Detection and Impact of Debit/Credit Card Fraud: Victims' Experiences

EMAN ALASHWALI, King Abdulaziz University (KAU) and King Abdullah University of Science and Technology (KAUST), Saudi Arabia
RAGASHREE MYSURU CHANDRASHEKAR, Carnegie Mellon University (CMU), United States
MANDY LANYON, Carnegie Mellon University (CMU), United States
LORRIE FAITH CRANOR, Carnegie Mellon University (CMU), United States

It might be intuitive to expect that small or reimbursed financial loss resulting from credit or debit card fraud would have low or no financial impact on victims. However, little is known about the extent to which financial fraud impacts victims psychologically, how victims detect the fraud, which detection methods are most efficient, and how the fraud detection and reporting processes can be improved. To answer these questions, we conducted a 150-participant survey of debit/credit card fraud victims in the US. Our results show that significantly more participants reported that they were impacted psychologically than financially. However, we found no relationship between the amount of direct financial loss and psychological impact, suggesting that people are at risk of being psychologically impacted regardless of the amount lost to fraud. Despite the fact that bank or card issuer notifications were related to faster detection of fraud, more participants reported detecting the fraud after reviewing their card or account statements rather than from notifications. This suggests that notifications may be underutilized. Finally, we provide a set of recommendations distilled from victims' experiences to improve the debit/credit card fraud detection and reporting processes.

ACM Reference Format:
Eman Alashwali, Ragashree Mysuru Chandrashekar, Mandy Lanyon, and Lorrie Faith Cranor. 2024. Detection and Impact of Debit/Credit Card Fraud: Victims' Experiences. In *The 2024 European Symposium on Usable Security (EuroUSEC 2024), September 30-October 1, 2024, Karlstad, Sweden.* ACM, New York, NY, USA, 36 pages. https://doi.org/10.1145/3688459.3688464

1 Introduction

Financial fraud represents a serious challenge globally to both individuals and society. Notably, identity theft fraud, a type of fraud that includes credit and debit card fraud according to the United States Federal Trade Commission (FTC) definitions, is the top-ranked reported type of fraud in 2021 and 2022 in the US, representing 23.43% and 20.47% of the reported frauds respectively [19]. In 2022, the top three payment methods used in the reported frauds were credit cards, debit cards, and payment apps or services, with $219.9 million, $195.2 million, and $163.5 million losses respectively [20]. In 2021, according to a report on victims of identity theft by the Bureau of Justice Statistics (BJS), which also considers credit card and bank frauds under identity theft, 9% of the US population aged 16 or older had experienced identity theft in the past 12 months, with nearly 4% had experienced credit card fraud, and 3% had experienced bank account

*Eman Alashwali was a Collaborating Visitor at CMU while working on this paper. Both Eman and Ragashree contributed equally.

Authors' Contact Information: Eman Alashwali, King Abdulaziz University (KAU) and King Abdullah University of Science and Technology (KAUST), Saudi Arabia , ealashwali@kau.edu.sa; Ragashree Mysuru Chandrashekar, Carnegie Mellon University (CMU), United States, ragashreeshekar@gmail.com; Mandy Lanyon, Carnegie Mellon University (CMU), United States, mandy@cmu.edu; Lorrie Faith Cranor, Carnegie Mellon University (CMU), United States, lorrie@cmu.edu.

Manuscript submitted to ACM

fraud. The identity theft experiences did not only affect victims financially, but also resulted in 10% of victims feeling extremely distressed, and 56% spending a mean time of four hours to resolve the financial or credit issues [25].

In the US, debit/credit card fraud victims are legally protected by laws and regulations, such as the Electronic Fund Transfer Act (Regulation E) [21]. This limits victims' liability for unauthorized transfers if they give timely notice to the financial institution. For example, consumer liability is limited to $50 if a notice is given to the financial institution within two business days [11]. Intuitively, this should limit the financial impact on victims as long as they are reimbursed or compensated for financial loss in a timely manner. While most fraud reports focus on financial loss, little attention is paid to understanding victims' experiences, such as how they detected the fraud and the psychological impact resulting from the fraud.

This paper aims to bridge the gap in understanding victims' experiences with fraud. To this end, we surveyed 150 participants in the US who experienced a debit/credit card fraud incident within the last three years and asked them to report on their most recent fraud experience.

This paper explores how victims detect fraud and to what extent fraud impacts victims psychologically. We also explore the relationship between psychological impact and the amount of financial loss. Finally, we use our data to provide recommendations for improving the fraud detection and reporting processes.

The key findings of this study are as follows:

- While notifications were related to faster fraud detection, fewer participants reported that they detected the fraud through notifications than through reviewing card or account statements, suggesting that notifications may be underutilized.
- Significantly more participants reported that they were psychologically impacted than financially impacted by fraud.
- Among our participants, the psychological impact was not related to the amount of financial loss, suggesting that people are at risk of being psychologically impacted regardless of the amount lost to fraud.

Based on our findings, we suggest that banks and card issuers: utilize basic notifications by default; provide victims with explanations about how the fraud happened (if applicable) with actionable advice on how to protect themselves from future fraud; and examine solutions to remediate psychological impacts of fraud.

2 Background and Related Work

In this section, we provide a summary of related work on debit/credit card fraud detection techniques (Section 2.1). We then summarize some challenges faced by victims in reporting financial fraud (Section 2.2). Finally, we summarize related work on the impact of financial fraud on victims (Section 2.3).

2.1 Fraud Detection

As fraudulent transactions often share common features, automated systems can be trained to detect them [42]. Generally speaking, before approving each transaction, financial institutions use fraud detection systems that employ a classifier to determine whether the requested transaction is suspicious or not [42]. Since fraud techniques evolve over time, fraud detection systems also need to learn continuously [42].

Researchers have proposed a plethora of automated financial fraud detection methods that use Artificial Intelligence (AI) and Machine Learning (ML) [10, 14, 27, 42, 44, 46]. However, Ryman-Tubb et al. evaluated 51 AI and ML published methods for payment card fraud detection and found that only 8 have performance applicable for deployment in the industry [42]. The technical details of financial fraud detection methods are beyond the scope of this paper.

Despite numerous published research papers on automated financial fraud detection techniques, we have observed that many victims of financial fraud, including some of this paper's authors, detected fraudulent transactions through self-realization when they found transactions they did not make appeared in their bank statements. For example, Jansen and Luekfeldt analyzed 600 cases of phishing and malware banking fraud in the Netherlands [26]. They found that participants played a major role in discovering the fraud, after which they contacted their bank [26]. This included cases where victims had uncomfortable or suspicious feelings regarding an interaction, consulted family or friends, noticed unfamiliar payments or changes in their balance, or could not log in to their online bank account [26].

Very little research has investigated how victims of financial fraud discovered that they have been defrauded. In our study, we investigate detection methods from victims' experiences (Section 4.3).

2.2 Fraud Reporting and Resolution

Prior studies reported some obstacles victims face in reporting fraud incidents, which in some cases affected victims' attitudes towards reporting and led them to not report the incident at all. A common reporting issue victims may face is the lack of information regarding the responsible authority [39] and a confusing list of reporting channels [12]. Victims have multiple reporting channels to choose from: the store or company's customer service, the bank, credit card company or other payment provider, law enforcement, and consumer protection organizations [16, 36]. Razaq et al.'s study on mobile-based financial fraud in Pakistan found that 49% of the victims did not report the incident at all [39]. Some of the documented issues that led to not reporting the fraud are: difficulties in reporting, unsatisfactory outcomes, lack of evidence or feeling responsible about the fraud, and embarrassment [9, 12, 16, 39]. Prior work identified victims' needs to improve the reporting and resolution processes, such as: having clear reporting channels, feeling like they are being listened to, receiving an acknowledgment that they have been victims of a crime, and receiving access to professional support services to treat the psychological consequences [12]. Button et al.'s survey on victims from the UK found that most victims need a single point of contact to report the fraud, sympathetic response, and be listened to [8].

In our study, we identify recommendations to improve the reporting process (Section 4.4).

2.3 Fraud Impact

Prior research showed that fraud can severely impact victims and their families. Ganzini et al. compared data for victims of violent (e.g. robbery) and non-violent (financial fraud) crimes [23]. They found that anxiety and depression disorders were the most common psychological implications for both types of crimes [23]. Cross et. al. interviewed 80 participants from Australia who experienced online fraud with losses of $10,000 or more in the past four years [12]. They found that financial impact was affected by the amount of money lost and other life circumstances of the victim [12]. However, most participants experienced significant emotional and psychological impacts, and some experienced impacts on their health and family relationships [12]. For many victims, the impact was long-lasting and led to behavior change [12]. DeLiema et al. examined the financial and psychological impact of identity theft victims from older adults (aged 65 or older) by analyzing data from 2000 self-reported victims [15]. Their results suggested that the resulting harm from identity theft goes beyond financial loss. While only 7% suffered from "out-of-pocket costs" (costs that were not reimbursed), 34% found the experience distressing [15]. They also found that the length of time the information was stolen before detecting the fraud and the time spent to resolve the issue were positively related to emotional distress [15]. Riek and Böhme surveyed 1242 victims of cybercrime from 6 European countries about 7 types of consumer-facing cybercrime [41]. They found that scams are the severest type of cybercrime [41]. Moreover, they found that non-financial losses such as time, including protection time, exceed out-of-pocket (non-reimbursed) losses in most countries in the study [41].

Unlike Cross et al.'s study [12], which included victims with high-value financial loss, and DeLiema et al.'s study [15], which included only older adult victims, our study included adult victims with any amount of loss from any age. Moreover, unlike prior work, our study provides both qualitative and quantitative insights and studies the relationship between financial and psychological impact in further depth (Section 4.5).

3 Methods

In this section, we describe our methods. We first present the study's scope and definitions (Section 3.1). We then describe the recruitment processes (Section 3.2), survey design (Section 3.3), analysis (Section 3.4), and ethical considerations (Section 3.5). Finally, we list some limitations (Section 3.6).

3.1 Scope and Definitions

Our study's scope is victims' experiences in financial fraud pertaining to debit/credit cards. For the purpose of our survey, we created a general definition of debit/credit card fraud and presented it to participants. Our definition includes fraud incidents that occurred with or without the victim's participation in the fraudulent transaction. It also does not restrict the fraud technique apart from a debit/credit card involved (associated with either a personal or business account). Thus, it includes incidents resulting from individual financial fraud [5], such as those related to products and services (e.g. overcharging), as well as those including identity theft (e.g. stolen card details that resulted in fraudulent purchases). We defined **credit/debit card fraud** to participants as follows: an "incident where any amount of money was charged to your debit/credit card without your knowledge or consent." This definition was embedded in the screening survey (Q.2 in Appendix B.2) that asked participants whether they had experienced a debit/credit card fraud incident.

Throughout the paper, we use the term **victim** to refer to the cardholder who experienced the fraud incident, and the term **fraudster** to refer to the adversaries behind the fraud execution. We use the term **fraud** to refer to debit/credit card fraud.

3.2 Recruitment

We recruited 150 participants for our online survey. The sample size was motivated by balancing cost-effectiveness and acceptable statistical power for scientific research [45]. A power analysis using the G*Power statistical tool [7] for the Chi-square (χ^2) test family with effect size w = 0.3 (medium), α err prob = 0.05, Power (1 - β err prb) = 0.90, Df = 2 suggests that 150 participants is sufficient.

We recruited survey participants using Prolific [37], a research-oriented online participant recruitment platform. We used a screening survey to identify participants who had experienced a financial loss in a debit/credit card fraud incident within the last three years. In addition, we screened for participants with at least a 90% approval rate on Prolific who were at least 18 years old, residing in the United States, and able to read and write in English. Those who met the screening criteria and provided at least a 20-character[1] description of a fraud incident and how they discovered it were automatically approved and immediately invited to take part in the main survey. After participants completed the main survey, we manually reviewed open-ended responses to both the screening survey and the main survey and excluded participants who gave invalid responses on either survey. We chose to approve the screening survey automatically and do manual validation later so that participants could do both surveys in one session.

[1]As part of the screening, participants were not told the minimum number of characters required. We chose 20 characters according to our rough estimate of a minimal valid response length.

Of the 268 participants who completed the screening survey, 170 were eligible for the main survey, and 154 completed the main survey. We excluded four invalid survey responses: two invalid responses reported $0 direct loss, conflicting with our requirement that participants have experienced financial loss "even if it was later compensated or reimbursed;" one participant provided a fraud description not related to debit/credit cards; and one participant's open-ended responses were of low quality, indicating inattention. We ended up with 150 completed responses included in our analysis.

We paid participants $0.50 for completing the screening survey and $3.75 for completing the main survey. We began recruiting survey participants on November 13, 2023 and ended recruitment the same day after we reached 154 responses.

3.3 Survey Design

We conducted the screening survey and main survey using Qualtrics [38], an online survey platform. The screening survey questions and main survey questions are detailed in Appendix B.

Our main survey had six sections. In the first section, we asked participants multiple-choice questions about the incident context, such as what type of card was involved in the fraud incident, the type of transactions they had been using the card for (online, in-person, or both), and details such as transaction frequency and how they typically performed transactions (e.g., using an app or website, digital wallet, ATM, point of sale machine, etc.). Next, we asked questions related to the detection of the fraud incident, including questions about what was the first thing that triggered their attention to discover the debit/credit card fraud. If detection was through an alert or notification, we asked them about the notification type, medium, and timing, as well as how helpful they found the notification, and asked them to explain in an open-ended response. Next, we asked a set of questions about whether and how they reported the fraud and sought or received compensation. We asked those who reported the incident multiple-choice questions about the reporting and compensation processes and an open-ended question about how their bank or card issuer could improve the support offered in the reporting and compensation processes. We asked those who did not report the incident an open-ended question about why they did not report it. In the fourth section, we asked participants to what extent the experience impacted them financially, psychologically, and on their level of trust in conducting financial transactions, both at the time of the incident and today (i.e. the time of filling the survey). In the fifth section, we asked questions about measures participants have taken to prevent future fraud. Finally, participants were asked a few demographic questions.

Several items in our survey benefited from an IRB-approved unpublished 5-participant pilot interview study conducted by some of this paper's authors and others in 2023. Some of the indirect financial impact items in Q.27 were inspired by the FINRA survey [4] and a report by the BJS [24]. The list of the psychological impacts in Q.28 was obtained from Agrafiotis et al's taxonomy of cyber harms (12 items from the psychological harm category) [1], and an additional 4 items from the FINRA survey [4].

Before launching our survey, we conducted two pilot surveys with 21 participants to help us further refine our questions. Pilot data is not included in our results.

3.4 Analysis

We used quantitative and qualitative methods to analyze our data. We analyzed quantitative results using descriptive statistics. To test significance, if the samples in the test were independent, we used the Chi-square test (denoted as χ^2) [34], given that no more than 20% of the expected frequencies are less than 5 and none of the cells is less than 1 (otherwise Fisher's exact test should be used, which we did not need to) [28]. If the samples in the significance test were

related (paired) in repeated measures, such as when we asked all our participants whether or not they were impacted from three different aspects: financially, psychologically, and trust, in this case, the Chi-square test cannot be used as it requires independent samples [34]. Thus, we used the Cochran Q test to identify whether there are significant differences between the three different scenarios [32]. If the Cochran test p-value was significant, we performed pairwise tests using McNemar's test to identify which pairs have significant differences [33]. For reliable McNemar tests, the sum of discordant cells (b + c; i.e. the shaded cells shown in Table 13 – Table 18 in Appendix A) in the contingency tables should be at least 5, 10, or 25, a condition that was met in our data where no discordant cells sum to less than 25 [33]. We used an alpha level of .05 for all statistical tests. If the p-value is less than .001, we report it as "p-value < .001." We performed corrections for multiple tests using the Bonferroni method. All tests were computed using the R statistical tool [48]. We computed the Chi-square effect size using Cramer's V (denoted as α_c), Cochran effect size using Eta Square (denoted as η_2), and the McNemar's effect size using Cohen's G (denoted as $|g|$).

We grouped some answer choice categories together to facilitate analysis. Namely, for Q.16 on fraud detection speed, we offered participants 10 answer choices including "immediately," "within a few minutes," "within an hour," up to "more than a month." We grouped the first three categories as "fast" and the remainder as "not-fast." We also grouped Q.26 categories which offered participants 12 direct financial loss choices starting from "$0.01 to $10" to "more than $10,000" into two categories "small," and "not-small." Finally, we grouped the fraud impact categories for Q.29 and Q.30, combining "strongly impacted me negatively" and "somewhat impacted me negatively" into one "impacted" category to contrast with "did not impacted me negatively at all." The latter is the extreme opposite category to having any level of impact. We grouped these categories for analysis for reasons deemed appropriate to collapse categories [13, 17]: to make them more relevant to our research problem, and to highlight patterns, especially as we combined relevant categories with low frequencies. The "strongly" impacted category has low frequencies in multiple measures (some measures have only one, six, and nine participants out of 150 participants). Also, our exploratory study's scope does not aim to investigate the impact severity levels, thus, treating the two impact categories (i.e. "strongly" and "somewhat") separately will not add new information to our findings. It is worth noting that the "strongly" impacted data has a similar pattern to that of "somewhat" impacted (see the red and yellow color bars in Figure 1). That is, more participants reported they were psychologically and trust impacted than financially impacted. Thus, combining the "strongly" and "somewhat" impacted categories allowed us to highlight those patterns without introducing new relationships [13].

To qualitatively analyze the open-ended responses, two researchers used Template Analysis, a style of thematic analysis that combines both inductive and deductive coding, with emphasis on hierarchical coding without specific prescription regarding the number of levels required and what levels represent [6, 29]. After the surveys were completed, both researchers familiarized themselves with the data by reading through the responses. The first researcher created an initial codebook (the template) and coded all the data. Then, the second researcher reviewed the codes applied by the first researcher. Both researchers met over multiple sessions to discuss any disagreements in the coding and adjusted the codebook (added, updated, and deleted codes) until they reached a satisfactory version of the codebook agreeable to both researchers. The codebook is provided in Appendix C.

3.5 Ethical considerations

We obtained approval from the CMU Institutional Review Board (IRB). All participants were presented with an online consent form at the beginning of the screening survey. We informed participants about the risk that some questions may bring unpleasant memories to some individuals. We also informed them that they have the right to opt out at any point during the survey.

3.6 Limitations

First, we used Prolific to recruit participants and Prolific workers are known to be more technically skilled than the general population. However, they are reasonably diverse, and Prolific has been shown to provide more generalizable results than other popular recruitment platforms [47]. Second, as we asked participants to self-report the most recent fraud incident that occurred within the last three years, responses might be prone to recall bias. However, this seems to have limited impact on our study as over than half of our participants (54%) reported that their fraud experience occurred "within the last year" or "within the last few months."[2] Third, the incident descriptions are limited to participants' understanding of what happened. We used self-reported data as we otherwise had no access to incident reports and our main interest was in participants' experiences and reflections on the incidents. Fourth, we acknowledge potential misinterpretation of one of the survey questions (Q.16) regarding the approximate length of time it took the participant to detect the fraud. The question asked about detection from the time the fraudulent transaction occurred but we suspect that some participants who detected the fraud when reviewing the account or card statement might have answered with respect to the time they reviewed the statement as we see more than expected short time frame for discovering fraud from reviewing statement. However, the implications of this potential misinterpretation are limited and would not change the conclusion (explained in further details in the results Section 4.3.3). Fifth, our study is focused on the US context, includes only US-based participants, and is framed around US financial regulations and practices. Regulations as well as bank and card issuer practices differ between jurisdictions, which needs to be considered when interpreting our results outside the US context. Sixth, our sample is limited to 150 participants. While this sample size is sufficient for our exploratory study that aims to identify high-level patterns and trends, a larger sample with sufficient data in scarce categories (such as large direct financial loss) might reveal relationships that our study could not reveal. Finally, our study is exploratory and does not measure nuanced levels of severity of impact. It also does not measure relationships between impact and income, or unreimbursed (a.k.a out-of-pocket) loss. Moreover, it does not capture pre-incident security behavior.

4 Results

In what follows we report our results. Where applicable, we denote participants as P, followed by the participant ID (e.g. P_001). We provide frequencies of each qualitative theme to provide a sense of our data and highlight the most/least common themes, but these numbers should not be interpreted as generalizable results. Finally, references to survey question numbers are for the main survey in Appendix B.3, unless stated otherwise.

4.1 Participants

Out of the 150 participants, 78 (52.0%) identified themselves as female, 71 (47.3%) as male, and one as non-binary. Their ages ranged from 18 to "75 or older," with a majority falling between 25–34 (42.7%) and 35-44 (22.7%). A total of 111 (74.0%) were employed, 9 (6.0%) were students, and the remaining were distributed among several other statuses. When asked about the name of the bank or card issuer, participants reported a wide variety of banks and card issuers, with 65 (43.3%) reporting one of the following major US banks as their card issuer: Bank of America, Capital One, Chase, Citi, and Wells Fargo. See Table 11 in Appendix A for further demographic data.

Almost all participants 149 (99.3%) reported that the fraud occurred on a personal account, while only one reported a business account. 89 (59.3%) reported that fraud occurred on a debit card, 58 (38.7%) on a credit card, and only 3 (2.0%)

[2]The full breakdown of the data is as follows: within the last: few months (17.33%); year (36.67%); 2 years (25.33%); 3 years (20.67%).

on a combination debit/credit card. Table 12 in Appendix A provides further details on participants' use of the card involved in the fraud incident they described.

4.2 Fraud Incidents

We asked participants to describe their most recent debit/credit card fraud experience and how they discovered the fraud in an open-ended question (Q.6 & Q.7 in the screening survey in Appendix B.2). Our qualitative analysis shows that only 6 (4.0%) participants mentioned incidents that involved the possession of the original physical card by the fraudster, such as lost or stolen cards, and one participant mentioned a skimmed card. This indicates that most of the reported incidents were card-not-present fraud, which includes online, phone, or mail transactions [18]. These results are in line with recent reports regarding the rise of card-not-present fraud in the US [18, 30].

We analyzed participants' descriptions of the incident to determine the fraudulent transaction mode. 53 (35.3%) of participants' answers indicated online transactions, such as "Someone used my credit card for an Amazon order" (P_001). Only 19 (12.7%) participants indicated offline transaction mode, which we identified from mentions of specific locations, such as "Unexpected charges showed up for pizza in an area where I do not reside" (P_021), or other cues such as fraud that involved cash withdrawals. The remaining participants did not specify the fraudulent transaction mode.

We also analyzed their descriptions to determine the type of fraudulent transaction. 87 (58.0%) participants indicated unauthorized purchases. Participants also mentioned other types of unauthorized transactions, such as overcharging (4), bank identity theft (3), unauthorized withdrawal (2), never-received items (1), and unauthorized check issuance (1). The remaining participants (54) did not specify the fraudulent transaction type, mentioning only that an unauthorized transaction was made: "There were online charges on my credit card that I didn't make" (P_013). Participants' descriptions of the fraud included mentions of shopping or stores in general (22), food and beverages (19), electronics (7), gas (7), subscription or membership (6), clothes (4), entertainment (3), transportation (3), money-laundering-like website (2), and porn (1).

Location was another significant detail mentioned by participants, with a total of 34 (22.7%) participants reporting the fraudulent activity occurred outside their geographic location including a different state (23), continent (4), area (3), city (2), or country (2).

Fourteen individuals indicated a compromise of a non-bank online account that contained the debit/credit card details, such as "Someone hacked my walmart account and used my card that was on there" (P_016). In one case, a participant mentioned, "My family took money out of my account" (P_050).

4.3 Fraud Detection

In this section, we summarize the reported method of detection that led participants to discover the fraud (Section 4.3.1). Then, we summarize the type and medium of notifications the participants received (Section 4.3.2). Finally, we analyze the impact of the detection method (checking card or account statement vs. receiving a notification) on the detection time (Section 4.3.3).

4.3.1 Method of Detection. We asked participants to identify the first thing that triggered their attention to discover their debit/credit card fraud (Q.9 in Appendix B.3). As shown in Table 1, nearly 89% of participants detected the fraud through one of three mechanisms: checking their card or account statement and finding transactions they did not make (50.0%), receiving a form of alert or notification from their bank or card issuer (34.7%), or receiving a form of alert or notification from a third-party (4.0%).

Table 1. The methods through which participants first discovered that they had been defrauded, ordered from the most to least reported method.

N = 150		
Method of detection	#	%
I checked my card or account statement and found a transaction(s) I did not make	75	(50.0%)
I received a form of alert or notification from my bank or card issuer (e.g. SMS, phone call, letter, email, etc. for withdrawal or fraud notifications)	52	(34.7%)
Other	10	(6.7%)
I received a form of alert or notification from a third-party (e.g. SMS, phone call, letter, email, etc. for withdrawal or fraud notifications) (*please specify what type of third-party):	6	(4.0%)
I realized I might have fallen for a scam or something did not seem right, which led me to do further checks and subsequently find the fraud	5	(3.3%)
I checked my card or account statement and found a transaction(s) that I made, but went to an unintended recipient(s)	1	(0.7%)
I learned about the fraud from family, friends, or other people, which led me to do further checks and subsequently find the fraud	1	(0.7%)
I learned about the fraud from public channels (e.g. social media), which led me to do further checks and subsequently find the fraud	0	(0.0%)

Table 2. List of reported notification types by the participants, ordered from the most to least reported type.

N = 58		
Notification Type	#	%
Suspicious transaction	36	(62.1%)
Fraudulent transaction	9	(15.5%)
Withdrawal	5	(8.6%)
Other	4	(6.9%)
I cannot remember	2	(3.4%)
Account balance	1	(1.7%)
International transaction	1	(1.7%)
Low balance	0	(0.0%)

Table 3. List of reported notification mediums by the participants, ordered from the most to least reported medium.

N = 58		
Notification Medium (multiple answers)	#	%
Short text message (SMS)	32	(55.2%)
Email	21	(36.2%)
Phone call	14	(24.1%)
Push notification through the bank or card issuer's app or Internet banking website	8	(13.8%)
Message through the bank or card issuer's app or Internet banking website	6	(10.3%)
Automated voice message	4	(6.9%)
Other	1	(1.7%)
Post letter	0	(0.0%)

4.3.2 Type and Medium of Notification. Out of the 58 participants who detected the fraud through a form of notification, a total of 45/58 (77.6%) reported that the notification type was either "Suspicious transaction" or "Fraudulent transaction." Only a few participants mentioned other specific types of notifications, including "Withdrawal" (5), "Account balance" (1), and "International transaction" (1). See Table 2 for a full list of the reported notification types.

Short Messaging Service (SMS) was the most reported notification medium with 32/58 (55.2%), followed by email at 21/58 (36.2%), and phone call at 14/58 (24.1%). 20 participants reported receiving the notification through multiple channels. See Table 3 for a full breakdown of the reported notification mediums.

Almost all the participants who received a form of notification from their bank or card issuer across all types of notifications (57/58) reported they found the notification helpful in detecting the fraudulent activity (Q.14 in Appendix B.3). 51 (87.9%) said that the notifications were "Extremely helpful," 5 (8.6%) said "Somewhat helpful," one "Slightly helpful," and only one said, "Not at all helpful."

4.3.3 Impact of Detection Method on Detection Time. We now look closer at the top two most reported detection methods, reviewing card or account statement and receiving notifications, to see which method is related to faster fraud detection. For each detection method, we analyzed participants' responses to our question about how long it took them to realize that they had been defrauded from the time the fraudulent transaction occurred (Q.16 in Appendix B.3). If the participant answered "Immediately," "Within a few minutes," or "Within an hour," we classified this as "fast" detection, otherwise, we classified it as "not fast." Participants who answered "I cannot remember" (1 participant from the bank statement detection method and 5 from the notifications detection method) were excluded from this analysis. Our data originally had a total of 76 participants who reported fraud detection by reviewing their bank or card statement and a total of 58 through receiving a form of alert or notification (see Table 1). This exclusion left us with a total of 75 participants who reported statement, and 53 participants who reported notifications as detection methods, respectively.

Our results show that notifications are more related to faster detection of the fraud, where 37/53 (69.8%) of the reported fraud incidents from the notifications group were detected within an hour or less, compared to 29/75 (38.7%) of incidents detected from the statement group. The difference is statistically significant (χ^2 = 12.061, p-value < .001, α_c = 0.291). However, despite the fact that notifications led to faster detection, our results show that more participants detected the fraud through statements (53 via notifications compared to 75 via statement). It should be noted that the number of participants who reported fast fraud detection through their card or account statement may be inflated due to potential misinterpretation of Q.16. We suspect that some participants provided the detection time from the time they checked their statement instead of what we asked in the question: "From the time your debit/credit card fraudulent transaction occurred" as it seems unlikely that a lot of people would happen to check their account statement within an hour of a fraudulent charge being made. We observed such confusion in our pilot studies, and therefore reworded this question placing the key part first, and using bold and italic font to emphasize the key parts of this question. Despite those changes to the question, more than expected number of participants reported fast detection through statements. We suspect some confusion about this question remains and the number of participants who reported fast detection through statements is inflated. Having said that, this potential confusion only suggests that the difference between notifications and statements in terms of enabling fast fraud detection might be larger than what our results indicate. The difference is already statistically significant and having it even larger difference would not change the conclusion. That is, in either case, notifications are related to faster detection of the fraud than reviewing the bank or card statement, and the difference is statistically significant.

4.3.4 How Alerting and Detection Can Be Improved. We asked participants to provide suggestions for improving the alerting and detection capabilities (Q.18 in Appendix B.3). Some of the suggestions were related to the alert type participants wanted to receive. For example, 11 participants suggested preventive notifications such as alerts for suspicious or fraudulent transactions, 11 suggested alerts for unusual behavior, and 12 participants suggested alerts to approve or decline transactions. As P_109 explained: "maybe like a quick text or call from the bank to make sure it's really me making a purchase." 16 participants suggested alerts for transactions originating from different geographical locations (2 of them specifically mentioned international transactions), alerts for any purchase transactions (8), large transactions (6), transactions over a certain limit (1), and alerts for repeated purchases within a short duration of time

(1). Five participants would like to receive alerts for any transaction, one participant suggested alerts related to security activities including change of PIN, password, etc., and 2 participants recommended enabling alerts by default. With respect to alert medium, SMS was the most suggested form of delivery (15), followed by email (7), phone call (5), and through the app (2). Additionally, 6 participants preferred receiving alerts through multiple channels. Many participants mentioned speed, with 11 participants stating they wanted alerts to be sent immediately. Two participants emphasized the importance of the legitimacy of these texts, without which they may be misinterpreted as scams.

Many of these requested alert capabilities are already offered by some US banks, although they may not be offered by default (they need to be configured by the cardholder).

4.4 Fraud Reporting and Compensation

In this section, we summarize participants' responses about their experiences reporting the fraud (Section 4.4.1), and what they believe can improve the reporting process (Section 4.4.2).

4.4.1 Reporting and Not Reporting. While under-reporting of financial fraud was found to be a problem in some countries such as Pakistan as reported in Razaq et al's study [39], which is mostly related to socio-cultural and regulation issues, it does not seem to be an issue with our US participants. The majority of our participants 129 (86.0%) said they reported the fraud to their bank or card issuer. Among those who reported the incident, the majority 102/129 (79.1%) sought compensation, and 109 (84.5%) of those who reported the incident said they were fully compensated. We asked those who did not report the fraud about the reasons for not doing so (Q.20 in Appendix B.3). Almost all of them explained that the bank or card issuer detected the fraud for them as P_40 explained: "It was the bank that notified me. So that was unnecessary," which eliminated the need for reporting. Two participants said that the loss was not important enough as P_074 explained: "I only lost a few dollars because the other transactions were declined," and in the case of P_050 where she described that the fraudster was a family member said: "Did not want to get my family in trouble."

We then asked participants for suggestions to improve the reporting and compensation processes (Q.25 in Appendix B.3). We found that speeding up the reporting and/or compensation processes was one of the key points mentioned by 22 participants. On the other hand, those who did not have any suggestions and expressed their satisfaction with their experience, appreciated the fast process overall (11).

4.4.2 Explaining What Happened. We asked participants who said they reported the fraud, whether the bank provided them with an explanation of the fraud incident (Q.23 in Appendix B.3). Only 22/129 (17.1%) said they received a full explanation, while the remaining majority either received no explanation at all 63/129 (48.8%), or a partial explanation 41/129 (31.8%).

Providing explanations and additional information about the fraud incident was a key point mentioned by 26 participants when asked for suggestions to improve the reporting and compensation processes (Q.25 in Appendix B.3). Participants wanted more information about how, what, where, and by whom the fraud occurred. In addition, some participants suggested banks or card issuers provide them with preventive tips "to prevent [this] from happening again" (P_069). Lack of explanation can negatively impact some people as P_045 explained: "The[re] was definatley some details left out that have me confused."

Table 4. Direct financial losses reported by participants who experienced the fraud, ordered from small to large loss.

N = 150		
Direct Financial Loss	#	%
$0 (no direct financial loss)	0	(0.0%)
From $0.01 to $10	11	(7.3%)
From $11 to $50	29	(19.3%)
From $51 to $100	34	(22.7%)
From $101 to $500	51	(34.0%)
From $501 to $1,000	10	(6.7%)
From $1,001 to $2,000	6	(4.0%)
From $2,001 to $4,000	4	(2.7%)
From $4,001 to $6,000	0	(0.0%)
From $6,001 to $8,000	1	(0.7%)
From $8,001 to $10,000	0	(0.0%)
More than $10,000	0	(0.0%)
I cannot remember	1	(0.7%)
Other	3	(2.0%)

4.5 Fraud Impact

In this section, we summarize participants' responses about the fraud's direct, indirect, and psychological impact (Section 4.5.1). Then, we analyze the reported financial vs. psychological vs. trust impact (Section 4.5.2) to find which type of impact has impacted more participants, and the relationship between the amount of direct financial loss and the different types of impacts. Finally, we analyze the fraud impact on behavior (Section 4.5.3).

4.5.1 Type of Impact.

Direct Financial Impact. We asked participants to report the direct financial loss resulting from the fraud incident, which we described to them as "the amount the fraudster charged" to their card "even if it was later compensated or reimbursed" (Q.26 in Appendix B.3). 83.3% of the reported direct financial loss did not exceed $500, suggesting that current detection techniques are reasonably helpful in limiting the amount of direct financial loss. See Table 4 for a full breakdown of the direct loss results.

Indirect Financial Impact. We then asked participants to report the indirect financial losses they had experienced. Participants selected one or more of eleven common indirect financial impacts or "Other," or the exclusive "None of these." A considerable number of participants 67/150 (44.7%) reported they did not experience any indirect financial loss. However, "Emotional distress" was selected by 69 (46.0%), followed by experiencing "Loss of trust from others" by 15 (10.0%), suggesting that emotional and psychological impacts are the top-ranked indirect losses, which we examine in further detail next. Issues such as "Difficulty obtaining loans or credit" were reported only by a few participants, while more serious indirect financial losses such as "Loss of job due to the fraud incident" were reported by none. The full list of reported indirect financial impacts is provided in Table 5.

Psychological Impact. To gain more insights, we asked participants to report all the psychological negative impacts they experienced from a list of 16 psychological impacts or provide their answer in the "Other" choice. 136/150 (90.7%) participants reported one or more negative psychological impacts, with an average of 3.8 impacts (excluding those who reported "None of these") per participant. The most reported impacts were: "Stress" 103 (68.67%), "Worry or anxiety" 79 (52.7%), "Frustration" 78 (52.0%), and "Feeling upset" 73 (48.67%). Sometimes people were worried about others besides themselves, as P_060 added: "I was worried, not only for my account, but several others who are family and elderly. I

Table 5. Indirect losses reported by participants who experienced the fraud, ordered from the most to least reported impact.

N = 150		
Indirect Loss (multiple answers)	#	%
Emotional distress	69	(46.0%)
None of these	67	(44.7%)
Loss of trust from others	15	(10.0%)
Costs of credit monitoring or identity theft protection services	11	(7.3%)
Loss of income due to the fraud incident	8	(5.3%)
Other	6	(4.0%)
Damaged personal reputation	3	(2.0%)
Negative impact on credit score or higher interest rates for borrowing	3	(2.0%)
Increased insurance premiums or difficulty obtaining insurance coverage	1	(0.7%)
Difficulty obtaining loans or credit	1	(0.7%)
Costs of therapy or counseling	0	(0.0%)
Loss of job due to the fraud incident	0	(0.0%)
Legal and attorney fees for pursuing legal action or defending against accusations	0	(0.0%)

Table 6. List of psychological negative impacts reported by participants who experienced the fraud, ordered from the most to least reported impact.

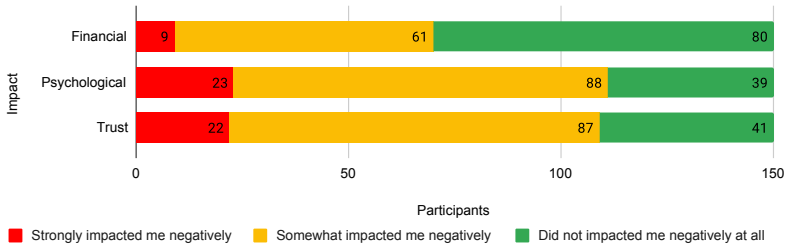
N = 150		
Psychological impact (multiple answers)	#	%
Stress	103	(68.7%)
Worry or anxiety	79	(52.7%)
Frustration	78	(52.0%)
Feeling upset	73	(48.7%)
Confusion	36	(24.0%)
Discomfort	31	(20.7%)
Feeling unsafe	28	(18.7%)
Difficulty in trusting others	25	(16.7%)
Guilt	15	(10.0%)
None of these	14	(9.3%)
Difficulty in sleeping	12	(8.0%)
Low satisfaction	10	(6.7%)
Negative changes in perception	10	(6.7%)
Shame	8	(5.3%)
Loss of self-confidence	5	(3.3%)
Other	3	(2.0%)
Depression	0	(0.0%)
Embarrassment	0	(0.0%)

had to spend time notifying people that their accounts might be compromised as well." The full list of reported impacts is provided in Table 6.

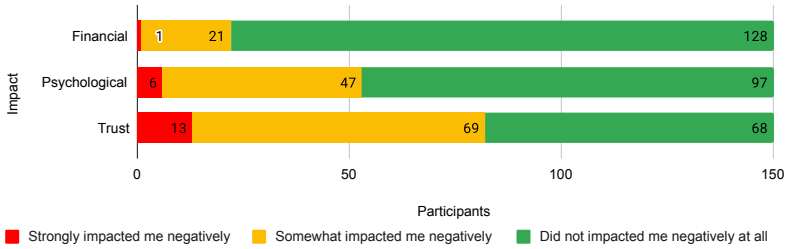
4.5.2 *Financial vs. Psychological vs. Trust Impact.*

Size of Financial, Psychological, and Trust Impacts. To measure the financial, psychological, and trust impacts on victims, we asked participants to rank how the fraud incident impacted them financially, psychologically, and on their level of trust in performing financial transactions. We asked them to rank those 3 impacts twice: with respect to the time of the incident and today (the time of filling out the survey). Participants were presented with 3 choices (Q.29 and Q.30 in Appendix B.3) as follows: "Strongly impacted me negatively," "Somewhat impacted me negatively," and "Did not impacted me negatively at all."

As Table 7 and Figure 1 show, more participants reported they were psychologically and trust impacted than financially impacted. This is for both questions: with respect to the time of the incident and today. Moreover, while the



(a) Impact at the time of the incident.



(b) Impact today.

Fig. 1. Financial vs. psychological vs. trust impact on victims with respect to the time of the incident and today.

Table 7. Number of participants who reported financial, psychological, and trust impacts at the time of the incident and today.

	N = 150					
	# Fin. impacted	%	# Psych. impacted	%	# Trust impacted	%
At time	70/150	(46.7%)	111/150	(74.0%)	109/150	(72.7%)
Today	22/150	(14.7%)	53/150	(35.3%)	82/150	(54.7%)

financial and psychological impacts of the fraud reduced over time, the loss of trust in performing financial transactions did not reduce as much.

To test whether there are significant differences between the number of participants who were impacted financially, psychologically, and on their trust in performing financial transactions, we coded participants who reported "strongly" or "somewhat" impacted as "impacted," and those who reported they were not impacted at all as "not impacted." We then performed the Cochran tests. We found significant differences between the three types of impacts at both points in time: at the time of the incident (Q = 38.166, p-value < .001, η_2 = 0.127) and today (Q = 74, p-value < .001 η_2 = 0.246).

Then, to identify which pair of impacts significantly differ, we conducted pairwise McNemar tests for each of the possible pair of impacts as follows: (financial vs. psychological), (financial vs. trust), and (psychological vs. trust). As detailed in Table 7 and Table 8, our results suggest that, at both points in time (at the time of the incident and today), more participants reported they were psychologically and trust impacted than financially impacted, and these differences are significant.

Relationship Between the Amount of Financial Loss and Financial, Psychological, and Trust Impacts. We now look at whether there is a relationship between the amount of direct financial loss (Q.26 in Appendix B.3) and the financial, psychological, and trust impacts. To this end, we classified participants into two categories based on the reported amount of direct financial loss: small loss of $100 or less coded as "small," and larger losses (more than $100) coded as

Table 8. Pairwise McNemar's tests for the financial vs. psychological vs. trust impacts. The p-values were adjusted using the Bonferroni method. The effect size for McNemar tests was computed using Cohen's G ($|g|$).

N = 150			
Impacted (at time)	McNemar's χ^2	Adjusted p-value	$\|g\|$
Fin. vs. Psych.	25.09	< .001	0.306
Fin. vs. Trust	23.4	< .001	0.3
Psych. vs. Trust	0.111	1.000	0.028
Impacted (today)	χ^2	Adjusted p-value	$\|g\|$
Fin. vs. Psych.	24.641	< .001	0.397
Fin. vs. Trust	56.25	< .001	0.469
Psych. vs. Trust	19.558	< .001	0.337

Table 9. Columns 2–4 respectively list the total number of participants who reported "small" vs. "not small" direct financial loss; the number of participants in the corresponding direct loss group who reported financial; psychological; and trust impacts (at the time of the incident).

N = 146							
Direct loss in $	# experienced loss in $	# Fin. impacted	%	#Psych. impacted	%	#Trust impacted	%
Small ($0.01 to $100)	74	33/74	(44.6%)	52/74	(70.3%)	52/74	(70.3%)
Not small (more than $100)	72	36/72	(50%)	56/72	(77.8%)	53/72	(73.6%)

"not small." We excluded participants who selected "I cannot remember" (1) or "Other" (3) for the direct financial loss question (Q.26). This left us with 146 participants included in this section's analysis. Similar to previous sections, we coded participants who reported being "strongly" or "somewhat" impacted as "impacted," and those who reported they were not impacted at all as "not impacted." We ended up with Table 9 listing the direct financial loss categories, the number of participants whose reported direct financial loss fit in that category, and the number of participants who reported they were financially, psychologically, and trust impacted in each direct financial loss category. Note that in this test we only consider impact with respect to the time of the incident (Q.29 in Appendix B.3).

We then used the Chi-square test for the following pairs of variables: (direct financial loss vs. financial impact), (direct financial loss vs. psychological impact), and (direct financial loss vs. trust impact).

Our Chi-square tests suggest that there is no relationship between the amount of direct financial loss and: the financial, psychological, and trust impact. That is, financial loss vs. financial impact (χ^2 = 0.427, p-value = 0.513, α_c = 0.040), financial loss vs. psychological impact (χ^2 = 1.068, p-value = 0.301, α_c = 0.069), and financial loss vs. trust impact (χ^2 = 0.201, p-value = 0.653, α_c = 0.021).

4.5.3 Impact of Fraud on Behavior. As a result of the fraud experience, 144 (96.0%) participants reported they had taken one or more security measures to prevent future fraud on their card (Q.31). As Table 10 details, the majority of participants primarily resorted to manual measures in their control to safeguard themselves, such as regularly checking their account or card statement, reported by 104 (69.3%) participants, and exercising caution and vigilance when conducting financial transactions, reported by 93 (62.0%) participants. However, more automated (smarter) techniques such as notifications and security configurations were mentioned at a lower scale. For example, 57 (38.0%) participants reported they set up alerting mechanisms for their account or card, 55 (36.7%) reported implementing security measures from the bank or card issuer, 26 (17.3%) reported implementing security measures from third parties, while 10 (6.7%) said they changed their bank or card issuer.

Table 10. List of measures participants reported had taken to prevent future fraud on their debit/credit card, ordered from the most to least reported measure.

N = 150		
Measure taken (multiple answers)	#	%
I now regularly check my account or card statement	104	(69.3%)
I am now more cautious and vigilant when conducting financial transactions	93	(62.0%)
I have set up alerting mechanisms for my account or card	57	(38.0%)
I have implemented security measures from the bank or card issuer to protect my financial transactions	55	(36.7%)
I have implemented security measures from third-parties to protect my financial transactions	26	(17.3%)
I switched my bank or card issuer	10	(6.7%)
I did not undertake any measures	6	(4.0%)
Other (please specify)	6	(4.0%)

5 Discussion

Our discussion is limited to our study's scope on victims' experiences, which is an important source to understand the debit/credit card fraud landscape, what consumers are experiencing, and their needs. We do not analyze what financial institutions are implementing due to a lack of such data, which is a common limitation in fraud research.

Notifications: Efficient, Yet Underutilized. Our results show that notifications are related to faster detection of fraud than reviewing the card or account statement. This might be intuitive, however, our results show that more participants reported that they detected the fraud through checking their card or account statement than through notifications, suggesting that notifications are underutilized. It is our experience that not all US banks enable notifications (e.g. for any transaction) by default. However, when we asked participants about suggestions for banks to improve their alerting and detection capabilities, many participants suggested a wide variety of notifications with the SMS as the most mentioned medium.

We recommend that well-tailored basic notifications, such as any transaction notifications or approve or decline card-not-present transactions, are best suited to be enabled by default, with the option to opt out. We acknowledge the trade-off in enabling basic notifications by default: they may incur additional costs to banks, may annoy some customers, or customers may become habituated to them such that they do not notice them. The literature has investigated the habituation to warnings and notifications [2, 3, 51]. However, Reeder et. al.'s study on browser warnings suggests that contextual factors affect users' decisions toward adherence or bypassing warnings, and that habituation has a smaller effect on users' decision-making process than previously thought [40]. Other studies also suggested that perceived disruption of mobile notifications is influenced by contextual factors, such as the sender-receiver relationship, the importance of the information the notification contains, and personality traits [22, 35, 43]. Mehrotra et al. found that users tend to click highly disruptive notifications if the content is important information [35]. Future work might explore notifications in the banking context including experimental studies on user perceptions and behaviors towards notifications in the banking context, which notifications should be enabled by default, and the most usable and secure delivery medium.

Explanation as a Preventive Mechanism. While most banks stress the importance of customer awareness to combat fraud, nearly half of our participants did not receive any explanation at all from their banks or card issuers regarding the fraud. When we asked participants for suggestions to improve the support provided to them in the reporting and compensation processes, our qualitative data shows that explanation was the most mentioned theme. Several participants particularly pointed out the need for an explanation to "avoid this happening again in the future" (P_148).

We recommend that banks or card issuers provide an explanation of the fraud incident to victims when applicable. Although card fraud is sometimes completely beyond the victim's control, some incidents could be prevented if victims were more aware of how to protect themselves from phishing, card skimmers, and other types of attacks. In addition, knowing that incidents can happen beyond their control may help motivate people to turn on notifications or be more vigilant about checking their statements for fraudulent transactions. We acknowledge that banks and card issuers may not always be able to provide an explanation of the fraud incident for various reasons, such as lack of information, cost of investigation, or security. However, card issuers may still be able to provide actionable and more tailored advice to help victims avoid future fraud.

The Forgotten Psychological Impact. Our results suggested that the psychological impact affects more participants than the financial impact, regardless of the amount of financial loss. Most of our participants were reimbursed for the direct financial loss, yet reported that they remain psychologically impacted months or years later. This suggests that reimbursement alone is not sufficient to remediate the psychological impact. It is unclear what banks and consumer protection organizations are doing to address the psychological impact on financial fraud victims.

We suggest that banks and consumer protection organizations examine and further research solutions to remediate the psychological impact. Offering professional psychological support for the psychologically impacted victims is a solution worth examining to remediate the issue. In addition, explanations may provide some assurance to victims, helping them to feel better prepared to protect themselves in the future. Moreover, future work could study the impact, harms, and potential benefits of psychological support in greater detail.

Behavioral Analytics to Combat Credit/Debit Card Fraud. Behavioral analytics, which can predict user behavior based on analyzing data from their past behavior, has long been associated with targeted advertisements in web and mobile applications. In the context of advertisements, behavioral analytics tend to be viewed as privacy-invasive techniques [49, 50], and users face difficulties in opting out of online advertisements [31]. However, in the banking context, ideally, banks and their customers have a form of trust relationship, and banks already audit customers' transactions. Our qualitative data shows that when customers see a value (security) in return for behavioral analytics of their financial behavior, behavioral analytics are viewed as a welcomed feature. Our qualitative results show that many participants would like their banks or card issuers to notify them if they identified out-of-ordinary behavior. While most banks may already use forms of behavioral analytics, many participants' answers indicate that they were not aware of them.

6 Conclusion

In this study, we surveyed 150 victims of credit/debit card fraud in the US to report on their most recent experiences. Our results show that the psychological impact affected more participants than the financial impact, regardless of the amount of financial loss. Among our participants, the psychological impact was not related to the amount of financial loss, suggesting that people are at risk of being psychologically impacted regardless of the amount lost to fraud. While notifications resulted in faster detection of fraud than checking the bank statement, they were less utilized in detecting the fraud.

Acknowledgments

Eman Alashwali acknowledges the financial support of the Ibn Rushd Program at King Abdullah University of Science and Technology (KAUST). This work was funded in part by the Innovators Network Foundation. We thank Prof. Marc

Dacier from KAUST for feedback on earlier versions of this paper; Jenny Tang, Elijah Bouma-Sims, and Eric Zeng for helpful discussions on statistical analysis; Talal Ali, David Mberingabo, Yiming Zhong, and Pauline Mevs for their contributions to the initial pilot interview study during the Usable Privacy and Security course at CMU.

References

[1] Ioannis Agrafiotis, Jason R C Nurse, Michael Goldsmith, Sadie Creese, and David Upton. 2018. A Taxonomy of Cyber-Harms: Defining the Impacts of Cyber-Attacks and Understanding How They Propagate. *Journal of Cybersecurity* 4, 1 (2018), 1–15.

[2] Bonnie Anderson, Anthony Vance, Brock Kirwan, David Eargle, and Seth Howard. 2014. Users Aren't (Necessarily) Lazy: Using Neurois to Explain Habituation to Security Warnings. In *Proc. Int. Conference on Information Systems (ICIS)*.

[3] Bonnie Brinton Anderson, Jeffrey L Jenkins, Anthony Vance, C Brock Kirwan, and David Eargle. 2016. Your Memory is Working Against You: How Eye Tracking and Memory Explain Habituation to Security Warnings. *Decision Support Systems* 92 (2016), 3–13.

[4] Applied Research & Consulting LLC. 2015. *Non-Traditional Costs of Financial Fraud.* https://www.finrafoundation.org/sites/finrafoundation/files/nontraditional-costs-financial-fraud_0_0_0.pdf Accessed Jan. 24, 2024.

[5] Michaela Beals, Marguerite DeLiema, and Martha Deevy. 2015. *Framework For a Taxonomy of Fraud.* https://www.finrafoundation.org/sites/finrafoundation/files/framework-taxonomy-fraud.pdf Accessed Aug. 10, 2024.

[6] Joanna Brooks and Nigel King. 2014. Doing Template Analysis: Evaluating an End of Life Care Service. *SAGE Research Methods Cases Part 1* (2014).

[7] Axel Buchner, Edgar Erdfelder, Franz Faul, and Albert-Georg Lang. 2024. *G*Power Statistical Power Analyses for Mac and Windows.* https://www.psychologie.hhu.de/arbeitsgruppen/allgemeine-psychologie-und-arbeitspsychologie/gpower Accessed Jan. 30, 2024.

[8] Mark Button, Chris Lewis, and Jacki Tapley. 2009. *A Better Deal for Fraud Victims: Research into Victims' Needs and Experiences.* https://researchportal.port.ac.uk/en/publications/a-better-deal-for-fraud-victims-research-into-victims-needs-and-e Accessed Dec. 27, 2023.

[9] Mark Button, Carol McNaughton Nicholls, Jane Kerr, and Rachael Owen. 2014. Online Frauds: Learning From Victims Why They Fall For These Scams. *Australian & New Zealand Journal of Criminology* 47, 3 (2014), 391–408.

[10] Chiao-Ting Chen, Chi Lee, Szu-Hao Huang, and Wen-Chih Peng. 2024. Credit Card Fraud Detection via Intelligent Sampling and Self-Supervised Learning. *ACM Trans. Intell. Syst. Technol.* (2024).

[11] Consumer Financial Protection Bureau. 2024. *§ 1005.6 Liability of Consumer for Unauthorized Transfers.* https://www.consumerfinance.gov/rules-policy/regulations/1005/6 Accessed Jan. 30, 2024.

[12] 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).

[13] David de Vaus. 2014. *Surveys in Social Research, 6th Edition.* Routledge. 161–163 pages.

[14] Linda Delamaire, Hussein Abdou, and John Pointon. 2009. Credit Card Fraud and Detection Techniques: A Review. *Credit card fraud and detection techniques: a review. Banks and Bank Systems* 4, 2 (2009), 57–68.

[15] Marguerite DeLiema, David Burnes, and Lynn Langton. 2021. The Financial and Psychological Impact of Identity Theft Among Older Adults. *Innovation in Aging* 5, 4 (2021), igab043.

[16] Marguerite DeLiema, Gary R Mottola, and Martha Deevy. 2017. *Findings from a Pilot Study to Measure Financial Fraud in the United States.* http://dx.doi.org/10.2139/ssrn.2914560 Accessed Dec. 27, 2023.

[17] Ben Van Dusen and Jayson M Nissen. 2020. Criteria for Collapsing Rating Scale Responses: a Case Study of the CLASS. In *Proc. Physics Education Research Conference Proceedings*.

[18] John Egan and Liz Bingler. 2023. *Credit Card Fraud Statistics.* https://www.bankrate.com/finance/credit-cards/credit-card-fraud-statistics Accessed Jan. 26, 2024.

[19] Federal Trade Commission. 2023. *The Big View: All Sentinel Reports.* https://public.tableau.com/app/profile/federal.trade.commission/viz/TheBigViewAllSentinelReports/TopReports Accessed Dec. 25, 2023.

[20] Federal Trade Commission. 2023. *Fraud Reports.* https://public.tableau.com/app/profile/federal.trade.commission/viz/FraudReports/FraudFacts Accessed Dec. 25, 2023.

[21] Federal Trade Commission. 2024. *Electronic Fund Transfer Act.* https://www.ftc.gov/legal-library/browse/statutes/electronic-fund-transfer-act Accessed Jan. 31, 2024.

[22] Joel E Fischer, Nick Yee, Victoria Bellotti, Nathan Good, Steve Benford, and Chris Greenhalgh. 2010. Effects of Content and Time of Delivery on Receptivity to Mobile Interruptions. In *Proc. Human Computer Interaction with Mobile Devices and Services (MobileHCI)*. 103–112.

[23] Linda Ganzini, Bentson McFarland, and Joseph Bloom. 1990. Victims of Fraud: Comparing Victims of White Collar and Violent Crime. *Bulletin of the American Academy of Psychiatry and the Law* 18, 1 (1990), 55–62.

[24] Erika Harrell and Lynn Langton. 2013. *Victims of Identity Theft, 2012.* https://bjs.ojp.gov/content/pub/pdf/vit12.pdf Accessed Jan. 17, 2024.

[25] Erika Harrell and Alexandra Thompson. 2023. *Victims of Identity Theft, 2021.* https://bjs.ojp.gov/document/vit21.pdf Accessed Dec. 26, 2023.

[26] Jurjen Jansen and Rutger Leukfeldt. 2015. How People Help Fraudsters Steal Their Money: An Analysis of 600 Online Banking Fraud Cases. In *Proc. Workshop on Socio-Technical Aspects in Security and Trust*. 24–31.

[27] Samidha Khatri, Aishwarya Arora, and Arun Prakash Agrawal. 2020. Supervised Machine Learning Algorithms for Credit Card Fraud Detection: A Comparison. In *Proc. International Conference on Cloud Computing, Data Science & Engineering (Confluence)*. 680–683.

[28] Hae-Young Kim. 2017. Statistical Notes for Clinical Researchers: Chi-Squared Test and Fisher's Exact Test. *Restor Dent Endod* 42, 2 (2017).

[29] Nigel King. 2023. *Template Analysis.* https://research.hud.ac.uk/research-subjects/human-health/template-analysis Accessed Dec. 18 2023.

[30] Sara Lebow. 2023. *Card-Not-Present Fraud to Make Up 73% of Card Payment Fraud.* https://www.insiderintelligence.com/content/card-not-present-fraud-payment Accessed Jan. 24, 2024.

[31] Pedro Leon, Blase Ur, Richard Shay, Yang Wang, Rebecca Balebako, and Lorrie Cranor. 2012. Why Johnny Can't Opt Out: A Usability Evaluation of Tools to Limit Online Behavioral Advertising. In *Proc. Conference on Human Factors in Computing Systems (CHI)*. 589–598.

[32] Salvatore S. Mangiafico. 2016. *Cochran's Q Test for Paired Nominal Data.* https://rcompanion.org/handbook/H_07.html Accessed May 22, 2024.

[33] Salvatore S. Mangiafico. 2016. *Tests for Paired Nominal Data.* https://rcompanion.org/handbook/H_05.html#_Toc507754342 Accessed May 22, 2024.

[34] Mary L. McHugh. 2013. The Chi-Square Test of Independence. *Biochem Med* 23, 2 (2013).

[35] Abhinav Mehrotra, Veljko Pejovic, Jo Vermeulen, Robert Hendley, and Mirco Musolesi. 2016. My Phone and Me: Understanding People's Receptivity to Mobile Notifications. In *Proc. CHI Conference on Human Factors in Computing Systems (CHI)*. 1021–1032.

[36] Rachel E. Morgan. 2021. *Financial Fraud in the United States.* https://bjs.ojp.gov/content/pub/pdf/ffus17.pdf Accessed Jan. 26, 2024.

[37] Prolific. 2023. *Quicly Find Research Participants You Can Trust.* https://www.prolific.com Accessed Dec. 18, 2023.

[38] Qualtrics. 2023. *Qualtrics XM | The Leading Experience Management Software.* https://www.qualtrics.com Accessed Dec. 18, 2023.

[39] Lubna Razaq, Tallal Ahmad, Samia Ibtasam, Umer Ramzan, and Shrirang Mare. 2021. "We Even Borrowed Money From Our Neighbor" Understanding Mobile-based Frauds Through Victims' Experiences. *Proc. ACM Hum.-Comput. Interact.* 5, CSCW1, Article 41 (2021), 30 pages.

[40] Robert W Reeder, Adrienne Porter Felt, Sunny Consolvo, Nathan Malkin, Christopher Thompson, and Serge Egelman. 2018. An Experience Sampling Study of User Reactions to Browser Warnings in the Field. In *Proc. CHI Conference on Human Factors in Computing Systems (CHI)*. 1–13.

[41] Markus Riek and Rainer Böhme. 2018. The Costs of Consumer-Facing Cybercrime: an Empirical Exploration of Measurement Issues and Estimates. *Journal of Cybersecurity* 4, 1 (2018), 1–16.

[42] Nick F Ryman-Tubb, Paul Krause, and Wolfgang Garn. 2018. How Artificial Intelligence and Machine Learning Research Impacts Payment Card Fraud Detection: A Survey and Industry Benchmark. *Engineering Applications of Artificial Intelligence* 76 (2018), 130–157.

[43] Alireza Sahami Shirazi, Niels Henze, Tilman Dingler, Martin Pielot, Dominik Weber, and Albrecht Schmidt. 2014. Large-Scale Assessment of Mobile Notifications. In *Proc. CHI Conference on Human Factors in Computing Systems (CHI)*. 3055–3064.

[44] Manjeevan Seera, Chee Peng Lim, Ajay Kumar, Lalitha Dhamotharan, and Kim Hua Tan. 2021. An Intelligent Payment Card Fraud Detection System. *Annals of Operations Research* (2021).

[45] Ceyhan Ceran Serdar, Murat Cihan, Doğan Yöucel, and Muhittin A Serdar. 2021. Sample Size, Power and Effect Size Revisited: Simplified and Practical Approaches in Pre-Clinical, Clinical and Laboratory Studies. *Biochem Med (Zagreb)* 31, 1 (2021).

[46] Abhinav Srivastava, Amlan Kundu, Shamik Sural, and Arun Majumdar. 2008. Credit Card Fraud Detection Using Hidden Markov Model. *IEEE Transactions on Dependable and Secure Computing* 5, 1 (2008), 37–48.

[47] Jenny Tang, Eleanor Birrell, and Ada Lerner. 2022. Replication: How Well Do My Results Generalize Now? The External Validity of Online Privacy and Security Surveys. In *Proc. Symposium on Usable Privacy and Security (SOUPS)*. 367–385.

[48] The R Foundation. 2024. *Victims of Identity Theft, 2012.* https://www.r-project.org Accessed Jan. 26, 2024.

[49] Joseph Turow, Jennifer King, Chris Jay Hoofnagle, Amy Bleakley, and Michael Hennessy. 2009. *Americans Reject Tailored Advertising and Three Activities that Enable it.* https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1478214 Accessed Aug. 10, 2024.

[50] Blase Ur, Pedro Giovanni Leon, Lorrie Faith Cranor, Richard Shay, and Yang Wang. 2012. Smart, Useful, Scary, Creepy: Perceptions of Online Behavioral Advertising. In *Proc. Symposium on Usable Privacy and Security (SOUPS)*. Article 4.

[51] Anthony Vance, David Eargle, Jeffrey L Jenkins, C Brock Kirwan, and Bonnie Brinton Anderson. 2019. The Fog of Warnings: How Non-Essential Notifications Blur With Security Warnings. In *Proc. Symposium on Usable Privacy and Security (SOUPS)*. 407–420.

A Results Tables

Table 11. Participants' general demographics.

N = 150		
Gender	#	%
Male	71	(47.3%)
Female	78	(52.0%)
Non-binary	1	(0.7%)
Prefer to self describe	0	(0.0%)
Prefer not to answer	0	(0.0%)
Age	#	%
18 to 24	19	(12.7%)
25 to 34	64	(42.7%)
35 to 44	34	(22.7%)
45 to 54	17	(11.3%)
55 to 64	10	(6.7%)
65 to 74	4	(2.7%)
75 or older	2	(1.3%)
Prefer not to answer	0	(0.0%)
Education	#	%
Doctorate	2	(1.3%)
Master degree	19	(12.7%)
Bachelor degree	60	(40.0%)
Associate degree	23	(15.3%)
High school diploma or GED	43	(28.7%)
Less than High school degree	1	(0.7%)
Other	2	(1.3%)
Current Occupation	#	%
Student	9	(6.0%)
Full-time employee	81	(54.0%)
Part-time employee	21	(14.0%)
Self-employed or business owner	9	(6.0%)
Full-time homemaker	4	(2.7%)
Unemployed, and looking for a job	12	(8.0%)
Unemployed, and not looking for a job	2	(1.3%)
Unable to work	4	(2.7%)
Retired	4	(2.7%)
Other	4	(2.7%)
Income	#	%
Less than $20,000	15	(10.0%)
$20,000 to $39,999	19	(12.7%)
$40,000 to $59,999	32	(21.3%)
$60,000 to $79,999	22	(14.7%)
$80,000 to $99,999	27	(18.0%)
$100,000 to $149,999	18	(12.0%)
$150,000 or more	13	(8.7%)
Prefer not to answer	4	(2.7%)
CS, IS, IT or CE degree	#	%
Yes	18	(12.0%)
No	132	(88.0%)
Cybersecurity Degree	#	%
Yes	1	(0.7%)
No	149	(99.3%)

Table 12. Details provided by participants about their use of the debit/credit card involved in the fraud incident they describe in the survey.

N = 150		
Account Type	#	%
Personal Account	149	(99.3%)
Business Account	1	(0.7%)
I cannot remember	0	(0.0%)
Other	0	(0.0%)
Type of Card	#	%
Debit Card	89	(59.3%)
Credit Card	58	(38.7%)
Debit and credit card in one card	3	(2.0%)
I cannot remember	0	(0.0%)
Category	#	%
Bank Visa or Mastercard debit/credit card	131	(87.3%)
Discover or American Express debit/credit card	6	(4.0%)
Co-branded debit/credit card	8	(5.3%)
I cannot remember	1	(0.7%)
I don't know	2	(1.3%)
Other	2	(1.3%)
Modes of Transactions (non-exclusive)	#	%
Online	121	(80.7%)
In person	111	(74.0%)
I cannot remember	6	(4.0%)
Avenues of Online Transactions (non-exclusive)	#	%
Apps and websites	113/121	(93.4%)
The bank or card issuer's app or website	47/121	(38.8%)
Digital wallets	47/121	(38.8%)
Third-party financial apps	64/121	(52.9%)
I cannot remember	3/121	(2.5%)
Other	2/121	(1.7%)
Frequency of Online Transactions	#	%
At least once a day	11/121	(9.1%)
At least once every few days	45/121	(37.2%)
At least once a week	30/121	(24.8%)
At least once every few weeks	21/121	(17.4%)
At least once a month	9/121	(7.4%)
At least once every few months	2/121	(1.7%)
At least once every six months	0/121	(0.0%)
At least once a year	1/121	(0.8%)
Less than once a year	2/121	(1.7%)
Never	0/121	(0.0%)
I cannot remember	0/121	(0.0%)
Avenues of In-Person Transactions (non-exclusive)	#	%
Automated Teller Machines	43/111	(38.7%)
Point of sale machine	101/111	(91.0%)
I cannot remember	1/111	(0.9%)
Other	2/111	(1.8%)
Frequency of In-Person Transactions	#	%
At least once a day	18/111	(16.2%)
At least once every few days	42/111	(37.8%)
At least once a week	24/111	(21.6%)
At least once every few weeks	11/111	(9.9%)
At least once a month	2/111	(1.8%)
At least once every few months	8/111	(7.2%)
At least once every six months	2/111	(1.8%)
At least once a year	1/111	(0.9%)
Less than once a year	2/111	(1.8%)
Never	0/111	(0.0%)
I cannot remember	1/111	(0.9%)

Table 13. Financial vs. psychological impact – **at the time of the incident.** The sum of all cells equals N = 150.

	Psych. impacted	Psych. not-impacted
Fin. impacted	57	13
Fin. not-impacted	54	26

Table 14. Financial vs. trust impact – **at the time of the incident.** The sum of all cells equals N = 150.

	Trust impacted	Trust not-impacted
Fin. impacted	57	13
Fin. not-impacted	52	28

Table 15. Psychological vs. trust impact – **at the time of the incident.** The sum of all cells equals N = 150.

	Trust impacted	Trust not-impacted
Psych. impacted	92	19
Psych. not-impacted	17	22

Table 16. Financial vs. psychological impact – **today.** The sum of all cells equals N = 150.

	Psych. impacted	Psych. not-impacted
Fin. impacted	18	4
Fin. not-impacted	35	93

Table 17. Financial vs. trust impact – **today.** The sum of all cells equals N = 150.

	Trust impacted	Trust not-impacted
Fin. impacted	20	2
Fin. not-impacted	62	66

Table 18. Psychological vs. trust impact – **today.** The sum of all cells equals N = 150.

	Trust impacted	Trust not-impacted
Psych. impacted	46	7
Psych. not-impacted	36	61

B Survey

Section B.1 lists the recruitment materials. Section B.2 lists the screening survey. Section B.3 lists the main study's survey. Section headings and text between [square brackets] were not shown to participants. We added them here for clarity.

B.1 Recruitment Materials

Title: Your debit/credit card fraud experiences
Reward: $.50 (screening) $3.75 (main) (approximately $15/hr)
Estimated completion time: 15 mins
Description: Our research team at Carnegie Mellon University is searching for people to participate in a survey about their debit/credit card fraud experiences. Participants should have experienced debit/credit fraud to participate.

If you are interested in participating in our survey, please complete this initial screening survey, which should just take 2 minutes. You will be paid $0.50 for completing the screening survey through Prolific.

If you are selected for the study's main survey, you will be asked if you agree to be taken to that survey and then be directed to the main survey that will last about 15 minutes. You will be paid $3.75 for completing this main survey through Prolific.

All responses to the survey will be kept confidential.
Devices you can use to take this study: Mobile, Tablet, Desktop

B.2 Screening Survey

Q.0: Please enter your unique Prolific ID.
Please note that this response should auto-fill with the correct ID.
[free response field]
Q.1: Do you have a debit or credit card(s)?

- Yes
- No

[If response to Q.1 is "yes"]
Q.2: Have you ever experienced a debit/credit card fraud incident, where any amount of money was charged to your debit/credit card without your knowledge or consent?

- Yes
- No

[If Q.1 and Q.2 answers are "yes"]
Q.3: Approximately, when was your **most recent** experience of debit/credit card fraud?

- Within the last few months
- Within the last year
- Within the last 2 years
- Within the last 3 years
- Within the last 4 years
- Within the last 5 years
- More than 5 years ago
- I cannot remember

[If Q.3 answer is "within the last 3 years" or less]
Q.4: In the past 3 years, approximately, how many times have you experienced debit/credit card fraud incidents?

- Once
- Twice
- Three times
- More than three times
- Other (please specify): [free response field]

[If Q.3 answer is "within the last 4 years" or more]
Q.5: In the past 5 years, approximately, how many times have you experienced debit/credit card fraud incidents?

- Once
- Twice
- Three times
- Four time
- Five times
- More than five times
- Other (please specify): [free response field]

Q.6: In your own words, please describe what happened in your **most recent** debit/credit card fraud experience?
[Free response field.]
Q.7: How did you discover the fraud in your **most recent** debit/credit card fraud experience?
[Free response field]
Q.8: What type of account was associated with the described debit/credit card fraud incident?

- Personal account
- Business account
- I cannot remember
- Other (please specify): [free response field]

[If Q.8 answer is "personal" or "business" account]
Q.9: What was the country of origin of the bank or card issuer associated with the described debit/credit card in which you experienced the fraud incident?

- United States
- Other (please specify): [free response field]

[If: Q.1 answer is "yes"; Q.2 answer is "yes"; Q.3 answer is "within the last 3 years" or less; Q.6 and Q.7 answers are at least 20 characters long; and Q8 answer is personal or business account]

Q.10: Are you willing to participate in an online survey about your experience of debit/credit card fraud? (it takes around **15 min**. and you will be paid **$3.75** for participation through Prolific)
If you selected "Yes" you will be redirected to the survey now.

- Yes
- No

[If Q.10 is "yes", the following text is shown]
Please think only about the time of **your most recent experience of debit/credit card fraud you described previously in the screening survey** and answer all the following questions in that context.

As a reminder, here is your answer for describing the fraud experience:
[Q.6 answer is shown here]

Here is your answer for how you discovered it:
[Q.7 answer is shown here]
[If Q.10 is "Yes", automatic direction to the main survey]

B.3 Main Survey

[Section headings were not visible to participants.]
SECTION #1: THE INCIDENT CONTEXT
Q.1: What type of card did you experience the debit/credit card fraud incident on?

- Debit card
- Credit card
- Debit and Credit card in one card (combination card)
- I cannot remember

Q.2: What type of debit/credit card did you experience the fraud incident on?

- Bank Visa or Mastercard debit/credit card
- Discover or American Express debit/credit card
- Co-branded debit/credit card (when organizations or companies such as retail stores or airlines partner with card issuer)
- I cannot remember
- I don't know
- Other (please specify): [free response field]

Q.3: What was the name of the bank or card issuer associated with the described debit/credit card that you experienced the fraud incident on?
[Free response field]
Q.4: At the time of the incident, what type of transactions had you been using this debit/credit card for? (select all that apply)

- Online
- In-person
- I cannot remember [exclusive]

[If Q.4 answer is "online"]
Q.5: At the time of the incident, which of the following had you been using to perform **online** transactions using this card? (select all that apply)

- Apps and websites (e.g. shopping apps/websites)
- The bank or card issuer's app or website (e.g. to transfer money)
- Digital wallets (e.g. Apple Pay and Google Pay)
- Third-party financial apps (Paypal, Venmo, etc.)
- I cannot remember [exclusive]
- Other (please specify): [free response field]

[If Q.4 answer is "online"]
Q.6: At the time of the incident, approximately how often had you been using this card for **online** transactions?

- At least once a day
- At least once every few days
- At least once a week
- At least once every few weeks
- At least once a month
- At least once every few months
- At least once every six months
- At least once a year
- Less than once a year
- Never
- I cannot remember

[If Q.4 answer is "in-person"]
Q.7: At the time of the incident, which of the following had you been using to perform **in-person** transactions using this card? (select all that apply)

- Automated Teller Machines (e.g. ATMs)
- Point of sale machine (e.g. those found in shops, restaurants, etc.)
- I cannot remember [exclusive]
- Other (please specify): [free response field]

[If Q.4 answer is "in-person"]
Q.8: At the time of the incident, approximately, how often had you been using this card for **in-person** transactions?

- At least once a day
- At least once every few days
- At least once a week
- At least once every few weeks
- At least once a month
- At least once every few months

- At least once every six months
- At least once a year
- Less than once a year
- Never
- I cannot remember

SECTION #2: DETECTION (POST-FRAUD)

Please think only about the time of **your most recent experience of debit/credit card fraud that you described previously** in this survey, and answer all the following questions in that context.

Q.9: Which of the following was **the first thing** that triggered your attention to discover your debit/credit card fraud?

- I checked my card or account statement and found a transaction(s) I did not make
- I checked my card or account statement and found a transaction(s) that I made, but went to an unintended recipient(s)
- I realized I might have fallen for a scam or something did not seem right, which led me to do further checks and subsequently find the fraud
- I received a form of alert or notification **from my bank or card issuer** (e.g. SMS, phone call, letter, email, etc. for withdrawal or fraud notifications)
- I received a form of alert or notification **from a third-party** (e.g. SMS, phone call, letter, email, etc. for withdrawal or fraud notifications) (*please specify what type of third-party): [free response field]
- I learned about the fraud from public channels (e.g. social media), which led me to do further checks and subsequently find the fraud
- I learned about the fraud from family, friends, or other people, which led me to do further checks and subsequently find the fraud
- Other (please specify): [free response field]

[If Q.9 answer is "I received a form of alert or notification from my bank or card issuer..." or "I received a form of alert or notification from a third-party..."]

Q.10: What was the type of the received alert or notification?

- Withdrawal
- Low balance
- Account balance
- Suspicious transaction
- Fraudulent transaction
- International transaction
- I cannot remember
- Other (please specify): [free response field]

[If Q.9 answer is "I received a form of alert or notification from my bank or card issuer..." or "I received a form of alert or notification from a third-party..."]

Q.11: Through what means did you receive the notification? (select all that apply)

- Email
- Post letter
- Phone call
- Automated voice message
- Short text message (SMS)
- Message through the bank or card issuer's app or Internet banking website
- Push notification through the bank or card issuer's app or Internet banking website
- Other (please specify): [free response field]

[If Q.10 answer is "Suspicious transaction" or "Fraudulent transaction"]

Q.12: Did the bank or card issuer take any action to stop the fraud automatically?

- Yes
- No
- I cannot remember

[If Q.9 answer is "I received a form of alert or notification from my bank or card issuer..." or "I received a form of alert or notification from a third-party..."]

Q.13: From the time your debit/credit card fraudulent transaction occurred, how long did it take **the notification to reach you**?

If the fraud incident consisted of multiple fraudulent transactions, please answer based on the first transaction.

- Immediately
- Within a few minutes
- Within an hour
- Within a few hours
- Within a day
- Within a few days
- Within a week
- Within a few weeks
- Within a month
- More than a month
- I cannot remember
- Other (please specify): [free response field]

[If Q.9 answer is "I received a form of alert or notification from my bank or card issuer..." or "I received a form of alert or notification from a third-party..."]

Q.14: Overall, how helpful or unhelpful were the notifications you received in detecting the fraudulent activity?

- Extremely helpful
- Somewhat helpful
- Slightly helpful
- Not at all helpful

[If Q.9 answer is "I received a form of alert or notification from my bank or card issuer..." or "I received a form of alert or notification from a third-party..."]

Q.15: Why did you think the notification was helpful or unhelpful?
[Free response field]

Q.16: **From the time your debit/credit card fraudulent transaction occurred**, how long did it take **you to realize that you had been defrauded**?

If the fraud incident consisted of multiple fraudulent transactions, please answer based on the first transaction

- Immediately
- Within a few minutes
- Within an hour
- Within a few hours
- Within a day
- Within a few days
- Within a week
- Within a few weeks
- Within a month
- More than a month
- I cannot remember
- Other (please specify): [free response field]

Q.17: How many fraudulent transactions occurred in that incident before you were able to detect it?

- One transaction
- Multiple transactions in the same day
- Multiple transactions over a period of time
- I cannot remember
- Other (please specify): [free response field]

Q.18: Do you have any suggestions for how your bank or card issuer could improve fraud alerting and detection capabilities?
[Free response field]

SECTION #3: REPORTING

Please think only about the time of **your most recent experience of debit/credit card fraud that you described previously** in this survey, and answer all the following questions in that context.

Q.19: Did you report the fraud incident to your debit/credit card's bank or card issuer?

- Yes
- No
- I cannot remember

[If Q.19 answer is "no"]

Q.20: Why did you not report this fraud incident to the bank or card issuer?
[Free response field]

[If Q.19 answer is "yes"]

Q.21: Did you seek compensation for the amount the fraudster charged to your card (the direct financial loss) from your bank or card issuer?

- Yes
- No
- I cannot remember

[If Q.19 answer is "yes"]

Q.22: Have you been compensated for the amount the fraudster charged to your card (the direct financial loss) by your bank or card issuer?

- Yes - Fully
- Yes - Partially
- No
- Other (please specify): [free response field]

[If Q.19 answer is "yes"]

Q.23: Did the bank or card issuer provide you with an explanation of the fraud incident **(what / how / where / by whom, the incident was)**?

- The bank or card issuer provided me with **full explanation** of the fraud details
- The bank or card issuer provided me with **partial explanation** of the fraud details
- The bank or card issuer **did not provide** me with **any explanation** of the fraud details
- Other (please specify): [free response field]

[If Q.19 answer is "yes"]

Q.24: How satisfied or unsatisfied were you with the support offered to you by your bank or card issuer in handling the incident's reporting and compensation processes?

- Extremely satisfied
- Somewhat satisfied
- Slightly satisfied

- Not at all satisfied

[If Q.19 answer is "yes"]

Q.25: What advice would you give your bank or card issuer to improve the support they offered to you in handling the incident's reporting and compensation processes?

[Free response field]

SECTION #4: FRAUD IMPACT

Please think only about the time of **your most recent experience of debit/credit card fraud that you described previously** in this survey, and answer all the following questions in that context.

Q.26: How much did **the fraudster charge to your card** (the direct financial loss)? **Please select the total amount, even if it was later compensated or reimbursed**.

- $0 (no direct financial loss)
- From $0.01 to $10
- From $11 to $50
- From $51 to $100
- From $101 to $500
- From $501 to $1,000
- From $1,001 to $2,000
- From $2,001 to $4,000
- From $4,001 to $6,000
- From $6,001 to $8,000
- From $8,001 to $10,000
- More than $10,000
- I cannot remember
- Other (please specify): [free response field]

Q.27: Which, if any, of the following indirect financial losses did you experience as a result of the fraud experience you had? (select all that apply)

- Damaged personal reputation
- Loss of trust from others
- Legal and attorney fees for pursuing legal action or defending against accusations
- Increased insurance premiums or difficulty obtaining insurance coverage
- Costs of credit monitoring or identity theft protection services
- Loss of job due to the fraud incident
- Loss of income due to the fraud incident
- Emotional distress
- Costs of therapy or counseling
- Difficulty obtaining loans or credit
- Negative impact on credit score or higher interest rates for borrowing
- None of these [exclusive]
- Other (please specify): [free response field]

Q.28: Which, if any, of the following psychological negative impacts did you experience as a result of the fraud experience you had? (select all that apply)

- Stress
- Difficulty in sleeping
- Difficulty in trusting others
- Confusion
- Discomfort
- Frustration
- Worry or anxiety
- Feeling upset
- Feeling unsafe
- Depression
- Embarrassment
- Shame
- Guilt
- Loss of self-confidence
- Low satisfaction
- Negative changes in perception
- None of these [exclusive]
- Other (please specify): [free response field]

Q.29: How did the fraud incident impact you **at the time of the incident**?

[Table 19 is shown here.]

Q.30: How does the fraud incident continue to impact you **today**?

[Table 19 is shown here.]

SECTION #5: BEHAVIORAL CHANGE

Please think only about the time of **your most recent experience of debit/credit card fraud that you described previously** in this survey, and answer all the following questions in that context.

Q.31: Have you taken any measures to prevent future fraud on your debit/credit card? (select all that apply)

- I have implemented security measures from the bank or card issuer to protect my financial transactions.
- I have implemented security measures from third-parties to protect my financial transactions.
- I am now more cautious and vigilant when conducting financial transactions.
- I have set up alerting mechanisms for my account or card.
- I now regularly check my account or card statement.

Table 19. Impact matrix used in questions Q29 and Q30.

	Did not impacted me negatively at all	Somewhat impacted me negatively	Strongly impacted me negatively
Financially	○	○	○
Psychologically	○	○	○
Your level of trust in performing financial transactions	○	○	○

- I switched my bank or card issuer.
- I did not undertake any measures [exclusive]
- Other (please specify): [free response field]

[If Q.31 answer is NOT "I did not undertake any measures"]

Q.32: Please elaborate more on the measures you took to prevent future fraud on your debit/credit card?

For your reference, you said you took the following measure(s) in the previous answer.

[Response to Q.31 is shown as bullet list]

[Free response field]

SECTION #6: DEMOGRAPHICS

Please answer the following demographic questions

Q.33: How do you describe your gender identity?

- Female
- Male
- Non-binary
- Prefer to self-describe: [free response field]
- Prefer not to answer

Q.34: How old are you (in years)?

- From 18 to 24
- From 25 to 34
- From 35 to 44
- From 45 to 54
- From 55 to 64
- From 65 to 74
- 75 or older
- Prefer not to answer

Q.35: What is your race or ethnic identity? (select all that apply)

- White
- Black or African American
- American Indian or Alaska Native
- Asian
- Native Hawaiian or Pacific Islander
- Hispanic and/or Latino/Latina/Latinx
- Prefer not to answer [exclusive]
- Other (please specify): [free response field]

Q.36: What is the highest educational degree you have received?

- Doctoral degree
- Master's degree
- Bachelor's degree
- Associate's degree
- High school diploma or GED
- Less than high school degree
- Other (please specify): [free response field]

Q.37: Do you have a university degree in, or currently work in, one or more of the following fields: Computer Science (CS), Information Systems (IS), Information Technology (IT), or Computer Engineering (CE)?

- Yes
- No

Q.38: What is your current employment status?

- Student
- Full-time employee
- Part-time employee
- Self-employed or business owner
- Full-time homemaker
- Unemployed, and looking for a job
- Unemployed, and not looking for a job
- Unable to work
- Retired
- Other (please specify): [free response field]

Q.39: What is your approximate annual household income?

Please answer based on your entire current household's income, before taxes.

- Less than $20,000
- $20,000 to $39,999
- $40,000 to $59,999
- $60,000 to $79,999
- $80,000 to $99,999
- $100,000 to $149,999
- $150,000 or more
- Prefer not to answer

[If Q.38 answer is "full-time employee" or "part-time employee" or "Self-employed or business owner"]

Q.40: What is the sector you currently work in?

- Pre-university Education
- University Education
- Health
- Communication and Information Technology
- Financial
- Industrial
- Agricultural
- Sales and retail
- Petrochemical
- Other (please specify): [free response field]

[If Q.38 answer is "full-time employee" or "part-time employee" or "Self-employed or business owner"]

Q.41: What is your current job title? (e.g. Teacher, Assistant Professor, Administrative staff, Nurse, etc.)

[Free response field]

[If Q.38 answer is "student"]

Q.42: What is the degree you are currently studying?

- Doctoral degree
- Master's degree
- Bachelor's degree
- Associate's degree
- High school diploma or GED
- Less than high school degree
- Other (please specify): [free response field]

[If Q.38 answer is "student"]

Q.43: What is the major you are studying for your current degree?

[Free response field]

Q.44: Do you have a university degree in cybersecurity or currently work in the cybersecurity area?

- Yes
- No

Q.45: If you have any other thoughts or feedback about this survey or the information you viewed, please let us know here. (optional)

[Free response field]

You now reached the end of the survey. To submit your response click the "Submit" button.

C Codebook

In this section, we list our codebook divided into tables. Each table represents the codebook for a question or a set of related questions. All question are from the main survey listed in Appendix B.3 unless stated otherwise. All codes are in small letters only.

Table 20. Codebook for Q.6 of the screening survey about fraud description (transaction mode).

Q.6 (screening survey): Fraud description → Transaction mode	
Code (# occurrence) [exclusive]	**Code Definition**
unspecified (78)	No cues about the transaction type
online (53)	Cues indicating an online transaction
offline (19)	Cues indicating an offline transaction

Table 21. Codebook for Q.6 of the screening survey about fraud description (transaction category).

Q.6 (screening survey): Fraud description → Transaction category	
Code (# occurrence) [non-exclusive]	**Code Definition**
unauthorized_purchase (87)	Transactions where any goods were purchased from any store in a any location
unauthorized_transaction (54)	A generic code for transactions/charges made to a bank account or cards, where there isn't a specific indicator or type mentioned
overcharging (4)	Transactions including purchases, tips, etc. which charged more than the authorized amount
identity_theft (3)	Transactions where the participant's bank account information was stolen or a new bank account or credit card was opened in their name without their knowledge or consent
unauthorized_withdrawal (2)	Transactions which explicitly mentioned withdrawal of amount from their account
never_received_items (1)	Transactions where a purchase was made but the participant never received the purchased item
unauthorized_check_issued (1)	Frauds associated with cash access checks

Table 22. Codebook for Q.6 of the screening survey about fraud description (location).

Q.6 (screening survey): Fraud description → Transaction location	
Code (# occurrence) [exclusive]	**Code Definition**
unspecified (116)	Transaction that did not specify location
different_state (23)	Transaction occurred in a state different than the participants' state (within USA)
different_continent (4)	Transaction occurred outside of North America
different_area (3)	Transaction occurred in an area different than the participants' area (within USA)
different_city (2)	Transaction occurred in a city different than the participants' city (within USA)
different_country (2)	Transaction occurred in a country different than the participants' country (USA)

Table 23. Codebook for Q.6 of the screening survey about fraud description (goods or service).

Q.6 (screening survey): Fraud description → Goods or service	
Code (# occurrence) [non-exclusive]	**Code Definition**
store (22)	Transaction that specified a store
food_and_beverages (19)	Transaction about purchasing food or beverages
electronics (7)	Transaction about purchasing electronics or services supporting these electronics (e.g. online gaming account) or stores that primarily sell electronics
gas (7)	Transaction about purchasing gas or occurred in a gas station
subscription_membership (6)	Transaction about purchasing/renewing a subscription or membership
clothes (4)	Transaction about purchasing clothes in an online/offline mode
entertainment (3)	Transaction about purchasing access to content primarily for entertainment including online avenues such as Amazon Prime Video or offline avenues such as wrestling or record companies
transportation (3)	Transaction about purchasing tickets for transportation or ride-sharing app transactions
horse_equipment (1)	Transaction about purchasing equipment for horses
like_money_laundering_website (2)	Transaction about money laundering
loan_agreement (1)	Transaction about loan agreement
porn (1)	Transaction about porn

Table 24. Codebook for Q.6 of the screening survey about fraud description (special cases).

Q.6 (screening survey): Fraud description → Special cases	
Code (# occurrence) [non-exclusive]	**Code Definition**
unspecified (115)	Transaction that did not specify special cases
online_account (14)	Online account hacked to make purchases they did not make
card_details (8)	Card details were accessed in an unauthorized manner
service_provider_notification (7)	When a notification originated from the service provider (e.g. store)
physical_card (6)	Someone took their physical card or smartphone
smartphone (1)	Physical theft for a smartphone that contains the app that contains the card
family (1)	Family was involved in the fraud
skimming (1)	Card skimming was involved in the fraud

Table 25. Codebook for Q.15 about reasons for notification helpfulness.

Q.#: Notifications helpfulness / unhelpfulness → Reasons for notification helpfulness	
Code (# occurrence) [non-exclusive]	**Code Definition**
awareness (49)	The notification made the subject aware of the fraud, such as being alerted, notified, etc.
fast (29)	The notification enabled fast awareness, action, or stopping of the fraud, such as within # [time unit], immediately, quickly, etc.
helped_take_action (29)	The notification enabled the subject to take actions based on on the notification to stop the current or future fraud
transaction_type (5)	The notification contained the transaction type (e.g. purchase) and number of transactions (single, multiple, etc.)
card_used (2)	The notification alerted the subject that their card was used
info_compromise (2)	The notification alerted the subject that their information was compromised or compromised in a data breach
late (2)	The notification arrived late
place (2)	The notification provided the place where the card used
suspicious_transaction (2)	The notification alerted the subject about suspicious transaction explicitly
amount (1)	The notification provided the amount taken
confidence_in_service (1)	The notification allowed them gain more confidence on the service
fear_phishing_msgs (1)	The subject mentioned fear of phishing attacks in notifications
helped_monitoring (1)	The notification helped monitoring accounts/cards
helped_resolved (1)	The notification helped in resolving the fraud
more_info (1)	The notification provided subsequent information about the incident (more than notification basic information)
no_loss_access (1)	The subject mentioned they did not lose access to their accounts/cards
stopped_psych_harm (1)	The notification helped protect the subject from psychological harm such as embarrassment

Table 26. Codebook for Q.15 of the main survey about reasons for notification unhelpfulness.

Q.#: Notifications helpfulness / unhelpfulness → Reasons for notification unhelpfulness	
Code (# occurrence) [non-exclusive]	**Code Definition**
fraud_occurred (1)	The fraud had already occurred

Table 27. Codebook for Q.18 about suggestions to improve alert and detection capabilities.

Q.18: Detection → Suggestion to improve alert and detection capabilities	
Code (# occurrence) [non-exclusive]	**Code Definition**
different_location_alert (16)	Send alerts of transactions initiated from geographical locations different than the card holder's resident location
sms_alert (15)	Send alerts through SMS
approve_decline_transaction (12)	Allow individuals to approve or decline certain transactions
fraud_or_suspicious_transaction_alert (11)	Send alerts of suspicious or fraudulent transactions
immediate (11)	Send alerts immediately
unusual_behavior_alert (11)	Send alerts of unusual behaviour
purchase_alert (8)	Send alerts for every purchase transaction
email_alert (7)	Send alerts through email
multi_channel_alerts (6)	Send alerts through multiple channels (e.g. phone/sms/email/etc.)
large_purchase_alert (6)	Send alerts for large transactions
any_transaction_alert (5)	Send alerts for any type of transaction
phone_call_alert (5)	Send alerts through phone call
app_notification (3)	Send alerts through app notifications
int_transaction_alert (2)	Send alerts for international or overseas transactions
alert_without_cardlock (2)	Send alerts instead of locking the card
default_alert (2)	Send alerts by default without having to opt-in
legitimate_text (2)	Ensure the alert themselves do not look fraudulent or suspicious
multi_channel_verification (2)	Verify transaction through multiple channels (e.g. phone/call/email)
phone_alert (2)	Send alerts on the phone device
require_verification (2)	Require verification of transaction
additional_info (1)	Provide additional information in alerts
blacklist_fraudulent_sellers (1)	Maintain a blacklist of fraudulent sellers and block transaction toward them
customizable_alerts (1)	Allow customization of alerts
enforce_pin_online (1)	Require pin for purchases online
enforce_pin (1)	Require pin for purchases offline
giftcard_transaction_alert (1)	Send alerts for gift card purchasing transactions
help_find_offenders (1)	Find the the fraudsters who caused the fraud
help_prosecute_offenders (1)	Prosecute the fraudsters who caused the fraud
improve_online_purchasing_security (1)	Improve security features/functionalities/measures offered by the bank or card issuer for online purchases
improve_security (1)	Improve security features/functionalities/measures offered by the bank or card issuer
lock_card_feature (1)	Offer consumers the ability to lock/unlock card by themselves
lock_upon_no_response_to_alert (1)	Lock the card if there isn't a response from the card holder after a predefined amount of time
monitor_small_transactions (1)	Monitor transactions that involve small amounts
online_reporting (1)	Provide means to report the fraud online
optional_alert (2)	Send alerts if the card holder opted for one
password_change_alert (1)	Send alerts if the bank account or cards password has changed
pin_change_alert (1)	Send alerts if the bank account or cards pin number has changed
reduce_false_positives (2)	Reduce alerts for non-fraudulent transactions (flase positive)
remind_to_configure (1)	Remind users to configure alerts/notifications
repeated_purchases_alert (1)	Send alerts upon repeated purchase of the same goods or services
skimming_detection_alert (1)	Send alerts if the users card was subject to card skimming
stop_mailing_cash_access_checks (1)	Stop mailing cash access checks without explicit request or authorization
track_card (1)	Track the location of the card
track_transaction_recipients (1)	Track the recipients of the transaction
over_limit_transaction_alert (1)	Send alerts for transactions over a specified limit

Table 28. Codebook for Q.25 about suggestion to improve the reporting and compensation process.

Q.25: Reporting → Suggestion to improve the reporting and compensation process.	
Code (# occurrence) [non-exclusive]	**Code Definition**
fraud_explanation (26)	The bank or card issuer provides an explanation of the fraud, such as how the fraud occurred, who the recipient/fraudster was, when and where did the incident occur, etc.
refund (14)	The bank or card issuer provides refund to the victims
fast_process (9)	The bank or card issuer provides faster process to report and resolve the fraud
fast_refund (8)	The bank or card issuer provides faster refund to the victims
fast_comm (7)	The bank or card issuer provides faster communication to the victims
full_refund (4)	The bank or card issuer provides complete/full refund of the amount fraudulently charged
preventive_tips (5)	The bank or card issuer provides tips to prevent such fraud in the future
automated_reporting_system (3)	The bank or card issuer provides an automated process to report and resolve the fraud
better_comm (3)	The bank or card issuer communicates with the affected parties in a better manner
proactive (3)	The bank or card issuer takes proactive action in identifying fraudulent transactions and resolving them
trust_customer (3)	The bank or card issuer trusts the consumer
direct_comm (2)	The bank or card issuer allows direct communication with a human representative
resolution (2)	The bank or card issuer provides a resolution to the fraud experienced by the victims
approve_decline_transaction (2)	The bank or card issuer provides means to approve or decline transactions
easy_freeze_card (2)	The bank or card issuer provides means to freeze the victim's card
fast_alert (2)	The bank or card issuer alerts the victims in a faster manner
fraud_or_suspicious_transaction_alert (2)	The bank or card issuer alerts the victims in the event of fraudulent or suspicious transaction
understanding (1)	Representatives from the bank or card issuer showcase understanding with the consumer in the incident reporting/resolution process
additional_compensation (1)	The bank or card issuer provides additional compensation in addition to the reimbursement of the fraudulently acquired amount
avoid_mistakes (1)	The bank or card issuer avoids making mistakes in the reporting/resolution process
better_emp_training (1)	The bank or card issuer provides better training to their employees
better_emp_wages (1)	The bank or card issuer provides better compensation to their employees
black_list_fraud_recipient (1)	The bank or card issuer maintains a blacklist of fraudulent sellers and block transactions toward them
fast_new_card (1)	The bank or card issuer provides a replacement card in a faster manner
fast_resolution (1)	The bank or card issuer provides faster resolution to the victims
fraud_detection (1)	The bank or card issuer provides better fraud detection capabilities
fraud_explanation_from_retailer (1)	The retailers/third-party service provider provides an explanation of the fraud, such as how the fraud occurred, who the recipient/fraudster was, when and where did the incident occur, etc.
keep_same_card (1)	The bank or card issuer retains the same card, and not have to get a new card
multi_channel_comm (1)	The bank or card issuer contacts the victims through multiple channels
patience (1)	Representatives from the bank or card issuer showcase patience with the consumer in the incident reporting/resolution process
prosecute_fraudster (1)	The bank or card issuer helps prosecute the fraudster
reporting_via_app (1)	The bank or card issuer provides means to report fraud through the bank or card issuer's mobile app
reporting_via_website (1)	The bank or card issuer provides means to report fraud through the bank or card issuer's website
use_email (1)	The bank or card issuer contacts victims or share alerts through email
use_mfa (1)	The bank or card issuer provides authentication checks with multi-factor authentication
use_sms (1)	The bank or card issuer provides authentication checks via SMS

Table 29. Codebook for Q.25 about suggestion to improve the reporting and compensation process (factors that led to satisfaction).

Q.25: Reporting → Factors that led to satisfaction.	
Code (# occurrence) [non-exclusive]	**Code Definition**
satisfied (17)	The participant was satisfied with the reporting and resolution process
fast_process(10)	Fast reporting and resolution process
refund (5)	Refund was provided
comm (2)	Communication efforts by the bank or card issuer representative
full_refund (2)	Full refund was provided
provided_resolution (1)	Resolution was provided
professionalism (1)	Professionalism exhibited by the bank or card issuer representative
fast_comm (1)	Fast communication by the bank or card issuer
provided_direct_comm (1)	Direct communication efforts by the bank or card issuer human representative
fast_refund (1)	Refund was provided in a fast manner
new_card (1)	New card was provided
provided_support (1)	Support was provided by the bank or card issuer
fraud_prevented (1)	The fraud was prevented by the bank or card provider

Table 30. Codebook for Q.25 about suggestion to improve the reporting and compensation process (fraud explanation).

Q.25: Reporting → Fraud explanation.	
Code (# occurrence) [exclusive]	**Code Definition**
culprit_info (7)	More information regarding who the culprit was
incident_details (5)	More information regarding the details of transaction that caused the incident
what_happened (5)	More information regarding what happened in this incident
how_happened (4)	More information regarding the how the incident occurred
preventive_tips (4)	More information on how to prevent such incident from happening in the future
investigation_details (2)	More information regarding the details of investigation conducted
legal_action (2)	Aid in legal action undertaken by the affected party
where_happened (2)	More information regarding the where the incident occurred
assessment (1)	Conduct an accurate assessment of the situation
automate_reporting (1)	Automated means to report the incident
online_or_offline (1)	More information regarding whether the transaction was online or offline
process_info (1)	More information regarding the process of incident reporting and resolution
recipient_info (1)	More information regarding who the recipient of this transaction/amount was
report_app_website (1)	Means to report the incident through the mobile app or website
support_channels (1)	More information regarding the support channels available for reporting the incident and seeking resolution
when_happened (1)	More information regarding the when the incident occurred
why_happened (1)	More information regarding the why the incident occurred

Table 31. Codebook for Q.32 about the measures taken to prevent future fraud (vigilance).

Q.32: Measures to prevent future fraud → Vigilance	
Code (# occurrence) [exclusive]	**Code Definition**
unspecified (28)	Did not specify the security measures of type "vigilance" undertaken post the fraudulent experience
cautious_on_websites (25)	Exercised additional caution while using websites
stop_saving_card_in_accounts (13)	Stopped saving card details in any digital account
cautious_card_physical (8)	Took additional caution in securing card physically including avoiding handing over card when out of sight
caution_card_pos_systems (7)	Exercised additional caution in using card in point-of-sale systems
cautious_card_use_general (6)	Exercised additional caution in general use
use_trusted_financial_services (6)	Switched to trusted financial services with better security features like paypal, apple pay, etc. for certain transactions
switch_usage_debit_to_credit (5)	Switched usage from debit card to credit card
cautious_skimming_device (4)	Exercised additional caution in ATM and point-of-sale systems to identify skimming device
limit_online_transactions (3)	Reduced online transactions
stop_using_impacted_service (3)	Stopped using the service which caused the fraudulent incident
caution_card_atm (2)	Exercised caution when conducting transactions at the ATM including isolating themselves, checking for skimming device, etc.
use_one_time_cards_for_online (2)	Utilized one-time card(s) referred as burner/virtual cards for online transactions
cautious_giving_card_info (1)	Exercised additional caution when providing card information
check_transaction_correctness (1)	Exercised additional caution to ensure transaction details are correct, such as checking recipient, amount etc.
diversify_funds_multiple_accts (1)	Diversified financial portfolio to include multiple bank or card issuers instead of one to reduce the risk/impact
exercise_caution_while_transacting (1)	Exercised additional caution while conducting any financial transaction online/offline, or any mode of transaction
limit_online_shopping (1)	Reduced online transaction, specifically online shopping
logout_websites (1)	Ensured Logging out of accounts after every usage to ensure that the accounts are not taken-over/misused
not_always_work (1)	When choosing not to save card info it doesn't work as expected (still save card details)
require_photo_id (1)	Opted for verification through photo ID for every transaction
stop_response_suspicious_msg (1)	Stopped responding to any suspicious message that might lead to information disclosure
urge_family_take_same_measures (1)	Urged family members to take same measures (as the victims) to safeguard their accounts
use_giftcard_on_questionable_websites (1)	Used gift card when conducting transactions of less popular, questionable, or small business websites
use_protected_wallet (1)	Used protected wallets to safeguard card information from being stolen

Table 32. Codebook for Q.32 about the measures taken to prevent future fraud (setup alerts).

Q.32: Measures to prevent future fraud → Setup alerts	
Code (# occurrence) [non-exclusive]	**Code Definition**
unspecified (20)	Did not specify the security measures of type "setup alerts" undertaken post the fraudulent experience
unspecified_alerts (10)	Setup alerts. Unspecified type of alert configured
any_transaction_alert (9)	Setup alerts for all transactions
sms_alert (7)	Setup alerts through SMS
suspicious_transaction_alert (7)	Setup alerts for suspicious transactions
large_transaction_alert (6)	Setup alerts for large transactions (this also includes transactions above a certain limit set by the user)
app_notifications (3)	Setup alerts through app, e.g. push notifications
email_alert (3)	Setup alerts through email
enable_notifications (3)	Setup alerts for the bank or card issuer of the impacted card only
all_accounts (2)	Setup alerts for all bank or card issuer accounts
adjust_minimum_balance_alert (1)	Adjusted minimal balance for the corresponding minimum balance alert
all_alerts (1)	Setup alerts for all activities on the bank or card issuer account
amount_transaction_alert (1)	Setup alerts transactions of a certain amount and above
check_phone_allow_alerts (1)	Verified the phone didn't suppress alerts configured on the bank or card issuer account
credit_report_alert (1)	Setup alerts for credit reports
daily_account_activity_alert (1)	Setup alerts for daily activities on the bank or card issuer accounts
multiple_channels_alerts (1)	Setup alerts in multiple channels, e.g. phone, SMS, email etc.
new_purchase_alert (1)	Setup alerts for any new purchases
security_alerts (1)	Setup alerts for security activities on the bank or card issuer

Table 33. Codebook for Q.32 about the measures taken to prevent future fraud (regular checks).

Q.32: Measures to prevent future fraud → Regular checks	
Code (# occurrence) [non-exclusive]	**Code Definition**
review_acct_or_card_or_statement (82)	Review the bank account or card statement
unspecified (27)	Did not specify the security measures of type "regular checks" undertaken post the fraudulent experience
daily (19)	Review the bank account or card statement on a daily basis
frequently (15)	Review the bank account or card statement frequently, without mentioning the periodicity
more_frequently (8)	Review the bank account or card statement more frequently as compared to before the fraudulent incident
every_few_days (7)	Review the bank account or card statement every few days
app (4)	Review the bank account or card statement on the bank or card issuer's application
few_times_a_day (4)	Review the bank account or card statement multiple times a day
weekly (4)	Review the bank account or card statement on a weekly basis
few_times_a_week (2)	Review the bank account or card statement multiple times a week
website (2)	Review the bank account or card statement on the bank or card issuer's website
before_making_payment (1)	Review the bank account or card statement before making any payment
constantly (1)	Review the bank account or card statement in a constant basis (without mentioning the periodicity)
few_times_a_month (1)	Review the bank account or card statement few times a month
immediately (1)	Review the bank account or card statement immediately
monthly (2)	Review their bank account or card statement in a monthly basis
multiple_time_a_week (1)	Review the bank account or card statement multiple times a week
phone (1)	Review the bank account or card statement on their phone

Table 34. Codebook for Q.32 about the measures taken to prevent future fraud (security measures).

Q.32: Measures to prevent future fraud → Security measures	
Code (# occurrence) [non-exclusive]	**Code Definition**
unspecified (30)	Did not specify the security measures of type "security measures" undertaken post the fraudulent experience
2fa (7)	Used software-based two-factor-authentication service for their bank or card issuer's accounts
apply_security_measures (6)	Utilized security measures in general, without mentioning what form of security measure were undertaken and applied
reset_password (4)	Reset the password associated with their affected bank or card issuer's accounts
change_card (3)	Changed the credit/debit card
lock_unused_card (4)	Locked the credit/debit card when not in use
all_accounts (3)	Took similar security measures for all the bank or card issue's accounts (not only the affected one)
lock_card (2)	Locked the credit/debit card
use_strong_password (2)	Configured strong password for the bank or card issuer's accounts
cautious_on_websites (1)	Exercised additional caution while using websites
esignature_all_transactions (1)	Setup e-signature on all transactions
extra_security_measures (1)	Utilized additional security measures as compared to before the fraud incident
freeze_card (1)	Froze the impacted card after the fraud incident
freeze_lost_card (1)	Froze the credit/debit card when losing the card
lock_card_after_suspicious_transaction (1)	Lock the credit/debit card when not in use
logout_websites (1)	Logging out of the accounts after every usage to ensure the accounts is not taken-over/misused
reset_pin (1)	Reset the PIN associated with the credit/debit card
without_card_or_acct_freeze (1)	Enabled alternate measure without freezing the cards

Table 35. Codebook for Q.32 about the measures taken to prevent future fraud (security measures from third party).

Q.32: Measures to prevent future fraud → Security measures from third party	
Code (# occurrence) [non-exclusive]	**Code Definition**
unspecified (12)	Did not specify the security measures of type "third party" undertaken post the fraudulent experience
credit_monitoring_svc (6)	Started using credit monitoring service
identity_protection_service (4)	Started using identity protection service to secure digital identities
2fa (1)	Started using software based two-factor-authentication service for digital accounts
any_transaction_alert (1)	Configured alerts for any transactions on third party services
2fa_hw (1)	Started using hardware token-based two-factor-authentication service for digital accounts
credit_report (1)	Started reviewing the credit report
fraud_app (1)	Started using fraud app
protection_sw (1)	Started using software to protect laptop, phone, or other devices
reset_password (1)	Reset the password of affected account(s)
reset_phone (1)	Performed factory reset for the affected phone
use_password_manager (1)	Started using password manager to secure their passwords

Table 36. Codebook for Q.32 about the measures taken to prevent future fraud (change bank or card issuer).

Q.32: Measures to prevent future fraud → Change bank or card issuer	
Code (# occurrence) [non-exclusive]	**Code Definition**
change_bank (8)	Changed the bank
unspecified (2)	Did not specify the security measures of type "change bank or card issuer" undertaken post the fraudulent experience
switch_usage_debit_to_credit (2)	Switched to using credit card instead of debit card owing to better security measures
change_bank_card (1)	Replaced the affected card with a new card with the same bank or card issuer
diversify_funds_multiple_banks (1)	Diversified financial portfolio to include multiple bank or card issuers instead of one to reduce the risk/impact