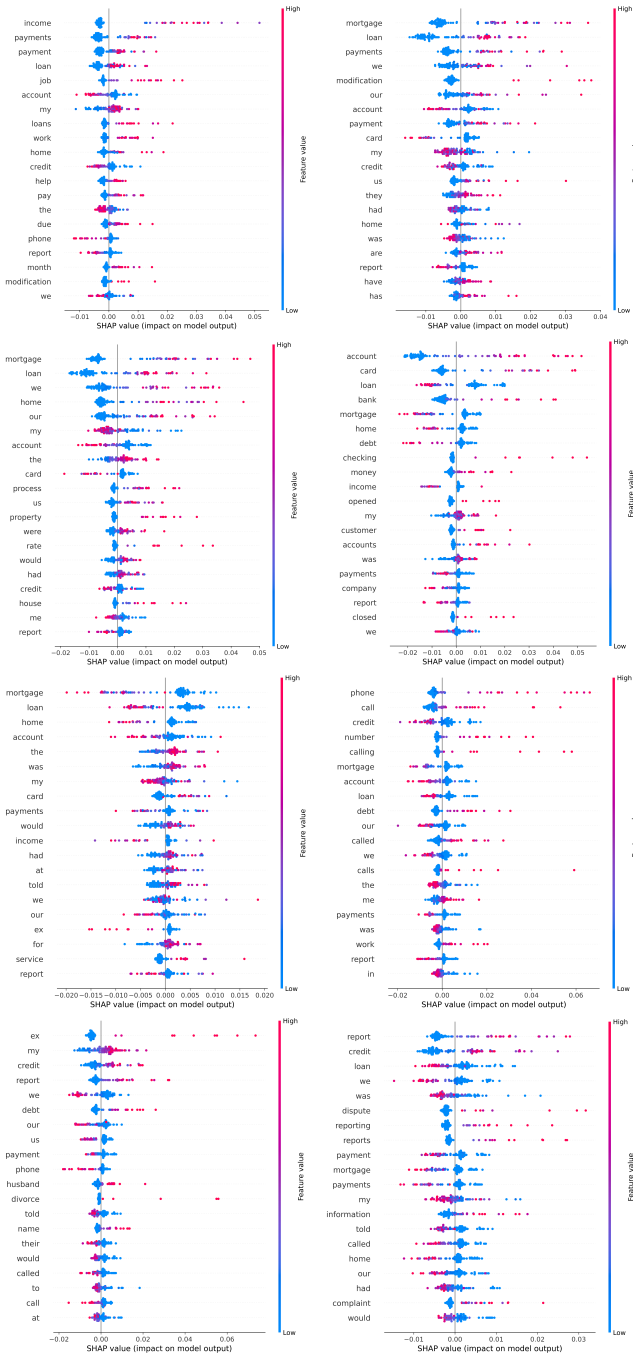## C CFPB SCHEMA AND WORKFLOW

Figure 7: SHAP scores for K-Clusters 0 to 7, numbered from top left to bottom right. The color bar corresponds to the raw values of the variables for each instance. If the variable for a particular word is high, it appears as a red dot, while low variable values appear as blue.

Data Field	Included
Date received	
Product	
Sub-product	*Optional*
Issue	
Sub-issue	
Consumer complaint narrative	*Optional*
Company public response	*Optional*
Company	
State	
ZIP code	
Tags	*Optional*
Consumer consent provided?	
Submitted via	
Date sent to company	
Company response to consumer	
Timely response?	
Customer disputed?	*Optional*
Complaint ID	

Table 6: Database schema for CFPB data.
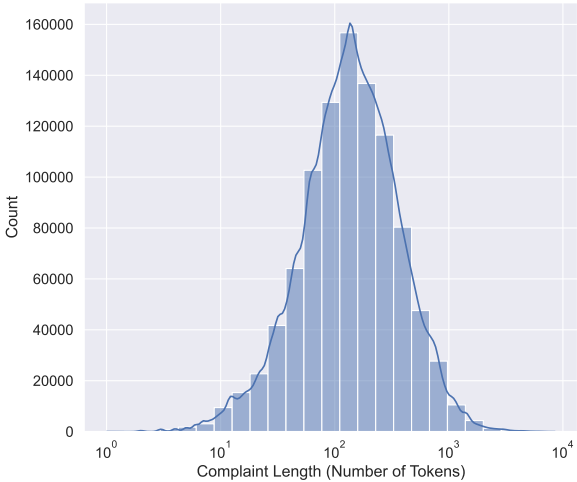
Figure 8: Distribution of complaint lengths within our CFPB Corpus

D TOOLS

Tool	Version
spacy	3.1.3
sentence-transformers	2.2.2
simcse	0.4
sklearn	1.1.2
shap	0.39.0

Table 7: The tools and versions used in the instantiation and execution of our workflow.

E   APPROACH TO QUALITATIVE CODING

Code category	Description of code category	Examples of low-level codes
Relationship Status	Relationship status described in the complaint	Partner, Ex-Partner, Deceased Partner
Financial Product/Service	Financial product(s) or service(s) contained in the complaint.	Loan: Car, Card: Credit, Account: [Unspecified]
Type of FA	Type of financial abuse described here	Forging C's signature, Restrict access to C's account
Point of Discovery	If otherwise unknown, the source of information on discovering FA	Online account: Bill due notice, Credit report
Method(s) of Resolution	Steps to try and address, resolve or minimize the impact of FA	Submitted complaint to FSP, Closed account
Barriers to Help	Barriers to deploying methods of resolution	Bank: "Lost" evidence, C: Lacks resources
Consequences of FA	The negative consequences of FA to complainant and/or other	Substantial financial loss; FSP/CB not responding
Intimate Threat	The presence of an intimate threat other than an intimate partner	Elder abuse, familial abuse, housemate abuse

Table 8: The eight high-level coding categories used in a framework analysis, alongside a code description and examples. FA denotes financial abuse, C denotes complainant, FSP denotes financial service provider and CB denotes credit bureau. Our full codebook can be found in our Appendix.
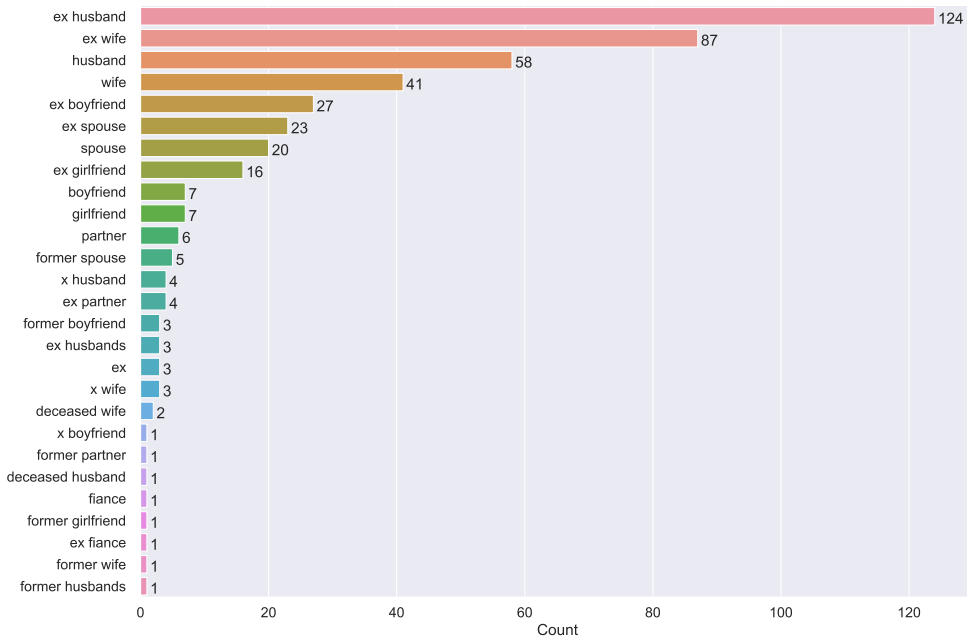
F   CORPUS GRAPHS

Figure 9: Total count of intimate partner related keywords in our corpus