School of Social Work
College of Education and Human Development

UNIVERSITY OF MINNESOTA
Driven to Discover®

WRITTEN TESTIMONY OF DR. MARTI DELIEMA

submitted to the

UNITED STATES SENATE
SPECIAL COMMITTEE ON AGING
on

Stopping Senior Scams: Empowering Communities to Fight Fraud

September 22, 2022

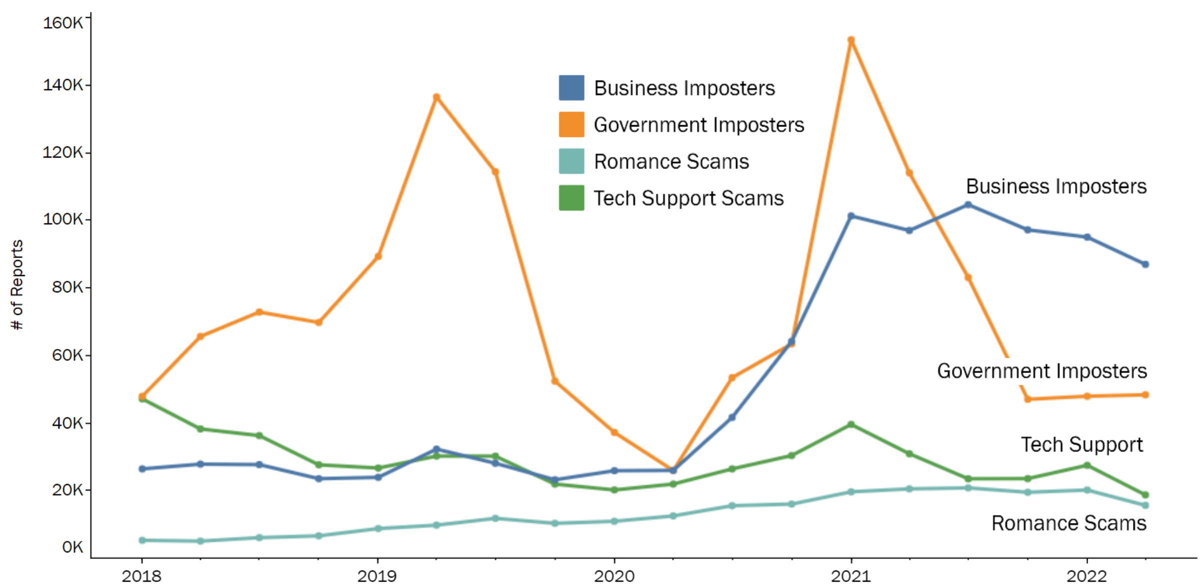
Marti DeLiema, PhD
Assistant Professor
University of Minnesota School of Social Work
mdeliema@umn.edu

Good morning. Thank you, Chairman Casey, Ranking Member Scott, and members of the Committee. My name is Dr. Marti DeLiema and I am an Assistant Professor at the University of Minnesota School of Social Work. I conduct research on consumer fraud and strategies to safeguard older Americans' financial security.

You have invited me today to describe current trends in consumer scams affecting older adults. I will start by stating the fraudster's playbook is in constant evolution. While core persuasion tactics remain the same, perpetrators routinely experiment with new storylines, new entities to impersonate, and new contact methods to outcompete consumer education and law enforcement efforts. Anyone, regardless of age, may be targeted by fraud, and many consumers are bombarded by fraud attempts multiple times a day.

We can use consumer complaint data compiled by the Federal Trade Commission (FTC) to explore current trends. Government imposter scams have been in the top five most reported categories of fraud affecting older adults for multiple years in a row,[1] but the government agency being impersonated has changed over time— the IRS, SSA, FBI, CMS, USPS, and so on. The challenge is to predict which agency's clothes the perpetrators will try on next, and to create consumer education campaigns that are robust to these changes.

Figure 1. Prevalence of imposter scams reported by consumers, 2018 - 2022 Q1, Q2



Data source: Federal Trade Commission Consumer Sentinel. (2022). Available at https://public.tableau.com/app/profile/federal.trade.commission/viz/TheBigViewAllSentinelReports/TopReports

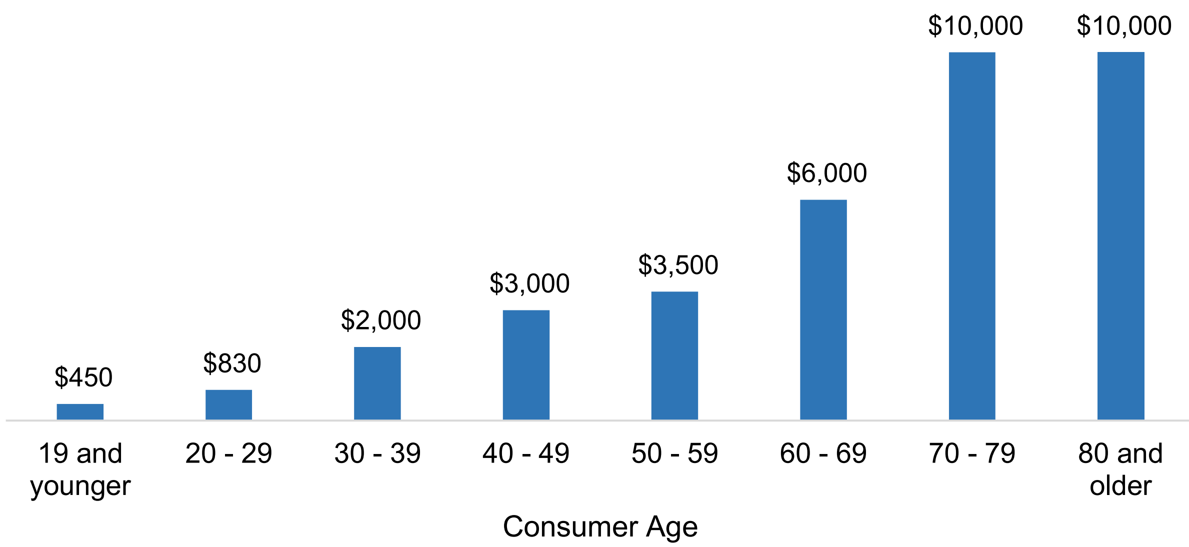
Throughout the pandemic, business impersonation scams grew exponentially, particularly retail company-imposters. Some of these scams start with a text message, a solicitation method that is much harder for consumers to authenticate. As online purchasing took off in response to social distancing, perpetrators took advantage of Americans' fear, confusion, and supply chain

[1] Federal Trade Commission (2022). *Age and fraud loss infographic.* Available at https://public.tableau.com/app/profile/federal.trade.commission/viz/AgeandFraud/Infographic

shortages by using a rash of online shopping scams. Older Americans, some with limited technological proficiency before the pandemic, turned to their personal computers and other digital devices to stay connected. Once again, scammers seized this opportunity to perpetrate new variations of the tech support scam.

Romance scams lead the pack in terms of personal financial costs. In a study I conducted with the FTC, we found that median reported losses for consumers in their 70s and 80s were $10,000, quadruple the losses reported by young adults. Romance scams can go on for many months, and perpetrators not only rob survivors of their retirement security, they completely shatter their social and emotional well-being.

Figure 2. Median reported losses for romance scams by consumer age, Nov 2020-Apr 2022

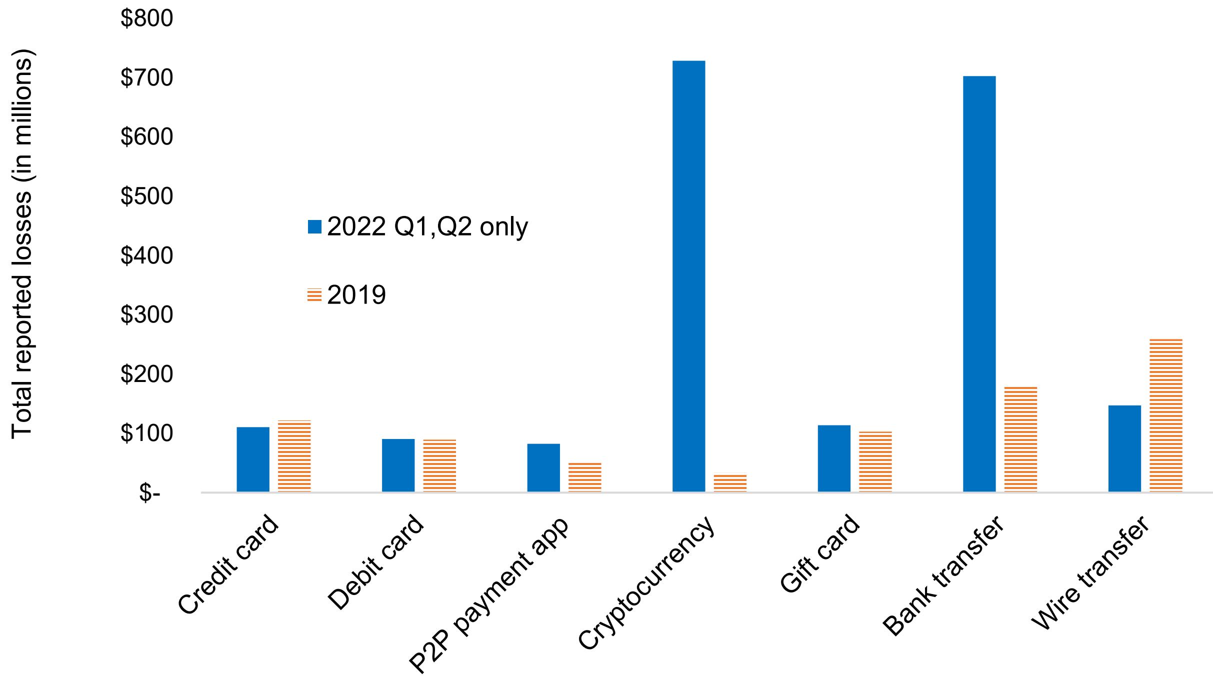


Data source: DeLiema, M., & Witt, P. (2022). Profiling consumer fraud reporters: Demographic characteristics and emotional sentiments associated with victimization. Available upon request from mdeliema@umn.edu.

In 2019, wire transfer was both the most common method of money transfer, and was associated with the highest losses. Today, credit cards are the most common method overall, but bank transfer and cryptocurrency are the clear frontrunners in terms of dollars lost. Together, these money transfer methods account for almost $1.5 billion in reported losses, more than double the losses from all other payment methods combined. While this is a great deal of money, research indicates that fewer than 3% of consumers report to law enforcement,[2] so true costs are many magnitudes higher.

[2] 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

Figure 3. Total reported losses by payment method in 2019 versus 2022 (Q1, Q2 only)



Data source: Federal Trade Commission Consumer Sentinel. (2022). Available at https://public.tableau.com/app/profile/federal.trade.commission/viz/FraudReports/FraudFacts

If we shine a spotlight on adults age 60 and older, gift cards are the most common money transfer method. They are used in a wide variety of scams, from government imposter to prize, sweepstakes, and lottery fraud. Gift cards are favored by perpetrators because they are easily available to consumers, anonymous, instantly redeemable, and have very few controls.

AARP recently conducted a survey and discovered that one third of respondents were targeted by a scam demanding gift cards. Of those who were targeted, a quarter complied with the scammers' request. In gift card-facilitated frauds, retail sales clerks are often the only individuals in position to intervene. In my research supported by AARP, my graduate students and I interviewed retail store managers from around the U.S., surveyed cashiers, and visited local stores to document what is being done to educate and protect customers.[3] We found that most major retailers had some type of signage warning customers about gift card scams, but the messages were typically small, placed out of eye level, or were nearly invisible in the sea of cards competing for shoppers' attention. Less than half of surveyed cashiers reported there were any limits on purchase amounts. The store managers we interviewed said they have not received any formal training from their employers on how to detect scams or how to effectively intervene. Ultimately, they said that they are not authorized to deny a gift card purchase if the customer is

[3] DeLiema, M., Sagnes, M., Hanson, W., & Bailey, D. (2021). Protecting Retail Customers from Gift Card Payment Scams: A Three Part Investigation. Report prepared for AARP. Available upon request from mdeliema@umn.edu.

insistent, even if they are certain the customer is involved in a scam. As the saying goes in retail: "customer is king."

In light of these findings, I believe that more education for frontline retail employees is warranted, but more importantly, we need to demand action from the gift card payments industry, including payment processors and card issuers. These entities can determine when money is loaded onto gift cards by customers in stores, and then redeemed immediately by scammers in remote locations. Additional controls might include temporary holds on suspicious attempts to redeem high-value cards remotely. This would give customers more time to identify and report fraud. Lower transaction limits could also reduce loss amount and make gift cards far less attractive to scammers.

Fraud victimization exacts a significant social, economic, and financial toll

Reports of consumer fraud have risen substantially every year, and so have the costs. But true costs extend beyond personal financial losses. In my research analyzing consumer complaints and in interviews with fraud survivors, I learn about survivors' feelings of shame, self-blame, anxiety, estrangement from friends and family members, and even thoughts of suicide. We have yet to quantify the societal and economic impact of fraud including diminished consumer trust in retail companies, in financial institutions, and in law enforcement's ability to bring criminals to justice and provide redress to those who are harmed.

Policy recommendations and future directions

What steps can we take to protect older Americans from fraud? Consumer education is critical. Research has shown that educating individuals about scams in advance of them being targeted significantly reduces the risk of victimization.[4,5] In other words, "forewarned is forearmed." However, we cannot ask individuals to shoulder the burden of consumer protection alone. Scams will continue to take new forms, and we will never be able to warn every consumer about every new variant of fraud.

In conjunction with education, we need the private sector to step up to help safeguard Americans. We are fortunate to sit in a rare area of policymaking where consumers, along with public and private sector entities, all want the same thing—to stop criminals from taking advantage of Americans and eroding consumer trust. Legislation, such as the TRACED Act, is a fantastic example of how phone companies, with help from Congress, can limit unwanted and fraudulent robocalls from ever reaching consumers. We need similar solutions applied to other methods of contact used by perpetrators, from bogus text messages to fake social media profiles. As a second line of defense, we need to expand the Senior Safe Act to encourage financial institutions to act quickly by placing temporary holds on suspicious transactions and reporting elder fraud to the proper authorities.

[4] DeLiema, M., Li, Y., & Mottola, G. R. (2021). Correlates of Compliance: Examining Consumer Fraud Risk Factors by Scam Type. Available at SSRN: https://ssrn.com/abstract=3793757
[5] Scheibe, S., Notthoff, N., Menkin, J., Ross, L., Shadel, D., Deevy, M., & Carstensen, L. L. (2014). Forewarning reduces fraud susceptibility in vulnerable consumers. *Basic and applied social psychology*, *36*(3), 272-279.

Last, based on what we are seeing in the most recent reporting data, cryptocurrency is playing an outsized role in today's fraud landscape. Consumer fraud thrives in complex environments, and cryptocurrency has created a playground for international scammers.

Ultimately, we need greater investment in fraud detection within the private sector; for companies to be proactive when fraud is suspected instead of reactive when the money is already gone. In addition, consumers need evidence that their complaints are taken seriously by law enforcement and that by reporting, recovery and redress are possible. Only through a coordinated response from policymakers, companies, law enforcement, and consumer protection advocates can we outsmart the criminals who prey on American consumers.