MICHIGAN RETIREMENT AND
DISABILITY RESEARCH CENTER
UNIVERSITY OF MICHIGAN

Promoting research on retirement, disability, and Social Security policy

Mixed Methods Analysis of Consumer Fraud Reports of the Social Security Administration Impostor Scam

Marguerite DeLiema and Paul Witt

MRDRC WP 2021-434

UM21-Q1

Mixed Methods Analysis of Consumer Fraud Reports of the Social Security Administration Impostor Scam

Marguerite DeLiema
University of Minnesota
School of Social Work

Paul Witt
Federal Trade Commission, Division of
Consumer Response and Operations

October 2021

Michigan Retirement and Disability Research Center, University of Michigan, P.O. Box 1248. Ann Arbor, MI 48104, mrdrc.isr.umich.edu, (734) 615-0422

Acknowledgements

The research reported herein was performed pursuant to a grant from the U.S. Social Security Administration (SSA) funded as part of the Retirement and Disability Research Consortium through the University of Michigan Retirement and Disability Research Center Award RDR18000002-03. The opinions and conclusions expressed are solely those of the author(s) and do not represent the opinions or policy of SSA or any agency of the federal government. Neither the United States government nor any agency thereof, nor any of their employees, makes any warranty, express or implied, or assumes any legal liability or responsibility for the accuracy, completeness, or usefulness of the contents of this report. Reference herein to any specific commercial product, process or service by trade name, trademark, manufacturer, or otherwise does not necessarily constitute or imply endorsement, recommendation or favoring by the United States government or any agency thereof.

Regents of the University of Michigan

Mixed Methods Analysis of Consumer Fraud Reports of the Social Security Administration Impostor Scam

Abstract

Most Americans have received fraudulent calls from impostors claiming to be officials from the Social Security Administration (SSA). Callers threaten those who respond with arrest and suspension of their bank accounts and Social Security numbers, but charges can be removed if the target agrees to buy retail gift cards, wire money, or deposit cash in cryptocurrency ATMs. This paper uses mixed methods to analyze SSA imposter scam consumer reports from victims and attempted victims filed in the Consumer Sentinel. Qualitative analysis of 600 case narratives reveals that SSA impostors use the persuasion principals of authority, reciprocity, liking, and scarcity to put pressure on consumers to comply with their requests. Expressions of fear, anger, anticipation, and trust in the imposter were present in the victim case narratives. Qualitative findings were supported using a quantitative sentiment analysis of more than 200,000 consumer reports to count the frequency of emotion words in case narratives. Emotional expressions were significantly associated with reported victimization versus attempted victimization. Quantitative models show that older adult consumers are significantly less likely to report victimization relative to those 30 and younger, but older victims lose significantly more money per incident on average. Results also indicate that consumers from majority Black, Asian, and Hispanic communities are more likely report victimization, although victims from non-Hispanic White communities report higher average loses. Consumer education on government imposter scams, specifically targeting young people and minorities, as well as greater controls on retail gift card sales, might help limit consumer losses.

Citation

DeLiema, Marguerite, and Paul Witt. 2021. “Mixed Methods Analysis of Consumer Fraud Reports of the Social Security Administration Impostor Scam.” Ann Arbor, MI. University of Michigan Retirement and Disability Research Center (MRDRC) Working Paper; MRDRC WP 2021-434. https://mrdrc.isr.umich.edu/publications/papers/pdf/wp434.pdf

Introduction

The Social Security Administration (SSA) impostor scam typically begins with an automated phone call. The targeted consumer is informed that his Social Security number will be suspended due to criminal activity and he is urged to press “1” to speak to an SSA official immediately. If the target presses “1,” the call is transferred to a live person who accuses him of drug trafficking and money laundering and tells him that the federal government will freeze his financial accounts. The purported SSA official says that in order to avoid arrest and to secure his funds, he must quickly withdraw money and use it to purchase retail gift cards, or in some cases, deposit cash directly into a cryptocurrency ATM or wire it to the officials who are helping with the case. The target is led to believe that a government official will arrive the following morning to return the “secured” funds. By the time the target realizes the whole story was a ruse, the gift cards are redeemed and any cash he deposited into a cryptocurrency ATM was withdrawn.

In the spring of 2019, government impostor scams topped the list as the most common category of fraud reported to the Federal Trade Commission (FTC) (Fletcher 2019a). This rise in government impostor scams was driven largely by an increasing number of reports of the Social Security Administration (SSA) impostor scam, which peaked in March 2019 (Fletcher 2019b). Between January 2018 and August 2021, more than 303,000 SSA impostor scam reports have been filed in the FTC’s Consumer Sentinel database (author’s calculations), with hundreds of thousands more reports received directly by the SSA or submitted as Do-Not-Call Registry violations to FTC. Four percent of consumers who reported the scam and are captured in the Consumer

Sentinel Network database are victims, losing a reported total of almost $90 million, although these figures significantly underestimate the true number of victims and extent of losses due to underreporting. Recent research suggests that only 4.8% of fraud victims report to the FTC or Better Business Bureaus (Anderson 2021).

The SSA impostor scam uses mass marketing tactics such as robodialing to solicit thousands of potential victims at a time. Nearly half of United States adults were targeted by the scam in a three-month period between October and December 2020, and 69% of Social Security beneficiaries reported that they were targeted by the scam in that three-month period. The majority were targeted more than once (SimplyWise 2021).

There is virtually no academic research on government impostor scams, including the SSA impostor scam. Given the pervasiveness of this problem, research is needed to uncover how impostors convince fraud targets to comply with their demands, the characteristics of consumers who report victimization, and what potential interventions might effectively prevent victimization. In light of these research gaps, the current study has three exploratory aims. The first is to qualitatively analyze the incident narratives in a consumer report database to determine what persuasion techniques SSA impostors use to convince consumers to pay money, what emotions consumers convey about their experience, and what interventions stop them from participating in scams. The second aim is to quantitatively investigate the correlates of reporting a loss (i.e., victimization) from the SSA impostor scam, including individual and neighborhood characteristics and incident-specific factors. The final aim is to analyze what demographic and contextual factors are associated with the magnitude of financial loss among those who lose money. Although this study is only representative of consumers who reported the scam, study findings can inform what steps the SSA, other federal agencies, and private sector industries may take to reduce the risks and consequences of government impostor scams.

Literature review

Persuasion

Unlike other financial crimes where a person's money or property is taken without their consent, the hallmark of fraud and scams is that perpetrators use deception to convince their targets to comply with their demands for payment. Scammers elicit compliance using sophisticated storytelling that involves false promises of rewards or fabricated threats of adverse and harmful consequences. They employ a range of persuasion tactics to make these stories, and themselves, appear credible. Cialdini (2007) describes six umbrella principles that underlie common persuasion tactics that are based on psychological phenomena. Although these tactics are used by scammers to manipulate their targets, they are also common in legitimate marketing and sales practices. The six principals include:

1. reciprocity — desire to return a favor or a gift (motivated by the discomfort of feeling indebted to another person);
2. social proof — desire to follow the lead of people one is similar to by emulating their behaviors;
3. commitment and consistency — desire to appear consistent in one's stated beliefs, attitudes, values and behaviors;

4. liking — tendency to comply with people one is similar to or whom one likes;
5. authority — tendency to comply with individuals and entities perceived as having influence, credibility, and power;
6. scarcity — desire for something that is limited in supply or to complete an action that is time sensitive.

Scammers may use any combination of these principles and various derivations to convince their targets to pay money. In an analysis of a fraudulent annuity company's sales training program, DeLiema et al. (2014) found that deceptive salespersons were trained to do small favors for potential clients, such as offering discounts on the price (reciprocity). They were also trained to say that the clients' neighbors bought the company's products (social proof) and to be excessively friendly (liking). Salespeople convinced clients to agree to small favors, such as inviting them into their homes just to "learn about the new opportunity" before gradually increasing the magnitude of the request and asking them to purchase the product (commitment and consistency).

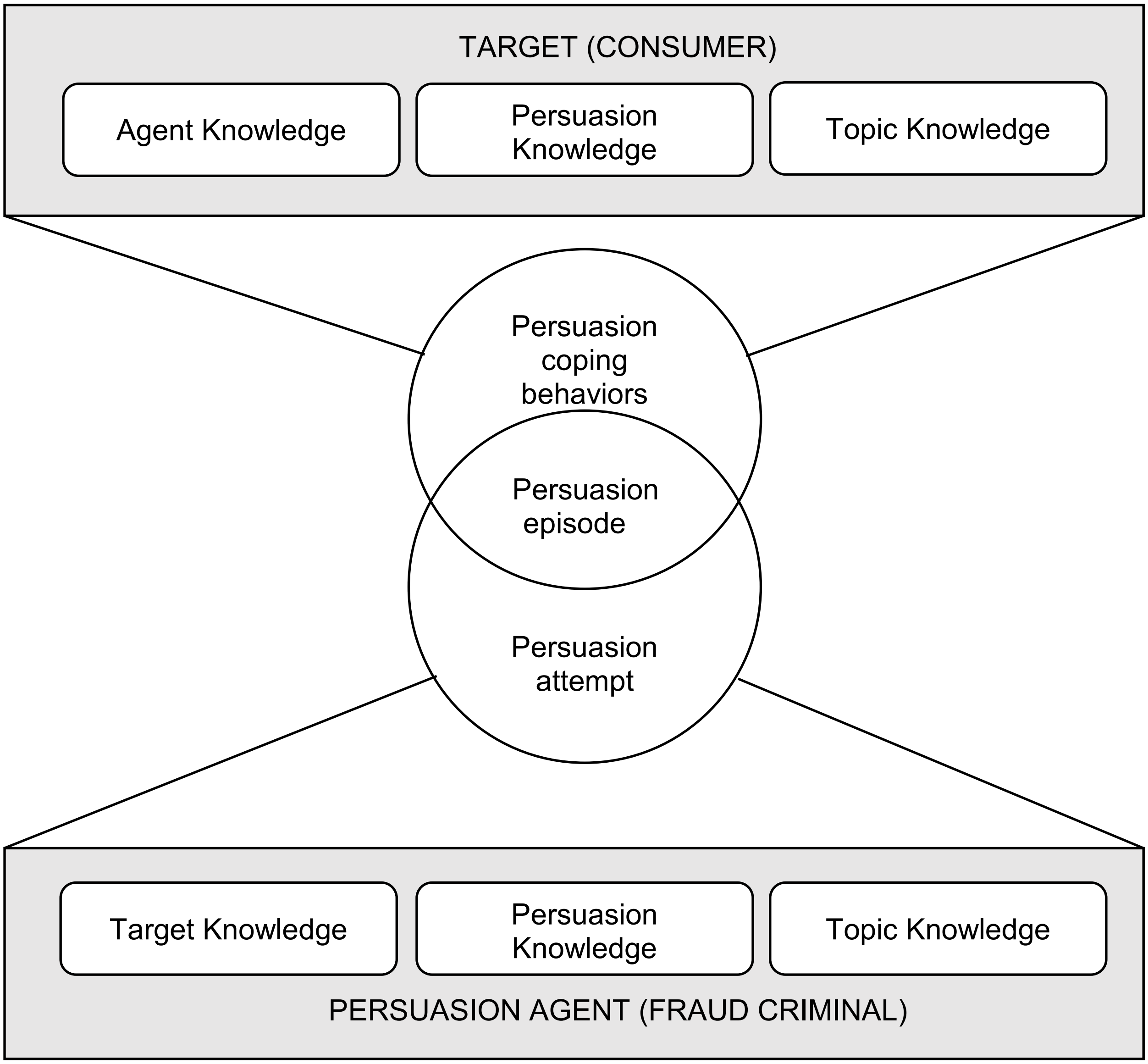
In the "419" scam, letters and emails from Nigerian criminals request the target's help moving money out of the country. The impostors use the authority principle by stating they are affiliated with plausible and legitimate-sounding companies (e.g., Nigerian National Petroleum Corporation) and by using esteemed titles (e.g., bank president) (Dyrud 2005). Romance scammers will use the liking principle by claiming that they come from the same region as the target but moved away for work or for military service (Whitty 2015). Each of these tactics helps instill trust in the scammer. Government impostor scams also incorporate these persuasion principles, but no research has investigated which are predominantly used and what effect they have on consumers.

Coping with persuasion

Prior research suggests that having knowledge about persuasion is important in coping with a persuasion attempt. According to the Persuasion Knowledge Model presented in Figure 1 (Friestad and Wright 1994), targets of persuasion draw on three types of prior knowledge when presented with a persuasion attempt — topic knowledge (what they know about the product/offer/threat), persuasion knowledge (ability to recognize persuasion attempts), and agent knowledge (information about the person or entity attempting to persuade). In the SSA impostor scam, targets might draw upon their knowledge of the roles and functions of the SSA (agent knowledge), how the U.S. government typically investigates crimes and interacts with citizens (agent knowledge and topic knowledge), and what they know about gift cards or cryptocurrency as methods of payment (topic knowledge).

Targets might be less susceptible to persuasion attempts if they know that SSA officials would never call to accuse people of committing crimes and would never demand that they purchase retail gift cards to keep their personal funds secure.

Figure 1: Adapted Persuasion Knowledge Model (Friestad and Wright 1994)



Emotion and scam susceptibility

Susceptibility to persuasion is greater when targets are in a state of high emotional arousal. According to the Elaboration Likelihood Model (ELM) of persuasion (Petty and Cacioppo 1986), individuals process persuasive information through either a “central route” that involves dedicating attentional resources to carefully scrutinize and cross-reference the message with prior knowledge, or a “peripheral route” which involves using heuristic shortcuts and reliance on basic cues to judge the legitimacy of the message. Incidental affect — sadness, excitement, etc. — can influence whether a persuasion message is processed through the central or peripheral route (Petty and Briñol 2015). In decision-making tasks in the laboratory, for example, incidental emotions have been shown to produce peripheral thinking and poor decision outcomes. For example, Duclos et al. (2013) found that subjects who felt isolated or ostracized were more likely to pursue risky decisions that had a higher potential payout, and Baumeister and colleagues (2002) showed that social exclusion produces a decline in cognitive performance. In another study, subjects who were manipulated to feel sad were more impatient and chose to accept an immediate payout of less money instead of waiting to receive more money after a delay (Lerner et al. 2013). Kircanski et al. (2018) found that older adults in positive and negative arousal states (excited and frustrated, respectively) were more likely to want to purchase a product featured in a misleading advertisement than older adults in a neutral emotional state.

The SSA impostor scam is one of many fraud types that incorporates powerful visceral appeals to put the target in a state of high emotional arousal. Impostors use threats of arrest and surveillance to intimidate the target. These tactics may evoke fear, dread, anxiety, and worry — emotional states that can overwhelm a target’s ability to make sound decisions, especially when paired with the need to act quickly and when used in combination with other influence tactics. More research is needed to identify how experiencing high-arousal, negative emotions influence decision making in an applied high-risk context, and how consumers reflect on their emotional states following the SSA impostor scam.

Demographic correlates of fraud victimization

In addition to the influence of contextual factors, such as emotional arousal, prior research has assessed the demographic correlates of scam victimization. Findings typically vary based on the sample and the method of data collection. Random sample surveys that ask whether the respondent lost money in a scam typically find that young and middle-aged adults are more likely than older adults to report victimization (Anderson 2019), however studies that assess behaviors associated with scam susceptibility find that vulnerability is associated with age-related declines in cognitive functioning and financial decision-making abilities (Han et al. 2016a, 2016b). Using consumer data from nine consumer protection cases related to healthcare, payday loan, student debt relief, and business opportunity frauds, Raval (2020) found that the victimization rate was 43% higher in zip codes with a median age of 55 compared to communities with a median age of 25.

Other research using FTC's consumer report data indicates that older adults are the least likely of any age group to report losing money to scams although there is some variation by scam type (FTC 2020). However, this same data show that adults 65 and older file no-loss fraud reports at higher rates than adults ages 20 to 59 relative to their share of the population. Although older consumers are less likely to report scams in which they lost money, when victimization is reported, median losses are between 1.5 to three times higher than median losses reported by adults younger than 60 (FTC 2020). This has been shown to be the case for government impostor scams in general (Fletcher 2019a), but no research has specifically investigated the relationship between age and reported victimization by the SSA impostor scam.

In addition to age, rates of victimization differ by the consumer’s socioeconomic status and gender, which is influenced by the type of fraud. Pak and Shadel (2011) found that compared to the general U.S. population 50 and older, a higher proportion of independently-identified (not self-report) investment scam victims were men and had higher average income and educational attainment. In contrast, sweepstakes and lottery fraud victims were disproportionately women with low income and education. Other research has found that victim report demographics differ by the nature of the reported fraud and the agency to which the consumer reported (Raval, 2020). This indicates that victim profiles may be unique to the type of fraud. No prior research has assessed the sociodemographic profile of victims of government impostor scams.

Rates of reporting fraud experiences also differ by race and education. Examining consumer report data, Raval (2020) found that majority Black communities reported at higher rates compared to communities with few Black residents, and that majority Hispanic communities reported 22% less than areas with a low proportion of Hispanic residents. There were relatively small differences in reporting rates between zip codes with different median household incomes and median ages, but more educated communities were more likely to complain. These findings, however, are influenced by which agencies contribute their consumer fraud report data to the sample.

In another study comparing law enforcement case data on known victims to consumer complaint data, Raval (2021) found that actual victimization for most fraud cases was substantially higher in majority Black communities, with the largest effects for payday loan and student debt relief frauds. For Hispanics, victimization rates were slightly higher in moderately Hispanic communities compared to 0% Hispanic communities, and the victim rate was 14% lower in 100% Hispanic areas compared to 0% Hispanic areas. Victimization rates were lower in 100% Asian versus 0% Asian communities.

There were also socioeconomic patterns in victimization rates. Raval (2021) reported slightly higher rates of victimization in communities with a median household income of $130,000 compared to communities with a median income of $20,000. However, using different socioeconomic status indicators — credit scores and percent of the population with a college degree — Raval (2021) found that victimization rates were lower in areas with higher median credit scores and where the majority of the population was college educated. Victim characteristics may differ for the SSA impostor scam, which uses threat-based messaging, versus opportunity/financial reward messaging, and where robodialing is used to contact as many targets as possible. The SSA impostor scam relies more heavily on mass marketing solicitation methods than the fraud cases in the Raval (2021) sample. Broad solicitation tactics could have the effect of reducing the significance of demographic and socioeconomic characteristics on reported victimization by the SSA impostor scam.

Study purpose

This study uses mixed methods to assess victim characteristics and experiences with the SSA impostor scam. First, we qualitatively analyze 600 consumer reports of the scam to identify common persuasion tactics, emotional responses to the scam experience, and sources of intervention. Next, we quantitatively analyze more than 200,000 SSA impostor scam reports to determine what factors are associated with reporting victimization (versus reporting attempted fraud), and what factors are associated with the magnitude of loss among victims. Correlates include consumer characteristics such as sex and age, neighborhood race and educational characteristics based on the consumer's zip code, incident characteristics such as the year and season the scam occurred, and the number of emotional sentiments consumers express in the case narrative describing the incident.

Qualitative analysis of consumer report data

Qualitative methods

Sample

Data come from the Federal Trade Commission's Consumer Sentinel, a database of tens of millions of consumer reports on fraud, identity theft, and Do Not Call Registry violations. The Consumer Sentinel was designed as an investigative search tool for law enforcement agencies to identify consumers who have been affected by financial crimes. It also serves as a database for examining fraud trends. Qualitative analysis for this study was restricted to reports of the SSA impostor scam submitted through the FTC's online and mobile channels between January 2018 and December 2020.[1] SSA impostor scam reports filed as Do Not Call Registry violations were excluded, as were reports filed with other consumer protection agencies and organizations.

[1] The majority (~95%) of cases of the SSA impostor scam in the Consumer Sentinel were reported through FTC's online, mobile, and telephone reporting channels.

Case selection

To develop an initial coding scheme, 300 SSA impostor scam reports were randomly selected without replacement from the Sentinel database and exported into Excel. The sampling frame contained approximately 120,000 cases. Each row in Excel represented a deidentified consumer report labeled with a unique case reference number. Columns in the spreadsheet contained data from the report entry fields that collect information about the fraud incident, such as the year the report was filed, the method of contact by the scammer, and age range of consumer. For consumers who reported losing money in the scam (i.e., victims), additional data columns denoted the method of payment and the amount of payment in U.S. dollars.

When consumers file reports with FTC, they are prompted to provide their personal contact information first, followed by incident-related information such as the date they were targeted, the scammer's identity (i.e., company name), how they were contacted (phone, email, social media, etc.), how they paid (if there was a loss), and how much they paid. Consumers complete a free-response narrative field last to provide a first-hand account of what happened during the incident. "No-loss" fraud reports (fraud targeting attempts) typically contain shorter narratives (average word count = 61) relative to reports that involve a loss (average word count = 119).

Sampling was restricted to cases that included text data in the incident narrative field, and that also included entries on participant age range, method of contact by the scammer, transaction date (date of the incident), and whether the person was filing a report on behalf of another person who experienced the SSA impostor scam, such as an older parent or spouse.

To ensure equal representation of cases from the three years the SSA impostor scam was most prevalent, 100 consumer reports were randomly selected from 2018, 100 from 2019, and 100 from 2020. Because the focus of the qualitative analysis is on persuasion tactics, emotions, and interventions, more victims than attempted victims were selected into the sample. Selection procedures were programmed so that 60% of the cases randomly drawn from each year involved victimization, and 40% of the cases were attempted fraud (no victimization). Table 1 describes the number of victim and attempted fraud cases randomly selected by year.

Table 1: Number of cases randomly selected into the initial sample

	2018	2019	2020
Victims (reported a loss)	60	60	60
Attempted fraud (no losses reported)	40	40	40

Coding approach

Codes are defined as, "labels that assign meaning to the descriptive or inferential information compiled during a study" (Miles et al. 2013; pg. 71). The purpose of coding is to identify, retrieve, and consolidate relevant information in and across documents — in this case, fraud incident narratives. Coding helps categorize large amounts of text data by consolidating it into manageable pieces that can be reviewed and compared across cases (Saldaña 2021). An initial coding scheme was developed based on reading the first 100 of the 300 case narratives and identifying recurrent patterns in the text. These codes were labeled (1) agencies impersonated, (2) scammer's story details, (3) consumer emotions, (4) personal information provided to the scammer, (5) scammer characteristics, and (6) intervention and consumer education. New columns in the Excel spreadsheet were labeled with these code names.

Narratives were read sequentially beginning with the earliest case in the sample (first row in Excel spreadsheet). Case narrative information relevant to each of the predetermined codes was entered in the cell for the corresponding row/column in the spreadsheet. For example, if a consumer wrote that they told the scammer their Social Security number, “social security number” was typed into the column labeled, “Personal information provided to scammers,” in the row pertaining to that consumer’s case. If the consumer said they were overwhelmed and anxious during the encounter, “overwhelmed; anxious” was typed in the column labeled “consumer emotions.” If no information in the case narrative pertained to a specific code, the cell within that column/row was left blank. After all 300 cases were coded, filters were applied (e.g., hiding empty cells) to compare across cases and identify repeat patterns. This preliminary analysis informed which codes should be added for the next analysis and revealed limitations in the initial sampling parameters, such as including reports filed with the FTC Call Center and including too large a proportion of attempted fraud victims.

New case selection

After the first 300 cases were coded and themes identified, a new sample of cases was randomly drawn without replacement and a final coding scheme applied. Sampling parameters and sample sizes are presented in Table 2. Parameters were adjusted to draw 200 new cases from each year of the SSA impostor scam (600 total), this time with 75% of cases involving victimization ($n_{\text{victims}} = 450$), and 25% involving attempted fraud ($n_{\text{no loss}} = 150$).

In addition to the earlier sampling parameters, the new sampling frame was restricted to consumers who filed a report through FTC's mobile and online complaint assistant only. Phone call reports to the FTC's Call Center were excluded because the case narratives were written by call center staff rather than by consumers, and thus were not in the consumers' own words.

Table 2: Number of cases included in the final sample of 600 cases

	2018	2019	2020
Victims (reported a loss)	150	150	150
Attempted fraud (no loss reported)	50	50	50

Narrative analysis

Based on patterns uncovered from the first round of coding 300 cases, the code list was further refined and applied to the new sample of 600 cases. The newly selected case narratives were analyzed using a combination of hypothesis coding, emotion coding, and magnitude coding (Saldaña 2021). In hypothesis coding, a code list is developed based on questions the researcher sets out to examine, such as what specific persuasion tactics impostors use. In emotion coding, the researcher codes emotional sentiments in a text corpus to identify subjective or relational experiences. The final coding list included (1) consumer emotions, (2) characteristics/qualities attributed to the scammer, (3) persuasion tactics used, (4) other federal/state agencies mentioned by the scammer, (5) elements of doubt, (6) elements used to instill trust, (7) points of intervention, and (8) consumer education/awareness.

In magnitude coding, the researcher applies an alphanumeric value or symbol, such as 0, 1, 2, 3, to denote the presence, absence, or magnitude of information contained in a text corpus (Saldaña 2021). In the present analysis, new columns were added to the Excel spreadsheet to document whether the scammer (1) threatened the consumer with arrest, (2) alleged that the consumer was laundering money, (3) alleged that the consumer was drug trafficking, (4) threatened to suspend the consumer's bank accounts or other financial accounts, (5) had a non-American accent (as indicated by the consumer), (6) collected personal information from the consumer, and (7) already had personal information about the consumer in advance of the interaction. If these pieces of information were not mentioned by the consumer in the case narrative, the corresponding data field was left blank. If they were present, "1" was entered in the corresponding row/column.

After all cases were coded, the magnitude codes were tabulated to determine the number or percent of cases in which consumers mentioned specific features/elements, such as threats of arrest. For nonalphanumeric codes, filters were applied to compare and summarize information across cases. Using the constant comparison method (Glaser 1965), coded data on persuasion tactics, consumer emotions, scammer characteristics, elements of trust and doubt, and consumer education opportunities were compared across cases. Key patterns and themes are described in the results.

Qualitative results

Four main themes emerged from the qualitative analysis of case data: (1) persuasion tactics, (2) emotional response; (3) scammer characteristics; and (4) sources of intervention.

Persuasion

Of Cialdini's (2007) six elements of persuasion, four were prominent in the narratives: *authority*, *reciprocity*, *liking*, and *scarcity*. Scammers were consistent in the tactics they used to signal authority. Consumers reported that impostors spoofed the phone numbers and caller IDs of local and federal Social Security Administration offices as well as police departments. One initially skeptical consumer wrote, “I asked to provide proof they were calling from Social Security and they had me Google a number which led me to the ssa.gov website and me believing them.”

When consumers responded to the call by pressing “1,” impostors identified themselves as SSA investigators, attorneys, agents, or officials and assumed classic American names like “John” and “Wilson.” Most impostors gave consumers phony badge and case ID numbers, asking them to retrieve a pen and paper to write the numbers down. Some consumers stated that they were told that the call was being recorded on a private line. These seemingly arbitrary details and requests by impostors increase the illusion of legitimacy and make the call seem more official.

Similarly, consumers reported that impostors’ inventions of bogus procedures and policies increased the credibility of their requests. For example, consumers were told that they could chose an “ADR-Alternative Dispute Resolution” to resolve their case instead of going to court. Scammers cited fabricated case laws (“Privacy Act 986, Subsection C”) and referred to retail gift cards as “virtual wallets,” “federal lockers,” “safety vouchers,” “electronic federal bank accounts,” “Social Security Bond Vouchers,” and other spurious terms.

In addition to evoking the authority of the SSA, impostors named other federal agencies that were supposedly involved in investigating the allegations. For example, consumers in more than 50 out of 600 cases reported that the impostor told them that U.S. Marshals were involved; 30 cases mentioned the Drug Enforcement Administration

(DEA), and another 28 cases mentioned the Federal Bureau of Investigation (FBI). Other agencies mentioned were Homeland Security, Internal Revenue Service (IRS), Department of Justice (DOJ), Federal Trade Commission, U.S. Treasury, and Health and Human Services (HHS). These mentions were designed to make consumers feel as though the full weight of the federal government was involved and would bring about severe consequences should they not comply.

Many consumers described that when they started to doubt the scammer and push back on his or her requests, they received a new call or a three-way call from someone posing as a local police officer. Again, using the authority persuasion principle, the new caller (who consumers occasionally described as being the same impostor), would tell the consumer to follow the SSA official's orders or face immediate arrest.

In 44 cases, consumers reported that the impostors already had their personal information before the call began. For example, "The person knew my SSN and he knew my address and previous addresses where I have lived." Another consumer stated that the scammer had a relative's address, and another reported that the scammer knew about the cars they previously owned. Because consumers might presume that SSA officials have access to their personal information, impostors who had this information were perceived as more credible. They were also more likely to convince the target to pay.

Two other persuasion principals (Cialdini 2007) emerged in tandem in many of the victims' case narratives: *reciprocity* and *liking*. At the start of each call, impostors would threaten the consumer with arrest for serious criminal charges and say that the consumer’s bank accounts will be suspended. When consumers deny the accusations, the impostors switch their tune, saying that they believe them and want to help. They tell consumers that they will work with them to keep their funds secure and “clear their names.” Some consumers described that they were given a choice in how their case was handled: “He gave me two options, I could either hire a criminal lawyer and fight the case in the Texas courts, or I could complete an Alternate Dispute Resolution (ADR) remotely that would protect me and my financial assets. I agreed to take the second option.” Another consumer stated, “They assured me that they could help me if I cooperated with them and that they would notify the authorities that I was cooperating.”

By appearing to take the consumers’ side, impostors suddenly are perceived as reasonable, accommodating, and empathetic to the consumers’ needs and circumstances. Consumers may feel indebted to the impostors, which in turn increases their motivation to cooperate. This demonstrates the persuasion principle of *reciprocity.* According to one consumer, “Throughout the entire call, they assured me that they were here to help me, and that they knew I was wrongly taken advantage of. They also told me that someone out there is using my Social Security, which increased my fears. They generally made it seem like they were on my side.” Another said, “My mind was all over the place not thinking things clearly of exactly was going on as I was in a panic stage and complied to their process of ‘protecting me’ and ‘helping me’ make sure I would be okay.” One consumer described how the scammer made them feel empowered, “He said if I cooperated, I would be helping multiple agencies to potentially catch these people in the crimes and that I would be coached and helped in the process.” These comments reflect a persuasion tactic called “scapegoating,” in which another entity is blamed to create more common ground (a shared enemy) between the target and the persuasion agent.

An important feature of scams is to put pressure on the target to comply right away. Scammers understand that the more time that passes, the more likely the target will second guess the request or that a third party will intervene. This reflects the *scarcity* persuasion principle (Cialdini 2007). In the SSA impostor scam, criminals present time as a scarce resource. They tell consumers that if they do not act fast, they will be arrested, their Social Security numbers will be suspended, and they will be unable to access their bank accounts (often for a period of nine years). One consumer wrote, “He was very smooth and always in my ear. Everything was very urgent and had to be done immediately.”

Appeals to urgency begin at the very start of the scam in the recorded voicemail message. For example, “The issue at hand is extremely time sensitive.” By presenting the problem as urgent and giving the target endless instructions to “secure their funds,” impostors allow consumers little opportunity to consciously process the situation. A number of consumers indicated that when the scam ended, they felt like they were emerging from a hypnotic daze: “I finally came to my senses after the damage was done.”

Although not one of the Cialdini’s (2007) six elements of persuasion, appeals to *secrecy* were important features of the case narratives. To prevent third party intervention, impostors told consumers that it is imperative to not tell anyone about who they were speaking to and what they were doing. If they broke their silence, the “real” criminals might come after them or the government would freeze their assets and suspend their Social Security numbers: “He said I had to stay on the line for my safety and that I could not tell anyone or my family would be in danger.” Impostors enforced obedience by keeping consumers on the phone throughout the ordeal, telling them that it is against the law to hang up, mute the call, or place the call on speaker phone while they were speaking. They coached consumers in how to respond to questions from concerned tellers and retail store employees.

Emotional arousal

The powerful effects of emotional arousal on decision making was a persistent theme throughout the case narratives. Calls typically began with threats of arrest for fabricated crimes and threats that bank accounts would be frozen if the consumer did not comply. For example, “I was told that there was a warrant out for my arrest in Texas for drug trafficking and money laundering and that they needed to put a freeze on my checking account so that the Federal Trade Commission and Federal Marshal can investigate the matter.” Of the 600 cases in the sample, 312 included threats of arrest, 220 mentioned drug-related charges, and 165 mentioned money laundering charges. Other fear arousal tactics included telling the consumer that they were under surveillance and being trailed by federal agents, and that the true criminals who committed the crime will try to harm them. For example, one consumer was told, “The real criminals are dangerous and could hurt me and my family.”

Consumers who complied with the scam described how these threats instilled fear, anxiety, and panic. The most common emotion word in the narratives was “scared.” This word and its derivatives such as “afraid,” “worried,” “terrified,” “paralyzed,” “panicked,” “shaking,” “nervous,” “fearful,” and others, were mentioned in 63 cases. Of those cases, 94% involved victimization.

Some consumers reported that an overwhelming sense of dread prevented them from rationally processing impostors’ demands. For example, “‘Steve’ had me so scarred and tired that nothing made sense.” And, “I felt completely helpless and brainwashed.” Feelings of fear persisted for some consumers who reported that they were still distraught and were experiencing anxiety: “I am completely traumatized from this experience and cannot sleep.” Other consumers described the severe impact victimization has had on their lives. For example, “I am broke. I am a single mom with two kids and I am desperate to get my money back.”

Anger, annoyance, and frustration were other common emotions but were typically expressed as reflections on the incident after it was over, not in the moment of victimization. The most common post-scam reaction by victims, however, was shame. For example, “I was so stupid to fall for this and am devastated!” Some consumers blamed themselves, going so far as to say they deserved it: “I'm embarrassed and I probably deserved this for being so stupid,” and “I know I acted stupidly and am paying for my ignorance.” Nearly 40 cases included mentions of feeling of foolish and embarrassed.

Impostor characteristics

Consumers often described the impostors as sounding professional and official. A few participants described how the impostors helped them calm down when they were panicked and scared. One consumer reported that the impostor “kindly” allowed him/her to go home to feed their dog and stop for food between gift card purchases.

Many comments on impostors' demeanors described them as being very persuasive. For example, "He was so convincing that I felt like I was hypnotized." Out of 450 victims in the analysis sample, 78 reported that the scammer(s) spoke with an accent, such as "Middle Eastern" or "Indian." One consumer noted that it was strange that the local police officers had the same accents as the purported SSA official: "…it didn't occur to me as they all three sounded Middle Eastern, as I assumed they were who they said (officers of government agencies and local authorities)."

In other narratives the impostors were described as angry and abusive. One consumer wrote, "He responded with threats, and claimed he would harm my family and rape my wife for hours." In most cases, these verbal assaults were in response to the consumer telling the impostors that they were not going to follow their directions anymore and would hang up. It is unclear whether the impostors' verbal assaults were effective in convincing consumers to continue or whether it further revealed that they were indeed fraud criminals.

Sources of intervention

Many consumers described the people and entities that stopped them from complying with the impostors' demands. Some consumers realized it was a scam when impostors' requests became too implausible, too relentless, or when impostors became unprofessional and violated consumers' expectations for how SSA officials should behave. A third-party intervened in many other cases. Sources of third-party intervention primarily fall into five categories: (1) retail store employees, including cashiers, store managers, and bank tellers; (2) law enforcement officers; (3) friends and family members; (4) SSA employees; and (5) financial institutions.

Gift card purchases attempted with a credit card were often declined, protecting the consumer from loss. As a result, most impostors demanded that consumers first withdraw cash from their bank to pay for gift cards or to deposit into cryptocurrency ATMs. In other narratives, consumers said that concerned bank representatives discouraged them from wiring money, but in some of these cases the impostors simply told them to go buy gift cards instead, or the bank allowed the consumer to withdraw their funds even after raising concerns: “When I went to my bank, the teller knew something was wrong because I never withdrawal [sic] that amount of money. Nevertheless I withdrew $1,500 and put it in the Bitcoin account the man instructed me to do. I then got a call from my bank alerting me that it was a scam.”

Although consumers were instructed not to speak to anyone during the process, after so many hours of driving from store to store and being on the phone with impostors, many consumers reported that they broke down and told a family member or friend what was happening: “I called my sister who told me that it was a scam and that it had just been on the news and to call the police.” Consumers described how family members helped them look up information about the scam, call the gift card issuer or retail store, and file police reports.

A number of consumers stated that they turned to the police or drove to an SSA office when they began to suspect it was a scam: “I became suspicious and called the Phoenix police myself with my landline phone while I was on the phone with the scammer.” Other consumers drove to their local police stations and handed their phones to officers to speak with the impostors. One consumer went so far as to flag down a patrol car and ask the officer to speak with the impostor. When consumers did seek help from authorities, police officers and SSA employees unanimously informed the consumer that what was happening was a scam and to hang up the phone. Many consumers stated that they reported to the local police after the incident was over.

Most losses reported were the result of gift card purchases in retail stores. A small number of consumers described intervention by store employees. For example, “[They] then directed me to Safeway on Del Paso Blvd where I tried to get six more [cards] and the manager was called. She asked why I needed them. (Earlier on the phone the man told me that this may happen and to tell them it’s for your kids.) I told her just that and she looked at me and asked if I was told to say that. I then pointed at my phone and nodded yes. She informed me that this was a scam. I then hung up the phone. She said that this has been a recent issue and to contact the police and to contact Google [Play].” Another consumer wrote, “The Sam's Club staff got suspicious and then asked me if I wanted to talk to the local police, I finally agreed.” Another person stated, “The grocery store employee said what has happening was a ‘red flag’ and I needed to contact authorities immediately.” This individual did not end up losing any money.

Unfortunately, most case narratives did not describe any interventions by retail store employees, even when consumers visited six or more locations and spent $1,000 on gift cards each time. Among those who did mention retail intervention, the majority occurred after the consumer had already purchased cards from other stores. Moreover, when consumers called the gift card issuers to try to recover the funds, they were typically told that the money had been spent, even minutes after purchase: “The Target employee told me that I was likely a victim of a scam. I called the Target gift card phone number and filed a case. They said they would do the best they can, but the gift cards I purchased had already been redeemed."

Reports by attempted victims

One hundred fifty cases in the sample were reports by consumers who did not lose money. Some attempted victims used expressions suggesting that they were motivated to file a report to provide information to the authorities that may lead to the identification and arrest of the fraud criminals. For example, "Hope that [*helps*] and good luck catching this scum." In some of the reports, nonvictims responded to the scam call (pressed "1") in order to collect more information that they could include in their reports.

Most attempted victims appear to have recognized it was a scam from the very beginning. Evidence of irritation with the robocalls is evident in attempted fraud victim reports. This frustration may motivate reporting: "These [*calls*] are coming more frequently and something needs to be done. Life in prison sounds good." However, a sizeable contingent of attempted victims do not appear to have been aware that the call was a scam from the beginning. These individuals engaged with the scammer after pressing "1" and provided personal information before becoming suspicious. These consumers were primarily motivated to report to prevent potential misuse of their identifying information in the future.

Compared to victims, attempted victims took more steps to verify the legitimacy of the call before paying money. If they were not certain it was a scam, attempted victims more often hung up the phone and contacted the SSA or other agencies directly to ask if the accusations were truthful. Some described being "tipped off" by the prerecorded robotic message and requests that were atypical for the SSA, such as asking the consumer for personal information that the SSA should already have on file. For example, “Message sounded computer generated and falsified, so I contacted my local Social Security.”

Attempted victims often applied their existing persuasion knowledge and topic knowledge when confronted with the accusations. For example, “I didn't call back because Social Security won't call me, they will send letters.” Reports point to evidence that many consumers have implicit behavioral rules that they apply when solicited by strangers. Implicit rules may include never providing personal information over the phone and independently verifying a stranger’s claims using known and trustworthy sources.

Quantitative analysis of consumer report data

Quantitative methods

The aim of the quantitative analysis is to identify what individual, community demographic, and incident-level factors are associated with losing money in the SSA impostor scam; and among those who lost money, which factors are associated with the magnitude of monetary loss.

Sample

The sample of 209,344 SSA impostor scam reports is from the FTC’s Consumer Sentinel Network database, subset with community-level demographic data from the 2018 American Community Survey (ACS) from the U.S. Census Bureau. Consumer report cases were restricted to SSA impostor scam reports filed with any Sentinel data contributor in 2018, 2019, and 2020. Cases that were missing the consumer’s zip code or where consumers reported from a zip code with a population of less than 100 people were excluded (n = 53,184, 19.7%) because they lacked community-level demographic data.

Independent variables

Individual and incident-level variables

When filing a report with the FTC, consumers self-select (or are prompted by an FTC Call Center representative) the type of scam they experienced (e.g., an impersonator, online shopping, job/money making opportunity). They are also asked what business or entity the scammer pretended to be if they selected “an impersonator.” Those who reported any derivation of “Social Security Administration” were included in the sample. Consumers are also asked to report their name, address, and select their age from a drop-down menu. Ages are grouped in 10-year increments (e.g., 20 to 29). Ages 19 and younger are grouped together as are ages 80 and older.

Consumers are not asked to report their sex when they file a report with the FTC. We used the Gender Guesser 0.4.0 package in Python (https://pypi.org/project/gender-guesser/) to assign sex based on the consumer’s first name. Forty percent of consumers were assigned female, 27% were assigned male, and 33% were unassigned. We manually assigned male or female to unassigned names if they belonged to 100 or more consumers and are traditionally associated with one gender (e.g., Mary, Kyle, Erin, Lynn, Lee). This reduced the percent of unassigned consumers and resulted in a sample that is 51% female and 35% male. The remaining 14% of unassigned consumers have names that are nontraditional or rare, not gender-specific, associated with different nationalities, or that were likely misspelled.

To identify seasonal victimization patterns and whether victimization was more likely to be reported in any given year, we included variables for the year the report was filed (2018 = reference) and the season the incident was reported. Spring, the reference category, was coded as any report filed in the months of March through May, summer was June through August, fall was September through November, and winter was December through February.

A new variable was created to identify whether a third party, such as a friend or family member, reported on the consumer's behalf (yes = 1). Approximately 2.3% of the cases were filed by a third party. More than 97% of consumers reported that the impostors contacted them by phone, so method of contact was not included as an independent variable.

Qualitative analysis uncovered the emotional states that targets reported they experienced and the tactics impostors use to convince them to comply, including using official titles, law enforcement terms, and other words to invoke trust. To build on these findings, we applied the NRCLex Python package (https://pypi.org/project/NRCLex/) to the case narratives to quantify affective words based on the National Research Council Canada (NRC) affect lexicon and the Natural Language Toolkit (*NLTK*) library's *WordNet* synonym sets. The library contains more than 27,000 affective words. For each case narrative, we counted the frequency of words synonymous with five affective states: *fear, anticipation, sadness, trust,* and *anger* (Table 3). Some words belong to multiple affective categories and are counted in each category. We controlled for character length in all models.

Table 3: Average frequency (SD) of emotion words in case narratives

Emotion	Mean	Standard Deviation (SD)	Range	
Trust	0.26	1.54	0	54
Anticipation	0.16	0.88	0	29
Fear	0.11	0.67	0	37
Sadness	0.08	0.48	0	20
Anger	0.13	0.70	0	34
Character length	473.45	423.82	1	4000

Data on the method of payment is collected only for those who paid money in response to the scam. Similar methods of payment were condensed to produce fewer categories. Final categories include gift card or reload card (reference category), bank account/debit card, credit card, cash, cryptocurrency, wire transfer, and "other" payment method. These independent variables were only used in the regression model estimating the correlates of loss amount among victims of the SSA impostor scam. The proportion of victim reports using of each method of payment and the median loss amount (with standard deviation) is presented in Table 4.

Table 4: Methods of payment used in the SSA impostor scam (N = 8,777)

Method of payment	Proportion of total sample	Median loss
Gift card/reload card	69.7%	$1,500
Bank account/debit card	1.9%	$1,000
Credit card	1.1%	$1,000
Cash	3.0%	$13,000
Cryptocurrency	6.4%	$4,900
Wire transfer	1.2%	$18,000
Other method	16.6%	$1,990

Community-level variables

We subset consumer report data from the Sentinel with community-level data from the 2018 American Community Survey, matching on consumer zip code. We exclude consumer reports from zip codes belonging to post office boxes, businesses and universities that have their own zip code, and zip codes with populations of less than 100 residents ($n_{excluded}$ = 6,234). Neighborhood demographic characteristics include the percent of the zip code population with a college degree or higher, and percent of the zip code population that is Black, that is Hispanic/Latino, and that is Asian. Race and ethnicity percentages were divided into ordered categories based on Raval (2020). For percent of the zip code that is Black and the percent that is Hispanic, categories were coded as less than 5% [Black/Hispanic] (reference category), between 5% and 25% [Black/Hispanic], between 26% and 50% [Black/Hispanic], between 51% and 75% [Black/Hispanic], and more than 75% [Black/Hispanic]. Due to smaller population sizes, categories for percent Asian were condensed: less than 5% Asian (reference), between 5% and 25% Asian, between 26% and 50% Asian, and more than 50% Asian.

To control for community-level differences in report filing, we controlled for complaint rate by zip code. This is calculated as the total number of all non-SSA fraud reports filed by each zip code between 2018 and 2020, divided by the 2018 population of that zip code.

Dependent variables

Victimization

Victimization is defined as whether the consumer reported a financial loss, where any loss of $1 or more was coded as “1,” and $0 losses (attempted fraud) was coded as “0”: 4.2% of consumers who complained reported victimization.

Magnitude of loss

Losses were natural log transformed to account for non-normality and positive skew (high dollar outliers) in reported losses. Only victims were included in this analysis (N=8,777).

Analysis

Using the StatsModel package in Python (https://www.statsmodels.org/stable/index.html), logistic regression was used to estimate the effects of individual, community, and incident-level factors on the likelihood of reporting victimization by the SSA impostor scam (N = 209,344). Data were weighted by zip code population size, where consumers reporting from more populated zip codes are given greater weight. Ordinary least squares (OLS) regression was used to examine how these factors relate to the natural log of loss amount among those who reported victimization (N = 8,777).

Quantitative results

Sample characteristics

Table 5 presents descriptive individual- and community-level characteristics of consumers who reported the SSA impostor scam (both victims and attempted victims) as well as incident-level characteristics. Most consumers were classified as female (51.1%), followed by male (34.5%), and 14.3% were unclassified. Nearly a quarter of those who reported the SSA impostor scam to FTC were age 60 to 69 followed by those age 50 to 59 (17.6%). Consumers 19 and younger represent the smallest group in the sample at 1.1% of total, and adults age 80 and older represent nearly 6% of the sample. In 2.3% of reports, another party filed the report on the targeted consumer’s behalf.

Five percent of consumers live in a rural zip code. Nearly 50% of consumers reside in zip codes with less than 5% Black residents, 34.5% live in areas between 5 and 25% Black, and 17.3% live in areas that are 26% or more Black. Approximately one-third of consumers live in zip codes with fewer than 5% Hispanic residents, 44.4% live in zip codes with 5% to 25% Hispanic residents, and 23% live in zip codes that are 26% or more Hispanic. Seventy three percent of consumers live in areas with fewer than 5% Asian residents, and a quarter of consumers live in areas that are 5% to 25% Asian.

Sixty percent of total reports were filed in 2019, followed by 23.3% in 2020, and 16.4% in 2018. Thirty percent of reports were filed in the fall and 30.7% in summer, with lower numbers filed in winter (19.2%) and in spring (20%).

Table 5: Sample characteristics (N = 209,344)

	N	%
Sex classification		
Female	107,031	51.1
Male	72,305	34.5
Unclassified	30,008	14.3
Consumer age		
19 and younger	2,368	1.1
20 – 29	19,663	9.4
30 – 39	25,640	12.2
40 – 49	27,099	12.9
50 – 59	36,778	17.6
60 – 69	46,653	22.3
70 – 79	27,247	13.0
80 and older	12,276	5.9
Missing age	11,620	5.6
Community characteristics		
% Black		
< 5%	102,933	49.2
5-25%	72,206	34.5
26-50%	20,399	9.7
51-75%	8,810	4.2
76-100%	4,996	2.4
% Hispanic/Latino		
< 5%	68,301	32.6
5-25%	92,987	44.4
26-50%	29,270	14.0
51-75%	13,823	6.6
76-100%	4,963	2.4
% Asian		
< 5%	152,920	73.0
5-25%	49,554	23.7
26-50%	5,926	2.8
51-100%	944	0.5
Lives in rural area	10,571	5.0
Incident characteristics		
Year		
2018	34,406	16.4
2019	126,219	60.3
2020	48,719	23.3
Season		
Fall	62,957	30.1
Spring	40,285	19.2
Summer	64,331	30.7
Winter	41,771	20.0
Victim (reported financial loss)	8,779	4.2
Report filed by another party	4,806	2.3

Who reports victimization by the SSA impostor scam?

As shown in Table 6, the results of the weighted logistic regression analysis show no statistically significant effect of consumer sex on the odds of reporting victimization, although a greater number of women, relative to men, report the scam overall. Individuals with names that were unclassified by the algorithm were 29% more likely to report victimization relative to consumers with traditionally female names (95% confidence interval (95%CI = 1.14, 1.44, p < 0.001). The unclassified group was comprised largely of consumers with nontraditional names and names associated with other nationalities, perhaps suggesting that foreign-born individuals and those belonging to minority groups face a higher risk of victimization by the SSA impostor scam.

The likelihood of reporting victimization (relative to attempted victimization) typically declined with age. Relative to the reference group of 30 year olds, consumers 19 and younger were 96% more likely to report victimization (95%CI = 1.47, 2.62, p < 0.001), and those who were in their 20s were twice as likely to report victimization (95%CI = 1.76, 2.36, p < 0.001). Adults in their 50s were 17% less likely to report a loss than adults in their 30s (95%CI = 0.71, 0.98, p = 0.026), and those in their 70s were 30% less likely to report a loss (95%CI = 0.57, 0.84, p <0.001). In the same trend, those age 80 and older were 43% less likely to report victimization than 30-year-olds (95%CI = 0.43, 0.75, p < 0.001). There were no statistically significantly differences in reporting victimization between adults in their 30s and adults in their 40s (p = 0.119) and in their 60s (p = 0.052). Consumers who reported the SSA impostor scam on behalf of the target of the scam were 67% more likely to report that the consumer was a victim (95%CI = 1.31, 2.14, p < 0.001).

Results show that consumers residing in more minority communities are more likely to report victimization by the SSA impostor scam. Consumers in areas that are more than 25% Hispanic are between 23% and 45% more likely to report victimization relative to communities that are less than 5% Hispanic (p < 0.05). Consumers residing in areas with greater than 5% Black residents are significantly more likely to report victimization by a magnitude of 14% to 50% (p < 0.05). The size of the effect increases as communities move from 5% to 25% Black to 75% to 100% Black. Similarly, those who reside in communities more than 5% Asian are more likely to report victimization than consumers living in areas that are less than 5% Asian. Consumers living in areas that are 51% to 100% Asian are 66% more likely to report victimization (95%CI = 1.06, 2.60, p = 0.026). Living in a rural area, zip code complaint rate, and the percent of the zip code population with a college degree were not significantly associated with reports of victimization.

Relative to consumers who were targeted by the scam when it first began in 2018, consumers who filed reports in 2020 were 52% more likely to report victimization (95%CI = 1.23, 1.76, p < 0.001). There was no difference in the odds of reporting victimization between reports filed in 2018 versus 2020. There were significant effects of seasonality on reporting victimization: Relative to consumers who were targeted in spring months (March to May), consumers who were targeted in other seasons were between 25% and 40% less likely to report victimization (p < 0.001).

Negative emotional sentiments expressed in the case narratives were significantly associated with victimization for all types of affective words. On average, for each additional word associated with *trust*, a consumer was 14% more likely to report victimization (95%CI = 1.12, 1.17, *p* < 0.001). For each additional word synonymous with *anticipation*, a consumer was 49% more likely to report victimization (95%CI = 1.44, 1.54, *p* < 0.001). Emotion words associated with *anger* were also positively associated with reports of victimization (odds ratio = 1.41, 95%CI = 1.36, 1.47, *p* < 0.001). In contrast, for every additional word synonymous with *sadness*, a consumer was 21% *less* like to report victimization (95%CI = 0.75, 0.84, *p* < 0.001). There was also a significant negative effect of *fear* words on the odds of reporting victimization, but the effect size was small (odds ratio = 0.95, 95%CI = 0.91, 0.99, *p* = 0.026).

Table 6: Odds of reporting victimization by the SSA impostor scam among all SSA impostor scam report filers (N = 209,344)

		95% Confidence Interval			
	Odds Ratio	**2.5%**	**97.5%**	**p-value**	
Intercept	0.03	0.01	0.04	0.000	***
Male	1.10	1.00	1.22	0.062	
Consumer sex unclassified	1.29	1.14	1.45	0.000	***
Report filed on consumer's behalf	1.67	1.31	2.14	0.000	***
19 and younger	1.96	1.47	2.62	0.000	***
Age 20-29	2.04	1.76	2.36	0.000	***
Age 30-39 (reference)	---	---	---	---	
Age 40-49	0.88	0.74	1.04	0.119	
Age 50-59	0.83	0.71	0.98	0.026	*
Age 60-69	0.86	0.73	1.00	0.052	
Age 70-79	0.70	0.57	0.84	0.000	***
Age 80 and older	0.57	0.43	0.75	0.000	***
Age not reported	0.47	0.36	0.62	0.000	***
Community characteristics					
<5% Hispanic (reference)	---	---	---	---	
5%-25% Hispanic	1.07	0.94	1.22	0.301	
26%-50% Hispanic	1.25	1.07	1.46	0.004	**
51%-75% Hispanic	1.23	1.02	1.48	0.027	*
76%-100% Hispanic	1.45	1.13	1.85	0.003	**
<5% Black (reference)	---	---	---	---	
5%-25% Black	1.14	1.03	1.27	0.011	*

26%-50% Black	1.22	1.05	1.43	0.012	*
51%-75% Black	1.33	1.06	1.66	0.015	*
76%-100% Black	1.50	1.13	1.99	0.006	**
<5% Asian (reference)	---	---	---	---	
5%-25% Asian	1.20	1.08	1.34	0.001	**
26%-50% Asian	1.59	1.29	1.96	0.000	***
51%-100% Asian	1.66	1.06	2.60	0.026	*
% college educated	1.00	1.00	1.00	0.984	
Lives in a rural community	1.07	0.65	1.76	0.799	
Zip code complaint rate	0.01	0.00	4.75	0.138	
Incident characteristics					
Scam occurred in 2018 (reference)	---	---	---	---	
Scam occurred in 2019	1.15	1.00	1.33	0.058	
Scam occurred in 2020	1.52	1.30	1.77	0.000	***
Scam occurred in spring (reference)	---	---	---	---	
Scam occurred in summer	0.60	0.53	0.68	0.000	***
Scam occurred in fall	0.74	0.65	0.84	0.000	***
Scam occurred in winter	0.75	0.66	0.86	0.000	***
Frequency of Emotional Sentiments					
Trust	1.14	1.12	1.17	0.000	***
Anticipation	1.49	1.45	1.54	0.000	***
Fear	0.95	0.91	0.99	0.026	*
Anger	1.41	1.36	1.47	0.000	***
Sadness	0.79	0.75	0.84	0.000	***
Narrative character length	1.00	1.00	1.00	0.000	***

Who loses more money in the SSA impostor scam?

Only reports where there was a reported loss (victims) are included in the OLS regression predicting the amount of financial loss (N = 8,777; Table 7). The exponentiated intercept ($e^{\beta 0}$) equated to a predicted average loss of $798.12, all else held constant. Variables denoting the method of payment were added to this model and had the largest effect sizes relative to other correlates. Compared to consumers who paid with gift cards, consumers who paid with a debit card lost 22% less money (β = -0.25, 95%CI = -0.47, -0.04, *p* = 0.022), and those who paid with a credit card lost 34% less money (β = -0.42, 95%CI = -0.71, -0.13, *p* = 0.004). Paying using cryptocurrency led to losses that were 140% higher than losses from gift cards (β = 0.89, 95%CI = 0.75, 1.01, $p < 0.001$). But on average, paying with cash and wire transfer led to the highest losses — 426% and 728% more than gift cards, respectively ($p < 0.001$). Note that consumers often purchased gift cards using cash or deposited cash into cryptocurrency ATMs, so some reports of cash as the final method of payment to impostors may be misclassified.

Table 7: OLS regression of natural log of reported losses among victims (N = 8,777)

			95% CI			
	β	S.E.	0.025	0.975	t	p-value
Intercept	6.68	0.11	6.47	6.90	60.30	0.000
Male	0.04	0.03	-0.03	0.10	1.09	0.274
Consumer sex unclassified	-0.02	0.04	-0.10	0.06	-0.45	0.655
Report filed on consumer's behalf	-0.07	0.08	-0.23	0.10	-0.83	0.409
19 and younger	-0.64	0.10	-0.83	-0.45	-6.48	0.000
Age 20-29	-0.26	0.05	-0.36	-0.16	-5.15	0.000
Age 30-39 (reference)	---	---	---	---	---	---
Age 40-49	-0.01	0.06	-0.12	0.11	-0.15	0.881
Age 50-59	-0.03	0.06	-0.14	0.08	-0.50	0.615
Age 60 to 69	0.08	0.05	-0.03	0.18	1.40	0.162
Age 70 to 79	0.34	0.07	0.21	0.47	5.02	0.000
Age 80 and older	0.66	0.09	0.47	0.85	6.95	0.000
Age not reported	0.02	0.09	-0.16	0.20	0.26	0.796
Community characteristics						
<5% Hispanic (reference)	---	---	---	---	---	---
5%-25% Hispanic	0.02	0.04	-0.06	0.09	0.40	0.686
26%-50% Hispanic	0.02	0.05	-0.08	0.12	0.33	0.744
51%-75% Hispanic	0.04	0.06	-0.09	0.16	0.58	0.562
76%-100% Hispanic	0.10	0.09	-0.09	0.28	1.04	0.299
<5% Black (reference)	---	---	---	---	---	---
5%-25% Black	-0.07	0.03	-0.14	0.00	-2.08	0.038
26%-50% Black	-0.14	0.05	-0.24	-0.03	-2.54	0.011
51%-75% Black	0.00	0.08	-0.15	0.14	-0.06	0.955
76%-100% Black	-0.25	0.10	-0.44	-0.05	-2.51	0.012
<5% Asian (reference)	---	---	---	---	---	---
5%-25% Asian	0.13	0.04	0.06	0.21	3.48	0.001
26%-50% Asian	0.15	0.08	0.00	0.30	1.94	0.052
51%-100% Asian	0.36	0.17	0.02	0.70	2.09	0.036

% college educated	0.01	0.00	0.01	0.01	10.23	0.000
Lives in a rural community	0.11	0.08	-0.05	0.27	1.31	0.189
Zip code complaint rate	0.52	1.01	-1.46	2.51	0.52	0.605
Method of payment						
Gift card/cash reload card (reference)	---	---	---	---	---	---
Bank account/debit card	-0.25	0.11	-0.47	-0.04	-2.29	0.022
Cash	1.66	0.09	1.49	1.84	18.66	0.000
Wire transfer	2.11	0.14	1.85	2.38	15.46	0.000
Credit card	-0.42	0.15	-0.71	-0.13	-2.88	0.004
Cryptocurrency	0.88	0.06	0.75	1.00	13.66	0.000
Other payment method	0.35	0.04	0.27	0.43	8.46	0.000
Other incident characteristics						
Scam occurred in 2018 (reference)	---	---	---	---	---	---
Scam occurred in 2019	-0.13	0.05	-0.23	-0.03	-2.49	0.013
Scam occurred in 2020	-0.01	0.05	-0.12	0.09	-0.21	0.832
Scam occurred in spring (reference)	---	---	---	---	---	---
Scam occurred in fall	0.10	0.04	0.02	0.19	2.36	0.018
Scam occurred in summer	0.15	0.04	0.07	0.24	3.43	0.001
Scam occurred in winter	0.03	0.05	-0.06	0.13	0.66	0.512
Frequency of Emotional Sentiments						
Trust	0.01	0.01	-0.01	0.02	0.98	0.329
Anticipation	0.03	0.01	0.01	0.05	3.18	0.001
Fear	0.05	0.01	0.02	0.07	3.93	0.000
Anger	0.02	0.01	0.00	0.05	2.07	0.039
Sadness	-0.04	0.02	-0.07	-0.01	-2.75	0.006
Narrative character length	0.00	0.00	0.00	0.00	-0.64	0.522

Note: Dependent variable was natural log-transformed. R-square = 0.173

Controlling for other case characteristics and neighborhood demographics, older adults lost significantly more money, on average, than adults in their 30s. Specifically, those ages 70 to 79 lost an average of 40% more (*p* < 0.001) than 30 to 39 year olds, and adults 80 and older lost an average of 93% more (*p* < 0.001). Although young adults ages 19 and younger and those ages 20 to 29 were the most likely to report fraud victimization as shown in the previous model, reported losses were between 47% and 23% lower for these age groups, respectively, compared to losses experienced by victims ages 30 to 39. There were no statistically significant differences in average loss amount between those in their 30s and those in the 40s, 50s, and 60s.

Consumers who resided in communities with a higher percentage of Black residents lost significantly less money, on average, than consumers from communities that are less than 5% Black. For example, those living in communities between 5% and 25% Black lost 7% less, on average (p = 0.038), and those living in communities between 26% and 50% Black lost 13% less, on average (p = 0.011), relative to consumers residing in communities with fewer than 5% Black residents. The effect size was largest for consumers residing in communities where 75% to 100% of residents are Black. These consumers reported 22% lower losses, on average (β = -0.25, 95%CI= -0.45, -0.05, p = 0.012).

The opposite trend was observed for consumers in communities with a lower to higher proportion of Asian residents. Compared to consumers living in communities with fewer than 5% Asian residents, those living in 26% to 50% Asian areas lost 14% more money on average, and those residing in 51% or more Asian areas lost 43% more on average. Loss amount was not significantly associated with the proportion of Hispanic residents residing in a community. For each percentage increase in the proportion of college educated residents in a community, the magnitude of loss increases by 1% (β = 0.01, 95%CI = 0.00, 0.01, p < 0.001).

Mentions of words associated with *anticipation*, *fear*, and *anger* in the narratives were positively associated with the magnitude of loss, while words associated with *sadness* were inversely associated with loss. Specifically, for every additional word related to the state of *anticipation*, a consumer lost 3% more money (β = 0.03, 95%CI =

0.01, 0.05, $p < 0.001$), and for every additional word associated with *fear*, a consumer lost an average of nearly 5% more (β = 0.05, 95%CI = 0.02, 0.07, $p < 0.001$). For every additional word associated with *sadness*, a consumer lost an average of 4% less (β = -0.04, 95%CI = -0.07, -0.01, $p = 0.006$). Expressions of trust were not significantly related to loss amount. Character length was also not significant.

While the prior model indicated that reports of victimization were more likely in 2019 and 2020 than in 2018, losses were, on average, 12% lower in 2019 than loses reported in 2018 (β = -0.13, 95%CI = -0.23, -0.03, $p = 0.013$). Relative to reports filed in the spring, losses were 11% higher, on average, for cases filed in the fall (β = 0.10, 95%CI = 0.02, 0.19, $p = 0.018$), and 16% higher, on average, in summer (β = 0.15, 95%CI = 0.07, 0.24, $p < 0.001$). There were no statistically significant differences in losses between spring and winter.

There were also no statistically significant differences in the magnitude of average losses between men and women, urban versus rural consumers, and consumers whose case was reported by a third party.

Discussion

This study presents findings from a mixed methods analysis of SSA impostor scam reports using data from the FTC's Consumer Sentinel and the 2018 American Community Survey. Findings illuminate the powerful persuasion tactics that SSA impostors use to incite fear and manipulate consumers to comply with their requests. Quantitative findings reflect themes uncovered in the qualitative analysis, showing that there is a significant association between emotion and reporting a financial loss, even after controlling for the length of the case narrative. Quantitative findings also add to the literature by showing that consumers from minority communities and young adults are more likely report victimization, although older adult victims and non-Hispanic white victims lose more money on average. Possible consumer protections may include more stringent controls around gift card sales and cryptocurrency exchange, as well as consumer education to help mitigate the risk of SSA impostor scams.

The impact of emotion on victimization and financial loss

According to the Elaboration Likelihood Model of persuasion (Petty and Cacioppo 1986), high emotional arousal promotes more superficial processing of information leading to errors in decision making. Emotional arousal is an extremely effective tool for SSA impostors who do not want consumers to scrutinize their unorthodox requests. Evidence of high intensity emotional arousal was present in nearly every victim report narrative. Victims described how impostors threatened them with arrest, informed them that their bank accounts and Social Security numbers would be suspended, and often told them that they were being followed by government agents. Some consumers reported that they were told that the real criminals would come after them and their families if they did not cooperate. Interestingly the presence of fear words was only marginally significant in the logistic regression model predicting victimization, and in the inverse direction (OR = 0.95). However, among victims, fear words were significantly positively associated with amount lost. Note that there was a considerable overlap between words associated with fear and words associated with anger, which may have suppressed the independent effects of fear words on the odds of reported victimization. For example, “criminal,” “aggressive,” “illegal,” and “threaten,” are counted as both fear and anger words.

Although expressions of sadness were common in the victims' case narratives, general synonyms such as "loss," "guilty," "shame," "abandoned," etc. — were inversely associated with reports of losing money and with the amount of money lost. This suggests that consumers who experienced attempted fraud were more likely to express remorse in their narrative accounts than victims. Qualitative interviews with victims and nonvictims could help identify the ways that sadness is experienced and articulated after being targeted by the SSA impostor scam. One possibility is that feelings of sadness translate to anger after losing money. Indeed, words that reflected and evoked anger (e.g., *frustrated, fraud, stolen*) were positively associated with victimization and with the average amount of money lost among victims.

Trust words like *officer, badge, legal, account*, and *bank* were positively associated with reports of victimization and the average loss. This finding reflects the persuasion principal of "authority," which was a prominent theme in the qualitative analysis. Scammers claimed to be with the federal government and stated that they had information on the consumer that a government official would presumably know. They also claimed to have law enforcement powers and could command local authorities to arrest the consumer. Recent qualitative research by Honick et al. (2021) indicates that consumers who place a high value on compliance with authority may be more likely to fall for scams. Indeed, the prevalence and success of the SSA impostor scam in the U.S. may stem from Americans' natural deference to government authority. Future research might explore whether citizens of countries where compliance with civil institutions is not a valued trait experience government impostor scams at the same rate as U.S. residents.

Scarcity (aka, urgency) is another popular persuasion principle that emerged in the qualitative analysis. In the quantitative analysis, words related to the state of anticipation (e.g., *immediately, time, worry*) were positively associated with victimization and with the amount of money lost.

Age and victimization

Reflecting the results of general sample surveys (Anderson 2019) and reports on other scam types using Sentinel data (FTC 2020), we find that younger consumers are more likely to report victimization by the SSA impostor scam compared to older consumers, but among those who lose money, victims 70 and older experience significantly higher losses. There are several explanations that may underlie these findings. First, time-poor young and middle-aged attempted victims may be less likely to file no-loss reports relative to older, retired adults. If this age-based selection effect in reporting were true, there may be no differences in susceptibility by age. Alternatively, younger adults could be more vulnerable to the SSA impostor scam because they have less experience with federal agencies like the SSA. According to the Persuasion Knowledge Model (Friestad and Wright 1994) having limited *topic* and *agent* knowledge make people more susceptible to influence. Moreover, young people are not priority targets for scam awareness messages relative to older adults. They are less likely to watch television news (Wonneberger, Schoenbach and Van Meurs 2011) where stories of consumer fraud are often highlighted. Because we find that older adults are more likely to file no-loss reports, it could indicate that fraud protection campaigns targeted at older people are successful in raising awareness.

Random sample survey of U.S. residents of all ages could help disambiguate the relationship between age and government impostor scam susceptibility. Given the challenges associated with underreporting losses, particularly among the oldest-old, those with cognitive impairment, and those who lack English proficiency, another approach would be to obtain data from the SSA impostors that contains information on what households they targeted and who responded, including the ages of targeted consumers. However, criminal enterprises that use robodialing as their primary method of solicitation generally do not have detailed demographic data on the people they target/victimize.

Although older adults were less likely to report victimization to FTC, older victims lost significantly more money than victims in their 30s and younger. This reflects data from reports filed directly with SSA (Office of the Inspector General of the SSA 2021). Higher losses may reflect differences in generational wealth. Baby boomers have substantially more wealth than millennials (Gale et al. 2020), so impostors may find that they are more remunerative targets. Alternatively, given the higher levels of social isolation among older adults (Cornwell and Waite 2009; Kotwal et al. 2021), older targets may interact with impostors for longer periods before someone in their social network discovers the fraud and intervenes.

Data on the length of time under the impostor's influence is not available in the Sentinel but could help illuminate differences in average loss amount between consumers of different ages. The study also lacked data on the number of individual gift card purchases, cryptocurrency exchanges, or wire transfers made by the consumers, who typically file a report on the entire fraud experience, not separate reports for each instance of payment. This data could show whether older consumers purchased higher denominations of gift cards, whether they visited more retailers, and whether they were less likely to be stopped by retail employees or bank tellers compared to young adults.

Race, ethnicity, and victimization by the SSA impostor scam

Results show that consumers reporting from zip codes with higher proportions of Black, Hispanic, and Asian residents are more likely to report victimization than consumers in nonminority areas, even after controlling for complaint rate. Again, due to selection bias in reporting, consumer report data does not definitively answer the question of whether race and ethnic minorities are indeed more susceptible to the SSA impostor scam or whether they are more likely to submit loss reports relative to no-loss reports compared to non-Hispanic white consumers.

Prior research on other types of alleged fraud indicates that individuals living in minority communities are more likely to be victims (Raval 2021). Comparing Sentinel complaint data to law enforcement data on fraud victims, Raval (2021) found that self-selection in reporting disproportionately reduces the report rate for minority communities compared to nonminority communities, and that people from more Black areas are more likely to be victims. Raval (2021) also found that victimization rates followed an inverted U-shaped pattern for Hispanics, such that the highest implied victimization rates were in moderately Hispanic communities. Areas that were majority Hispanic and areas with a low proportion of Hispanic residents had lower victimization rates. That research did not include substantial data on government impostor scam victims, so direct comparison to the present study is not possible.

We found that the odds of reporting victimization were higher in majority Hispanic areas relative to areas with few Hispanic residents, and a similar trend was observed for Asian communities. As the proportion of Asian residents in a community increased above 5%, so did the odds of reporting victimization. These results could indicate that immigrants, especially non-English speakers who live in concentrated immigrant communities, may be particularly at risk, perhaps because they have less experience with U.S. federal agencies and the American marketplace (Friedman et al. 2000). In other words, they lack *agent* and *topic* knowledge about how the SSA operates, what powers the agency has, and what interactions and requests are within its charter (Friestad and Wright 1994). A report by Choi (2014) suggested that immigrant Hispanics were frequent targets of impostor scams during the rollout of the Affordable Care Act. Scammers capitalized on confusion on eligibility requirements and enrollment procedures to deceive targets without legal resident status. Similarly, Lema (2018) documents the experience of Ethiopian immigrants targeted by tax return scams, immigration scams, and other forms of fraud, noting how age, education, employment status, and level of financial knowledge influence susceptibility.

Seasonal and annual patterns in victimization

Although 60% of the SSA impostor scam reports were filed in 2019, we find that the odds of reporting victimization were highest in 2020. One explanation is that when the scam first emerged in mid-2018 and 2019, a higher proportion of targeted consumers reported to inform the FTC about the new scam, regardless of whether they lost money. As time went on and the scam became ubiquitous, fewer attempted fraud victims were motivated to file no-loss reports and share that they were targeted, while those who lost money continued to report. Alternatively, impostors may have refined their deceptive “story” over time or altered their approach to become more persuasive, such as by targeting specific consumers whose personal information they had obtained. However, the qualitative analysis does not support that impostors changed their story or used different persuasion tactics in 2020 relative to earlier years. If law enforcement data were to become available, future research could investigate whether the same or different criminal enterprises were operating the fraud in 2020 versus 2018 and 2019, and whether impostors began working off lead lists of consumers for whom they had personal information such as Social Security numbers and addresses.

No prior academic research has investigated the relationship between fraud victimization and seasonality. For the SSA impostor scam, reports in the Consumer Sentinel were highest in summer and fall months overall, suggesting that impostors were more active then, although the odds of reporting victimization were highest in the spring. On the other hand, losses were significantly higher in the summer and fall than in the spring. This could reflect seasonal differences in consumers’ propensity to report attempted versus experienced victimization, the timing of consumer education campaigns which might motivate people to report, or differences in the effectiveness of the scam each season.

Reports directly to SSA show very different seasonal patterns when broken down by year (Office of the Inspector General of the SSA 2021). In 2019, reports directly to SSA steadily rose from January to May, fell slightly in June and July, peaked in August, then fell and steadily rose throughout the fall. Total reports were higher in 2020. In 2020 reports rose from April to September before falling in December and then rising again in

January in February. Additional research could assess how patterns in the SSA impostor scam victimization rate compare to other types of fraud, and whether consumers' motivation to report fraud changes based on the season.

Implications

Results of the qualitative analysis provide insights on how to better protect consumers from the SSA impostor scam. According to the Persuasion Knowledge Model (Friestad and Wright 1994), individuals are better able to recognize and resist influence attempts if they possess understanding of the persuasion agent, knowledge about the topic presented, and methods of persuasion. Recent research by DeLiema et al. (2021) found that consumers who were already aware of the specific scam they were targeted by were between 40% and 60% less likely to pay money to the scammer. Qualitative analysis of the attempted victim case narratives shows how nonvictims apply their existing knowledge about the SSA ("SSA does not call, they send letters") and about fraud and persuasion ("they used scare tactics") to avoid being deceived. Attempted victims also conveyed that they did research during and after the call to verify the information they were told, including calling their local SSA office or the FTC to ask questions. This indicates that local SSA offices may serve as important sources of protection against the scam.

Other consumer education may focus on informing consumers about the SSA impostor scam and the established ways that the SSA may contact individuals for legitimate purposes, and also that the SSA will not threaten consumers with arrest or suspension of their benefits. Based on results from this investigation, messaging may be most beneficial if it is focused on people living in heavily minority areas and areas with a high proportion of immigrants who may be less familiar with the roles of U.S. government agencies. Future research could test what fraud awareness messaging campaigns are most effective for these populations and what dissemination strategies are best.

Seventy percent of payments to impostors were made using gift cards, suggesting that there may be opportunities to intervene in retail environments. Many stores have posted warning signs about scams near gift card sales kiosks and registers and have trained sales clerks and managers on the red flags of gift card payment scams (Sherr 2021). Employee intervention may be an effective tool in the fight against fraudulent gift card sales because it interrupts the hold that impostors have over the customer by casting doubt over the impostors' authority and drawing attention to the absurdity of their requests. Still, impostors provide persuasive explanations for why gift cards are necessary, and coach targets on how to respond to store employees' questions. Another strategy used by some retailers is limiting the amount of money that can be loaded onto gift cards and the number of cards that can be purchased on a given day (Garbato 2020). Future research may explore the effectiveness of employee training, warning signs, and gift card purchase limits on reducing the magnitude of fraud losses.

Gift card issuers and the companies that provide payment processing services for major retail brands may have additional strategies to identify and flag potentially fraudulent purchases. A potential indicator of fraud is when someone remotely attempts to redeem the card's value immediately following an in-store purchase. This suggests that the consumer is not the individual redeeming the card, and that it was not intended as a gift. One potential solution is for gift card issuers and payment processors to institute a temporary 24-hold, or “cooling off” period, before the card can be redeemed electronically (versus in person). This would allow more time for the target to realize they are involved in a scam and to request their money back.

In addition to retailer interventions, employees at financial institutions may need more tools to recognize fraud and intervene. For many consumers, the SSA impostor scam begins at their bank where they request large cash withdrawals to use for gift card purchases. Like retailers, tellers may benefit from additional training on how to detect this type of fraud and inform the customer about the risks of large cash withdrawals following telephone requests from someone they do not know in person. New protocols and training may help protect consumers from losing money as a result of a large wire transfer, as data from this study show that wire transfers are associated with substantially higher losses. Similarly, cryptocurrency ATMs may be equipped with warning messages about impostor scams and require that the consumer acknowledge the warning message (click to accept) before they can proceed with depositing cash.

Limitations

Data only represent SSA impostor scam reports available in the FTC Consumer Sentinel database. These cases represent only a portion of the total SSA impostor scam reports and exclude consumers who reported to the SSA directly, which is a higher number than reports filed with the FTC (see Office of the Inspector General SSA 2021). Data also exclude reports filed as Do Not Call Registry violations, where the vast majority do not involve victimization.

Consumer report data reflects both victimization *and* the propensity to complain, which varies across demographic groups (Raval 2020). Models attempted to control for underreporting in certain communities by controlling for zip code complaint rate. This does not perfectly adjust for underreporting since the weight variable was not created by using data from the true rate of SSA impostor scam victimization.

While 4.2% of consumers in the sample are victims, the true rate of victimization by the SSA impostor scam is likely much lower as most U.S. residents with access to a phone have been targeted but did not pay money and did not complain to the FTC or SSA. Consumers who lose money are likely more motivated to submit a report than nonvictims, which skews the sample toward victims. Still, many victims do not report because they feel ashamed or do not know who to contact following victimization. Therefore, many victims are also missing from the data.

Another limitation of the data is that the FTC does not collect information on consumer sex, race, ethnicity, education, and other socioeconomic and demographic characteristics. The variables representing these characteristics in the models are community-level proxies or assigned using a gender guesser. Future survey research on fraud may attempt to measure these characteristics at the individual level.

There are several limitations to the sentiment analysis. One is that the NRCLex library does not recognize compound words such as “police officer,” and in the analyses these words are counted individually. This produces double counting of some emotions. Second, the lexicon does not consider the context in which words are presented, which could change their emotional meaning. And third, narratives are written *after* the scam. Consumer emotions and interpretations of what happened and why it happened can change as the person retrospectively reports their experience. They may have felt afraid in the moment but reported feeling angry after the fact. Future qualitative research may attempt to probe consumers on what they were thinking and feeling while the scam was happening, versus after they recognized they were deceived.

Conclusion

This study uses mixed methods to analyze consumer report data to explore the factors associated with reporting victimization by the SSA impostor scam. We find that SSA impostors use powerful persuasion tactics such as authority, reciprocity, scarcity, and secrecy to deceive targets into paying money. Although older consumers are less likely to report victimization compared to young adult consumers, older victims lose significantly more money on the scam on average. Consumers living in more heavily minority areas are more likely to report victimization, suggesting that greater education on how the SSA officially interacts with consumers and awareness on government impostor scams may benefit them. Qualitative analyses of consumer report narratives reveal promising opportunities for consumer protection at banks and retailers, such as establishing stricter controls around gift card sales and empowering employees to intervene.

References

Anderson, K. B. (2021). To whom do victims of mass-market consumer fraud complain? Available at SSRN: https://ssrn.com/abstract=3852323 or http://dx.doi.org/10.2139/ssrn.3852323

Anderson, K. (2019). Mass-Market Consumer Fraud in the United States: A 2017 Update. Federal Trade Commission. Available at https://www.ftc.gov/reports/mass-market-consumer-fraud-united-states-2017-update

Baumeister, R. F., Twenge, J. M., & Nuss, C. K. (2002). Effects of social exclusion on cognitive processes: anticipated aloneness reduces intelligent thought. *Journal of personality and social psychology*, *83*(4), 817-827.

Cialdini, R. B. (2007). *Influence: The psychology of persuasion*. New York, NY: HarperCollins.

Choi, D. S. (2014). Health care scams on immigrants in the age of the Affordable Care Act. *Clearinghouse Review*, *48*, 80-85.

Cornwell, E. Y., & Waite, L. J. (2009). Measuring social isolation among older adults using multiple indicators from the NSHAP study. *Journals of Gerontology Series B: Psychological Sciences and Social Sciences*, *64*(suppl_1), i38-i46.

DeLiema, M., Li, Y., & Mottola, G. R. (2021). Correlates of compliance: Examining consumer fraud risk factors by scam type. *Available at SSRN 3793757*.

DeLiema, M., Yon, Y., & Wilber, K. H. (2014). Tricks of the trade: Motivating sales agents to con older adults. *The Gerontologist*, *56*(2), 335-344.

Duclos, R., Wan, E. W., & Jiang, Y. (2013). Show me the honey! Effects of social exclusion on financial risk-taking. *Journal of Consumer Research*, *40*(1), 122-135.

Dyrud, M. A. (2005). I brought you a good news: An analysis of Nigerian 419 letters. In *Proceedings of the 2005 Association for Business Communication Annual Convention* (pp. 20-25).

Federal Trade Commission. (2020). Protecting Older Consumers. 2019-2020. A Report of the Federal Trade Commission to Congress. Available at https://www.ftc.gov/system/files/documents/reports/protecting-older-consumers-2019-2020-report-federal-trade-commission/p144400_protecting_older_adults_report_2020.pdf

Fletcher, E. (2019a). Government impostor scams top the list of reported frauds. Federal Trade Commission. Available at https://www.ftc.gov/news-events/blogs/data-spotlight/2019/07/government-imposter-scams-top-list-reported-frauds

Fletcher, E. (2019b). Growing wave of Social Security imposters overtakes IRS scam. Federal Trade Commission. Available at https://www.ftc.gov/news-events/blogs/data-spotlight/2019/04/growing-wave-social-security-imposters-overtakes-irs-scam

Friedman, M., Gurwitz, S., & Herrera, P. (2000). New dimensions of consumer fraud. *Consumer Interests Annual*, *46*, 197-199.

Friestad, M., & Wright, P. (1994). The persuasion knowledge model: How people cope with persuasion attempts. *Journal of Consumer Research, 21*(1), 1-31. doi: 10.2307/2489738

Garbato, D. (2020). What grocers need to know about gift card fraud. *Progressive Grocer,* 82-83.

Glaser, B. G. (1965). The constant comparative method of qualitative analysis. *Social problems*, *12*(4), 436-445.

Han, S. D., Boyle, P. A., James, B. D., Yu, L., & Bennett, D. A. (2016a). Mild cognitive impairment and susceptibility to scams in old age. *Journal of Alzheimer's Disease*, *49*(3), 845-851.

Han, S. D., Boyle, P. A., Yu, L., Arfanakis, K., James, B. D., Fleischman, D. A., & Bennett, D. A. (2016b). Grey matter correlates of susceptibility to scams in community-dwelling older adults. *Brain Imaging and Behavior*, *10*(2), 524-532.

Honick, C., DeLiema, M., Fletcher, E., Mottola, G., Pessanha, R., & Trumpower, M. (2021). *Exposed to scams: Can challenging consumers' beliefs protect them from fraud*? FINRA Investor Education Foundation, University of Minnesota and BBB Institute for Marketplace Trust.

Kircanski, K., Notthoff, N., DeLiema, M., Samanez-Larkin, G. R., Shadel, D., Mottola, G., ... & Gotlib, I. H. (2018). Emotional arousal may increase susceptibility to fraud in older and younger adults. *Psychology and Aging*, *33*(2), 325- 337. https://doi.org/10.1037/pag0000228

Kotwal, A. A., Cenzer, I. S., Waite, L. J., Covinsky, K. E., Perissinotto, C. M., Boscardin, W. J., ... & Smith, A. K. (2021). The epidemiology of social isolation and loneliness among older adults during the last years of life. *Journal of the American Geriatrics Society*. https://doi.org/10.1111/jgs.17366

Lema, B. (2018). Thematic Analysis of Consumer Frauds and Scams Against Ethiopian Immigrants in the USA; A Phenomenological Case Study in Washington Seattle. Available at http://dx.doi.org/10.2139/ssrn.3175496

Lerner, J. S., Li, Y., & Weber, E. U. (2013). The financial costs of sadness. *Psychological Science*, *24*(1), 72-79.

Miles, M.B., Huberman, M. and Saldana, J. (2013) Qualitative data analysis: A methods sourcebook. 3rd Edition. Sage Publication, Beverly Hills.

Office of the Inspector General of the Social Security Administration (2021). Congressional status update Social Security-related phone scams. Available at https://oig.ssa.gov/files/Congressional_Status_Update_on_%20SSA_Related_Phone_Scams_%20FY_21_Q3_1.pdf

Petty, R. E., & Cacioppo, J. T. (1986). The elaboration likelihood model of persuasion. In *Communication and persuasion* (pp. 1-24). Springer, New York, NY.

Petty, R. E., & Briñol, P. (2015). Emotion and persuasion: Cognitive and meta-cognitive processes impact attitudes. *Cognition and Emotion*, *29*(1), 1-26.

Pak, K., & Shadel, D. (2011). AARP Foundation national fraud victim study. *Washington DC*. Available at https://www.aarp.org/money/scams-fraud/info-03-2011/fraud-victims-11.html

Raval, D. (2020). Which communities complain to policymakers? Evidence from consumer sentinel. *Economic Inquiry*, *58*(4), 1628-1642.

Raval, D. (2021). Who is victimized by fraud? Evidence from consumer protection cases. *Journal of Consumer Policy*, *44*(1), 43-72.

Saldaña, J. (2021). The coding manual for qualitative researchers. Sage Publications.

SimplyWise (2021). SimplyWise Retirement Confidence Index January 2021. Available at https://www.simplywise.com/blog/retirement-confidence-index/.

Sherr, I. (November, 2021). People are fighting back against gift card scammers. Here's how. *CNET*. Retrieved from https://www.cnet.com/news/people-are-fighting-back-against-gift-card-scammers-heres-how/

Whitty, M. T. (2015). Mass-marketing fraud: a growing concern. *IEEE Security & Privacy*, *13*(4), 84-87.

Wonneberger, A., Schoenbach, K., & Van Meurs, L. (2011). Interest in news and politics—or situational determinants? Why people watch the news. *Journal of Broadcasting & Electronic Media*, *55*(3), 325-343.