Testimony of

Odette Williamson

National Consumer Law Center

On

"Frauds, Scams and COVID-19: How Con Artists Have Targeted Older Americans During the Pandemic"

Before the

United States Senate

Senate Special Committee on Aging

September 23, 2021

Testimony of Odette Williamson, National Consumer Law Center
Before the United States Senate
Senate Special Committee on Aging
Regarding
"Frauds, Scams and COVID-19: How Con Artists Have Targeted
Older Americans During the Pandemic"
September 23, 2021

I. Introduction

Mr. Chairman, Ranking Member Scott, and Members of the Special Committee on Aging, thank you for inviting me to testify today regarding the fraudulent financial practices and scams aimed at older adults during the COVID-19 pandemic. I offer my testimony on behalf of the low-income clients of the National Consumer Law Center.

The National Consumer Law Center uses its expertise in consumer law and energy policy to work for consumer justice and economic security for low-income and other disadvantaged people, including older adults and people of color. NCLC's resources and expertise include policy analysis and advocacy; consumer law and energy publications; litigation; expert witness services; and training and advice for advocates. NCLC works with nonprofit and legal services organizations, private attorneys, policymakers, federal and state government and courts across the nation to stop exploitative practices, help financially stressed families build and retain wealth, and advance economic fairness. NCLC provides training to elder advocates through its annual conference and the National Center on Law and Elder Rights.

Reports of scams and fraudulent practices increased significantly during the COVID-19 pandemic. In 2020, the Federal Trade Commission ("FTC") received over 4.7 million reports of fraud, identity theft and other scams, an increase from the prior year.[1] Older adults were targeted by romance scammers, imposters, identity thieves and other fraudsters. While older adults were less likely to report losing money to scams than younger consumers, when they did report such loss the dollar amount was significantly higher. Consumers eighty years old and over reported a median loss of $1,300 to fraud in 2020, an amount two to four times the median loss reported for consumers in other age groups.[2] Taken together, consumers age 60 and over reported losing $592M to fraud during 2020.[3] This number underestimates the extent of the loss to older consumers as scams are significantly underreported.

All consumers are vulnerable to scams and fraudulent practices. Scammers may target older adults whom they suspect are lonely, isolated, confused or financially distressed. Widespread illness and death combined with the social isolation and distancing measures brought on by the

[1] Federal Trade Commission, *Consumer Sentinel Data Book* 2020, February 2021, at 5, available at https://www.ftc.gov/system/files/documents/reports/consumer-sentinel-network-data-book-2020/csn_annual_data_book_2020.pdf.
[2] Id. at 13 (for consumers age 20 and older).
[3] Id. at 13.

COVID-19 pandemic created fertile ground for the proliferation of certain scams primarily aimed at older adults. This includes romance scams and government imposter scams, which result in the highest monetary losses for older consumers.[4] High unemployment, the threat of eviction and economic uncertainty put other consumers at risk as they searched for government programs or financial assistance. Low-income older adults living on fixed or limited income in particular are vulnerable to identity theft and other scams as they seek financial relief and government assistance.

Fraudulent practices and scams impact every community. Older adults in communities that are racially, ethnically or linguistically isolated are particularly at risk. The FTC Fraud Surveys, for example, found that Latinos experience higher rates of fraud than other populations.[5] This includes government imposter scams, multi-level marketing and pyramid schemes advertised in both English and Spanish, fake job opportunities, and fake immigration assistance schemes.[6] Limited English proficient (LEP) elders are exposed to scams in their own language, and may lack in-language information from reputable sources.[7] Scammers purchase ads on Spanish language radio and other ethnic media to exploit misinformation and confusion regarding COVID-19 treatment, vaccines, and related financial assistance. These populations have long been at risk for fraud. A 2017 FTC survey revealed that 19.2% of African Americans, and 17.3% of Hispanic consumers were victims of fraud, compared to 14.9% of non-Hispanic white consumers.[8] Given the disproportionate impact of the pandemic on communities of color, we expect to see a further uptick in frauds and scams.

Despite the proliferation of these fraudulent schemes older adults face structural and other barriers to reporting scams to law enforcement and other authorities. Older adults with diminished capacity may not recognize that they have been scammed, and are at high risk for revictimization if the perpetrator shares the victim's name with other scammers. Other victims may be embarrassed, or worry that exposing the scam may lead to a loss of independence if they are perceived as incapable of handling their financial affairs. Many scams are reported by third parties, including family members, friends and caregivers on behalf of the elder. The elder's separation from family and friends during the pandemic may mean that the scam goes undetected, or discovered long after money is transferred to the scammer. Moreover, to the extent that scams have moved online, employees at financial institutions are not able to report suspicious activities or warn elder customers of possible fraud.[9]

---

[4] *See* Federal Trade Commission, Report to Congress, *Protecting Older Consumers, 2019-2020*, October 2020, at 8, 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

[5] Vaca, Monica, et al., *Protecting Latino Communities, Information from the FTC*, NACA Webinar Series, September 2020, at slide 8.

[6] Id. at 12-15.

[7] *See, e.g., HUD files charge alleging California foreclosure rescue companies scammed Hispanic homeowners*, HUD archives, HUD No. 16-002 (Jan. 12, 2016), https://archives.hud.gov/news/2016/pr16-002.cfm.

[8] Anderson, Keith, *Mass-Market Consumer Fraud in the United States: A 2017 Update*, Federal Trade Commission, Bureau of Economics, October 2019, at --, available at https://www.ftc.gov/system/files/documents/reports/mass-market-consumer-fraud-united-states-2017-update/p105502massmarketconsumerfraud2017report.pdf.

[9] *See Suspicious Activity Reports on Elder Financial Exploitation: Issues and Trends*, Consumer Financial Protection Bureau, Office of Older Americans, February 2019.

The impact of financial fraud and scams on older adults is devastating. Depending on the amount of money or assets taken, older adults can fall into poverty or homelessness. Older adults may be forced to rely on family members and friends, or need government assistance. Unlike their younger peers, older adults have less time and resources to rebuild their nest egg or otherwise recover financially from the scam. Financial scams also impact the emotional and physical health of victims as they struggle to live with fewer resources for food, medicine, housing and other basic necessities. The financial strain and embarrassment may cause older victims to become fearful, depressed or even suicidal.

Scams are perpetrated by a wide variety of individuals and businesses, including family members and caretakers. This testimony focuses on scams perpetrated by strangers and businesses rather than financial exploitation by family members, caretakers or trusted advisors, although the scams may be the same or share similar features.

II. Scams Aimed at Older Consumers in the Age of COVID-19

Scams aimed at older adults include a wide range of illegal behavior from imposter scams to mortgage fraud. Individuals perpetrating scams follow the headlines closely. With the emergence of COVID-19, fraudsters began marketing fake treatments, cures, and products with unsubstantiated health claims aggressively to consumers. Other types of COVID-related scams evolve month to month or year to year depending on issues highlighted in the media. When the Internal Revenue Service (IRS) distributed the Economic Impact Payments, for example, scammers impersonating agency officials contacted consumers with fake offers of assistance.[10] Other scammers impersonated IRS officials to demand payment and threaten arrest. Within days of the announcement of the Federal Emergency Management Agency's COVID-19 Funeral Assistance Program, scammers offered grieving relatives access to the program for a fee and solicited personal information.[11] These COVID-19-specific scams join the roster of scams that disproportionately impact older adults year after year. This includes prize, sweepstakes, and lottery scams, charity fraud, work from home schemes, and family and friend impersonation scams.[12]

Most scams aimed at older adults are perpetuated over the telephone, including through robocalls and texts to cell phones. Upon gaining the trust of the older adult, the scammer requests money or personal information. Money is transferred via gift cards, wire transfer, peer-to-peer ("P2P") platforms and other means. Personal financial information is used to access the consumer's bank account, open credit card accounts or create other fake accounts in the consumer's name. Scams are also promoted heavily through email and online phishing scams, social media and direct mail. Older adults with special types of assets (e.g., homes, pension plans) may be targeted for particular types of scams. Common types of scams include:

---

[10] *See*, Internal Revenue Service, *IRS Warns about COVID-19 Economic Impact Payment Fraud*, available at https://www.irs.gov/compliance/criminal-investigation/irs-warns-about-covid-19-economic-impact-payment-fraud.

[11] *See* Gressin, Seena, *Scammers target loved ones of COVID-19 victims*, Federal Trade Commission, Feb. 2021, available at https://www.consumer.ftc.gov/blog/2021/04/scammers-target-loved-ones-covid-19-victims.

[12] *See* Federal Trade Commission, Report to Congress, *Protecting Older Consumers, 2019-2020*, October 2020, at 3, 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.

Fake COVID-19 Treatments, Vaccines and Tests

Consumers report companies offering fake vaccines and products to cure, treat or prevent COVID-19 to regulators who often take swift action to stop these false claims or shut down the companies.[13] However, given the volume of scam products and treatments and diversity of companies, consumers lose money to these companies. These products may also put consumers' health at risk if they delay treatment based on companies' fraudulent claims and promises. Other scammers pretend to be contact tracers affiliated with state departments of public health and send text messages with embedded links that allow them to access personal and financial information on the consumer's device if the consumer clicks on the link.[14] Some scammers even offer fake COVID-19 antibody tests.[15]

Imposter Scams

An imposter scam involves an individual pretending to be someone else to get money or personal information from a consumer. Government imposters trick older adults into disclosing personal or financial information by offering assistance in obtaining health or government benefits. Others extract personal information through a fake verification process by pretending, for example, to investigate fraudulent activity on Social Security accounts.[16] Imposters also pose as family members or employees of well-known businesses. Popular scams include offers of technical support to fix non-existent computer problems by individuals claiming affiliation with well-known technology companies. Other imposters pose as family members, such as grandchildren in need of emergency financial assistance. Romance scams occur when scammers adopt a fake identity to gain a victim's affection and trust. The scammer then uses the illusion of a romantic or close relationship to manipulate and steal money from the victim. Older adults suffer the greatest financial loss due to romance scams and imposter scams, including those where the scammer poses as a government official.[17] These scams are on the rise as older adults seek resources and assistance from government agencies to weather the pandemic.

---

[13] *See, e.g.*, Federal Trade Commission, *Report to Congress, Protecting Older Consumers, 2019-2020*, October 2020, at 29-32, 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; U.S. Food and Drug Administration, *Fraudulent COVID-19 Products*, available at https://www.fda.gov/consumers/health-fraud-scams/fraudulent-coronavirus-disease-2019-covid-19-products.

[14] *See* Walker, Shameka, *Help COVID-19 Contact Tracers not Scammers*, Federal Trade Commission, June 2020, available at https://www.consumer.ftc.gov/blog/2020/06/help-covid-19-contact-tracers-not-scammers.

[15] *See* Federal Bureau of Investigation, *FBI Warns of Potential Fraud in Antibody Testing for COVID-19*, June 2020, available at https://www.fbi.gov/news/pressrel/press-releases/fbi-warns-of-potential-fraud-in-antibody-testing-for-covid-19.

[16] Social Security Administration, FAQ: What should I do if I get a call claiming there is a problem with my social security card or account?, December 2020, available at https://faq.ssa.gov/en-us/Topic/article/KA-10018.

[17] *See* Federal Trade Commission, Report to Congress, *Protecting Older Consumers, 2019-2020, October 2020*, at 8, 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.

Identity Theft

Older adults unwittingly disclose financial and personally identifiable information (e.g., date of birth, social security number) to government imposters and other scammers. Disclosure of this sensitive information leads to identity theft, the unauthorized access and use of an elder's financial or personal information. This may lead to credit card fraud, tax fraud and other financial scams. With tax-related identity theft, for example, scammers file fraudulent tax returns using stolen Social Security numbers to claim victims' Economic Impact Payment and unemployment benefits.[18] A person's identity is also stolen as a result of phishing or other online scams; a lost or stolen wallet or purse; a data breach at a financial institution, retailer or other business; high tech skimming of credit card information with a tool during a legitimate business transaction; or a dishonest employee's appropriation of a customer's information.[19] In 2020 the FTC received 406,375 complaints from consumers who reported that their information was misused to apply for a government document or benefit, such as unemployment insurance.[20]

Home and Mortgage-Related Scams

Older homeowners in financial distress due to the COVID-19 pandemic may be targeted by scammers promising access to federal or state anti-foreclosure programs or assistance obtaining relief from the mortgage company in exchange for an up-front fee. Unfortunately, these foreclosure rescue scammers provide little or no service, and disappear with the money, leaving the homeowner in a worse position with little time to save the home. The frequency and type of mortgage-related scams varies with changes in the real estate market.[21] With property values rising, financially distressed homeowners are likely to have equity in their property and scammers will focus on stealing that equity through a variety of equity-theft schemes. Homeowners also lose money to home improvement scams, and scams related to utilities and energy-efficiency upgrades. Information on homeownership and homes in foreclosures is obtainable from publicly-available databases, making it easy for scammers to tailor their solicitation to appeal to older consumers.

---

[18] *See* Internal Revenue Service, *IRS Warns about COVID-19 Economic Impact Payment Fraud*, available at https://www.irs.gov/compliance/criminal-investigation/irs-warns-about-covid-19-economic-impact-payment-fraud

[19] Even sharing a picture of a COVID-19 vaccination card online can lead to identity theft. See Gressin, Seena, *Social media is no place for COVID-19 vaccination cards*, Federal Trade Commission, Feb. 2021, available at https://www.consumer.ftc.gov/blog/2021/02/social-media-no-place-covid-19-vaccination-cards.

[20] *See* Federal Trade Commission, Consumer Sentinel Network, Data Book 2020, at 4, available at https://www.ftc.gov/system/files/documents/reports/consumer-sentinel-network-data-book-2020/csn_annual_data_book_2020.pdf.

[21] Gov't Accountability Office, *Foreclosure Rescue Schemes Have Become More Complex, and Efforts to Combat Them Continue*, GAO-14-17 (Oct. 29, 2013) (finding "[f]oreclosure rescue schemes remain at historically high levels and have become more complex"), *available at* www.gao.gov; Creola Johnson, *Stealing the American Dream: Can foreclosure-rescue companies circumvent new laws designed to protect homeowners from equity theft?*, 2007 Wis. L. Rev. 649, 656–659 (2007) (discussing how market conditions facilitate exploitation of vulnerable homeowners).

III. Older Consumers Have Limited Options for Recovering Money and Assets Lost to Scams and Financial fraud

With any type of financial scam, the money and assets that are depleted or stolen are difficult to recover. Quick action is necessary to recover money, if possible, and preserve elders' remaining assets. This includes reporting the scam to a law enforcement agency, the FTC through Reportfraud.FTC.gov, other consumer complaint hotlines, and the payment provider. Victims with impairments due to physical or mental disabilities may need the assistance of Adult Protective Services.

If the scam is discovered early the older adult and his or her advocate can try to secure bank accounts and stop or reverse charges, and examine credit card and other financial accounts for unauthorized access and charges. Victims of identity theft and other frauds can examine their credit reports for new and fraudulent accounts, and request a fraud alert or credit freeze from the three credit bureaus. The consumer can also contact the IRS and Social Security Administration to report the disclosure of sensitive financial information. If an older adult is hospitalized or otherwise incapacitated, family members can obtain permission to submit complaints on the person's behalf. To tamp down on the incidence of fraud older adults inundated with telemarketing calls can register their telephone number with the National Do-Not-Call Registry, maintained by the FTC.[22]

The most popular payment methods used by scammers to extract money from victims cannot be reversed, however. In 2020, of the fraud reports that identified a payment method, consumers sustained $311 million in losses to scammers through wire transfers, compared to $266 million through credit and debit cards combined.[23] Wire transfers are the same as sending cash and typically there is no way to reverse the transaction or trace the money, though the fraud should still be reported to the wire transmitter. In the unlikely event that a gift card's value has not been depleted, the card issuer may voluntarily block transfer of the money to the scammer if it receives a complaint. However, scammers are known for speed in redeeming gift cards and picking up money wired to them, and consumers are rarely able to retrieve such funds.

Despite the best efforts of the older adult and their advocate, money sent to a scammer may not be recoverable. Many scams are not discovered early, and the consumer's attempt to stop or reverse the payment is often too late or not possible. Finding the scammer, bringing a lawsuit and recovering a judgment is not practical for individual victims. Rather, consumers must rely on government enforcement actions against scam companies, or other companies that facilitated the fraud.[24] The FTC, for example, brought several actions against companies that processed payments for scammers, including a company that "laundered credit card payments for, and

[22] https://www.donotcall.gov/index.html.

[23] *See* Federal Trade Commission, *Consumer Sentinel Data Book* 2020, February 2021, at 11, available at https://www.ftc.gov/system/files/documents/reports/consumer-sentinel-network-data-book-2020/csn_annual_data_book_2020.pdf.

[24] *See, e.g.*, Federal Trade Commission, *Report to Congress, Protecting Older Consumers, 2019-2020*, October 2020, at 21, 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

assisted and facilitated" two tech support scam companies previously sued by the agency.[25] Financial services companies and other businesses must be proactive in spotting these scams, routinely monitoring for fraud, and putting protections in place to avoid the transfer of consumers' hard-earned money to scammers. They can deploy artificial intelligence and other technology to assist in this effort.

Even if money or assets are recovered it is unlikely to make the older adult financially whole. Therefore, older adults will need the support of legal services and social support organizations to navigate a post-scam financial reality. This includes assistance staving off eviction or foreclosure, termination of utilities, and pushing back against abusive debt collectors and help with other issues that arise for financially distressed consumers. More resources to legal services and other organizations to provide such assistance would benefit scam victims.

IV. Older Consumers Need Additional Protections from Scams and Financial Crimes

As highlighted above, scammers reach vulnerable consumers in multiple ways: in person, through the mail, online, through email, and via the telephone – either voice calls or texts. Most scams aimed at older adults are facilitated through the telephone. Common scams like social security verification scams, alerts that one's bank account has been hacked, and fake offers of credit are primarily conducted through robocalls over the telephone.[26]

A. Prevent use of the telephone system by scammers

One clear way to protect older consumers from these scams would be to make it harder for scammers to exploit consumers using the nation's telephone system. The Federal Communications Commission ("FCC") has already been working to require additional authentication of telephone calls by requiring implementation of the Stir/Shaken technology; allowing terminating telephone providers to refuse to accept telephone traffic from originating providers who do not register with the Robocall Mitigation Database (which requires the provider to certify to the FCC how it is implementing call-authentication mandates);[27] and requiring telephone providers to "know their customers" such that the providers are responsible for keeping bad actors from accessing the network.[28]

The steps taken to date and scheduled in the near future by the FCC will have meaningful impact. But much more needs to be done. NCLC has been advocating that Congress should pass additional protections for consumers from scam callers, including:

---

[25] Id.

[26] *Id.* at 10.

[27] *See, e.g.* Robocall Mitigation Database, *available at* https://www.fcc.gov/robocall-mitigation-database.

[28] *See, e.g.* FCC Fact Sheet, Numbering Policies for Modern Communications, et al. Further Notice of Proposed Rulemaking – WC Docket Nos. 13-97, 07-243, 20-67, IB Docket No. 16-155, July 15, 2021, *available at* https://docs.fcc.gov/public/attachments/DOC-374109A1.pdf.

- Clarify that the Telephone Consumer Protection Act's[29] protections against telephone solicitations include scam calls and improve the rights of action for violating those rules.
- Require telephone providers who have not fully implemented robust caller authentication assurances to post bonds before they are permitted to process calls through the telephone network.
- Limit the exemptions for fake charitable calls.
- Require that the Caller-IDs displayed on our telephones reflect the accurate name of commercial callers, as well as a bona-fide telephone number through which the caller can be reached during business hours.

NCLC is working with a bipartisan group of state attorneys general and members of Congress in the House and Senate on legislation to accomplish these and related goals.

B. Protect consumers from fraud in P2P payment systems, including in the coming FedNow system

Outside of limiting access to potential victims over the telephone, more protections are needed on the back end to give consumers a fighting chance of recovering money transferred to scammers. New payment platforms, such as the peer-to-peer ("P2P") payment platforms offered by PayPal (which owns Venmo), and Square (which owns Cash App) offer few protections.

Here is an example:

> Mary Jones of Kansas City paid $1,700 through Venmo in "rent" to a man who claimed to own the house she wanted to move into. He even gave her and her daughter access to tour the house before she signed the lease. After she saw a For Lease sign in the front yard she called the rental company and discovered that she had paid a scammer. She filed a police report but has not been able to retrieve her money.[30]

US PIRG noted in its recent report: that "[A]s consumers grow increasingly reliant on payment apps, more and more consumers are running into problems that cost them money and time. This is clearly evidenced by the explosion of digital wallet consumer complaints in the CFPB's Consumer Complaint Database over the past year."[31]

The Federal Reserve Board ("Fed") is in the middle of developing a new P2P instant payment system called FedNow, but the rules recently proposed replicate the problems of existing P2P payments systems by failing to provide consumers and other users with protection against fraud and consumer errors. A wide variety of stakeholders recently filed comments with

---

[29] Telephone Consumer Protection Act (TCPA), 47 U.S.C. § 227.

[30] Tia Johnson, *Kansas City woman warns others after losing nearly $2,000 in rental home scam*, Fox4, May 3, 2021, available at https://fox4kc.com/news/kansas-city-woman-warns-others-after-losing-nearly2000-in-rental-home-scam/.

[31] U.S. PIRG Educ. Fund, *Virtual Wallets, Real Complaints*, June 2021, at 9, *available at* https://uspirg.org/sites/pirg/files/reports/VirtualWallets/Virtualwallets_USP_V3.pdf.

the Fed pointing out the concerns about fraud and limited ability to reverse fraudulent payments.[32]

The Fed must make FedNow a model for other payment systems and must not value speed and convenience at the expense of safety. Consumers need protection against fraudulently induced payments and errors that are too easy to make in today's P2P systems. A single mistaken or fraudulent payment can be devastating to an individual. The financial system can absorb the costs of protecting consumers, spread those costs among participants, and work to make the system safer for all.

Payment system providers need to take responsibility for -- and do more to prevent -- the fraud that they allow into their systems. Whenever a P2P payment is sent, there is an account on the receiving end where the scammer receives the funds. Financial institutions and payment providers have a responsibility to know their customers, ensure that they are not using stolen identities, and prevent accounts from being used for illegal purposes. Putting the liability for fraudulent payments on the receiving institution rather than on the consumer will protect consumers from harm, provide confidence in payment systems, and create incentives for sophisticated measures to prevent and detect fraud.

Scammers are extraordinarily creative and are constantly developing creative ways to steal people's money. The FCC's website includes a Scam Glossary detailing dozens of different ways individuals have lost money to scams.[33] And P2P payments are specifically identified as a primary means for executing these scams.[34] The warnings provided by the payment apps that consumers should be aware of scams is not adequate to protect consumers from the losses.

As a group of 43 consumer and other nonprofit organizations recently wrote to the Fed about FedNow: "disclosures and warnings to consumers are an old-fashioned and ineffective method of consumer protection, especially in combating fraud, since fraudsters create and abuse trust. In this modern era of big data, artificial intelligence, and machine learning, payment systems that take responsibility for fraud will develop sophisticated, ever-improving methods of preventing, detecting and remedying it that are far more effective than warnings to consumers. For that to happen, however, the system needs to incorporate incentives for the financial services providers

[32] See these three sets of comments to Federal Reserve Board on Collection of Checks and Other Items by Federal Reserve Banks and Funds Transfers Through Fedwire, Docket No. R-1750; RIN 7100-AG16: Comments of 43 undersigned consumer, small business, civil rights, community and legal service groups (Sept. 9, 2021), https://www.nclc.org/images/pdf/banking_and_payment_systems/fintech/FedNow-coalition-comments-final.pdf; Comments of 13 financial industry, retail and consumer groups (Sept. 9, 2021), https://www.nclc.org/images/pdf/banking_and_payment_systems/fintech/Reg_J_Fed_Now_joint_comments.pdf; Comments of National Consumer Law Center, National Community Reinvestment Coalition, National Consumers League (Sept. 9, 2021), https://www.nclc.org/images/pdf/banking_and_payment_systems/fintech/FedNowNCLC-NCRC-NCL.pdf.

[33] Federal Communications Commission, Scam Glossary, *available at* https://www.fcc.gov/scam-glossary.

[34] Federal Communication Commission, *As More Consumers Adopt Payment Apps, Scammers Follow*, updated Feb. 25, 2021, *available at* https://www.fcc.gov/more-consumers-adopt-payment-apps-scammers-follow.

in the payments chain to design robust fraud and error prevention and remediation methodologies."[35]

Congress and the Consumer Financial Protection Bureau can also modernize the federal law that governs these payment platforms, the Electronic Funds Transfer Act ("EFTA"). [36] The EFTA, as currently implemented through Regulation E, has loopholes and ambiguities. In some instances, consumers may be protected by Regulation E. But if the consumer initiated the transfer or is viewed as having furnished the access device to the scammer, most financial institutions and P2P apps take the position that the consumer is unprotected.[37]

The EFTA was enacted over forty years ago. While Regulation E has been updated over the years, and most recently in 2019 to incorporate prepaid accounts, the statute and the regulation do not directly answer questions posed by today's P2P systems such as authorization requirements for one-time payments, fraudulently induced payments, or mistakes by consumers in new payment systems that were not contemplated in 1978. Relying on Regulation E as it currently exists to provide a bulwark of protection for consumers in P2P transactions will simply not work.

The EFTA and/or Regulation E need to be updated to provide protection against fraud in the inducement and consumer errors. Regulators must require the P2P platforms to investigate errors and fraud, even when the consumer sent the payment erroneously or as a result of fraud in the inducement; and P2P platforms should display a customer service telephone number and respond to customer service inquiries in a timely manner.

We also see far too many clear violations of existing rules, such as financial institutions failing to remedy unauthorized charges despite the fact that the EFTA puts the burden on financial institutions to show that a disputed payment was authorized and protects consumers even if they were negligent. The CFPB recently issued a set of FAQs,[38] and the Fed recently published compliance articles,[39] to address these issues. More oversight is needed to ensure compliance with the EFTA and to protect consumers' accounts.

---

[35] Comments of 43 undersigned consumer, small business, civil rights, community and legal service groups to Federal Reserve Board on Collection of Checks and Other Items by Federal Reserve Banks and Funds Transfers Through Fedwire, Docket No. R-1750; RIN 7100-AG16 (Sept. 9, 2021), https://www.nclc.org/images/pdf/banking_and_payment_systems/fintech/FedNow-coalition-comments-final.pdf.

[36] 15 U.S.C. §§ 1693 et seq.

[37] *See* Reg. E, 12 C.F.R. § 1005.2(m). While Regulation E requires financial institutions to investigate errors, and does not exclude errors committed by the consumer, many financial institutions refuse to investigate p2p errors or to help to resolve them, and virtually none protects consumers or small businesses from those errors.

[38] *See* CFPB, Electronic Fund Transfers FAQs, https://www.consumerfinance.gov/compliance/compliance-resources/deposit-accounts-resources/electronic-fund-transfers/electronic-fund-transfers-faqs/.

[39] Scott Sonbuchner, Examiner, Federal Reserve Bank of Minneapolis, Consumer Compliance Outlook, *Error Resolution and Liability Limitations Under Regulations E and Z: Regulatory Requirements, Common Violations, and Sound Practices,* Second Issue 2021, https://consumercomplianceoutlook.org/2021/second-issue/error-resolution-and-liability-limitations-under-regulations-e-and-z/.

Conclusion

Older adults who suffered the devastating health and economic consequences of the COVID-19 pandemic are now being targeted by unscrupulous businesses and individuals. Older consumers need the highest level of protection from fraud and scams. Government, businesses, and advocates must protect older adults from these devastating scams, and robustly prosecute those who have victimized consumers.

Thank you for the opportunity to testify today. I would be happy to answer your questions.