Personal Financial Fraud and Financial Identity Theft

Talal Ali
Carnegie Mellon University Qatar

Ragashree Mysuru Chandrashekar
Carnegie Mellon University

David Mberingabo
Carnegie Mellon University

Pauline Mevs
Carnegie Mellon University

Yiming Zhong
Carnegie Mellon University

1 Introduction

In 2017, The United States' Office of Justice Programs estimated 3.0 million persons, or about 1.25% of those age 18 or older, reported being victims of personal financial fraud during the prior 12 months. Financial fraud victims lost $ 1,090 on average and more than $ 3.2 billion in total. [11] Financial identity theft and other types of fraud usually require social engineering conducted over some mode of communication the victim trusts or identity information leaks. With social engineering, the attacker gains trust and achieves some form of information leakage or theft, or simply has the victim transfer funds to them. The unwanted (or unauthorized) transaction can occur with or without the direct or indirect knowledge and participation of the victim. The unwanted transaction must occur via cash or some financial platform or service, such as bank transfer, Paypal or an online shopping website payment portal. Given the variety of ways a person can experience a personal financial fraud event, we have found no holistic study on methods of discovery and resolution. We discuss fraud studies in the Related Works section and note that most studies have a narrow focus on specific types of fraud. Few studies on fraud focus on the user-experience related to detection and resolution of fraud. From these studies we can abstract victim discovery methods to common themes, such as self-detection.

The main goal of this study is to gain an in-depth understanding of the experiences of individuals who have been victims of personal financial fraud and financial identity theft. Specifically, the study aims to explore the ways in which victims become aware of the fraud, the negative impacts they suffer as a result, and the steps they take to resolve the issue. To achieve this goal, the study will address a number of key research questions. First, the study will explore how victims discover they have been targeted by fraudsters, focusing on the process of alerting victims to the fraudulent activity. Second, the study will examine the harms that victims experience as a result of financial fraud, including financial loss, psychological distress, and any other negative effects. The study will also investigate the methodologies used by victims to seek resolution and the outcomes of their efforts. This will include exploring both positive and negative outcomes of the resolution process.

In addition, the study will examine the impact of the resolution process on the privacy attitudes and behaviors of the victims, seeking to understand how their perceptions of privacy and security are shaped by their resolution experiences. Finally, the study will look for opportunities to improve the experience of resolving financial fraud, with a focus on identifying practical recommendations that can be used to enhance the process and minimize the negative impact of fraud. The study intends to provide valuable insights into the experiences of victims of financial fraud and financial identity theft, and offer recommendations for improving the resolution process to better support victims and protect their privacy and security.

2 Related Work

Our study builds on the prior literature, particularly the study objectives from Li Y. et al. [8] and Rosoff et al. [14] by considering the harm and impact, short-term and long-term implications of financial fraud and identity theft, and Button et al.'s [4] approach and methodology of interviews to get candid information from the participants. We will add two key aspects - how the participants realized they were defrauded and their experience in seeking resolution to the fraud into the study to holistically explore and find common patterns across differing post-fraud experiences.

2.1 Fraud Classification

No consensus on personal financial fraud or financial identity theft has been achieved. Our study holistically classifies fraud events as we encounter them during our interviews. Many respected institutions produce terminology that classifies personal financial fraud and financial identity theft, and we borrow their terminology as we conduct our exploration of the post-fraud experience.

The United States' Office of Justice Programs described 7 categories for personal financial fraud. By order of most frequently reported, they are a) Products and services, b) Charity, c) Phantom debt, d) Prize and grant, e) Relationship and trust, f) Employment Fraud and g) Investment Fraud. [11]

In 2019, the US Federal Trade Commission defined personal financial fraud that involved the victim paying for or otherwise giving money to fraudulent representatives for products and services the victim never received, dubbing this category as Consumer Fraud. [1] Their large study used interviews and surveys to distill Mass-Market Consumer Fraud into 19 scam categories. Blanton categorizes financial-product consumer fraud as either an Investment Fraud, Tax Fraud, Insurance Fraud or an Advance-Fee Scam. [2] Razaq et al. categorize phone-based social engineering fraud in Pakistan as either Lucky Draw scams were the victim is promised to win a prize; Bank Fraud which includes tricking victims for their banking credentials; Government Fraud where an attacker portrays themselves as a source of government authority; and finally, the Damsel in Distress scam where the attacker pretends to be a girl in trouble seeking financial help.

Identity Theft often leads to personal financial fraud. Financial Identity Theft is a type of Identity Theft that involves unauthorized use of a victim's financial and identity data for fraudulent purposes. This fraud category is especially painful for victims as this can lead to cases of mistaken identity that can last a long time without effective resolution due to the complicated and distributed nature of identity systems in the United States. Li et al. conducted a self-report survey on identity theft and found that "time elapsed since the incident negatively influences perceived distress". Some fraud types may be resolved faster than others. [8] By recognizing different types of personal financial fraud events, we can better identify common patterns in the resolution processes across multiple types of fraud. These patterns can then be examined and improved upon separately. Recognizing the most important or prominent types of fraud can also direct our exploration and lead to findings with a more holistic impact on personal financial fraud as a whole.

2.2 Fraud Mechanism

The mechanism through which fraud transactions occur is crucial to deciding which methods of notification, discovery, and resolution should be employed. Most studies on personal financial fraud focus on a narrow set of mechanisms specific to the type of fraud being studied. Fraudsters usually work through a scripted series of steps, and these modus operandi are what we call fraud mechanisms.

Razaq et al., interviewed victims of mobile-based scams in Pakistan. [13] They constructed a four-step social-engineering attack framework, in which they shed light on how victims' came to understand they were experiencing mobile fraud. Social engineering can be simplified to a few generic steps include spoofing trusted entities, engaging with a victim, stealing information and funds, then ending the process by delaying the victim's realization and ceasing communication. According to Razaq et al.'s findings, self-realization was the most prominent method of discovery. As an example, when those involved with prize-based fraud could no longer reach the fraudster they realized they had been defrauded. They also found that family and friends could be either enablers or limiters of the fraud while it was occurring.

Razaq et al. found that only 22% of the participants reported the fraud to relevant authorities, while 49% did not attempt to report it at all. [13] They cited a lack of awareness of relevant authorities to report to as the most common challenge victim's face when reporting.

2.3 Fraud Victim Characterisation

In an attempt to measure what makes a person more susceptible to a fraud event, several studies focused on various demographic groups, such as the elderly, students and so on. [16] [6] [3] Other studies explore the relationship between different victim behaviors, knowledge, skills, characteristics, and their impact on their likelihood of victimization.

Another example is J. Jansen and R. Leukfeldt study common characteristic victims shared, with a focus on detection and prevention. [7]

> "Several respondents reported having insufficient knowledge and skills regarding the safety and security of online banking and finding it difficult to assess to what extent protective measures help them to safeguard against fraudulent attacks."

Findings by DeLiema et. al suggest that elderly female victims were 40% more likely to report distress than elderly male victims. [6] Even Razaq et al. in Pakistan found that of the 22% that reported to the relevant authorities, all were from urban areas, and they observer gender trends in the reporting behaviour as well. [13] Razaq et al. claim that interviewed women

> "tend to not report because of dependency on male family members for reporting to relevant authorities and also driven by the misconception that frauds need to be reported at Police Stations where women find it difficult to go alone because of fears of harassment and security."

We consider victim's demographics, psychological and behavioural characteristics when determining the most usable methods of detection and resolution. Studies on victim psychology use Susceptibility to Persuasion (StP) scale to determine an individual's susceptibility to fraud crimes. It has demonstrated "good construct validity in relation to self-report scam plausibility across large samples". [12] Victim characterization provides insight on why a victim falls for a scam and how to assist different victims in their post-fraud experience.

2.4 Improving The Fraud Resolution Process

Banks, mobile payment apps, vendor sites, and credit card companies (among others) employ advanced technology to monitor for and notify customers of suspicious activity. Accordingly, there is an entire corpora dedicated to this and it includes such topics as application of AI/Machine Learning to detecting bank fraud [15], predicting fraud based on user behavior [5], detecting fraudulent accounts [10], and victim prevention [9]. However, this does not include how institutions intend to use this technology to help customers resolve fraud events.

Likewise, there is very little included in the literature on fraud victims, malware, and phishing that details how victims were notified [4]. Consistent with mobile-based fraud and product and services fraud, transaction fraud is often self-detected and may be the only way a victim discovers they have been defrauded. Studies like Jansen and Luekfeldt's 2015 analysis of 600 phishing and malware incidents obtained from a Dutch bank, in which they noted that 20 customers contacted the bank because they noticed unfamiliar transactions on their account [7].

To address the lack of clarity in the discovery and resolution process thereby aiding victims, system engineers, and UX designers, our study will include several questions about the victims' discovery process.

3 Methodology

This section elaborates on the methodology of our study. We chose a semi-structured interview which supports the explanatory nature of our research questions, and allows us to better understand the experience of victims of financial fraud which otherwise would not be.

3.1 Participants Criteria

Our study focuses on individuals who have experienced personal financial fraud as well as financial identity theft. We chose the criteria as experiencing fraud in the last one to five years, so we could obtain information while the memory associated with the incident is still fresh. To account for the interpretation limitations of the researchers and the transaction processes of the regions, we limited the participation to individuals who are fluent in English, based in the United States, and who are above the age of 18.

3.2 Screening Survey and Recruitment

We plan for purposive sampling to recruit participants. We conducted a preliminary survey on Prolific to screen the participants and we will to contact screened participants to seek interest in participating in an interview elucidating their experience. There is no other constraint other than the one listed in the Participant Criteria subsection, and we encouraged diverse participants across ethnicities, age, gender, education etc. The participants who state their interest and availability to the follow-up study were scheduled for the interviews in a slot of their choosing through Calendly. A compensation of 0.85*wasgivenforthescreeningsurveyand*15 was given to the interview participants.

3.3 Interview procedure

The interview is divided into 3 sections – participant's background and financial practices, how did the participant detect the fraud and what was the their experience with fraud.

Of the team of five researchers, three were involved in the script development and two who were not part of script development would test these questions and script on each other as part of the pilot study, and improve with feedback.

Participants were informed of the intent of the study, data collected, and their right to terminate the study at any point, and we sought their consent prior to the interview. The interview will last around 60 mins, with an interviewer and a scribe. Interview audio recordings and transcripts were made that enabled us to analyze the responses.

3.4 Demographics

In the screening survey of this survey with 75 participants 18 years or older, 69 consented to the study, of which 36 stated they have experienced financial fraud. Out of these 36 participants, 16 were interested in the follow-up interview, 15 of whom were actually available for the interviews.

Given our study criteria, we had to filter 6 individuals since their experience of fraud was beyond 5 years to date. Thus we landed on the 9 shortlisted participants. Of these 9 participants, 2 identified as male and 7 identified as female. The age group of participants are spread as follows - 1 participant was 21-29 years old, 4 are 30-39 years old, 2 are 40-49 years old, 1 is 50-59 years old and 1 is 60 years or older.

3.5 Data protection and processing

Our team plans to review the auto-generated transcription and correct inconsistencies in comparison with the audio of interview recordings. This transcript will also filter sensitive information and anonymize the content prior to the next phases of coding and analysis. The data collected will be stored on Google drive whose access is restricted to the members of the team. Should any participant not consent for the study or drop out prior to the conclusion of the interview, we will destroy the data associated with them and not consider it in the study.

4 Data Analysis Plan

4.1 Quantitative Analysis

Using R studio as our main coding platform for data analysis, we plan to calculate frequencies and percentages for multiple categories in the code-book across all sets of questions. Doing this will help in providing an overview of the participants' financial behavior, habits, experiences of financial fraud, steps taken to resolve it, the outcome of their efforts, and their recommendations for changing the reporting or resolution process, as well as spot trends among them.

Furthermore, cross tabulations will also be created via the coding platform to explore relationships between different categorical variables across the interview questions. This technique will not only assist us in conducting statistical tests, but will also provide a clear overview of frequencies and percentages of observations that fall into various categories defined by the variables.

Lastly, statistical tests, such as Chi-square tests of independence, will be conducted to test the significance of the relationship between categorical variables across all sets of questions. For example, we can test if there is a significant association between the satisfaction with the resolution process and whether the fraud was resolved or not. Non-parametric tests such as Mann-Whitney U or Kruskal-Wallis tests could also be used when assumptions of parametric tests are not met, such as normal distributions and equal variances. These can provide more accurate results in situations where the sample size is small, and the outliers may have a greater impact on the results of the analysis, which could be the case with our results.

4.2 Qualitative Analysis

Since the nature of our data is mainly qualitative, thematic analysis will also be used to analyze the coded open-ended responses in the code-book across all sets of questions. The responses will be read multiple times to identify themes and patterns in participants' financial behavior, experiences of financial fraud, steps taken to resolve it, the outcome of their efforts, and their recommendations for changing the reporting or resolution process.

The identified themes will then be categorized and coded, and for reliability and consistency purposes, this will be done and checked between multiple people in our team. Then, we can calculate the frequency of occurrence of each theme and code in the data set across all sets of questions for analysis purposes.

5 Lessons Learned

Our pilot studies helped us refine distinctions between what is and is not considered financial fraud for the purposes of our research. While defining our research questions and developing the survey, we came up with a team definition of personal financial fraud and financial identity theft. We include these definitions in the our initial surveys. However, during the pilot studies we discovered that, though our definitions needed to be shortened and include examples, they were useful in creating common terms among our team and participants. For those who were not inline with our definition, they fell into three categories: corporate or market fraud, contract disputes, and labor scams. They described financial fraud in terms of wage theft, contract disputes, commodities fraud, securities fraud, money laundering. a contract dispute. Though these are all varieties of scams, they are outside the scope of our study as it focuses more on individual fraud, not market fraud and situations where the victim does not lose any money they already owned.

From our preliminary work, we learned to improve our questions in terms of clarity, but also to make them applicable to a broader audience. For example, *"How much money was taken"* changed to *"How much money did the attacker take or attempt to take?"*. This way, instead of just victims, we capture a wider picture that includes people who don't consider themselves as victims. Similarly, since interviews and surveys were short, we learned to remove extraneous questions and only keep those that directly addressed the research questions. For this topic of study, the more insightful and revealing responses come from free-form text responses which take longer to answer. Due to the time limitations, we could not add as many of these as we would have preferred and instead opted for additional multiple-choice questions to attempt to capture these details in faster ways. At the same time, for the open-response questions that we did include, we received less content than desired, which confirmed our need to do interviews rather than rely on surveys. In our research pre-screening survey, we removed all free-form questions in favor of questions that let us choose more diverse fraud experiences and ask more detailed questions regarding discovery and resolution during the survey.

In terms of information gained, our pilot surveys confirmed some of what we learned through our literature review – financial fraud happens even if unreported, self-discovery is frequently how a person finds they have been a victim, and generally, respondents want more proactive notifications and actions from financial institutions.

6 Limitations

Early in our team discussions, we speculated we could experience difficulties in finding participants for several reasons, including the fact that talking about personal financial fraud can be difficult and not something a person wants relive. However, throughout our pilot studies we found a continuous stream of participants who had experienced fraud and were willing to participate. Most notably, through our pilot survey where nearly all of our 20 participants experienced some type of financial fraud. However, when we ran our screening survey, about 50% of participants said they have not experienced fraud. Of those who did, about 20% said they would be willing to talk about their experience in an interview. This left us with a bare minimum of potential interview participants once filtered by our criteria.

Another challenge that reduced our team's flexibility is that IRB policy does not allow our teammate located on CMU-Qatar to be included as a participant on our study. We either had to remove him and change his role, or significantly delay our IRB approval. We lost flexibility in terms of availability for interviews. To compensate, we reduced the number of interviews we will conduct and assigned him to other tasks.

7 Group Work

Now that we have published our screening survey and determined who to send interview requests to, we are in the process of scheduling these. We have broken into teams of two, one interviewer and one scribe. Each team will conduct 5 interviews and post-interview analysis, then share it with the rest of the team for validation according to our data analysis plan. Once we are done coding, we will conduct statistical analysis.

For our paper, we plan to divide the remaining work (Abstract and Intro expansion, Data Analysis Results, Discussion, Future Work) into sections, distribute among the team, and have one person working as an editor. Our final presentation will be based on this work and reviewed as a team. Individual contributions will correspond to the section on which they worked.

8 Appendix

8.1 Screening Survey

Below is the screening survey used to seek participants who align with the criteria set for our study

1. Are you 18 years or older?

   (a) Yes, I am at least 18 years old

   (b) No, I am under 18 years old

1. Do you consent to participate in this study?

   (a) Yes, I consent to participating. Begin the study

   (b) No, I do not consent. I do not want to participate in this study

1. What is your Prolific ID? Please note that this response should auto-fill with the correct ID

Start of Block: Financial Fraud and Identity Theft

1. Have you experienced financial fraud or financial identity theft?

   (a) Yes, identity theft

   (b) Yes, financial fraud

   (c) Yes, I have experienced both of these

   (d) No, I have never experienced either of these

1. If you answered that you have experienced both financial fraud and financial identity theft, please answer for the more recent of the two.

1. When did you last experience financial fraud or financial identity theft?

   (a) Less than a month ago

   (b) 1 - 12 months ago

   (c) 1 - 5 years ago

   (d) Beyond 5 years

1. On which Financial Service or Financial Service Platform did you experience the fraud? (Select all that apply)

   (a) Credit Card / Debit Card (e.g. fraudulent charges)

   (b) Online Payment Services (e.g. Zelle, Venmo, Paypal)

   (c) Banking Services (Checking, Savings, loans, etc)

   (d) Marketplace Platforms (e.g. eBay, Facebook Marketplace, etc)

   (e) Application for financial service (e.g. Loan, credit card, account application)

   (f) Other

1. How did you discover the fraud? (Please check all that apply)

   (a) Notification from financial service provider

   (b) Notification from credit reporting service

   (c) Self-discovery - noticed suspicious financial activity on account(s)

   (d) Self-discovery - received suspicious account login notice

   (e) Other (please specify)

1. Did the financial fraud or financial identity theft result in a financial loss?

   (a) Yes

   (b) No

1. Did you report the fraud or seek a resolution? For example, resolution can be reimbursement, restoring credit, actions to reestablish your identity, or similar.

(a) I did not report it

(b) I did not report it but took actions to seek resolution

(c) I reported it, but took no other action to seek resolution

(d) I reported it and took other actions to seek resolution

1. Which category below includes your age?

   (a) 18 - 20

   (b) 21 - 29

   (c) 30 - 39

   (d) 40 - 49

   (e) 50 - 59

   (f) 60 or older

1. Which most closely describes your identity?

   (a) Female

   (b) Male

   (c) Non-Binary

   (d) Prefer not to disclose

   (e) Prefer to self-describe / not listed

   (f) Other

1. Are you willing to participate in an online interview to talk about your financial fraud or financial identity theft experience? * Interview will be over Zoom. Cameras will not be on, microphones and audio capability are required. The interview will be recorded to aid follow-on research.

   (a) Yes

   (b) No

1. If you answered yes to the previous question, will you be available during April 01 - 15, 2023 to participate in the online interview? Additional compensation of 15.00*willbepaidforcompletedinterviews*.

   2. Yes

   3. No

1. Thank you for taking part in this study! Please click the button below to be redirected back to Prolific and register your submission.

8.2 Interview Script

Below is the interview script used to conduct follow-on interviews

Introduction

Hello, Good Morning, I'm (interviewer's name, and qualifications/credentials), and this is (Scribe's qualifications/credentials). Thank you for sharing your time for a research study on financial fraud. We understand this is a sensitive topic for you to discuss with us and we are grateful to you for sharing your experience with us. I will be conducting the interview and (Scribe) will be taking the notes while we discuss. The purpose of our interview is to understand your personal experience with financial fraud. This interview will be included in our investigation into the discovery and notification methods for financial fraud and the financial and non-financial impact of those who experience this. This interview will be broken down into three parts:

- Your background and financial activities online and offline
- Your discovery of personal financial fraud
- Your experience with resolving personal financial fraud

Consent Reconfirmation

Before I proceed further, I would like to see if you have any questions about the consent form you submitted (Pause for questions).

Are you in a quiet place where you will not be disturbed for the duration of this interview?

I would like to remind you that your participation in this interview is voluntary, you can decline to participate or withdraw your consent at any time with no consequences. You are not required to share any personally identifiable information or sensitive information. This discussion will be kept private and confidential;however the data of the discussion will be used in an attempt to better understand and improve the financial fraud experience. To aid our analysis, we will be recording this interview. Your camera does not need to be on. The recording will not be shared. So please freely share your candid input based on your personal experience. At any point in time, if you feel the need to stop the recording or discontinue the interview, please let us know.

Interview Runbook

Here are some definitions for terms in we will use during the interview

Financial Service: Financial service encompasses the services to the individuals including but not limited to:

- Account management (account opening/closing, account preferences)
- Fund transfers (personal accounts or to other individuals)
- Credit services

- Online purchases

Financial Service Platform: Financial Service Platform refers to the methods of delivering the financial service. The financial service could be provided through person-to-person transactions, Brick & mortar offices, website based services like Paypal or applications like Venmo.

Part - 1: Background and financial practices
I would like to get started with a few questions related to your background and financial practices.

1. Where do you primarily perform financial transactions?
   (a) How much of these transactions are in-person?
   (b) How much of these transactions are online?
2. How often do you review your financial accounts (this can include statements, checking your balance etc)?
3. Which, if any, financial services or financial service platforms have you used?
4. Clarification prompt: please list the financial services or financial service platforms you use?)
5. How do you typically perform these transactions or access the financial service and its platforms (e.g. desktop computer, mobile app, ATM)?
6. When did you first start using these platforms?
7. Have you ever shared your financial account information with anyone else (e.g. family member, friend, financial advisor)?
   (a) If yes, what led you to share the account information?
8. Do you use any particular features for your online financial transactions (e.g. two-factor authentication, password manager)?

Part - 2: Detected the fraud Thank you for your answers to these questions. Before I move on to the next section,do you have any questions for me? If not, I will now move to the second part. In this part of our interview, I will ask you some questions regarding your exposure with the platform where you had this fraud experience.
(Pause for response)

1. When and where did you most recently experience financial fraud?
   (a) (if applicable) How much money was taken?
   (b) (if applicable) How many accounts were opened?
2. How did you learn that you have been defrauded?
3. Did you detect it yourself or was there someone or something alerted you
4. Can you elaborate more how you detected it yourself (or how someone or something alerted you)?

Part - 3: Experience of the fraud Thank you for your answers to these questions. This can be a very difficult topic to discuss. Please let me know if you have any question or opinion regarding the interview until now. If not, we are now going to the third and last part of the interview.
(Pause for response)

1. What steps did you undertake to resolve this incident?
2. Did you report the fraud to the financial service provider or law enforcement? If so, what was their response?
   (a) What was the outcome of your efforts in resolving this?
3. Did the financial service provider offer any assistance or compensation for the fraud?
4. Do you feel that the financial service provider handled the situation appropriately and effectively?
5. If you could make a recommendation to change the reporting or the resolution process, what would it be?
6. Do you think experience influenced the way you operate your finances? *Probing questions if the participant is not talkative:*
   (a) If yes, how?
7. Did the experience changed your level of trust in financial service providers or online transactions?
8. Did the experience changed your security behavior?
   (a) If yes, how?
9. Have you taken any measures to prevent future fraud on the platform (such as changing passwords, enabling additional security features, etc.)?
10. What impact did this experience have on your and your immediate family's life?
11. Were there any effects on your physical health or mental health as a result of this experience?
12. Did you and your family face any significant life changes?
    (a) unemployment due to this experience?
    (b) delayed retirement due to this experience?

13. Can you elaborate on the effects on you from facing the threat of (foreclosure/ loss of your house/ loss of retirement funds)?

14. Are you still experiencing these impacts?

    // Question 15 will be repeated if participant reported multiple impact

15. On a scale of 1-10, 1 being the least, and 10 being the most, how much did this experience impact your life in [insert the impact mentioned in the prior question]?

16. Have you shared your experience with others to raise awareness or prevent similar incidents from happening to them?

    (a) In what forms have you shared your experience?

    (b) Can you tell me more about why you chose not to share / not-share this experience?

Thank you very much for your time and cooperation to this research study, we really appreciate your support. As a token of our gratitude, you will be compensated through prolific. Please let me know if you received it.

References

[1] Keith B. Anderson. Mass-market consumer fraud in the united states: A 2017 update. Technical report, The Bureau Of Economics Federal Trade Commission, 2019.

[2] Kimberly Blanton. The rise of financial fraud: Scams never change but disguises do. Technical report, Center for Retirement Research, 2012.

[3] Roderic Broadhurst, Katie Skinner, Nick Sifniotis, Bryan Matamoros-Macias, and Yuguang Ipsen. Phishing and cybercrime risks in a university student community. *SSRN Electronic Journal*, 11 2018.

[4] Mark Button, Carol McNaughton Nicholls, Jane Kerr, and Rachael Owen. Online frauds: Learning from victims why they fall for these scams. *Australian amp; New Zealand Journal of Criminology*, 47(3):391–408, 2014.

[5] Jipeng Cui, Chungang Yan, and Cheng Wang. A credible individual behavior profiling method for online payment fraud detection. In *2021 4th International Conference on Data Storage and Data Engineering*, DSDE '21, page 22–30, New York, NY, USA, 2021. Association for Computing Machinery.

[6] Marguerite DeLiema, David Burnes, and Lynn Langton. The Financial and Psychological Impact of Identity Theft Among Older Adults. *Innovation in Aging*, 5(4), 10 2021. igab043.

[7] Jurjen Jansen and Rutger Leukfeldt. How people help fraudsters steal their money: an analysis of 600 online banking fraud cases. In *2015 Workshop on Socio-Technical Aspects in Security and Trust*, pages 24–31, 2015.

[8] Yuan Li, Adel Yazdanmehr, Jingguo Wang, and H. Raghav Rao. Responding to identity theft: A victimization perspective. *Decision Support Systems*, 121:13–24, 2019.

[9] Mark Lokanan and Susan Liu. Predicting fraud victimization using classical machine learning. *Entropy*, 23(3):300, 2021.

[10] Fang Lv, Wei Wang, Yuliang Wei, Yunxiao Sun, Junheng Huang, and Bailing Wang. Detecting fraudulent bank account based on convolutional neural network with heterogeneous data. *Mathematical Problems in Engineering*, 2019:1–11, 2019.

[11] Rachel E. Morgan. Financial fraud in the united states. Technical report, US Department of Justice, Office of Justice Programs, 2017.

[12] Gareth Norris, Alexandra Brookes, and David Dowell. The psychology of internet fraud victimisation: A systematic review. *Journal of Police and Criminal Psychology*, 34(3):231–245, 2019.

[13] Lubna Razaq, Tallal Ahmad, Samia Ibtasam, Umer Ramzan, and Shrirang Mare. "we even borrowed money from our neighbor": Understanding mobile-based frauds through victims' experiences. *Proc. ACM Hum.-Comput. Interact.*, 5(CSCW1), apr 2021.

[14] Heather Rosoff, Jinshu Cui, and Richard John. Behavioral experiments exploring Victims' response to cyber-based financial fraud and identity theft scenario simulations. In *10th Symposium On Usable Privacy and Security (SOUPS 2014)*, pages 175–186, Menlo Park, CA, July 2014. USENIX Association.

[15] Nick F. Ryman-Tubb, Paul Krause, and Wolfgang Garn. How artificial intelligence and machine learning research impacts payment card fraud detection: A survey and industry benchmark. *Engineering Applications of Artificial Intelligence*, 76:130–157, 2018.

[16] Chunxia Zhang, Lin Liu, Suhong Zhou, Jiaxin Feng, Jianguo Chen, and Luzi Xiao. Contact-fraud victimization among urban seniors: An analysis of multilevel influencing factors. *ISPRS International Journal of Geo-Information*, 11(3), 2022.