TESTIMONY OF MARTI DELIEMA, PHD

ASSISTANT PROFESSOR OF SOCIAL WORK AT THE UNIVERSITY OF MINNESOTA SCHOOL OF SOCIAL WORK

BEFORE THE ELDER JUSTICE COORDINATING COUNCIL

ON

"GOVERNMENT IMPOSTER SCAMS: WHAT CAN WE LEARN FROM CONSUMER COMPLAINTS ABOUT THE SOCIAL SECURITY ADMINISTRATION IMPOSTER SCAM?"

JUNE 21, 2022

Good morning members of the Elder Justice Coordinating Council. My name is Marti DeLiema and I am an Assistant Professor at the University of Minnesota School of Social Work. I was invited to present on my recent work performed in collaboration with the Federal Trade Commission's Division of Consumer Response and Operations[i]. This research involves a mixed methods analysis of consumer complaints of one of the most common scams targeting millions of Americans in recent years—the Social Security Administration (SSA) imposter scam. I will share the techniques that government imposters use to deceive consumers and the characteristics of those who report losing money. I will end my presentation with ideas for what policy makers, law enforcement, and private sector companies can do to better protect consumers from government imposter scams. The suggestions, opinions, and conclusions I will express are solely my own and do not represent the opinions or policy of the SSA or any agency of the Federal Government, including the Federal Trade Commission.

The Social Security Administration imposter scam

According to consumer reports, the SSA imposter scam became one of the most prevalent frauds in America, overtaking the IRS imposter scam beginning in early 2019. A survey by a financial technology startup found that 46% of adult respondents experienced at least one attempted SSA imposter scam in just a three month period, from October to December 2020[ii]. Extrapolating to the entire US population, that equates to 130 million Americans who were targeted, primarily by phone.

The good news is that the majority of Americans targeted by government imposter scams do not become victims. So who does? And why? What are the tactics that perpetrators use to convince targets to comply with their demands? We set out to explore those research questions using data from the largest consumer complaint database available—the Federal Trade Commission's Consumer Sentinel Network.

Persuasion tactics used in government imposter scams: Evidence from consumer complaint narratives

First we conducted a qualitative analysis of 600 randomly selected consumer complaints describing the SSA imposter scam. In their narrative reports, consumers frequently described what the fraud criminals said and did to make their stories convincing. Of Robert Cialdini's[iii] six elements of persuasion, three were common throughout the case narratives: authority, scarcity (or urgency), and reciprocity. In addition to these three common persuasion tactics, imposters also used a fourth influence tactic—*secrecy*.

SSA imposters were consistent in their use of *authority*. Consumers reported that impostors spoofed the phone numbers and caller IDs of local and federal Social Security Administration offices as well as local

police departments. One initially skeptical consumer wrote in their complaint, “I asked [them] 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.” Most impostors gave consumers phony badge and case ID numbers. They would ask consumers 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 and that they were under surveillance. Each of these invented policies and procedures increased the credibility of the imposters’ stories.

The criminals also named other federal agencies that were supposedly involved with the investigation. In more than 50 out of 600 cases reported, the impostor told the consumer that U.S. Marshals were coming to arrest them; 30 cases mentioned the Drug Enforcement Administration (DEA), and another 28 cases mentioned the Federal Bureau of Investigation (FBI). In 44 cases, consumers reported that the impostors already had their personal information, such as name, address, and social security numbers before the call began, suggesting that some criminals may be using contact lists.

At the start of each call, impostors threatened the consumer with arrest for serious criminal charges. When consumers denied the accusations, the impostors switched 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.” This fabricated sympathy for the consumers’ plight increases trust and the consumers’ motivation to reciprocate by cooperating. 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.”

Like all imposter scams, the 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. By claiming the problem is urgent, impostors give consumers no opportunities to cognitively process the situation rationally. Many consumers are running on adrenaline throughout the entire interaction. Some indicated that when the scam was over, 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 Cialdini’s six elements of persuasion, demands for *secrecy* were common. Impostors told consumers not to 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. 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. They coached consumers to deflect questions from concerned bank tellers and retail store employees.

Key takeaways from the quantitative analysis of consumer complaints

We also conducted a quantitative analysis of more than 200,000 consumer reports of the SSA imposter scam. Results show that older adults were significantly less likely to report victimization by this scam compared to younger adults. In other words, older adults were more likely than those in their 30s to file “no loss” reports compared to victim reports. That said, when victimization was reported, average losses were 40% to 93% greater for victims in their 70s and 80s compared to victims in their 30s, all else held equal. The FTC has observed similar age and median loss trends in the Sentinel data overall.

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 a quarter Hispanic are between 23% and 45% more likely to report victimization relative to communities that are less than 5%

Hispanic. Consumers residing in areas with greater than 5% Black residents are significantly more likely to report victimization by a magnitude of 14% to 50%. However, it could be that it takes losing money for members of these communities to decide to report the scam to the FTC, and that they are simply not bothering to report targeting attempts as much as non-Hispanic white communities.

Although the majority of victims paid the criminals using retail gift cards, victims who paid with cryptocurrency lost 140% more money, on average. Paying with cash and wire transfer resulted in the highest average losses—$13,000 and $18,000, respectively.

Applying a sentiment analysis to the case narratives to count emotion words, we found that consumers who used more words associated with the feelings of trust, anticipation, and anger were more likely to be victims than consumers who did not express those emotions.

Implications for consumer education and intervention

Based on what we learned from the qualitative analysis of case narratives, many consumers are unaware that official phone numbers can be spoofed. Consumers need more education about number spoofing and information that they cannot count on caller ID.

Second, the Federal Communications Commission must continue to demand that VoIP providers stop facilitating fraudulent robocall campaigns that target Americans. If these VoIP providers fail to take action, the FCC can have network operators block call traffic from those VoIP providers altogether. This solution is so important, because it stops the messages from reaching consumers in the first place.

Seventy percent of victims paid using retail gift cards. Many consumers do not recognize that this anonymous form of payment is like giving the criminals cash. Retail stores that sell gift cards should display large, visible warning signs about imposter scams in areas where gift card shoppers are most likely to encounter them. In addition to gift card sales kiosks, warning labels and signs may be placed at checkout lanes, at the register, near the pharmacy or customer service desk.

As part of an AARP-funded research project, my graduate students and I photographed warning signs at major retailers throughout Minnesota. Many of these signs were vague, too small, had significant wear and tear, were outdated (only warning customers to beware of the IRS imposter scam, for example). Others were placed above or below eye level. The best signs were large and stood out from the noise of the gift cards sales kiosk. Other signs helped interrupt the purchase altogether, like a warning message on the credit card reader. Given that the greatest losses were among those who paid with cryptocurrency and with wires, however, consumers also need to see warning messages on cryptocurrency ATMs and at financial institutions and businesses that provide wire transfer services.

A limitation of consumer education is that it puts the burden of protection on the targets of fraud. As we learned from this study, fraud targets are often in states of emotional distress. We need to do more to empower retail employees to step in and say something when they suspect a customer is being targeted by a fraud criminal and told to buy gift cards. Retail clerks and bank tellers need support from their managers to understand that it is perfectly reasonable to deny a transaction when red flags are present. They also need training on what to ask customers and how to respectfully talk them out of risky purchases.

In combination with consumer education and direct interventions by retail employees, gift card issuers, sellers, and payment processors can enforce stricter limits on gift card sales and use technology to identify when the card is being redeemed by a remote fraud criminal. Retail companies should also have pre-programmed gift card purchase thresholds: a lower dollar amount, such as $150, that would trigger a warning message on the register to prompt cashiers to ask *why* the customer is purchasing gift cards and

for whom, and also a purchase limit that customers cannot exceed. Importantly, employees should be trained to never work around gift card purchase limits by splitting the transaction.

Protecting consumers against government imposter scams will require a comprehensive, multipronged approach that includes more visible warning signs, training for retail employees and their supervisors to be proactive, and greater enforcement of anti-money laundering laws. We need to shine a spotlight on the gift card payments industry and VoIP providers for their roles in facilitating these frauds.

Government imposter scams have evolved and will continue to take new forms. Which federal agency will the criminals impersonate next? The earlier we can identify the next government imposter scam, the earlier we can warn consumers before the imposters get a foothold. We also need to be mindful of new and emerging payment methods, such as cryptocurrency transfers, that are increasingly a favorite among scammers.

I appreciate the opportunity to appear before the EJCC and will now take questions.

---

[i] DeLiema, M., & Witt, P. (2022). *Mixed-methods analysis of consumer fraud reports of the Social Security impostor scam.* UM21-Q1. University of Michigan Retirement and Disability Research Center. https://mrdrc.isr.umich.edu/pubs/mixed-methods-analysis-of-consumer-fraud-reports-of-the-social-security-administration-impostor-scam/

[ii] SimplyWise (January 2021). Retirement Confidence Index. SimplyWise Retirement Confidence Index | SimplyWise

[iii] Cialdini, R. B. (2021). Influence, New and Expanded: The Psychology of Persuasion. United States: HarperCollins.