

The Aftermath of Technology-Mediated Scams: Strengthening Older Adults' Efforts toward Redress

SAM ANKENBAUER and ROBIN BREWER, School of Information, Regents of the University of Michigan, Ann Arbor, Michigan, USA

Technology-mediated scams are a pervasive and enduring form of digital harm affecting older adults. While prior research has largely emphasized prevention, awareness, and risk perception, comparatively little attention has been paid to what follows after a scam occurs. Conceptualizing the scam as an unfolding event, we argue that each stage of the scam—before, during, and after—is shaped by distinct sociotechnical arrangements and relational dynamics that demand tailored forms of analysis and intervention. Through a multi-method study, we examine the during and after, paying specific attention to the post-scam, during which older adults navigate the affective, social, and material aftermath of scams. In doing so, we extend HCI's engagement with digital harm by articulating the post-scam as a critical site of coordination, redress, and justice-seeking, offering new directions for research and intervention.

CCS Concepts: • **Social and professional topics** → **Computer supported cooperative work**; *Computer crime*; *Seniors*; • **Human-centered computing** → *Collaborative and social computing*;

Additional Key Words and Phrases: Scams, Digital Harm, Older Adults, Affect, Redress, Resonance, Justice

ACM Reference format:

Sam Ankenbauer and Robin Brewer. 2026. The Aftermath of Technology-Mediated Scams: Strengthening Older Adults' Efforts toward Redress. *ACM Trans. Comput.-Hum. Interact.* 33, 3, Article 33 (June 2026), 41 pages. <https://doi.org/10.1145/3805036>

1 Introduction

While a substantial body of work addresses scams involving older adults, much of this literature concentrates on raising awareness, fostering digital literacy, and developing preventative interventions [21, 51, 64, 96]. Within this framing, scams are often approached as discrete “things” to be avoided—and interaction with a scam can be either explicitly or implicitly framed as an unfortunate outcome attributed to poor judgment, insufficient caution, or a lack of appropriate technological safeguards [72]. This framing narrows the scope of analysis to a single stage in the broader trajectory of a scam: the pre-scam stage, before the scam's execution. While this stage is undoubtedly important to mark the conditions under which a scam is or is not realized, it represents only one stage of a larger, temporally unfolding event.

This study builds on previous work in **Human-Computer Interaction (HCI)** and **Computer-Supported Cooperative Work (CSCW)** that examines temporality—an orientation that shifts

Authors' Contact Information: Sam Ankenbauer (corresponding author), School of Information, Regents of the University of Michigan, Ann Arbor, Michigan, USA; e-mail: samank@umich.edu; Robin Brewer, School of Information, Regents of the University of Michigan, Ann Arbor, Michigan, USA; e-mail: rnbrew@umich.edu.



This work is licensed under Creative Commons Attribution International 4.0.

© 2026 Copyright held by the owner/author(s).

ACM 1557-7325/2026/6-ART33

<https://doi.org/10.1145/3805036>

analytical focus from things, such as devices or platforms, to unfolding events, such as situated processes, interactions, and experiences shaped across time [115, p. 264]. From this perspective, scams unfold through distinct yet interrelated stages: the *pre-scam* conditions of possibility that render a scam possible, the execution of the *scam* itself, and the *post-scam* in which individuals reckon with the scam’s affective, social, and material consequences. In this research, we focus on the latter two stages, with particular attention to the under-researched work of post-scam *redress*. In doing so, we advocate for a more holistic response to scams—one that complements ongoing efforts to raise awareness, foster digital literacy, and implement preventative measures with sustained attention to post-scam life. In doing this work, we ask the following **research questions (RQs)**:

- *RQ1*: How do older adults experience the affective, social, and material impacts of scams?
- *RQ2*: How do older adults make sense of the post-scam and its ongoing impacts?
- *RQ3*: What practices do older adults undertake in the post-scam to address these impacts?

To investigate these questions, we conducted a multi-method study with older adults (aged 65+) who had recently endured a scam.¹ Our study combined a survey, semi-structured interview, and diary study to examine the nature of the scams encountered and their longer-term impacts. We focus in particular on two post-scam phenomena: *resonance* and *redress*. Resonance captures the ongoing affective, social, and material impacts that extend beyond the scam itself. Redress refers to the practices older adults undertake in response to these impacts. In doing so, we show how older adults process, navigate, and attempt to recover from scams. In short, our study reveals how older adult participants *feel*, what they *need*, and what *practices* they undertake in the aftermath of a scam, amid structural, technological, and institutional constraints.

This article makes two primary contributions. First, we contribute an empirically grounded reframing of scams as temporally unfolding events with lasting consequences rather than discrete things or moments of vulnerability and deception. By amplifying the lived experiences of older adults—a group described as underrepresented in privacy and security research [51]—we surface how scams unfold affectively, socially, and materially over time. Our findings contribute qualitative insights to a body of literature that has largely relied on surveys [21, 64, 75] or secondary analyses of existing data [10] and build on HCI’s emphasis on situated practice [27] and interest in unfolding events [115]. Second, we extend HCI’s conceptual and ethical understanding of technology-mediated scams by identifying the post-scam as a distinct and critical stage of inquiry. We draw attention to the ongoing ways redress and justice are negotiated in everyday life. In doing so, we position the post-scam as a site for research, design, and ethical reflection—one that challenges ageist assumptions, foregrounds the moral and infrastructural conditions of trust, and calls for equitable, transparent systems of redress that respond to the lived realities of older adults.

2 Related Work

2.1 Scams and Older Adults

We use the term “scam” to refer to a deliberately deceptive act intended to take away something of value, and “older adult” to refer to individuals aged 65 and above. We use the age 65 as an older adult benchmark as it is commonly used by the U.S. federal government to delineate age-based eligibility for programs like Medicare. While we discuss scams throughout this article with these definitions in mind, the term “scam” can be complicated.²

¹We define “endured” as having experienced a scam that came to “completion”—resulting in the theft of identity, personal information, or money.

²It should be noted that “older adult” can be complicated as well—for instance, the U.S. Department of Justice uses the term “elderly” to describe any person 60 years or older.

The overarching issue of what is known as “elder financial exploitation” can be divided into two categories: elder financial abuse and elder financial fraud and scams. Elder financial abuse “occurs when an older adult’s resources are improperly or illegally used by a person in a relationship involving an expectation of trust, such as a family member, friend, home care aid, or someone else who is entrusted to protect the older adult’s interests or care” [21, p. 14]. This is in contrast to elder financial fraud and scams, which have been defined by the Centers for Disease Control and Prevention as, “Deception carried out for the purpose of achieving personal gain while causing injury to another party” [57, p. 35]. The distinction, then, is that of trust and relationship—elder financial abuse is targeted financial exploitation by someone known to the older adult, while elder financial fraud and scams are financial exploitation by a party unknown to the older adult. According to Burnes et al., “To date, our knowledge about the prevalence of elder financial exploitation is mostly limited to the category of elder financial abuse. Little is known about the other major category” [21, p. 14]. Existing research often collapses these categories, a gap that limits our understanding of how these different forms emerge and unfold. We aim to fill this gap by examining elder financial fraud and scams, foregrounding the lived experiences of older adults and the sociotechnical conditions that shape their encounters.

In the past 2 years, three out of four older adults (75%) reported encountering at least one scam attempt through digital or traditional communication channels such as phone, text, e-mail, or mail [75]. Additionally, 3 in 10 older adults (30%) reported enduring compromised credit cards or bank accounts, hacked online accounts, stolen funds, or identity theft [75]. These numbers may be higher due to issues of self-reporting such as embarrassment, the lack of reporting from particularly vulnerable populations, and a lack of specificity on what “counts” as a scam or instance of fraud [10, 21, 99]. Additionally, in a review of 12 studies, Burnes et al. note that a low response rate in several studies may be due to “victims who have become cautious of participating in a process involving the provision of personal information” [38, p. 19]. Put another way, it may be difficult to collect information on the scammed due to their abundance of caution post-scam. It is also important to note that previous research suggests older adults are not more susceptible to fraud or scams [99] but are a specifically targeted group differentiated by “tailored fraud-scam schemes” [21, p. 14]. These demographic-specific components of elder financial fraud and scams have led to work by policymakers [67], law enforcement [37, 44], and consumer protection agencies [35, 46] that focuses on this area and, in particular, the pre-scam’s conditions of possibility.

2.2 Stages of a Scam

2.2.1 The Pre-Scam’s Conditions of Possibility. The pre-scam can be understood as the enabling conditions that render a scam possible. This stage unfolds prior to any direct contact from a scammer and encompasses the individual, social, technological, and structural circumstances that together configure potential vulnerability and exposure. At the individual level, for example, heightened social isolation may increase receptivity to a scam (e.g., [22]), while a compromised medical record in a data breach may supply scammers with personally identifying details to build credibility (e.g., [2]). From the scammer’s perspective, the pre-scam stage may involve preparatory activities like setting up fraudulent infrastructures such as spoofed web sites. Technological developments have expanded the range and sophistication of possible scams, including the widespread availability of tools such as generative AI, which can simulate convincing interactions, and voice over internet protocol systems that allow scammers to spoof local area codes [104, p. 5]. Structurally, insufficient consumer protections or exploitable regulatory frameworks—such as provisions in U.S. Banking Regulation CC, which governs the timing of fund availability after deposit and can enable scammers to exploit access to funds before detection—can expand the potential window of opportunity for future scams [30]. Taken together, these circumstances form the enabling environment, shaping

the possibilities of the scam and the stages that follow. The pre-scam stage ends when contact is made or interaction is initiated—when the scam shifts from a latent possibility to an active event.

Within the pre-scam stage, existing research has primarily focused on individual-level factors, often with the explicit aim of informing prevention efforts (e.g., [51, 104]). This body of work seeks to identify the characteristics that may render older adults more susceptible to scams or more likely to be targeted by scammers. Frequently cited factors include social isolation and loneliness (e.g., [23, 85]), limited digital literacy and technological proficiency (e.g., [21, 73, 101]), absence of a guardian (e.g., [22]), cognitive decline (e.g., [22, 59, 70]), accumulated or perceived wealth (e.g., [22, 54, 64]), and a generally trusting or prosocial disposition (e.g., [43, 59]). Collectively, these studies frame scam susceptibility as a function of individual vulnerability, often to motivate interventions designed to “teach older adults how to be safer online (i.e., less suitable victims)” [104, p. 1]. Pre-scam research interventions largely focus on prevention through education and skills-building aimed at improving older adults’ digital literacy and ability to identify scams [16, 53, 86]. These can take the form of interactive training programs to game-based interventions that build confidence and fraud-prevention self-efficacy [26, 28, 88]. Complementary community-based strategies—such as outreach campaigns, intergenerational programs, and embedding anti-scam messaging within trusted networks—have been shown to increase recognition and prevention [25, 86].

2.2.2 The Scam’s Enactment. The scam stage begins with the first meaningful interaction initiated by the scammer, when the older adult is drawn into the scam itself: from the initial point of contact, through manipulation over time, to the mechanisms that enable the transfer of money, identity, information, or artifact. Manipulative practices in this stage operate across both social and technical dimensions, including emotional appeals, impersonation of trusted entities, the imposition of artificial time constraints, the creation of manufactured dependence, and the implementation of hostile interfaces that have been designed to look authentic and keep the older adult engaged [32]. The structural conditions of this stage also matter: minimal friction in financial and data-transfer systems enables funds or sensitive information to move almost instantaneously, leaving little opportunity for detection or reversal [109]. Cryptocurrency infrastructure, for instance, further complicates the scam stage by obscuring transactional trails, making recovery nearly impossible once the transfer is complete, with Bitcoin ATMs reducing the barrier to entry [117]. The scam stage ends when the older adult recognizes the scam, the scammer acquires whatever they were after, or the relationship is severed.

Within the scam stage, research has primarily focused on uncovering the mechanisms of persuasion and deception that sustain scam interactions. Studies analyze scammers’ psychological and technological techniques, such as appeals to authority, urgency, or trust [32, 64, 83]. This corpus also analyzes the linguistic patterns characteristic of scams, aiming to identify recurring features of scams and their calls to action [4, 81]. Such work can draw on a range of materials, including primary scam artifacts such as phishing e-mails [4] and the interfaces utilized in scams [120], as well as retrospective accounts collected from individuals who have experienced scams [10]. Interventions have explored real-time disruption mechanisms, including fraud detection algorithms, scam-blocking systems, and systems to interrupt potential scam conversations, which can each be effective in halting scams in progress [25, 92, 122]. For instance, Zhai et al. [122] highlight the role of disengagement—the act of deliberately stepping away from an urgent situation—as a practical in-scam intervention, when combating deepfake-driven scams. Here, prompts could help older adults reassess the scam situation and inform more deliberate decision-making practices. This line of research emphasizes the value of reintroducing friction into digitally mediated interactions. Research has also highlighted the importance of evidence collection in scam cases, suggesting

opportunities for interventions designed to facilitate and streamline the process of documenting scams [26].

As such, while prior work has examined the pre-scam and scam stages—from the conditions that render scams possible to the manipulative practices that sustain them—far less is known about what happens after a scam concludes. Our research extends this trajectory by examining the post-scam: the period in which older adults navigate the affective, social, and material consequences of a scam. In doing so, we address an underexplored domain within the already limited scholarship on elder financial fraud and scams, foregrounding how older adults pursue redress within fragmented, stigmatizing, and institutionally constrained environments.

3 Methodology

This study reports on findings from a survey, semi-structured interview, and diary study. Below, we unpack our recruitment process, study methodology, data analysis, and a statement about the ethical considerations of the work, informed by previous literature [113]. This study was approved by our university's institutional review board.

3.1 Recruitment

We recruited older adults (aged 65+) who had recently endured a scam within 3–4 weeks of completing the initial survey. Recruitment combined online and offline approaches, reflecting prior findings that some older adults disengage from digital spaces following a scam [41, 51]. Recruitment took place across five neighboring communities in a Midwestern U.S. state, selected based on the first author's familiarity with local support systems and institutional actors, which enabled more responsive post-scam support. This place-based focus shaped the study demographics, with most participants identifying as white, reflecting the broader composition of these communities. To engage a cross-section of older adults within this context, we distributed flyers and newsletter announcements through libraries, senior centers, and community organizations; partnered with a local center serving Black older adults; used a university health and wellness research registry; and posted calls on Nextdoor, a hyperlocal platform with high use among adults [6, 7].

We structured compensation for participation in sections, offering participants up to \$90 for full participation. Participants who met our criteria and completed the survey received \$10. Those who completed our semi-structured interview received an additional \$10. Consistent with previous research on diary studies and participant retention [65], we offered compensation in stages to incentivize continued participation. Since the diary study took place over 1 week with interval-based entries, each diary entry (or day in the diary study) paid \$10. Given that each diary study took around 30 min to an hour, this rate aligned with the minimum wage in our state. Participants who completed all stages received a total of \$90.

3.2 Survey

We designed the survey as both a data collection instrument and a screening tool to identify potential participants for follow-up interviews and the diary study. Hosted on Qualtrics, an online survey platform [95], the survey included 1 consent question, 11 questions related to scams, 4 demographic questions, a request for continued participation, and a text-entry box for participants to provide their first name and preferred method of contact if they desired compensation and further involvement in the study. This format allowed us to gather valuable contextual data, understand participants' recent scam experiences, and assess their eligibility and willingness for continued participation. Prior to full deployment, we piloted the survey with three individuals who provided feedback on wording and survey flow. These pilot sessions averaged 9.5 min and were used exclusively for refinement; their data were not included in the final analysis.

Table 1. Participant Summary with Asterisk Denoting Diary Participation

Pseudonym	Gender	Race/Ethnicity	Age	Educational Background	Medium of Scam
James*	Male	White	70	4-year undergraduate	e-mail
Robert*	Male	White	71	2-year associate's	SMS
Mary	Female	White	71	4-year undergraduate	SMS
Linda*	Female	White	74	Graduate school	SMS
John*	Male	White	71	Some college/technical school	Phone
Charles	Male	White	67	4-year undergraduate	Web site
Kenneth*	Male	White	69	4-year undergraduate	Pop-up
Deborah*	Female	White	69	2-year associate's	Website
Ronald	Male	White	67	Graduate school	Web site
Susan*	Female	White	70	High school graduate	SMS
Nancy*	Female	White	71	Two-year associate's	Web site
Thomas*	Male	White	72	Four-year undergraduate	Phone
Donna*	Female	Black	72	Graduate school	SMS
Cynthia	Female	Asian/Pacific Islander	79	Graduate school	Pop-up
Pamela	Female	Black	68	Some college/technical school	SMS

In total, 44 participants consented and completed the survey. In one instance, the first author administered the survey by phone, as requested by the participant. Of the 44 respondents, 18 reported enduring a scam within the past 3–4 weeks *and* indicated willingness to participate further. Of those 18, 15 scheduled a follow-up interview with the first author. These 15 participants are listed in Table 1, with pseudonyms randomly assigned based on popular U.S. names from their birth year. Survey data from all 44 participants were included in our broader analysis and findings; full survey results are included in Appendix A. To compensate participants, we followed ethn.io's UX research incentive calculator [42], which recommends approximately \$5 for a 10-min survey. However, given the sensitivity of the topic and the distinct needs of an at-risk population [12], we increased this amount to better acknowledge participants' time and emotional labor.

3.3 Interviews

We interviewed participants to gather first-hand accounts of their experiences with scams and reflections on post-scam practices. Each interview featured five sections, with 1–10 questions in each. The sections were: "Definitions" (to understand what participants consider "scams"), "Encounters" (to explore participants' experiences with scams, such as: "How do you take precautions against scams?"), "Endurance" (to discuss participants' personal endurance of scams, such as: "Having undergone this experience, what is it that you wanted to happen next?"), "Community" (to identify the family, friend, online, corporate, and government resources participants used), and "Other" ("Is there anything else you'd like to add that I haven't touched on?"). We also used the interview time to provide materials and instructions for the diary study, set expectations for the diary study portion of the research, and ask if participants had any specific accessibility or modality requests (for instance, having the diary pages printed and sent to their home). We audio recorded and transcribed the interviews, which lasted an average of 52 min. After the diary study, we conducted an additional follow-up exit interview. During this session, the first author asked participants if they had any further questions, needed additional information, or required further assistance. During this exit interview, we tried to support participants in their redress practices, identifying resources for them that may support their unique needs post-scam.

3.4 Diary Study

Diary studies allow researchers to examine everyday events over time (across short or long durations), focusing on emotional and contextual details surrounding a given phenomenon [61]. Through a diary study, one is able to uncover social settings and actors, feelings, and day-to-day events that might otherwise be forgotten in an interview. Thus, we thought it would be an effective method to contextualize interview data. We asked participants to respond daily over the course of 1 week to a diary prompt. We used an “interval-based” style, which is common in diary studies, and asked participants to reflect once a day on four prompts [61]. These prompts aligned with our RQs: emotion/affect (“In general, how do you feel today?”), material and affective redress (“How did you attempt to remedy your scam experience today? What was the outcome of that attempt?”), and support (“Have you contacted anyone today regarding your recently endured scam, or did anyone mention it to you? Why or why not? How did that go?”). Additionally, we provided a free space for participants to share other thoughts (“What other thoughts do you have, concerning scams today? Feel free to list those thoughts below—or any other general thoughts or ideas you have today”). The free-text space is commonly used in diary studies to capture participant-led musings that help shape and structure the work [65].

We gave participants the option to complete the diaries in their preferred modality. Some preferred a digital copy of all the diaries, which they downloaded, completed, and e-mailed back to the first author. Others chose to print out the diaries and hand-write their entries, which they either scanned and e-mailed, mailed, or returned in person. In one case, a participant asked the first author to e-mail her the diary prompts each day, so she wouldn’t forget, and she responded to the e-mail with her diary entry. We also informed participants that they could attach or e-mail any ephemera related to scams that might help with the diary process, as has been discussed in other diary study work [60]. Many participants sent artifacts, including newspaper clippings about scams, envelopes and fake checks from scammers, senior center newsletters, screenshots from scam attempts, and, in one case, chat transcripts between the participant and their scammer. We asked participants to anonymize these materials, and if they didn’t, the first author anonymized them digitally. Of the 15 participants interviewed, 10 completed the diary study phase.

3.5 Analysis

As per our consent form, we audio-recorded each interview and, after removing names, transcribed them using Otter.AI, an automated transcription tool. To conduct thematic analysis [18, 90], we began with familiarization: reading through transcripts, highlighting significant passages, memoing, and summarizing the scams that participants endured and the redress that followed. As we conducted additional interviews concurrently, this iterative process informed updates to our interview protocol and deepened our understanding of scams and redress practices. Highlighted excerpts served as the basis for initial codes.

This early analysis phase was inductively driven, aimed at identifying patterns grounded in participants’ language and situated experience [47]. After reviewing several transcripts, we critically refined the codes and developed a codebook, which included each code, its abbreviation (e.g., “LOS” for “Level of sophistication”), a definition, and sample excerpts. Though the initial stages were inductive, later phases incorporated deductive structuring to group codes into larger thematic categories. This hybrid approach allowed us to remain grounded in the data while bringing conceptual clarity to themes [17]. Two researchers were involved in the coding process. The first author completed the initial coding and codebook creation. The second author independently reviewed and discussed a subset of the coded work, contributing to code refinement and

clarifying interpretations through analytic memoing. We resolved discrepancies through discussion, consistent with interpretivist approaches to qualitative research [11, 17].

With this codebook, the first author applied the same codebook to a sample of diary entries to conduct a secondary review and ensure its relevance. During this review, we remained open to inductive additions that reflected the diary's introspective and temporally structured nature—new codebook entries were added and retroactively integrated across the transcribed interviews to maintain consistency. With the finalized codebook, we fully coded all interview transcripts. In the findings section, we present a focused set of themes most relevant to our RQs and theoretical commitments: specifically, the temporal stages of scams and the post-scam's resonance and redress. We chose to highlight these themes because they reflect the most conceptually rich, recurrent, and underexplored aspects of participants' experiences—offering insight into how older adults endure, process, and respond to scams over time.

3.6 Ethical Considerations

We approached this study with deep ethical consideration, drawing on a growing body of work that emphasizes compassion, care, and responsibility in research with at-risk populations [12]. This work concerns “at-risk users” and the importance of centering the participant, conducting research with compassion, considering potential harms of the research, making sure the research does not add additional harms in an already sensitive situation, and advocating for the well-being of participants. Our approach was inspired by work in community gerontology that advocates an “action orientation,” in which researchers take an active role in fostering individual- and community-level change to “facilitate more optimal experiences of aging” [56, p. 804]. We were also influenced by the arts- and community-based participatory research of Lu et al., which is marked by a distinctly ethical and compassionate orientation (see [78]).

In keeping with this corpus of work, we attempted to minimize potential harm and support our participants throughout the research process. For instance, we reminded participants that they could skip questions, drop out at any time, restrict personal information, discourage certain forms of self-disclosure, and use pseudonyms [12, p. 9]. The first author provided “direct, individual assistance” [12, p. 11] to participants who were struggling to redress their scams after the research was conducted. This included helping participants navigate scam recovery resources, assessing which services they had already attempted, and identifying new ones—ranging from local institutions and nonprofit organizations to state programs. In some cases, the first author also supported participants in scam prevention, such as checking the legitimacy of web sites, checks, or unsolicited communications after the formal research period had ended.

The language used to describe scams and older adults shapes public perception and lived experience. As such, it is crucial to critically examine and reframe common terminology. For example, the *Journal of the American Geriatrics Society* discourages stigmatizing terms and warlike metaphors—such as “struggle” or “battle” in favor of language that affirms the capacities and contributions of older adults [80]. Similar concerns apply to the term “victim,” commonly used in scam discourse. While this term, rooted in criminal justice, rightly signals harm and the need for accountability [84], it also carries disempowering connotations—suggesting passivity, fragility, or poor judgment [52]. Such framing can reinforce victim-blaming, discourage reporting, and exacerbate shame or isolation [54]. To challenge these implications, we use the term “endure,” referring to individuals as having “endured a scam” rather than as “victims of a scam.” This framing acknowledges the experience of harm without prefiguring how individuals respond to it or suggesting passivity.

Table 2. Comparison of Three Portraits

	James	Cynthia	Ronald
Scam Type	Overpayment and Identity Theft	Tech Support and Crypto	Investment and Pig Butchering
Technology	Computer, Online Marketplace, Physical Mail	Computer, Phone, Crypto	Phone, WhatsApp, Zoom, Online Marketplace, Crypto
Inciting Action	Marketplace private message from supposed buyer	Falsified security breach warning on computer	Phishing through supposedly accidental text message
Length	Scam itself lasted over a week, as check went through mail and ID used online	Scam itself took several hours, from pop-up to Crypto ATM used	Scam itself lasted months, over daily communications

4 Findings

4.1 The Scam: Older Adults' Endurance of Scams

Our findings section draws from all three data sources in our study: a survey ($N = 44$), in-depth interviews ($N = 15$), and week-long diaries with a subset of participants ($N = 10$). According to our survey data, scams were a recurring feature of everyday life for many participants. Over half of our respondents ($N = 24$) reported encountering scams more than once per week, while the same number of respondents ($N = 24$) indicated they had been successfully targeted and endured two to three scams or more over the course of their lives. When asked to reflect on their most recent scam, respondents most commonly encountered the scam through digital technologies. These included scams through text messages ($N = 10$), e-mail ($N = 10$), web sites ($N = 6$), digital advertisements ($N = 3$), and computer pop-up messages ($N = 3$). Such findings suggest that for this group of older adults, scams were not rare incidents, but rather recurrent experiences embedded in technology-mediated interactions. To situate this broader pattern in lived experience, we present narrative portraits of three older adults who recently experienced a scam [116]. Through these portraits, we give specificity and texture to the broader phenomenon of scams. Each portrait highlights the sequence of actions taken during the scam encounter, the decision-making processes involved, and the technologies through which the scam was mediated. In doing so, we foreground scams not merely as abstract risks or technical problems but as lived experiences shaped by sociotechnical conditions. These individual accounts offer insight into the heterogeneity of scam events—demonstrating how they vary in form, content, and consequence—before we transition into an analysis of the post-scam landscape. The post-scam landscape necessarily depends on the individual scam that is endured. A comparative summary of these three scam incidents is provided in Table 2.

James and Selling Motorcycles Online. James, a 70-year-old man, was no stranger to scams. During our conversation, he reflected, “I’ve probably been scammed six to eight times—and I regard myself as cautious. I’m one of those guys that’s gonna say, ‘You’re not gonna fool me.’” Despite his vigilance, he had recently found himself ensnared in another scam while attempting to sell his motorcycles. Initially, he considered using Facebook Marketplace and Craigslist but ultimately opted for CycleTrader, a specialized platform where users can sell, trade, and buy motorcycles nationally and locally. Buyers can communicate with sellers with one click, in which an automated message is generated (“Is this 2025 Honda CRF 125F still available?”) and sent. CycleTrader is itself

part of the broader Trader Interactive network that collectively has 13 million monthly unique visitors.

Such a large platform paid off—the response to his post was immediate. “So, I get offers right away,” James recalled. “The unusual part of it is this: I get offers that exceed my asking price—and they want to buy the motorcycles sight unseen. So, a little flag went up, and I thought, we’ll see.” One particular buyer stood out, engaging in prolonged negotiations before mailing James a check featuring a Huntington Bank logo—\$7,000 over the agreed-upon price. When James questioned the overpayment in a message back to the buyer, the buyer insisted the extra funds were meant to blanket cover transportation costs, the exact amount to be settled later.

What James didn’t realize at the time was that he had become the target of an overpayment scam. These scams exploit banking procedures that allow deposited checks to appear as “cleared” before their legitimacy is fully verified. Banks within the U.S. follow Regulation CC that requires deposited funds to be readily available—between next business day and two to five business days, depending on the check’s amount. Regulation CC was designed specifically to ensure people have access to their money promptly but this promptness can be exploited. Scammers send counterfeit checks with excess funds, later fabricating a reason—such as shipping costs or an accounting mistake—to request a refund via wire transfer. By the time the bank detects the counterfeit check and retracts the funds from the bank account of the scammed, the scammer has already pocketed the excess funds and disappeared, leaving the seller at a financial loss and, in some cases, without their goods that had already been shipped in the meantime.

Fortunately, James’ prior encounters with scams made him wary. Instead of depositing the check, he took it directly to a local Huntington Bank branch, where staff confirmed it was fraudulent and forwarded it to their fraud department. Though relieved to have avoided a financial loss, his motorcycles were still unsold, and he had wasted time dealing with a scammer. But the situation soon took a more troubling turn: during his initial interactions with the buyer, James had sent a photograph of his driver’s license. “The guy who sent me the Huntington Bank check reversed all the questions I was asking, trying to figure out if I was legitimate,” James explained, “In a weak moment, he asked for my license—and guess what? I sent it to him.” Soon after, James received an unexpected text from a man in another US state:

The message said, “Are you James? Do you live on [street name]?” I said yes. Then he asked, “Have you been trying to buy my Honda vehicle?” I told him no. He said, “Well, this person has your license and is claiming to be you.”

When the man confronted the scammer, the scammer became defensive and belligerent, insisting they were James before disappearing. In light of this new information, James realized he had not only encountered an overpayment scam but also identity theft. The scammer was now using his personal information—including his name, address, and driver’s license—to pose as him in other fraudulent transactions. A few days later, a friend e-mailed James after stumbling upon James’ license while attempting to buy a motorcycle: “My Ohio buddy e-mailed me and said, ‘James, you’re being scammed, your license is out there.’” In our conversation, James remained uncertain about the full extent of the harm and was unsettled by the possibility that his identity might continue to be misused. “I don’t know what someone can do with your license other than trying to be an imposter,” he admitted, concerned about how his personal details might be facilitating further scams.

Cynthia and a Sudden Security Breach. Cynthia, a 79-year-old woman, was using her computer when an unexpected pop-up alert took over her screen. Designed to resemble a legitimate Windows security notification, with its Windows Protection shield and authoritative tone, the message warned of an urgent system breach. The pop-up disabled navigation on her browser, seemingly

freezing the screen and preventing Cynthia from navigating away, intensifying her sense of alarm. The alert displayed a toll-free number, urging her to call immediately to prevent further breaches.

Concerned, Cynthia dialed the number and was connected to a supposed Windows support technician. The technician, adopting the tone and language of a professional IT specialist, claimed that hackers had gained access to her computer and had drained portions of her bank account. Over the next hour, she spoke with multiple representatives, each reinforcing the severity of the breach. Unbeknownst to Cynthia, she had fallen victim to a tech support scam. These scams often begin with unclosable alerts that leverage fear and confusion to manipulate individuals into compliance with instructions. In her case, Cynthia was asked to call a provided number that took her to a call center, where scammers work in coordinated teams to assume various roles that reinforce an illusion of legitimacy—a team of technicians, working together to solve the individual’s issue. In doing so, the scammers gain access to personal data and coerce the individual into transferring money to secure their finances.

In Cynthia’s case, the scammers instructed her to withdraw thousands of dollars and deposit those funds into a cryptocurrency kiosk, to secure her finances. They provided precise details, including the location of her bank, the nearest Bitcoin ATM, and a QR code linked to their digital wallet. Exploiting her unfamiliarity with cryptocurrency transactions, they framed the deposit as a necessary security measure to protect her funds from unauthorized access. Cynthia later recalled, “They knew where the bank was, they knew there was a kiosk nearby. They even estimated how long it would take me to get there.” Following their step-by-step guidance, Cynthia went to her bank, took out requested amount, and went to the Bitcoin ATM. There, Cynthia selected “Buy Bitcoin,” scanned the Bitcoin wallet QR code from her phone, inserted her money, and confirmed her purchase—an intuitive process that mirrors traditional ATMs. When she attempted to call back the technicians for further confirmation, the call went straight to a generic voicemail that, eventually, was disconnected and the scammers were not heard from again. Reflecting on her experience, Cynthia remarked, “I was very impressed with the scammers. The way they threaded their stories and everything—I thought it was very good because, otherwise, I don’t think I would have been convinced.” Cynthia’s story underscores the technical sophistication and social engineering employed in tech support scams. By combining malicious web script, coordinated calls, and untraceable cryptocurrency transactions, Cynthia’s scammers constructed a high-pressure environment where she felt compelled to act without fully processing the situation. Afterwards, with only a phone number and no additional evidence to support her, Cynthia was unsure of what to do next.

Ronald and a Chance Text. Ronald, a 67-year-old man, received a wrong-number text: “The first text I got from her, she was inviting me to a party, a Christmas or New Year’s party. She realized she sent the text to the wrong number. And so things started from there.” As a naturally sociable person, Ronald responded in good faith, and what began as a simple wrong-number exchange evolved into a sustained digital friendship. The woman on the other end of his texts—a self-identified Japanese immigrant living in Los Angeles—seemed warm, engaging, and relatable. Their conversations initially revolved around shared interests in exercise and spirituality, gradually deepening over time into lengthy discussions about particular passages of the Bible. The exchanges moved from sporadic text messages to daily WhatsApp conversations, occasionally punctuated by Zoom calls. “Most of my communication was on chats with WhatsApp,” Ronald recalled. “Before I went to bed one night, I started printing [our chats] and ran out of paper with all the stuff that I had—I think I had over 600 pages, at least.”

In their daily conversations, the woman disclosed details of her background, claiming to manage a family business with her parents and uncle. The conversations remained casual and comforting but occasionally drifted into discussions of finance and investment until, eventually, she pivoted to

cryptocurrency trading, positioning herself as an experienced investor. Her pitch was direct, yet persuasive:

I am willing to help you. Let us get more wealth together. Do you know Crypto.com cryptocurrency exchange? (...) I have been investing in the cryptocurrency market for almost five years. Just follow the prompts to register for authentication. If you don't understand, you can send me the picture, and I can guide you.

Over the next 6 months, discussions about cryptocurrency became a regular fixture in their conversations. Ronald initially exercised caution, placing small test investments through Coinbase, where he saw modest returns. Encouraged by these initial successes, he increased his investments, soon funneling thousands of dollars into crypto trades under the woman's guidance. The woman urged Ronald to take bolder steps toward crypto wealth, leading him to leverage a home equity loan, injecting tens of thousands of dollars into what he believed was a promising investment opportunity. Their WhatsApp transcripts reveal increasing pressure, culminating in messages like: "You now only need to raise \$110,000 by the 20th to apply for new coins."

This deadline, however, was derailed by an intervention: Ronald's credit union flagged unusual transactions tied to his investments and contacted his wife. Confronted with the reality of his financial situation, Ronald sought advice from his financial advisor, ultimately realizing he had been ensnared in a pig butchering investment scam. This type of scam—cruelly named for the practice of fattening a pig before slaughter—operates over extended periods, relying on frequent communication and carefully cultivated trust to deceive victims. Its insidious nature lies in the asymmetry between scammer and scammed: perpetrators often operate internationally, leverage encrypted messaging platforms like WhatsApp and Signal, and guide individuals through reputable exchanges like Coinbase before transitioning them to fraudulent investment dashboards—this combination of cross-border operations, digital anonymity, and deceptive financial tactics leaves individuals with few meaningful avenues for recourse. Per Ronald:

What your study is trying to do, right, is [uncover] how we can deal with this going forward? Because it's obviously a big problem. And people are being taken for a lot of money. I mean, I know before this scam thing happened to me, my financial advisor told me I could retire and have enough money to live until 95 or 100. Now... well...

When our study began, Ronald was still trying to recover what he had lost. In looking at his chat transcripts, nearly 400,000 words exchanged over months, one can't help but scroll to the end of the transcripts. There, Ronald attempts to confront his scammer, "You always said you would help me. I am questioning whether you are a liar and I am very worried." The scammer replies: "I'm also questioning you because I don't know your situation (...) I don't want to do this, but I've been thinking a lot lately (...) Maybe you're just cheating me out of my money."

If scams are fundamentally extractive, the scam stage, then, begins at the point of contact and ends once the extraction of information, money, or identity is complete (as above). Yet for our participants, this moment marked only an inciting incident within a larger scam landscape. In practice, the boundaries of a scam are diffuse and difficult to pinpoint—instead they produce ongoing consequences that ripple through daily life. We refer to this period as the post-scam stage. It is shaped by two interrelated dynamics: resonance and redress. Resonance captures the affective, social, and material aftermath of a scam—what lingers after the scam stage itself—while redress refers to the practices individuals undertake to address these lingering effects in pursuit of closure or justice. Together, these dynamics organize our findings that follow.

4.2 The Post-Scam: Affective Resonance and Redress

In this section, we explore *affective resonance*—the emotional impacts that follow a scam—and *affective redress*, the strategies individuals employed to cope with and mitigate these emotional consequences over time.

4.2.1 Affective Resonance. According to our survey responses, the two most frequently selected responses to the question, “What has been the result of your being scammed?” were “Loss of Trust” (N = 25) and “Emotional Distress” (N = 19). A follow-up short-answer prompt, “How did you feel after being scammed?” further illuminated participants’ emotional landscapes in their own words: responses included, “broken-hearted,” “embarrassed,” “scared, anxious,” “depressed and discouraged,” and “I felt inferior, like I was stupid.” These responses point to the affective resonance of scam experiences.

Notably, despite scams being deliberate acts of deception, most participants in our interviews blamed themselves, interpreting the experience through shame and personal failure. James, for example, directed his harshest judgment inward—“I’m the idiot, the guy that walked in”—even as he expressed a begrudging empathy toward the scammer, remarking, “I just wish they had a real job.” In describing his post-scam frustration, Kenneth explicitly collapsed the distinction between the pejorative “gullible” and the virtue “trustworthy,” framing deception as a personal failure: “I felt really bad, because you think you’re a competent adult, and yet you’re hoodwinked or fooled by somebody who took advantage of your gullibility or your trustworthiness...” Susan, who had recently experienced her second relationship scam, described how self-blame surfaced alongside not only the pain of betrayal but also memories of intimacy and an imagined future:

I just felt stupid, because I knew better—I just knew better. And yet... not once, but twice. But the second time, it was just—we were just planning a whole life together. We were going to do this, and we were gonna go here, we were going to go to festivals, and just, I mean, he wasn’t promising the moon or anything, but just being a couple, you know?

Susan’s reflections reveal how affective resonance unfolds across time. While her immediate reaction was to blame herself, her retrospective narration also preserves the emotional significance of the relationship. The scam, in this way, operates as a hinge between the possibility of emotional connection and the experience of emotional distress—binding hope and harm together. Her reflection underscores the ongoing, unresolved nature of her feelings toward the scammer. This continual negotiation illustrates how the emotional impact of scams is not fixed but is shaped and reshaped over time. As we explore in the next section, this evolving emotional terrain prompts individuals to seek affective redress—efforts to process, reframe, and ultimately restore a sense of emotional stability.

4.2.2 Affective Redress. If affective resonance captures the emotional impacts that follow a scam, affective redress encompasses the practices through which individuals attempt to live with, process, and stabilize those emotions over time. Affective redress is an uneven process, often shaped by ongoing encounters with technology. We focus on two primary practices—cultivating self-compassion and managing feelings of safety—alongside two persistent challenges, emotional fatigue and lingering distrust, which frequently constrained not only emotional recovery but also participants’ capacity to pursue further forms of redress.

Self-Compassion and Emotional Fatigue. As discussed above, participants often internalized scams as personal failures, describing themselves as “stupid” and expressing shame. Over time, some participants worked to reframe these feelings by situating scams as widespread and systemic rather

than individual shortcomings. For James, whose confidence in digital interactions had been shaken, cultivating self-compassion became an important step toward affective redress:

I am ashamed for being stupid—it's a pride thing. But I've got to swallow my pride (...) I think most people now are sympathetic to other people who get scammed. And, my feeling about that is that they all know it could have happened to them. We're all on an equal plane, you know, and we're all... what, *capable* of being [scammed].

James' shift from internalized shame to shared vulnerability reframes the scam as a collective condition rather than an individual failure. Others, like John, found meaning-making practices such as journaling helpful for emotional processing. In his diary, John wrote:

[Scams] to me are (...) kind of an inevitable part of being in this world, so no reason to carry it around. This diary feels like part of healing the scar of that incident. Talking and writing about it seems to help put it in context.

Multiple participants described redirecting negative emotions into small acts of agency as a way of practicing self-compassion. Donna, for example, explained that writing letters to senators about scams helped her "feel better about [myself], like I'm doing something." Donna's advocacy allowed her to acknowledge the emotional impact of the scam while giving herself room to act and recover on her own terms.

However, efforts toward self-compassion were often entangled with emotional fatigue. Ongoing encounters with technology-mediated scams—such as repeated scam attempts or notifications of data breaches—reanimated feelings of exhaustion, helplessness, and self-doubt. Deborah documented her fatigue in her diary as she encountered a new Facebook scam. While she initially tried to let the experience not bother her, subsequent entries reflected growing resignation: "Trying to let it go. It is what it is. I have to be more cautious and quit doubting myself. (...) [What a] stupid world we live in!" After receiving four scam e-mails in one evening, which she linked to a data breach at her local hospital, she wrote, "I feel helpless, with no recourse to stop this." Deborah's experience shows how attempts at affective redress can be undermined by the continued presence of the conditions that caused harm, resulting in the feeling of moving one step forward and two steps back.

Managing Feelings of Safety and Lingering Distrust. Participants described an ongoing sense of digital vulnerability that persisted beyond the initial scam encounter. Even routine interactions were sometimes met with suspicion, as John explained: "I have more of a radar... A thought actually crossed my mind—no offense to you—but I thought, 'Is this [interview] a scam too?'" Such remarks show how scams eroded participants' sense of safety, influencing even routine interactions and benign exchanges.

To manage these feelings, participants adopted a range of technological practices aimed at restoring a sense of safety and control. These included installing antivirus software, updating passwords, enabling multi-factor authentication, blocking spam calls, and seeking help from local IT professionals. While these practices helped reduce immediate risk, they also functioned as affective strategies—ways of managing fear and regaining confidence. For instance, Robert reported feeling more secure after installing new antivirus software, while Thomas described how the robocall-blocking service Nomorobo eased his anxiety by filtering spam calls and messages.

Despite these efforts, participants emphasized that feelings of distrust often lingered. Kenneth captured this chronic vigilance in his diary: "Every day is a challenge. We have to be on guard every day." Such statements point to a recalibrated emotional baseline in which distrust becomes a default stance rather than a temporary response. James's diaries illustrate how this distrust was continually reinforced through ongoing encounters with scam-related information. He described

receiving a “Scam Alert” in the county newsletter, e-mails from an identity theft protection service, a PDF from the U.S. Treasury Financial Crimes Enforcement Network, and news articles about older adults targeted by scams. In one instance, James sent a photo attachment of personal mail, making sure to tape a piece of paper over his name and home address—a privacy tactic he picked up from the county newsletter. Despite his vigilance and knowledge, James expressed a growing disconnect between his efforts to safeguard his information and his ongoing experiences with scams. This dissonance prompted reflection on a deepening sense of distrust, one that persisted despite his precautions:

It’s my stupidity. I let down my guard, and I sent some of my personal information out there. So shame on me. (...) There’s an anonymity associated with the internet. And there’s a lot of bad out there and they’re coming to your e-mail address. And when I open up an e-mail, I don’t automatically suspect that this person is a bastard. I want to trust the e-mail I’m reading, you know? But if I trust it, I’m probably gonna get taken. So I don’t know... I’m kind of fighting [my] altruistic outlook with this anonymity that presides on the internet. You just don’t know when you’re going to get punched in the mouth.

James’s reflections highlight how managing feelings of safety involves more than technical fixes. While tools such as spam filters, antivirus software, and identity protection services can reduce exposure to scams, they do not resolve the underlying emotional disruption produced through repeated encounters with risk, warnings, and uncertainty. In James’s case, the erosion of confidence in his own judgment extended into broader hesitations about other people, illustrating how affective resonance can spill into social resonance and complicate efforts toward affective redress.

4.3 The Post-Scam: Social Resonance and Redress

In Section 4.3, we discuss *social resonance* as the lingering effects scams have on a participant’s social world—namely, the ways in which interpersonal relationships, routines of communication, and social trust are disrupted. For example, participants began to second-guess answering phone calls or had become reluctant to ask family or friends for help in the post-scam, fearing blame or judgment. We also introduce *social redress* as the practices aimed at addressing these social impacts as they occur over time.

4.3.1 Social Resonance. While the previous section focused on how scams affected participants’ self-perception and emotional well-being, here we examine how these experiences extended into the social sphere. Beyond shaping how participants felt about themselves, scams influenced how they approached others, altering social interactions, relationships, and trust. We refer to these effects as social resonance. Notably, social resonance often begins at home—frequently the site where the scam took place. Thomas reflected on the lingering presence of his scam in his daily life at home:

[Today,] my wife reflected back to me how the scam had sounded to her, me dealing with these idiots on the phone for over an hour, yelling and cursing. That really affected the household. It was really bad, getting pulled in. So it was an acute attack—a scam—that then reflected poorly on the world, on me, and on other people... so, it was quite something.

Thomas’ account shows how a scam resonates beyond the immediate interaction, shaping household dynamics and contributing to a broader sense of disillusionment with others. Participants further described how these relational effects emerged not only through others’ awareness of the scam but through the scam’s concealment, as decisions about whether to disclose introduced new

forms of distance within close relationships. Susan, for instance, chose not to tell her children about her recent scam, explaining that if they found out, “My kids probably would have me committed.”

Such nondisclosure reflected a broader orientation toward withdrawal. Participants often avoided sharing their experiences due to anticipated judgment and stigma. Robert, for example, explained that he kept his scam to himself to avoid being seen as foolish: “There’s a lot of judgments that can be made... ‘You should know better.’” As Robert’s account suggests, shame operated not only as an individual emotional response but as a socially produced barrier that constrained disclosure and redress. For older adults, this shame was exacerbated by ageist assumptions about cognitive decline, financial ineptitude, and lack of judgment. Kenneth articulated these concerns:

No man is an island, and we’re all vulnerable. I am a senior, and one thing that really is uncomfortable is that when you get to be my age, people think you’re incompetent, and they think you’re not able to take care of yourself. That’s the biggest fear, is when people take away your freedom, when they say, “you need to be institutionalized” or “you need somebody to take care of you” when in fact, I’m qualified, competent, and able to take care of myself. When you get to be this age, there’s more possibility of people trying to step on your toes.

Scams thus intersect with broader fears about aging and the erosion of autonomy. For participants, disclosing a scam can feel tantamount to relinquishing control and opening oneself up to questions of competency. This fear of being unjustly judged incapable—of both navigating digital environments and being independent—led some participants to refrain from discussing their scams socially, even with their closest family for fear of, as Susan put it, “being committed.” These dynamics shaped how participants attempted to repair social ties through social redress.

4.3.2 Social Redress. If we conceptualize social resonance as the social behaviors and dynamics that emerge in the wake of a scam, then social redress encompasses the practices through which individuals attempt to repair, renegotiate, and re-establish trust, connection, and social stability over time. Social redress involves not only the restoration of strained interpersonal ties, but also a forward-looking orientation toward collective vigilance and mutual care. Yet, these efforts are often shaped—and at times constrained—by the structural conditions of digital life, such as balancing the use and consolidation of one’s digital footprint or the systemic gaps older adults face when trying to report new scams.

Rebuilding Trust and Social Ties, and the Consolidation of Engagement. Social redress involved efforts to rebuild trust, renegotiate boundaries, and reconfigure everyday social and digital engagement. Many participants shared their experiences to make sense of the scam and counter feelings of isolation. Individuals who initially felt ashamed found that disclosing their experiences to trusted others helped reframe the scam as a common, systemic issue rather than a personal failure. Reflecting on conversations with friends, John wrote in his diary, “So many people have been scammed, it seems like there is a shared experience among us,” highlighting how disclosure helped normalize his experience and create a makeshift community.

Institutional actors also played a role in social redress by offering reassurance and validation. Thomas, who initially hesitated to contact Medicare after scammers impersonated the agency, described speaking with a Medicare representative as a turning point:

I think talking to you has helped, and talking through it with the Medicare fraud people helped. They said, “It’s not your fault. You didn’t do anything wrong.” Those words of assurance and support resonated a bit with me... I needed to hear that.

For Thomas, this interaction helped differentiate legitimate institutional support from fraudulent actors, allowing him to rebuild a degree of trust while reducing self-blame and distrust. Such

moments underscore how social redress often depended on supportive responses from others, including family members, peers, and frontline institutional staff.

However, social redress was not linear or uniform. While some participants sought renewed connection, others responded by narrowing their social and digital engagement as a protective strategy. These practices included avoiding phone calls from unknown numbers, limiting e-mail interactions, and relying only on familiar companies or platforms. John reflected on this shift, saying he had become “unfortunately, more jaded.” Thomas described refusing to answer calls unless he recognized the number, even when this meant missing recent calls from neighbors. Charles, who once described himself as an “open book,” explained that he now avoids unfamiliar platforms entirely, preferring established ones like Amazon. Robert similarly emphasized sticking with companies he already trusted, noting that he had become “leery of new or smaller [companies].”

This consolidation of engagement suggests that social redress does not necessarily lead to a full return to pre-scam behaviors; rather, it often results in a restructuring of trust that prioritizes known, vetted entities over new interactions. For these participants, social redress emerged not through re-engagement but through the careful curation of sociotechnical environments. However, while this curation can be beneficial, as when a potential scam is averted through stricter boundaries, it can also carry costs, such as missing a neighbor’s important call or, as some participants noted, checking health portals and other previously meaningful digital resources less frequently. In either case, social redress was shaped not only by the desire to reconnect but also by efforts to regain a sense of safety and control.

Strengthening Community Defenses and Inadequate Reporting Processes. Beyond individual efforts to rebuild trust and social ties, many participants understood social redress as a collective responsibility. Participants emphasized educating others, sharing experiential knowledge, and contributing to broader scam prevention efforts as ways of transforming personal harm into broader community protection. By recounting their experiences, participants sought to equip others with practical awareness. James, for instance, described sharing his experience with friends “as a learning experience... ‘this is what happened to me. Don’t let it happen to you.’ That’s part of my sharing.” John discussed a similar desire:

I tried to tell as many people as I could, in my realm of people, to let them know [about this scam], and then they could let other people know. To try to spread [the information] in a way where it multiplies.

For many participants, this sense of responsibility extended into formalized efforts to combat scams. Participants reported new scams when they encountered them, providing information to corporations, banks, and regulatory bodies, and, in some cases, signing petitions or participating in online discussions. These practices were grounded less in expectations of personal benefit than in a feeling of responsibility and a commitment to care. Deborah said she started reporting scams out of principle, explaining that after her own experience, she “reported [scams] anywhere I could possibly think of to try to put a stop to it, for other people.” John similarly expressed a sense of solidarity with other older adults online in discussing his scam reporting practices: “I just knew that if I was scammed, there were probably hundreds or thousands of us that have been scammed the same way.”

This orientation toward community responsibility underscores a broader desire to protect others and contribute to systemic change. John’s frequent practice of reporting scam e-mails and signing petitions advocating for stricter regulation reflects this. As he explained, these actions were about “being part of a group that wants change.” In this way, these practices supported social redress by protecting others and, in doing so, restoring participants’ sense of connection and participation in a shared social world.

However, these practices were frequently constrained by the inadequacy of reporting processes. Participants who attempted to report scams often received little to no feedback, leaving them uncertain whether their efforts had any tangible impact. Thomas, for example, described ambivalent feelings about reporting scam e-mails:

There's an automated thing in the e-mails. If I get [spam or a scam e-mail], I can click on a thing that says, "report as spam." So I do that frequently, but I don't know if it stops them... but at least it feels good that I report it as spam and that it may go into something.

While reporting offered Thomas a momentary sense of contribution, he remained unsure whether these actions meaningfully strengthened community defenses. Others expressed deeper frustration. Nancy explained that she stopped reporting scams altogether, noting that reporting systems "never have any feedback—none," concluding that she was "not wasting my time doing all that if they're not going to do [anything]." James captured this disillusionment: "Why bother reporting, if you're never going to know anything? Why should I waste my time?"

These accounts reveal a critical gap in these reporting systems. Although participants demonstrated a desire to contribute time and effort toward protecting others, their actions were often met with institutional silence. This lack of reciprocity undermined sustained engagement, ultimately constraining participants' capacity to translate individual experience into collective impact. While participants sought to transform their experiences into actionable knowledge for the greater good, insufficient institutional support limited their ability to enact meaningful change beyond their immediate social worlds.

4.4 The Post-Scam: Material Resonance and Redress

The general goal of a scam is to shift ownership of something valuable from the scammed to the scammer. While this exchange under false pretense occurs in an instant, there is a *material resonance* to scams, as material consequences are felt over time. If we understand material resonance as the tangible consequences that emerge in the aftermath of a scam—such as stolen identities, financial losses, or damaged credit—then *material redress* refers to the practices aimed at mitigating, recovering, or compensating for these material harms. Below, we unpack material resonance and redress.

4.4.1 Material Resonance. Material resonance encompasses the tangible, economic, and logistical consequences that scams impose over time, including direct financial loss, disruptions to financial stability, and enduring administrative burdens. These effects often persist long after the initial interaction, reshaping daily routines, financial planning, and broader life trajectories. Among our participants, direct monetary loss was the most commonly reported material impact ($N = 17$), followed by identity theft ($N = 6$) and damage to credit scores ($N = 3$).

Susan, for example, experienced two prolonged romance scams in which scammers embedded themselves into her daily life before requesting money. In the second case, the scammer claimed he needed his legal fees covered after being jailed and asked for an amount Susan could not afford:

I told him, "Are you gonna scam me too?" Then, he got really mad, he said, "I'm not a scammer. That's humiliating." I'm sorry, you know, but it just sounds like the same thing all over again... So, I did end up sending him some money for lawyers and stuff. But, then, that was it. I never heard back from him.

Despite her doubts, and after months of talking each day, the scammer disappeared with approximately \$10,000 of Susan's money. Combined with her earlier experience ("I had money for my granddaughter's graduation... he took that..."), these losses left Susan in significant debt and forced

her to take out a home equity line of credit to pay off her credit cards. Ronald described a similar trajectory: a months-long scam drained tens of thousands of dollars, disrupting his retirement plans and long-term financial security. In these cases, material resonance extended beyond a single loss to include longer-term financial constraints and altered life planning.

Material resonance also emerged through identity theft and the administrative work required to address it. After James's identity was stolen and used for further fraud, he delayed replacing his government-issued ID, deterred by both the bureaucratic burden and the anticipated embarrassment of potentially explaining what had happened. When the first author suggested going to the Secretary of State weeks later, James replied, "I know, I know... that's what my wife said too..." Mary experienced a drop in her credit score after a scam interfered with automatic banking payments—particularly distressing given the care she had taken to maintain her score over the years. Regaining her score required contacting her bank and the three major credit bureaus while repeatedly recounting the incident, taking days of effort.

For Linda, material resonance took the form of cascading administrative burdens. After a scam targeting her online investment account, she canceled her credit card and began the process of updating payment information across multiple subscriptions. Near the end of this process, she received an e-mail stating that her SiriusXM satellite radio account had expired:

I gave them all [my new credit card] information thinking I was redoing my Sirius billing. (...) If you looked at everything on the e-mail, it looked very legit. It was verified by the checkmark with a little shield. (...) Then it had the McAfee sign and a whole bunch of different verification signs... it looked very legitimate. Worryingly so.

Relying on familiar cues of legitimacy, Linda entered her information into the false SiriusXM portal and was scammed again. Hours before our interview, she had canceled her second credit card in a single week, restarting the entire administrative process again.

Together, these accounts illustrate how material resonance encompasses not only the immediate loss of money, information, or identity but also the recurring logistical labor that follows—canceling accounts, correcting records, navigating bureaucracies, and adjusting financial practices. In some cases, the same systems required to recover from harm can expose participants to further risk or demand sustained time, effort, and emotional energy. For participants like Susan and Ronald, material resonance thus raised an unresolved and pressing question: what comes next?

4.4.2 Material Redress. In pursuing material redress, participants more frequently engaged with corporate resources than with government resources.³ Survey responses indicate that most participants (N = 26) contacted banks, credit card companies, or other corporate entities after a scam, reflecting an immediate focus on recovering money or securing compromised accounts. Fewer participants (N = 12) contacted government agencies, including local law enforcement or federal institutions. Some participants engaged multiple institutional domains. Donna, for example, described her recovery efforts as relying on a "three-legged stool" of governmental, financial, and corporate support, emphasizing the need for assistance at multiple levels. Across these pathways, however, participants' efforts toward material redress were often constrained by limited information, unclear jurisdiction, and uneven institutional responsiveness.

Navigating Material Redress Resources and a Lack of Information. Participants' attempts to achieve material redress were shaped by uneven access to legal and financial infrastructures and by a lack

³Corporate resources were defined in the survey as: "A bank to check your credit statement, a credit or debit card company, a retailer like Amazon or JCPenney, an e-mail provider like AOL or Google, or a phone provider like Apple or Verizon" while government resources were defined in the survey as "A local resource such as the police department or city government; a state resource such as the Michigan Department of Insurance and Financial Services; or a federal resource, such as the FTC."

of clear, actionable guidance. For some, success depended on persistence and the ability to navigate opaque systems. John, for instance, ultimately recovered his losses, but only after sustained effort. As he explained, “For me, it just felt like I had to keep going—not giving up, no matter what.” Although he initially considered contacting the FTC or his congressional representative, John concluded that these avenues would not lead to short-term financial recovery. His first interaction with his bank ended in refusal, with the loss attributed to his own actions. Rather than accepting this outcome, he continued to press his case:

I couldn’t afford to lose that much money. So that was my main incentive, I was not going to accept it. I just knew that somebody had my money, and I was gonna get it back. (...) I would ask the people that I talked to: What’s my way into the whole system? And what department is the best department [to talk to]? Then they would refer me to another department. And, then, sometimes, I would make kind of a friend or an ally in that department. (...) It was many, many calls, and then I’d call the one person [who could help] for as many times as it took (...) And then, eventually, people had been at the bank for a long time, and they kind of knew where there was a workaround, and they were able to do something to help. I just kept going.

John’s experience illustrates how material redress can hinge on sustained self-advocacy, informal knowledge of institutional hierarchies, and access to sympathetic intermediaries. His diary entry—“So glad I don’t have to continue with trying to get money back”—captures both relief and the exhaustion produced by prolonged engagement with a fragmented redress landscape.

For many participants, however, persistence alone was insufficient. A recurring barrier was uncertainty about where to turn in the first place. Participants described not knowing which organizations had jurisdiction, how to reach a human representative instead of a chatbot or phone tree, or whether a given resource would be relevant to their situation. This uncertainty often prevented engagement altogether. Survey data reflect this pattern: most respondents ($N = 19$) did not consider contacting government agencies, and interview accounts suggested that these institutions were frequently perceived as distant or ineffective in post-scam recovery. Despite this disengagement, participants consistently articulated a desire for a clear and trusted source of post-scam guidance. Linda proposed a fraud hotline with the same visibility and legitimacy as 911, while Mary imagined a single point of contact that could offer tailored, actionable advice:

I would just really like a central number (...) that I could have called and said, “Look, this is happening, what do I do?” and they would have the answers for me and directed me.

Mary’s suggestion highlights a broader issue: the uneven dissemination of post-scam information across communities. Donna described this gap using the metaphor of an umbrella: large institutions such as the FTC or state police exist overhead, but their guidance does not consistently reach individuals at the community level:

We’re all under this big umbrella. But every umbrella stretcher needs to lead to a community... I need the information to filter down so that it reaches me in my community.

While Donna envisioned a stronger central institution to facilitate this flow of information, other participants expressed skepticism. James questioned the feasibility of a centralized solution given budget constraints, while Robert voiced distrust in sharing personal information with government agencies, even as he acknowledged the scale of financial harm caused by scams. Thomas instead advocated for local intermediaries, such as senior or recreation centers, to connect older adults with formal resources: “They should have a support group for scams—or at least a phone number to a staff person who’s [knowledgeable] about scams.”

Taken together, these accounts point to two intertwined barriers to material redress: the absence of a widely recognized and trusted point of entry for post-scam assistance, and the lack of effective local channels for translating institutional resources into community-specific support. These gaps mean that even when material redress mechanisms exist, they are not always accessible or actionable for those who need them most.

Attempting Material Redress and Institutional Unresponsiveness. Material redress following scams often required participants to navigate multiple institutions, including banks, credit card companies, investment firms, and digital payment services—a complex assemblage of resources. Participants engaged with these resources through e-mails, online forms, phone calls, and, in some cases, in-person visits. Outcomes varied widely. Some participants received restitution within days, while others saw little progress despite sustained effort. This variability reflects the contingent nature of material redress, shaped by the type and extent of scam, institutional policies, and participants' capacity to persist through complex systems.

As with social redress above, a central barrier during material redress was the absence of meaningful feedback from post-scam stakeholders. Participants described the process as a “black box”: information was submitted, but outcomes were opaque, delayed, or never communicated. Many recounted long phone calls, repeated transfers between departments, and the need to retell their experiences to unfamiliar representatives, often without resolution. Over time, this repetition became a form of bureaucratic endurance that compounded the original harm, amplifying frustration and eroding trust in institutional responsiveness. Mary described this process:

I contacted them over... I mean, I can't tell you how many times, and they did nothing. The worst part is, “Well, I need to transfer you,” then you have to tell your story again. “Well, I'm going to put you in touch with the person who can help.” And you tell your story again. The process is horrible.

Mary's account illustrates how institutional processes, when lacking coordination or continuity, can reproduce the harms they are intended to remedy. Rather than fostering resolution, the cycle of repetition and non-responsiveness became its own source of distress, adding procedural burden to the original financial loss. Echoing this, James reflected:

If you go to an agency, like the fraud agency at the bank, for example, you'll never know the results of what they're going to do anyway. There's no feedback. You just wave a white flag and say help. And then you walk away from the battle. There's no reciprocity, and nothing comes back to you, where you can say justice has been served.

For many participants, material redress became a cycle of effort without visible outcome. Actions taken were rarely acknowledged, progress was unclear, and accountability remained elusive. Ronald's experience illustrates how even sustained engagement across institutions could stall. Despite engaging both financial and legal channels—each referring him to the other—his case did not progress:

The woman from Charles Schwab was a fraud investigator. She recommended I contact the police. (...) The police were cautiously optimistic that they might be able to help. Nothing came from that. The county sheriff said he had contacts with the state police, and there were people that he could contact (...) I never heard anything back. So, the fraud investigator from Charles Schwab I would call, I just felt like she was there for me. But, you know, in the end, there's nothing she could do.

Ronald's account highlights a recurring pattern: interpersonal support from individual representatives did not translate into institutional resolution, and referrals to broader networks of support

rarely materialized into meaningful action. Even when participants felt heard, structural limits constrained what could be done. Faced with prolonged unresponsiveness, participants diverged in how they approached “what comes next.” Some emphasized persistence. John described continued pressure as necessary: “you’ve got to work hard (and) be willing to not stop until you get some kind of gratification.” Others recalibrated their expectations, reframing closure as a personal rather than institutional outcome. Robert, reflecting in his diary, described choosing to let go:

Hopefully, I have learned enough that I will not fall victim to frauds/scams again. In the past, I might have tried to obtain justice, but the older me (because of my aging body and mind) finds that contemplating such events is more destructive to the mind and body than forgiving and letting go. I want to pursue knowledge and helpfulness rather than negative thinking.

Here, Robert’s response illustrates a shift from material to affective priorities, reframing closure as an internal process. For others, redress was deferred rather than abandoned, constrained by competing demands. Linda documented in her diary the overlap of scam recovery and caregiving for her husband:

Tired. Recovering from husband in hospital earlier this week. Although there is more that I need to do (after being scammed), I have put things on hold. Annoyed every day by scammers calling my husband who has Alzheimer’s. Have tried to block his phone number but that did not work. Have to find an app that was recommended and install it—when he doesn’t have his phone. I am also still getting calls and e-mails but not as many as he gets.

Linda’s account underscores how material redress unfolds within broader life contexts. The labor of recovery competes with existing responsibilities, requiring ongoing judgment about where limited time and energy should be directed.

Even when financial restitution did occur, participants questioned whether it constituted meaningful redress. Deborah pointed out that while her fraudulent charges might be reversed, her scammers were not held accountable: “[banks] expect x amount of dollars every year [in scams], but what do they do with [our] reports? What happens to the scammers?” Such reflections suggest that closure was not simply about recovering lost funds, but about achieving some form of justice, reciprocity, or acknowledgment—outcomes that institutions rarely provided. Linda expressed a similar sense of unfinished business, calling for, in her words, justice: “Who goes after these people? Nobody?”

4.5 The Recursive Post-Scam: Scammed while Seeking Redress

During the process of redress, several participants reported being targeted by additional scams—this time by individuals posing as recovery agents who claimed they could help retrieve the money lost in the initial scam. These secondary scams capitalized on participants’ desperation, turning their efforts toward redress into opportunities for further harm. Ronald, for instance, recounted how he was scammed again by someone who promised to help recover his losses—for a fee. As he described:

There are people out there that say they can get the money back, and I actually reached out to somebody, then I put out like \$6,000 or \$8,000 to try to get the money back. And he said he could do it. He sent me a document, basically, like a contract, but it couldn’t be used in a court of law, I don’t believe [...] I talked with the guy so many times. I trusted him, but still, there’s this, you know... I’ve trusted people before. [...] He told me that there was something going on, where he could get my money back but for the next step he needed, like, \$10,000 or \$20,000. And at the time, I didn’t have it...

Ronald's experience exemplifies how the pursuit of material redress can itself become a risk. So-called "recovery scams" exploit not only the financial precarity but also the affective aftermath of being scammed—grief, hope, and a longing to regain agency. The scammers' tactics—offering restitution, issuing contracts, maintaining steady communication, and cultivating a tone of trust—mimic the processes participants were seeking from legitimate channels. In this way, where institutional redress fell short or proved inaccessible, scammers stepped in to fill the gap. Rather than resolving harm, these secondary scams prolonged participants' ordeals, compounding their losses, corroding trust, and intensifying emotional strain.

Even after the formal study concluded, several participants continued to contact the first author to share ongoing encounters with scams, underscoring the prevalence of this recursive post-scam experience. In a follow-up conversation, Susan described a recent event: "I just got something from some kind of recovery [law firm]. It's an actual company that goes after scammers. And I think there's a charge of like 15% of whatever they recover." She had reached out to a law firm she found through a Facebook advertisement claiming to help scam victims reclaim their lost funds. The ad, tapping into the affective and material aftermath of online scams, made a direct appeal: "Have you ever been scammed? [...] Get your money back! The recovery rate is as high as 90%!" Following the URL included in the e-mail, the first author visited the firm's web site. On the surface, the site presented as credible and professional: it featured an official landing page, detailed profiles of its lawyers, a prominent TrustScore backed by hundreds of reviews, and a New York City address corresponding to a Google-reviewed law office. A Consumer Financial Protection Bureau shield appeared on the site, labeling it an "officially licensed law firm." The web site claimed specialization in several high-stakes legal domains—immigration, medical malpractice, premises liability, and, notably, fraud and scam recovery.

However, closer inspection revealed that the firm was part of a network of cloned web sites sharing identical content, fabricated credentials, and coordinated domain registrations—indicating a large-scale scam operation rather than a single fraudulent entity. These sites were carefully crafted to simulate credibility, borrowing the visual language and institutional markers of trust. For participants like Susan, this blurred the line between genuine support and deceptive promises, adding yet another layer of complexity to an already fraught landscape. After falling victim to a relationship scam, Susan had taken out a home equity line of credit to stabilize her finances. The offer of legal help—purportedly from an accredited firm—seemed like a lifeline, and the upfront finder's fee felt like a reasonable investment. Unfortunately, it was just another scam, leaving Susan more distrustful of online environments that seemed to prey on her desires.

5 Discussion

5.1 Mapping a Multi-Stage Research Agenda on Scams and Older Adults: The Pre-Scam and Scam Stages

We undertook this research to examine scams as lived sociotechnical experiences, focusing specifically on older adults—a population described as underrepresented in privacy and security research [51]. In our preparatory work, we observed that much of the existing literature conceptualizes the scam as a discrete incident or static artifact—a message, a transaction, or a singular moment of deception—in other words, as a bounded "thing" [115]. Such framings can obscure the temporal and relational processes through which scams emerge, are sustained, and later made sense of and (hopefully) redressed.

To address this, we draw on scholarship in HCI and CSCW that treats interaction as a fundamentally temporal phenomenon, emphasizing unfolding events, situated processes, and lived experience rather than isolated moments or artifacts [13, 94, 98, 105, 115]. From this perspective, a scam can be

Table 3. Pre-Scam and Scam Stages

Stage	Temporal Boundaries	Sociotechnical Conditions	Current Research	Current Interventions
Pre-Scam	Stage before direct contact; ends when interaction is initiated.	<i>Individual</i> : Personal vulnerabilities, capabilities, and dispositions shaping potential exposure. <i>Social</i> : Trusted networks and support systems. <i>Technological</i> : Properties of technologies scammers exploit. <i>Structural</i> : Institutional and policy contexts conditioning risk (e.g., financial regulations).	Identifies susceptibility and risk factors to support prevention efforts. Surveys, experiments, interviews map risk profiles and measure digital literacy.	Education and awareness campaigns; community outreach; digital literacy training; simulations to improve detection.
Scam	Stage begins with first scam interaction; ends when scam's goal is met, older adult disengages, or scam is disrupted.	<i>Social</i> : Interactions between scam and older adult, often trust- and dependence-building. <i>Technological</i> : Systems that mediate scams, spoofing (e.g., area codes, hallmarks of trust), urgency cues, AI-generated content. <i>Structural</i> : Rapid transfer systems, lack of friction in financial transactions.	Analyzes dynamics and mechanisms of persuasion, deception, and engagement. Studies draw from scam artifacts, linguistic analysis, and retrospective accounts.	Scam-blocking systems; conversation interruption mechanisms; "digital buddy" systems; AI-driven alerts.

understood not as a singular thing in isolation, but as an extended, temporally distributed process that unfolds through a series of loosely bounded and interdependent stages. Understanding scams in this way highlights how each stage entails distinct sociotechnical dynamics, actors, methodological challenges, and opportunities for intervention. We conceptualize this as comprising three stages: (1) the pre-scam enabling conditions that render a scam possible, (2) the scam itself, as it is enacted and endured, and (3) the post-scam period, during which individuals and their networks negotiate the ongoing consequences of the scam.

If scams unfold across distinct yet interrelated stages, research on scams and older adults must be attentive to which stage is being theorized and intervened in. In what follows, we map a multi-stage research agenda by outlining each stage's temporal boundaries and sociotechnical conditions, along with corresponding research directions and interventions. Table 3 summarizes prior work on the pre-scam and scam stages and highlights gaps that remain. In doing so, we advance a temporally grounded understanding of scams.

5.1.1 The Pre-Scam Research Agenda. Existing research into the pre-scam and scam stages has identified the conditions that make scams actionable and the tactics that sustain them once underway. Within the pre-scam stage, this body of work has been especially effective in articulating potential and realized risk factors for scams targeting older adults (e.g., [21, 40, 104]). Such prevention-oriented research has been instrumental in identifying and mitigating particular forms of risk. Building on this foundation, scholars have translated these insights into practical

prevention efforts—shaping public awareness campaigns, community outreach initiatives, and technical systems designed to reduce the likelihood of scams before they occur [24, 71, 104].

While these efforts have advanced understanding and awareness, their impacts can be limited: for instance, even after training, older adults may remain unable to detect scams, despite feeling more confident in their abilities [71]. Moreover, as Herrera et al. note, technological prevention tools “only work for those who utilize them,” emphasizing how differential access and adoption limit prevention’s effectiveness in practice [63, p. 7]. Additionally, much pre-scam work reasonably focuses on individual knowledge, vigilance, or skill as sites of intervention. However, when these factors become the primary or exclusive focus, responsibility for prevention can appear to rest largely with individuals themselves. This framing can make it harder to see how broader sociotechnical conditions—such as platform design, institutional practices, and policy decisions—also shape the scam’s conditions of possibility and distribution of risk [30, 55]. In this sense, an emphasis on individual-level prevention may unintentionally align with what Vines et al. describe as a deficit model of aging, one that centers remediation of individual shortcomings rather than attending to how older adults act within, and are constrained or supported by, sociotechnical contexts that, in our case, mediate exposure, harm, and recovery [111].

Looking ahead, a more comprehensive understanding of scams therefore does not replace pre-scam, prevention-oriented research but, rather, should extend it. Future work in HCI and CSCW should investigate how sociotechnical systems distribute risk and responsibility among their users. This includes examining how infrastructural and policy decisions influence which users are most exposed to scams and how intergenerational, institutional, and community relationships can play an important role in scam prevention. To capture these dynamics, future research would benefit from longitudinal and participatory approaches that trace how everyday practices of technology use, trust, and safety shape exposure to scams over time [115]. In sum, the strengths of current pre-scam research provide a necessary foundation for—but not a complete picture of—the broader dynamics that characterize the pre-scam stage.

5.1.2 The Scam Research Agenda. If research within the pre-scam stage has emphasized risk and prevention, then work within the scam stage has primarily focused on disruption. This body of research examines how scams take shape and explores interventions designed to interrupt them in real time [39, 92, 104, 122]. Yet, this research also underscores the persistent challenges in designing interventions that can respond effectively to the evolving dynamics of the scam stage. Some work has proposed human-in-the-loop models, such as digital “buddy systems” designed to encourage disengagement from active scams [87]. While promising in theory, these systems raise complex ethical questions, including the potential for overreach or even financial abuse by trusted “buddies” [21, 58]. Technological approaches, particularly those leveraging AI for real-time detection, introduce a similar tension between surveillance and support [122]. Such systems may offer protective benefits but risk infringing on privacy or introducing paternalistic oversight—concerns that are especially relevant for older adults already subject to heightened suspicion, monitoring, and regulation [24, 51, 100]. Additionally, as AI-enabled detection tools proliferate, they risk reinforcing a reliance on technological fixes, leaving underexplored the potential of non-technological or collective strategies in the scam stage. For instance, training trusted intermediaries—such as bank tellers, community center staff, or customer-facing employees at grocery stores where gift cards are sold—to recognize and respond to signs of scams could complement or replace purely technical solutions [31].

Moreover, many proposed interventions are necessarily partial, as they aim to interrupt scams at the level of individual incidents rather than address the broader social, infrastructural, and economic conditions that enable them [63]. Much existing work on the scam stage also relies on scam simulations or secondary analyses of existing datasets (e.g., [19, 99]). While valuable

for isolating specific scam mechanisms, these approaches offer limited insight into how scams operate in practice or evolve over time. Our study instead examines scams as lived experiences, foregrounding older adults' perspectives and tracing both recent scams and those unfolding in real time. In Section 4.1, we show how scams are shaped through constellations of sociotechnical factors, including platform design, check-clearing policies, proximity to banks, and dynamics of interpersonal and institutional trust. This analysis underscores the need for methods that can capture scams as lived and evolving processes [115]. We position diary studies as one such approach.

A defining challenge of the scam stage is its dynamism: scammers continually adapt their tactics in response to new technologies, shifting platforms, and changing social and economic conditions [1]. This dynamism is not merely a practical challenge for researchers but a temporal condition of scams themselves, which evolve alongside the infrastructures, institutions, and everyday practices that enable or constrain them. As a result, interventions designed for the scam stage may quickly lose effectiveness as conditions change [77]. Addressing this challenge requires research and design approaches that are sufficiently situated to capture the specificity of individual scams while remaining flexible enough to inform broader insights [106]. For example, can insights from tech support scams meaningfully inform deepfake scams [122]? Designing for the particularities of context and practice is especially challenging when antagonism serves as the scam's organizing principle.

Looking ahead, future HCI work within the scam stage could examine how scammers, systems, and users co-evolve, tracing how new technologies and interventions give rise to new forms of scams. This work could also be informed by the life-cycles of scams themselves—when a new scam becomes prevalent, what measures are taken to curb the scam's success, and how do those measures, in turn, reshape the scam's form? For instance, during the writing of this article, text message scams about unpaid toll fees briefly surged in the United States before fading as new scams emerged and preventative information about toll scams became available [45]. Such approaches would move scam-stage research beyond one-off disruptions toward a deeper understanding of how scams and interventions co-evolve over time.

In sum, scholarship on the pre-scam and scam stages has provided a strong empirical and technical foundation for the prevention and disruption of scams. However, enduring challenges remain: the long-term feasibility of awareness and training interventions, the limited exploration of collective or infrastructural prevention strategies, the ethics of real-time detection systems, and the lifecycle dynamics through which scams emerge, proliferate, and adapt in response to new preventative measures. Addressing these questions will require research that is temporally sensitive, methodologically plural, and attentive to the sociotechnical systems in which scams are embedded and addressed. It is also important to note that less is known about what follows once the scam stage concludes.

5.2 Mapping a Multi-Stage Research Agenda on Scams and Older Adults: The Post-Scam Stage and the Need for Justice

While the pre-scam and scam stages have received extensive attention, the post-scam stage remains comparatively underexamined. Existing efforts, even at the federal level, reveal this neglect: documents from the FTC-led Scams Against Older Adults Advisory Group, formed under the Stop Senior Scams Act, reference the post-scam only once. Similarly, HCI research in adjacent areas such as financial abuse and online harassment has begun to note a broader absence of inquiry into post-harm experiences (e.g., [15, p. 2]). We can extend this call to HCI research on technology-mediated scams. For the millions scammed out of billions, the post-scam stage warrants closer attention.

Table 4. Summary of Post-Scam Resonance and Redress

Domain	Resonance	Redress	Barriers to Redress
Affective	Emotional impacts that follow a scam—such as shame, anger, fear, or self-blame—that linger and resurface over time.	Regulating emotions through self-compassion; reframing distressing experiences; rebuilding a sense of safety.	Emotional fatigue; difficulty managing feelings of safety; lingering distrust.
Social	Lingering disruptions to interpersonal relationships, routines of communication, and social trust.	Reestablishing trust and social connections; strengthening community defenses.	Social withdrawal or consolidation of lifeworlds that limits social engagement; inadequate reporting and support processes.
Material	The tangible and ongoing material consequences of scams—stolen identities, financial losses, or damaged credit.	Navigating institutional and financial systems in pursuit of recovery, restitution, or compensation.	Structural information barriers; institutional unresponsiveness; difficulty recovering lost funds.

Responding to this gap, our work examines the post-scam stage as one of ongoing negotiation—what we term processes of resonance and redress. Through interviews and diary studies with older adults, we traced how scams resonate across affective, social, and material dimensions of everyday life (RQ1), how older adults make sense of the aftermath of scams, including their needs, desires, and concerns that emerge (RQ2), and how efforts to respond constitute practices of redress (RQ3). Redress, we found, was rarely linear or complete. It unfolded through iterative cycles of reflection, interaction, and adaptation—often mediated, and sometimes constrained, by technological systems. Taken together, our findings position the post-scam as a distinct and critical stage of inquiry, with its own sites for design and intervention. Table 4 summarizes the three domains through which we characterize post-scam life— affective, social, and material—each encompassing distinct forms of resonance, redress, and barriers to redress.

Participants’ efforts extended beyond individual redress toward a broader concern with *justice*. In HCI, justice has been described as “the social concerns, obligations, and ethical commitments created through our interactions with each other” [50, p. 3294]. Seen this way, redress is not merely a practical response to harm but a condition through which ethical commitments become grounded in lived experience: “the identification of redressable injustice is not only what animates us to think about justice and injustice—it is also central (...) to the theory of justice” [103, p. vii]. In this sense, justice becomes actionable when specific harms are recognized as redressable. Without redress, justice remains abstract. Without justice, redress becomes fragmented, left to individuals rather than supported collectively. Redress, then, is the lived terrain through which justice—and its absence—is experienced and enacted.

Building on this framing, we identify three recurring ways older adults’ efforts toward redress break down, revealing the structural conditions that constrain justice in post-scam life. These are not isolated incidents but patterns that show how post-scam experiences are shaped by entanglements of power, accountability, and care that determine who is heard, who is helped, and whose needs remain unacknowledged. We show how justice is both conceptually and operationally constrained, and how HCI researchers might respond to these limitations.

5.2.1 Ageism Constrains Redress. One such condition that constrains the possibilities for redress—and, by extension, justice—in the post-scam stage is ageism. Ageism, “the stereotyping, prejudice, and discrimination toward people on the basis of age,” operates not only interpersonally

but also through technological, institutional, and policy infrastructures [66, 91]. Ageism shapes how older adults' competence is interpreted—by others and by older adults *themselves*. Research on this self-ageism demonstrates that pervasive discourse around decline can lead to internalized limiting beliefs about one's own digital competence, discouraging online participation (e.g., [74, 118]). Miche et al. call this process "subjective aging," wherein individuals come to see themselves as "too old" to engage confidently with technology [82].

Existing research complicates such stereotypes. While older adults are disproportionately targeted, they are not inherently more susceptible to scams [10, 99]. Scam prevalence appears higher among older adults because scams constitute a larger share of the crimes they encounter overall, not because of age-related deficits [99, p. 438]. Moreover, many health, disability, and social variables show no consistent association with scam susceptibility [68, p. 7]. Together, these findings shift responsibility away from perceived individual deficiencies and toward the tactics and infrastructures through which scams operate.

Even so, presumptions of age and ability directly shaped how participants in our study experienced and responded to the post-scam stage. In our work, ageist assumptions—whether internalized, externalized or anticipated—shaped how participants sought help, disclosed their experiences, and pursued redress. Many described silence as a form of self-protection, fearing that disclosure to family, partners, or friends would invite ageist judgments about their abilities. Recall Kenneth, who described how disclosing a scam felt like an invitation to scrutiny, making help-seeking feel like a threat to his autonomy. The pursuit of redress was constrained not by a lack of awareness or motivation but by *the perceived costs of visibility*. Elsewhere, participants characterized themselves as uninformed or gullible, linking these characterizations to their age. When scams are framed as individual failings, disclosure can feel like an admission of guilt, prompting withdrawal or avoidance. Prior research shows that older adults who have endured scams are less likely to respond to surveys about scams [10, 36] and may limit technology use as a way to circumvent further risk [41, 51]. Our study extends these insights, showing how non-use emerged as a deliberate, situated practice in which participants described shrinking their technology-mediated footprint. While these practices reduced immediate exposure to risk, they had cascading consequences: participants missed neighbors' calls, disengaged from online health portals, and restricted their digital activities to a few trusted spaces.

Confronting age-based bias has been shown to improve older adults' self-efficacy and well-being [121]. Building on this, future research should further our findings by examining non-use as a situated practice against scams and other forms of digital harm—one that protects against immediate risk yet may, over time, deepen digital exclusion and reinforce structural inequities. Mapping if, when, and how avoidance becomes exclusion can clarify design priorities for equitable redress. Building on this, HCI interventions could be designed to counter ageist assumptions and mitigate the shame and self-blame that often accompany the post-scam stage. For instance, outreach, support tools, and reporting interfaces could normalize being scammed, affirm competence, and offer peer stories early in the redressal process—something noted as meaningful in Section 4.3.2 (see also [5]). Such interventions could be evaluated to assess how affirmation influences self-blame, help-seeking, and re-engagement with digital systems. Participatory approaches could further identify what constitutes affirming design for older adults through co-design sessions that surface which tones, wordings, visuals, and forms of disclosure feel supportive or, otherwise, stigmatizing [34, 80]. In general, research in this space should remain attentive to Vines et al.'s agenda for HCI and aging, which calls for "challeng[ing] any taken for granted assumptions and predominantly negative societal attitudes of ageing" [111, p. 17]. Such affirming design can smooth pathways toward redress by countering ageism and supporting help-seeking in the aftermath of scams.

5.2.2 Distrust Constrains Redress. If ageism constrains redress by shaping how older adults are perceived and how they perceive and present themselves, the erosion of trust constrains redress by destabilizing the relations through which redress must occur. Across participants' accounts, scams did not merely weaken confidence in a single actor or domain but, instead, fractured multiple, interdependent layers of trust that structure everyday sociotechnical life. This included: epistemic trust, as in James's growing sense that online information and interactions could no longer be taken as credible; interpersonal trust, as in Ronald's discovery that a new friend was, in fact, a scammer; and institutional or sociotechnical trust, as in Susan's realization that confidence markers such as TrustScore reviews or Consumer Financial Protection Bureau shields could themselves be weaponized. These breakdowns rarely occurred in isolation—Susan's experience, for instance, entailed epistemic, interpersonal, and institutional trust simultaneously, complicating her efforts to determine whom or what to believe when pursuing redress.

Accounts of trust in moral philosophy help clarify the moral and epistemic weight of the fractures evident in our empirical work. Baier describes trust as a moral relation grounded in vulnerability and risk—the risk inherent in believing that others will act as they ought to [8]. Trust, in this sense, always carries the possibility of loss: we entrust others with something of value in the expectation of shared good faith. For instance, James's potential buyer and Cynthia's Microsoft tech support contact each appeared as cooperative partners pursuing a shared goal: the sale of a motorcycle or the resolution of a technical issue. In trusting them, James shared personal information in the form of his ID and Cynthia sent money via a Bitcoin ATM. When trust is violated, it can lead to distrust, and our findings show how participants' post-scam experiences were marked by this distrust in whether, and under what conditions, they could trust (strangers, platforms, phone calls) again. When individual violations of trust are repeated at scale, they can erode what Baier calls a "climate of trust," in which trustworthiness can be reasonably presumed, giving rise instead to a climate where suspicion becomes a norm [9, 93]. As legal scholars Citron and Solove observe: "Over time, as people are individually inundated by a swarm of small harms, the overall societal impact is significant" [30, p. 797].

From an HCI perspective, our findings align with and extend existing work that conceptualizes trust as dynamic and negotiated rather than a static presupposition. Because scams fracture trust across multiple layers—epistemic, interpersonal, and institutional—and do so over time, they render static or one-off models of trust insufficient. Future research should examine how experiences of digital harm shape trust over time: which platforms, affordances, and interactions cultivate trust, and which undermine it [62]? Longitudinal work might further trace how distrust is enacted, sustained, and mitigated across subsequent interactions with people, platforms, and institutions [6, 110].

As distrust accrued, participants developed an ambient awareness of risk that reoriented how they approached technology-mediated environments. As scams and other digital harms become increasingly visible, it becomes important to understand how this ambient awareness of risk reorients older adults' engagement with digital systems. For example, Susan needed to distinguish between a fake law firm and a legitimate one, yet both deployed Consumer Financial Protection Bureau shields and images of attentive lawyers. Here, markers meant to signal legitimacy became unstable, transforming trust cues themselves into contested infrastructure. This raises design questions about how confidence markers might be embedded in sociotechnical systems in ways that are harder to replicate by scammers [69, 89, 108].

Taken together, these findings illustrate how trust is a negotiated, ongoing accomplishment rather than a stable resource that can simply be restored when broken. Participants' experiences show how repeated violations across epistemic, interpersonal, and institutional domains produce an ambient awareness of risk that reshapes how technology use in general and redress practices in

specific are imagined and pursued. In such conditions, confidence markers and institutional signals no longer function as reliable anchors, rendering trust itself a site of ongoing work. Designing for post-scam redress therefore requires attention to how trustworthy relations are made, sustained, and repaired across sociotechnical systems. Without such attention, redress remains constrained, underscoring trust as a moral and infrastructural condition for justice rather than an assumed backdrop.

5.2.3 Systemic Constraints on Redress. If ageism constrains redress by shaping how older adults are seen and see themselves, and the erosion of trust constrains redress by destabilizing the relations through which it must occur, the design of sociotechnical systems can constrain redress by obscuring the processes intended to enable it. Systems ostensibly designed to support redress—such as “report spam” features, bank and credit card dispute channels, consumer protection portals, and fraud reporting web sites—are sociotechnical arrangements that integrate automated classifications, institutional procedures, and human judgment. Yet for many participants, these systems obscured rather than enabled redress. Participants often did not know which institutions were relevant, what would happen after submitting a report, or how to interpret delayed, automated, or ambiguous responses. As a result, redress efforts frequently felt as though they disappeared into a void—“nothing comes back to you, where you can say justice has been served,” as James reflected—undermining both participants’ sense that action had been taken *and* their motivation to pursue reporting *into the future*. Together, these dynamics point to systemic constraints on redress that operate not only at the level of system usability but at the level of how justice itself is structured and recognized.

Even when money was returned back to their accounts, participants rarely felt that justice had been served. Linda and Deborah, for instance, noted that their scammers “were still out there.” James’s experience—in which his stolen identification continued to circulate in other scams—left him bound to his scam through the continued circulation of his stolen identity. These accounts illuminate a deeper tension between redress and justice. Scams operate through an economy of extraction that demands individualized acts of recovery. This mirrors the logics of corrective justice [114]. Corrective justice seeks to restore equilibrium between the wrongdoer and wronged, premised on an “arithmetic proportion” between harm and restitution [14]. Yet, as our findings demonstrate, corrective justice falters when there are no clearly identifiable parties or traceable harms. As scams often involve anonymous scammers operating through diffuse means, accountability and, therefore, restitution, are impossible [33]. Even when participants recovered their funds, they did not receive them from the scammer but through institutional reimbursement programs—mechanisms that redistribute loss across the financial ecosystem rather than correct a direct wrong.

While corrective justice reveals the limits of current redress mechanisms, it also exposes a broader issue: the narrow conception of harm that underpins them. Scams extend beyond quantifiable losses to encompass affective and social impacts. These, from participants’ perspectives, remain unacknowledged in formal redress systems and, in previous work, are noted for being “too speculative and hypothetical” to warrant recognition [29, p. 798]. Yet our findings show that these so-called “non-traditional costs” shape older adults’ everyday lives [48]. Restorative justice approaches suggest that redress should move beyond material compensation to include recognition of relational harm and acknowledgment of wrongdoing—for instance, through apologies or dialogue that reestablish trust and accountability [102, 112]. Similar to corrective justice, however, at present, the anonymity and distributed nature of scams make restorative processes like apology largely unattainable. In this way, older adults who have been scammed must pursue redress through sociotechnical systems that both adjudicate recognition and obscure their own operations. This opacity compounds feelings of invisibility, confusion, and futility, while even successful outcomes

tend to restore funds without holding scammers accountable or addressing affective and social harm.

From an HCI perspective, addressing systemic constraints on redress and justice requires research and design into more legible, accessible, and equitable redress systems. This includes improving interoperability across reporting systems, creating multimodal and accessible interfaces, and ensuring information continuity across institutional boundaries, including clearer communication about how individual reports are used, what outcomes are possible, and what forms of justice these systems can—and cannot—provide [97, 107]. Given HCI's emphasis on interaction and information dissemination, the field is well positioned to strengthen older adults' connections to existing resources and to enhance the responsiveness of formal redress mechanisms. Such work can be community-based and informed by participants—in keeping with our own recommendation, we partnered with our state's Senior Medicare Patrol, a wing of the Medicare/Medicaid Assistance Program that helps beneficiaries prevent and report health care fraud and scams, to develop and distribute informational flyers to our state's more than 600 libraries. These flyers feature clear reporting instructions and resource contacts, addressing feedback from participants who felt lost in the initial material redress steps post-scam and participants who did not feel comfortable accessing their computer. Future research could consider supporting, as Linda proposed, a coordinated system—akin to 911 for scams—that could streamline post-scam support, a need policymakers have also recognized [57].

Efforts to improve systems for redress should be paired with research that informs structural change in the post-scam landscape. As Lessig observes, digital technologies often evolve faster than law and policy, producing forms of governance that operate outside formal regulation [76]. When technologies function as moral infrastructures that shape ethical action [20], documenting where and how technology-mediated harm occurs—and how redress is pursued or foreclosed—becomes essential. In this way, HCI can help translate lived experiences of post-scam harm into evidence that supports more accountable and responsive policy and institutional change [119]. Importantly, our findings also show that older adults are not passive recipients of injustice but active agents in cultivating individual and collective forms of redress. John and Deborah's efforts to warn and support other older adults, as well as Donna's letter-writing campaign to her senator, illustrate how post-scam redress can extend into civic and community action. Building on such ground-up initiatives, HCI can support post-scam redress as a collective endeavor and one grounded in community practices and the recognition of older adults as contributors to more just sociotechnical futures [79].

6 Limitations

As with all interpretivist research, the findings presented here should be understood in relation to the specific contexts and participants involved. Our study focused on older adults' experiences of scams and post-scam life, drawing on a sample of participants who were in their 60s and 70s, who resided in a single U.S. state, and were predominantly white. While our participants provided rich, detailed accounts of the post-scam stage, it also reflects certain demographic and geographic limitations. The experiences of those 80 and above, as well as older adults from more racially and socioeconomically diverse backgrounds, may differ in both how scams are encountered and how redress is sought: in the types of scams prevalent, the platforms used, the accessibility of resources, or the support assemblage available. In interpretivist research, the goal is not generalization but analytical insight: to illuminate situated themes from empirical insights that can inform future studies and design interventions within and beyond the immediate context (see [49]). Future work should build on this study through comparative or cross-cultural research that examines how sociotechnical infrastructures of redress vary across regions, institutions, and communities. For

instance, excellent work concerning scams and their resonances can be seen in research from China [122] and Iran [3]. Attending to these distinctions will clarify how intersecting factors influence both the scams themselves and the possibilities for redress.

7 Conclusion

In this study, we examined technology-mediated scams that affect older adults, focusing on the underexplored post-scam stage. Through a multi-method approach involving surveys, interviews, and diary studies, we traced how scams resonate through the affective, social, and material dimensions of older adults' lives. Our findings reveal that the aftermath of scams is not a single moment of loss but ongoing processes of resonance and redress—constrained by ageism, the erosion of trust, and systemic opacity. These dynamics challenge the prevailing emphasis on prevention and personal responsibility, underscoring the limitations of frameworks that isolate scams as individual failures rather than collective issues. HCI has a vital role to play in the post-scam: designing equitable and legible systems for redress, rebuilding trust in sociotechnical relations, countering ageist framings of competence, and translating lived experiences into structural and policy change that make justice actionable. Finally, it should be noted that our study affirms older adults as not passive recipients of harm but active agents of redress. Their efforts—through advocacy, peer support, and collective action—constitute grassroots practices of redress and justice-making that HCI can amplify. We call for a post-scam research agenda that positions justice not as a distant ideal but as a relational and designable condition of everyday life—one that can sustain affective, social, and material redress in the aftermath of scams.

Author Statement on Prior Work

This submission presents original research that has not been submitted or published elsewhere. While entirely original, this work is related to an accepted case study. However, the two works are distinct in scope, focus, and contribution, with no overlap in findings or discussion. The case study specifically examines the methodological and ethical considerations involved in recruiting at-risk populations for research, using the recruitment process as an illustrative example. The case study does not analyze or present the empirical findings, theoretical contributions, or design implications explored in this submission. Instead, it explores conversations had with potential research subjects before the study began.

Given these clear distinctions, we affirm that the current submission offers a novel and independent contribution to the field, aligned with the ACM policy on prior publication and plagiarism.

References

- [1] Jay S. Albanese. 2005. Fraud: The characteristic crime of the twenty-first century. *Trends in Organized Crime* 8, 4 (2005), 6–14.
- [2] American Medical Association. 2025. DEA and CMS Warn Physicians That They Are Being Targeted by Scams. Retrieved from <https://www.ama-assn.org/practice-management/digital-health/dea-and-cms-warn-physicians-they-are-being-targeted-scams>
- [3] Sima Amirkhani, Mahla Alizadeh, Dave Randall, Gunnar Stevens, and Douglas Zytka. 2025. “Society encourages the killing of girls like me”: Layers of victimization in online dating romance scams in Iran that target sexual access over financial gain. *Proceedings of the ACM on Human-Computer Interaction* 9, 7 (2025), 1–25.
- [4] Comfort Anafo and Richmond S. Ngula. 2020. On the grammar of scam: Transitivity, manipulation and deception in scam emails. *Word* 66, 1 (2020), 16–39.
- [5] Nazanin Andalibi. 2020. Disclosure, privacy, and stigma on social media: Examining non-disclosure of distressing experiences. *ACM Transactions on Computer-Human Interaction* 27, 3 (2020), 1–43.
- [6] SamAddison Ankenbauer and Robin N. Brewer. 2025. The right to be skeptical: Insights from recruiting at-risk users on nextdoor. In *Proceedings of the Extended Abstracts of the CHI Conference on Human Factors in Computing Systems*, 1–11.

- [7] Brooke Auxier and Monica Anderson. 2021. Social Media Use in 2021. Retrieved from <https://www.pewresearch.org/internet/2021/04/07/social-media-use-in-2021/>
- [8] Annette Baier. 1986. Trust and antitrust. *Ethics* 96, 2 (1986), 231–260.
- [9] Annette Baier. 2004. Demoralization, trust, and the virtues. In *Setting the Moral Compass: Essays by Women Philosophers*. Cheshire Calhoun (Ed.), Oxford University Press, New York, NY, 176–189.
- [10] Jan Bailey, Louise Taylor, Paul Kingston, and Geoffrey Watts. 2021. Older adults and “scams”: Evidence from the mass observation archive. *The Journal of Adult Protection* 23, 1 (2021), 57–69.
- [11] Rosaline S. Barbour. 2001. Checklists for improving rigour in qualitative research: A case of the tail wagging the dog? *The BMJ* 322, 7294 (2001), 1115–1117.
- [12] Rosanna Bellini, Emily Tseng, Noel Warford, Alaa Daffalla, Tara Matthews, Sunny Consolvo, Jill Palzkill Woelfer, Patrick Gage Kelley, Michelle L. Mazurek, Dana Cuomo, et al. 2024. SoK: Safer digital-safety research involving at-risk users. In *Proceedings of the 2024 IEEE Symposium on Security and Privacy (SP)*. IEEE, 635–654.
- [13] Steve Benford and Gabriella Giannachi. 2008. Temporal trajectories in shared interactive narratives. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, 73–82.
- [14] Peter Benson. 1991. The basis of corrective justice and its relation to distributive justice. *Iowa Law Review* 77 (1991), 515.
- [15] Arkaprabha Bhattacharya, Kevin Lee, Vineeth Ravi, Jessica Staddon, and Rosanna Bellini. 2024. Shortchanged: Uncovering and analyzing intimate partner financial abuse in consumer complaints. In *Proceedings of the CHI Conference on Human Factors in Computing Systems*, 1–20.
- [16] Carlene Blackwood-Brown, Yair Levy, and John D’Arcy. 2021. Cybersecurity awareness and skills of senior citizens: A motivation perspective. *Journal of Computer Information Systems* 61, 3 (2021), 195–206.
- [17] Virginia Braun and Victoria Clarke. 2021. *Thematic Analysis: A Practical Guide*. SAGE Publications Ltd.
- [18] Virginia Braun and Victoria Clarke. 2025. Reporting guidelines for qualitative research: A values-based approach. *Qualitative Research in Psychology* 22, 2 (2025), 399–438.
- [19] Casey Breen, Cormac Herley, and Elissa M. Redmiles. 2022. A large-scale measurement of cybercrime against individuals. In *Proceedings of the 2022 CHI Conference on Human Factors in Computing Systems*, 1–41.
- [20] Philip Brey. 2010. Values in technology and disclosive computer ethics. *The Cambridge Handbook of Information and Computer Ethics* 4 (2010), 41–58.
- [21] David Burnes, Charles R. Henderson, Jr., Christine Sheppard, Rebecca Zhao, Karl Pillemer, and Mark S. Lachs. 2017. Prevalence of financial fraud and scams among older adults in the United States: A systematic review and meta-analysis. *American Journal of Public Health* 107, 8 (2017), e13–e21.
- [22] Alexandra Burton, Claudia Cooper, Ayesha Dar, Lucy Mathews, and Kartikeya Tripathi. 2022. Exploring how, why and in what contexts older adults are at risk of financial cybercrime victimisation: A realist review. *Experimental Gerontology* 159 (2022), 111678.
- [23] Mark Button and Cassandra Cross. 2017. *Cyber Frauds, Scams and Their Victims*. Routledge.
- [24] Mark Button, Vasileios Karagiannopoulos, Julak Lee, Joon Bae Suh, and Jeyong Jung. 2024. Preventing fraud victimisation against older adults: Towards a holistic model for protection. *International Journal of Law, Crime and Justice* 77 (2024), 100672.
- [25] Mark Button, David Shepherd, Chloe Hawkins, and Jacki Tapley. 2024. Disseminating fraud awareness and prevention advice to older adults: Perspectives on the most effective means of delivery. *Crime Prevention and Community Safety* 26, 4 (2024), 385–400.
- [26] Jacob Camilleri, Ashley Sheil, Michelle O’Keeffe, Moya Cronin, Melanie Gruben, and Hazel Murray. 2025. Cybersafety card game: Empowering digital educators to teach cybersafety to older adults. In *Proceedings of the Extended Abstracts of the CHI Conference on Human Factors in Computing Systems*, 1–12.
- [27] JohnM. Carroll. 2009. Human–computer interaction (HCI). In *Encyclopedia of Human-Computer Interaction*. Mads Soegaard and Rikke Friis Dam (Eds.), Interaction Design Foundation, Aarhus, Denmark.
- [28] Edwin Ka Hung Chung and Dannii Yuen-Lan Yeung. 2023. Reducing older people’s risk of fraud victimization through an anti-scam board game. *Journal of Elder Abuse & Neglect* 35, 2–3 (2023), 121–138.
- [29] Danielle Keats Citron. 2016. The privacy policymaking of state attorneys general. *Notre Dame Law Review* 92 (2016), 747–818.
- [30] Danielle Keats Citron and Daniel J. Solove. 2022. Privacy harms. *Boston University Law Review* 102 (2022), 793–850.
- [31] Carrie Clark, Catherine C. Classen, Anne Fourn, and Maithili Shetty. 2014. *Treating the Trauma Survivor: An Essential Guide to Trauma-Informed Care*. Routledge.
- [32] Rebecca Cole. 2024. Scammed by love: The role of loneliness, trust, and age in financial losses from US online romance scams. *Innovation in Aging* 8, Suppl 1 (2024), 1339.

- [33] Anna Coluccia, Andrea Pozza, Fabio Ferretti, Fulvio Carabellese, Alessandra Masti, and Giacomo Gualtieri. 2020. Online romance scams: Relational dynamics and psychological characteristics of the victims and scammers: A scoping review. *Clinical Practice and Epidemiology in Mental Health: CP & EMH* 16 (2020), 24.
- [34] Elena Comincioli, Eemeli Hakoköngäs, and Masood Masoodian. 2022. Identifying and addressing implicit ageism in the co-design of services for aging people. *International Journal of Environmental Research and Public Health* 19, 13 (2022), 7667.
- [35] Consumer Financial Protection Bureau (CFPB). 2024. Money Smart for Older Adults: Resource Guide. Retrieved from <https://www.consumerfinance.gov/consumer-tools/educator-tools/resources-for-older-adults/money-smart-for-older-adults/>
- [36] Cassandra Cross, Kelly Richards, and Russell G. Smith. 2016. The reporting experiences and support needs of victims of online fraud. *Trends and Issues in Crime and Criminal Justice* 518 (2016), 1–14.
- [37] Debbie Deem and Erik S. Lande. 2018. Transnational scam predators and older adult victims: Contributing characteristics of chronic victims and developing an effective response. *Department of Justice Journal of Federal Law and Practice* 66 (2018), 177–211.
- [38] Martha Deevy and Michaela Beals. 2013. *The Scope of the Problem: An Overview of Fraud Prevalence Measurement*. Financial Fraud Research Center.
- [39] Yue Deng, Changyang He, Yixin Zou, and Bo Li. 2025. “Auntie, please don’t fall for those smooth talkers”: How Chinese younger family members safeguard seniors from online fraud. In *Proceedings of the 2025 CHI Conference on Human Factors in Computing Systems*, 1–17.
- [40] Natalie C. Ebner, Didem Pehlivanoglu, and Alayna Shoenfelt. 2023. Financial fraud and deception in aging. *Advances in Geriatric Medicine and Research* 5, 3 (2023), 1–19.
- [41] Isioma Elueze and Anabel Quan-Haase. 2018. Privacy attitudes and concerns in the digital lives of older adults: Westin’s privacy attitude typology revisited. *American Behavioral Scientist* 62, 10 (2018), 1372–1391.
- [42] Ethn.io. 2025. Incentive Calculator. Retrieved from <https://help.ethn.io/article/124-incentive-calculator>
- [43] Federal Bureau of Investigation. 2013. The FBI’s Efforts to Combat Elder Fraud. Testimony. Retrieved from <https://www.fbi.gov/news/testimony/the-fbis-efforts-to-combat-elder-fraud>
- [44] Federal Bureau of Investigation (FBI). 2024. Scams and Safety—Seniors. Retrieved from <https://www.fbi.gov/scams-and-safety/common-fraud-schemes/seniors>
- [45] Federal Communications Commission. 2025. How to Spot and Avoid Toll Road Payment Scam Texts. Retrieved from <https://www.fcc.gov/consumer-governmental-affairs/how-spot-and-avoid-toll-road-payment-scam-texts>
- [46] Federal Trade Commission. 2024. Second Scams Against Older Adults Advisory Group Meeting. Retrieved from https://www.ftc.gov/system/files/ftc_gov/pdf/final_transcript_-_second_scams_against_older_adults_advisory_group_meeting_-_april_2_2024.pdf
- [47] Jennifer Fereday and Eimear Muir-Cochrane. 2006. Demonstrating rigor using thematic analysis: A hybrid approach of inductive and deductive coding and theme development. *International Journal of Qualitative Methods* 5, 1 (2006), 80–92.
- [48] FINRA Foundation. 2015. The Non-Traditional Costs of Financial Fraud: The Impact on Victims and Society. Retrieved from https://www.finrafoundation.org/sites/finrafoundation/files/2024-10/non-traditional-costs-financial-fraud_0_0.pdf
- [49] Bent Flyvbjerg. 2006. Five misunderstandings about case-study research. *Qualitative Inquiry* 12, 2 (2006), 219–245.
- [50] Sarah Fox, Mariam Asad, Katherine Lo, Jill P. Dimond, Lynn S. Dombrowski, and Shaowen Bardzell. 2016. Exploring social justice, design, and HCI. In *Proceedings of the 2016 CHI Conference Extended Abstracts on Human Factors in Computing Systems*, 3293–3300.
- [51] Alisa Frik, Leysan Nurgalieva, Julia Bernd, Joyce Lee, Florian Schaub, and Serge Egelman. 2019. Privacy and security threat models and mitigation strategies of older adults. In *Proceedings of the 15th Symposium on Usable Privacy and Security (SOUPS ’19)*, 21–40.
- [52] Claire Garbett. 2016. From passive objects to active agents: A comparative study of conceptions of victim identities at the ICTY and ICC. *Journal of Human Rights* 15, 1 (2016), 40–59.
- [53] Vaibhav Garg, L. Jean Camp, Katherine Connelly, and Lesa Lorenzen-Huber. 2012. Risk communication design: Video vs. text. In *Proceedings of 12th International Symposium on the Privacy Enhancing Technologies (PETS ’12)*. Springer, 279–298.
- [54] M. George, C. Graham, and L. Lennard. 2015. *Only the Tip of the Iceberg: Fraud Against Older People*. Technical Report. Age UK, London, UK.
- [55] Gillespie Tarleton. 2018. *Custodians of the Internet: Platforms, Content Moderation, and the Hidden Decisions That Shape Social Media*. Yale University Press.
- [56] Emily A. Greenfield, Kathy Black, Tine Buffel, and Jarmin Yeh. 2019. Community gerontology: A framework for research, policy, and practice on communities and aging. *The Gerontologist* 59, 5 (2019), 803–810.

- [57] Jeffrey E. Hall, Debra L. Karch, and Alex Crosby. 2016. *Uniform Definitions and Recommended Core Data Elements for Use in Elder Abuse Surveillance*. National Center for Injury Prevention and Control, Centers for Disease Control and Prevention.
- [58] LaToya Hall, Jennifer M. Gómez, and Peter A. Lichtenberg. 2023. Trust and betrayal in older adult financial exploitation. *Aging & Mental Health* 27, 12 (2023), 2466–2473.
- [59] S. Duke Han, Patricia A. Boyle, Bryan D. James, Lei Yu, and David A. Bennett. 2015. Mild cognitive impairment and susceptibility to scams in old age. *Journal of Alzheimer's Disease* 49, 3 (2015), 845–851.
- [60] Desirée Henderson. 2019. *How to Read a Diary: Critical Contexts and Interpretive Strategies for 21st-Century Readers*. Routledge.
- [61] Emily F. Henderson. 2021. How short is too short? Exploring diary study duration from the perspective of researching conferences and other short-term phenomena in higher education and beyond. In *Exploring Diary Methods in Higher Education Research*. Xuemeng Cao and Emily F. Henderson (Eds.), Routledge, 29–43.
- [62] Michael Henderson, Nicola F. Johnson, and Glenn Auld. 2013. Silences of ethical practice: Dilemmas for researchers using social media. *Educational Research and Evaluation* 19, 6 (2013), 546–560.
- [63] L. D. Herrera, London Van Sickle, and Ashley Podhradsky. 2024. Bridging the protection gap: Innovative approaches to shield older adults from AI-enhanced scams. arXiv:2409.18249. Retrieved from <https://arxiv.org/abs/2409.18249>
- [64] Kristy Holtfrete, Michael Dean Reisig, Daniel P. Mears, and Scott E. Wolfe. 2014. Financial Exploitation of the Elderly in a Consumer Context. In *Final report to the National Institute of Justice, Grant number 2010-IJ-CX-0008. NCJ 245388*. U.S. Department of Justice, Office of Justice Programs, National Institute of Justice.
- [65] Lauri L. Hyers. 2018. *Diary Methods*. Oxford University Press.
- [66] Loredana Ivan and Stephen J. Cutler. 2021. Ageism and technology: The role of internalized stereotypes. *University of Toronto Quarterly* 90, 2 (2021), 127–139.
- [67] Shelly L. Jackson. 2017. Senate special committee on aging hearings and GAO reports. In *Elder Abuse: Research, Practice and Policy*. Xin Qi Dong (Ed.). Springer International Publishing, 595–613.
- [68] Bryan D. James, Patricia A. Boyle, and David A. Bennett. 2014. Correlates of susceptibility to scams in older adults without dementia. *Journal of Elder Abuse & Neglect* 26, 2 (2014), 107–122.
- [69] Carlos Jensen, Heather Lonsdale, Eleanor Wynn, Jill Cao, Michael Slater, and Thomas G. Dietterich. 2010. The life and times of files and information: A study of desktop provenance. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, 767–776.
- [70] Rebecca Judges. 2021. *Scams and Aging: Factors Impacting Effective Decision Making*. Ph.D. Dissertation. University of Toronto.
- [71] Stella Kazamia, Chris Culnane, Daniel Gardham, Suzanne Prior, and Helen Treharne. 2024. Phish and tips: Phishing awareness and education for older adults. In *Proceedings of the International Symposium on Human Aspects of Information Security and Assurance*. Springer, 200–214.
- [72] Heather Kelly. 2024. Sick of scams? Stop answering your phone. *The Washington Post* (2024).
- [73] Steven Kemp and Nieves Erades Pérez. 2023. Consumer fraud against older adults in digital society: Examining victimization and its impact. *International Journal of Environmental Research and Public Health* 20, 7 (2023), 5404.
- [74] Hanna Köttl, Laura D. Allen, Ittay Mannheim, and Liat Ayalon. 2023. Associations between everyday ICT usage and (self-) ageism: A systematic literature review. *The Gerontologist* 63, 7 (2023), 1172–1187.
- [75] Jeffrey Kullgren, Erica Solway, Scott Roberts, Dianne Singer, Matthias Kirch, Nicholas Box, Emily Smith, and Lauren Hutchens. 2023. *National Poll on Healthy Aging: Experiences with Scams Among Older Adults*. Technical Report. University of Michigan Institute for Healthcare Policy and Innovation.
- [76] Lawrence. 2006. *Lessig. Code: Version 2.0*. Basic Books.
- [77] Brian D. Loader and Douglas Thomas. 2013. *Cybercrime: Law Enforcement, Security and Surveillance in the Information Age*. Routledge.
- [78] Alex Jiahong Lu, Shruti Sannon, Cameron Moy, Savana Brewer, Jaye Green, Kisha N. Jackson, Daivon Reeder, Camaria Wafer, Mark S. Ackerman, and Tawanna R. Dillahunt. 2023. Participatory noticing through photovoice: Engaging arts-and community-based approaches in design research. In *Proceedings of the 2023 ACM Designing Interactive Systems Conference*, 2489–2508.
- [79] Alex Jiahong Lu, Shruti Sannon, Cameron Moy, Savana Brewer, Jaye Green, Kisha N. Jackson, Daivon Reeder, Camaria Wafer, Mark S. Ackerman, and Tawanna R. Dillahunt. 2023. Shifting from surveillance-as-safety to safety-through-noticing: A photovoice study with eastside Detroit residents. In *Proceedings of the 2023 CHI Conference on Human Factors in Computing Systems*, 1–19.
- [80] Nancy E. Lundebjerg, Daniel E. Trucil, Emily C. Hammond, and William B. Applegate. 2017. When it comes to older adults, language matters: Journal of the American Geriatrics Society adopts modified American Medical Association style. *Journal of the American Geriatrics Society* 65, 6 (2017), 1386–1387. DOI: <https://doi.org/10.1111/jgs.14941>

- [81] Zeya Lwin Tun and Daniel Birks. 2023. Supporting crime script analyses of scams with natural language processing. *Crime Science* 12, 1 (2023), 1.
- [82] Martina Miche, Allyson Brothers, Hans-Werner Wahl, and Manfred Diehl. 2015. Subjective aging and awareness of aging: Toward a new understanding of the aging self. *Annual Review of Gerontology and Geriatrics* 35, 1 (2015), 1–28.
- [83] Rennie Naidoo. 2015. Analysing urgency and trust cues exploited in phishing scam designs. In *Proceedings of the 10th International Conference on Cyber Warfare and Security*, 216–222.
- [84] Andrew Nash. 2007. Victims by definition. *Washington University Law Review* 85, 6 (2007), 1419–1462.
- [85] 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, Psychological Sciences and Social Sciences* 76, 5 (2021), 996–1004.
- [86] James Nicholson and Jill McGlasson. 2020. CyberGuardians: Improving community cyber resilience through embedded peer-to-peer support. In *Proceedings of the Companion Publication of the 2020 ACM Designing Interactive Systems Conference*, 117–121.
- [87] James Nicholson, Ben Morrison, Matt Dixon, Jack Holt, Lynne Coventry, and Jill McGlasson. 2021. Training and embedding cybersecurity guardians in older communities. In *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems*, 1–15.
- [88] Jean-Robert Nino, Gustav Enström, and Alan R. Davidson. 2017. Factors in fraudulent emails that deceive elderly people. In *Human Aspects of IT for the Aged Population*. Jia Zhou and Gavriel Salvendy (Eds.), Lecture Notes in Computer Science, Springer, 360–368.
- [89] Gregory Norcie, Emiliano De Cristofaro, and Victoria Bellotti. 2013. Bootstrapping trust in online dating: Social verification of online dating profiles. In *Proceedings of the International Conference on Financial Cryptography and Data Security*. Springer, 149–163.
- [90] Lorelli S. Nowell, Jill M. Norris, Deborah E. White, and Nancy J. Moules. 2017. Thematic analysis: Striving to meet the trustworthiness criteria. *International Journal of Qualitative Methods* 16, 1 (2017), 1–13.
- [91] Alana Officer and Vânia de la Fuente-Núñez. 2018. A global campaign to combat ageism. *Bulletin of the World Health Organization* 96, 4 (2018), 295.
- [92] Daniela Oliveira, Harold Rocha, Huizi Yang, Donovan Ellis, Sandeep Dommaraju, Melis Muradoglu, Devon Weir, Adam Soliman, Tian Lin, and Natalie Ebner. 2017. Dissecting spear phishing emails for older vs. young adults: On the interplay of weapons of influence and life domains in predicting susceptibility to phishing. In *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems*. ACM, 6412–6424.
- [93] Nancy Nyquist Potter. 2002. *How Can I be Trusted? A Virtue Theory of Trustworthiness*. Bloomsbury Publishing PLC.
- [94] Larissa Pschetz and Michelle Bastian. 2018. Temporal design: Rethinking time in design. *Design Studies* 56 (2018), 169–184.
- [95] Qualtrics, Inc. 2024. Qualtrics: Experience Management Platform. Retrieved from <https://www.qualtrics.com>.
- [96] Anabel Quan-Haase and Dennis Ho. 2020. Online privacy concerns and privacy protection strategies among older adults in East York, Canada. *Journal of the Association for Information Science and Technology* 71, 9 (2020), 1089–1102.
- [97] Bogdana Rakova, Renee Shelby, and Megan Ma. 2023. Terms-we-serve-with: Five dimensions for anticipating and repairing algorithmic harm. *Big Data & Society* 10, 2 (2023), 1–14.
- [98] Madhu C. Reddy, Paul Dourish, and Wanda Pratt. 2006. Temporality in medical work: Time also matters. *Computer Supported Cooperative Work (CSCW)* 15, 1 (2006), 29–53.
- [99] Michael Ross, Igor Grossmann, and Emily Schryer. 2014. Contrary to psychological and popular opinion, there is no compelling evidence that older adults are disproportionately victimized by consumer fraud. *Perspectives on Psychological Science* 9, 4 (2014), 427–442.
- [100] Suleiman Saka and Sanchari Das. 2025. “Watch my health, not my data”: Understanding perceptions, barriers, emotional impact, & coping strategies pertaining to IoT privacy and security in health monitoring for older adults. In *Proceedings of the 2025 CHI Conference on Human Factors in Computing Systems*, 1–18.
- [101] Dawn M. Sarno, Joanna E. Lewis, Corey J. Bohil, and Mark B. Neider. 2020. Which phish is on the hook? Phishing vulnerability for older versus younger adults. *Human Factors* 62, 5 (2020), 704–717.
- [102] Sarita Schoenebeck, Oliver L. Haimson, and Lisa Nakamura. 2021. Drawing from justice theories to support targets of online harassment. *New Media & Society* 23, 5 (2021), 1278–1300.
- [103] Amartya Sen. 2009. *The Idea of Justice*. Penguin Books, London.
- [104] Lauren R. Shapiro. 2025. Cyber-enabled imposter scams against older adults in the United States. *Security Journal* 38, 1 (2025), 1–28.
- [105] Stephanie B. Steinhardt and Steven J. Jackson. 2014. Reconciling rhythms: Plans and temporal alignment in collaborative scientific work. In *Proceedings of 17th ACM Conference on Computer Supported Cooperative Work & Social Computing*, 134–145.

- [106] Lucille Alice Suchman. 1987. *Plans and Situated Actions: The Problem of Human-Machine Communication*. Cambridge University Press.
- [107] Sharifa Sultana, Sadia Tasnuva Pritha, Rahnuma Tasnim, Anik Das, Rokeya Akter, Shaid Hasan, S. M. Raihanul Alam, Muhammad Ashad Kabir, and Syed Ishtiaque Ahmed. 2022. ‘Shishushurokkha’: A transformative justice approach for combating child sexual abuse in Bangladesh. In *Proceedings of the 2022 CHI Conference on Human Factors in Computing Systems*, 1–23.
- [108] Grindr Editorial Team. 2025. Announcing ‘Taken on Grindr’: Real In-App Photos for a Better Grindr Experience. Retrieved from <https://www.grindr.com/blog/announcing-taken-on-grindr-real-in-app-photos-for-a-better-grindr-experience>
- [109] Paolo Vanini, Sebastiano Rossi, Ermin Zvizdic, and Thomas Domenig. 2023. Online payment fraud: From anomaly detection to risk management. *Financial Innovation* 9, 1 (2023), 66.
- [110] Mark Verstraete and Derek E. Bambauer. 2017. Ecosystem of distrust. *First Amendment Law Review* 16 (2017), 129.
- [111] John Vines, Gary Pritchard, Peter Wright, Patrick Olivier, and Katie Brittain. 2015. An age-old problem: Examining the discourses of ageing in HCI and strategies for future research. *ACM Transactions on Computer-Human Interaction* 22, 1 (2015), 1–27.
- [112] Margaret Urban Walker. 2006. *Moral Repair: Reconstructing Moral Relations After Wrongdoing*. Cambridge University Press.
- [113] 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 2022 IEEE Symposium on Security and Privacy (SP)*. IEEE, 2344–2360.
- [114] Ernest J. Weinrib. 2012. *The Idea of Private Law*. Oxford University Press.
- [115] Mikael Wiberg and Erik Stolterman. 2021. Time and temporality in HCI research. *Interacting with Computers* 33, 3 (2021), 250–270.
- [116] Jill Palzkill Woelfer and David G. Hendry. 2012. Homeless young people on social network sites. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, 2825–2834.
- [117] Ryan Wyeth, Dariusz Ilnicki, and Krzysztof Janc. 2025. Cryptocurrency ATMs and cryptofication of everyday life: The uneven diffusion of crypto into quotidian spaces and places. *Progress in Economic Geography* 3, 2 (2025), 100047.
- [118] Mary F. Wyman, Sharon Shiovitz-Ezra, and Jürgen Bengel. 2018. Ageism in the health care system. Providers, patients, and systems. In *Contemporary Perspectives on Ageism*, 193–212.
- [119] Qian Yang, Richmond Y. Wong, Steven Jackson, Sabine Junginger, Margaret D. Hagan, Thomas Gilbert, and John Zimmerman. 2024. The future of HCI-policy collaboration. In *Proceedings of the CHI Conference on Human Factors in Computing Systems*, 1–15.
- [120] Guoyi Ye, Geng Hong, Yuan Zhang, and Min Yang. 2024. Interface illusions: Uncovering the rise of visual scams in cryptocurrency wallets. In *Proceedings of the ACM Web Conference 2024*, 1585–1595.
- [121] Hyun-E. Yeom, Eunyong Park, and Misook Jung. 2020. Age-related difference in the relationship between age stereotypes and health behavior in midlife Koreans. *Innovation in Aging* 4, Suppl 1 (2020), 447–448.
- [122] Yuxiang Zhai, Xiao Xue, Zekai Guo, Tongtong Jin, Yuting Diao, and Jihong Jeung. 2025. Hear us, then protect us: Navigating deepfake scams and safeguard interventions with older adults through participatory design. In *Proceedings of the 2025 CHI Conference on Human Factors in Computing Systems*, 1–19.

Appendix

A Survey Questions

Survey Responses	N	%
<i>How frequently do you encounter scams?</i>		
Never	0	0%
Once a week	1	2%
More than once a week	23	52%
Once a month	8	18%
More than once a month	5	11%
Once a year	1	2%
Other	6	14%
<i>How frequently have you endured a scam?</i>		
Never	1	2%
One time	19	43%
2–3 times	17	39%
4–5 times	3	7%
More than 5 times	4	9%
<i>When was the last time you endured a scam?</i>		
Within the past week	5	12%
Within the past month	17	40%
Within the past year	15	36%
1–2 years ago	2	5%
3–4 years ago	1	2%
More than 4 years ago	2	5%
<i>Think about the last time you endured a scam: How did you receive the scam?</i>		
In person	3	7%
Over the phone	8	19%
Over e-mail	9	21%
Through text message	10	23%
On a Website	6	14%
Through a pop-up ad	1	2%
Other	6	14%

Survey Responses	N	%
<i>How were you convinced this scam was legitimate?</i>		
Nothing, it was an accident or mistake	1	2%
The scam used my name	3	7%
The scam said they were someone I know	5	12%
The scam said they were a government agency	4	9%
The scam said they were a corporation	8	19%
The scam said I had won or received something	5	12%
Other	17	40%
<i>What has been the result of your being scammed? (Check all that apply)</i>		
Financial loss	17	40%
Identity theft	6	14%
Emotional distress	19	44%
Damage to credit score	3	7%
Legal consequences	1	2%
Loss of trust	25	58%
Impact on personal and professional life	8	19%
Other	8	19%
<i>After enduring this scam, did you... (Check all that apply)</i>		
Try to get your money back	16	37%
Cancel your credit card(s)	16	37%
Delete your Internet history	5	12%
Restart your phone/computer	10	23%
Change your password(s)	20	47%
Other	14	33%

Survey Responses	N	%	Free Text Response
<i>Did you use a government resource after being scammed?</i>			<i>How did you feel after being scammed?</i>
No, I did not (I chose not to)	13	30%	Felt used, and also “dumb”; vulnerable; a bit stupid;
No, I did not (I didn’t think about)	19	44%	Stupid; like an idiot!; I’m not one to talk about my feelings so I don’t know; it made me mad that they misled me; concerning; upset and angry as a result of the ease in which these fraudulent activities occur; I felt violated and ridiculed; panicked, worried, will this ever stop; angry; angry, worried, frightened, stupid, vulnerable; violated; like a fool for falling for it. If a deal sounds too good to be true, it usually isn’t; pretty dumb, but I kept going, so instead of stopping and listening to my intuition, I bought into the urgency of the scammer and made the Zelle transfer anyway. Regret and depression were also in the mix; stupid; I felt weak and sick to my stomach; I felt inferior; like I was stupid; frustrated because I now need to pay closer attention to details; I am very distrustful. My first time led to financial loss and a great learning experience; here we go again! I get depressed and discouraged; embarrassed; really stupid, vulnerable, and elderly; stupid; stupid; I’m educated, cautious, and prudent with money...I feel sucker punched; Stupid; totally shocked at first, very hurt, still can’t believe it, want to do something to them; Scared, anxious; very, very hurt, stressed, mad; It scared me that I bought into it so easily. Thinking it was my boss reaching out to me... I know of many scams (recently a friend) and one of my brothers. My mother all the time. We’re all intelligent, educated people, and it angers and scares me how this is happening; broken-hearted, used; I feel scared that as careful as I am, I could not see it coming; horrible; I felt devastated and I’m still scared because I don’t know if my identity is still out there; Disappointed, distrustful; Stupid; I felt grateful that I asked questions and followed through because it enabled me to protect myself; Stupid; like a jerk, stupid.
Yes, I did (please list the resources below)	12	28%	
<i>Did you use a corporate resource after being scammed?</i>			
No, I did not (I chose not to)	8	19%	
No, I did not (I didn’t think about)	8	19%	
Yes, I did (please list the resources below)	26	62%	
<i>Did you contact your friends or family after being scammed?</i>			
No, I did not (I chose not to)	9	21%	
No, I did not (I didn’t think about)	3	7%	
Yes, I did (please list the resources below)	30	70%	
<i>Which of the following best describes your gender?</i>			
Male	14	33%	
Female	29	67%	
<i>Which is your race or ethnic origin? (Check all that apply)</i>			
Asian, Hawaiian/Pacific Islander	3	7%	
Black or African American	2	5%	
White or Caucasian	38	88%	
<i>What is the highest level of education you have completed?</i>			
High school graduate or GED	2	5%	
Some college/AA degree/Technical school training	8	19%	
2-year associate’s degree	5	12%	
4-year undergraduate degree	14	33%	
Graduate school degree: Master’s or doctorate degree (MD, PhD, JD)	13	30%	
Other	1	2%	

“Other” Responses

How frequently do you encounter scams?

4–5 times a year; don’t know; Facebook; not sure which are scams; I haven’t had it happen for a while. I was getting scam every couple of weeks or so; I’m not sure how often.

Think about the last time you were endured a scam: How did you receive the scam?

Computer pop-up; bank card used; via computer; got e-mail first then follow up in the mail; Facebook ad; Facebook ad.

How were you convinced this scam was legitimate?

The text said it was USPS; they said that they worked for my bank; selling a dementia product; secured my credit card number and ID number through some unknown source; impersonated my credit card company; cc stolen; something I was looking to buy and a search on the item led me to the fake Honey pot web site. They made it look like a big box store’s web site; The web site address I found to get contact phone number was fraudulent; bank notified me of suspicious activity; offer of employment; my own hopes and stupidity; said it was my bank; Used hometown city, used another’s info on site to appear small town local; I think a bot not sure let me think about this?; asking to download apps and to enter credit card numbers; I called listed number and they could not give me information regarding transaction; looked like a normal text from my bank.

“Other” Responses

What has been the result of your being scammed?

Fraudulent use of credit card information; all of which was ultimately recovered; fraudulent charges to my credit card which I then had to cancel immediately; my daughter caught the scam before they stole money; I reached a resolution and credit to my account after several calls, contacting Better Business Bureau and dispute on my credit card; having to redo my entire retirement account and my husband’s; first, it was financial loss but then through persistence and not giving up I got all my money back over \$1,200.00; Spend so much time to remedy; had to get a new credit card.

After being scammed, did you... (Check all that apply)

Called Geek Squad; nothing; added my daughters to my bank account so that they could have online account to monitor, they also changed the settings on my phone to silence unknown callers/texters; I did not follow up. I would get an e-mail stating I was to go to a store (like Walmart) and interview a clerk. They then would send me a money order from a bank. Usually between \$3,000 and \$5,000 dollars. I was to use the money for the interview. Leaving me \$2,500 payout. I had presence of mind to call the bank to check on the validity. It would be fake always. The money orders looked perfect.

What is the highest level of education you have completed?

Some graduate school.

“Other” Responses

Did you use a government resource after being scammed?

FTA; local police; I filed a police report 10 months ago; FCC, County Sheriff’s Dept.; Better Business Bureau; police, federal trade comm, all banks issuing cards, all credit agencies; filed a report; city police and police detective; federal tax people.

Did you use a corporate resource after being scammed?

Credit card companies; bank who issued the credit card; Geek Squad; My bank; mastercard for a dispute of charges; credit card company; I gave a fake check to Huntington Bank that used its logo; Wells Fargo, Capital One, FNBO, Barclays; worked with fidelity to reset all accounts; Bank of America; Bank of America; reported it to my Senator and a few other agencies including Zelle and Bank of America; Credit card company, Amazon; KeyBank; Experian; Credit card company; PayPal; I checked my account online; Called credit card company fraud division; My credit union; I thought about contacting the IRS; my bank, Apple Help, Internet companies; target; credit union; bank fraud investigative team.

“Other” Responses

Did you contact your friends or family after being scammed?

Spouse; daughter; I told everyone to be careful; daughters helped me; wife; sister also got hacked; jeweler; had to tell husband with Alzheimer’s, told my son and daughter; friends and relatives; another friend that I forwarded the “great deal” to; told everyone to watch out for this particular scam; spouse; I told my girlfriend; wife; college roommate who works in Criminal Justice, my wife and children; son; friends; my spouse; my sister, people who knew me for several years from work; told a few people who asked me where I’ve been; I screenshot and copied my other boss; my son and daughter; I contacted my son; posted on Facebook; my sister; my son and daughter; spouse; everybody (they said “that happened to me”).

Received 27 February 2025; revised 17 February 2026; accepted 7 March 2026