

**FRAUDS, SCAMS AND COVID-19:
HOW CON ARTISTS HAVE TARGETED OLDER
AMERICANS DURING THE PANDEMIC**

HEARING
BEFORE THE
SPECIAL COMMITTEE ON AGING
UNITED STATES SENATE
ONE HUNDRED SEVENTEENTH CONGRESS

FIRST SESSION

WASHINGTON, DC

SEPTEMBER 23, 2021

Serial No. 117-08

Printed for the use of the Special Committee on Aging



Available via the World Wide Web: <http://www.govinfo.gov>

U.S. GOVERNMENT PUBLISHING OFFICE

46-487 PDF

WASHINGTON : 2022

SPECIAL COMMITTEE ON AGING

ROBERT P. CASEY, JR., Pennsylvania, *Chairman*

KIRSTEN E. GILLIBRAND, New York
RICHARD BLUMENTHAL, Connecticut
ELIZABETH WARREN, Massachusetts
JACKY ROSEN, Nevada
MARK KELLY, Arizona
RAPHAEL WARNOCK, Georgia

TIM SCOTT, South Carolina
SUSAN M. COLLINS, Maine
RICHARD BURR, North Carolina
MARCO RUBIO, Florida
MIKE BRAUN, Indiana
RICK SCOTT, Florida
MIKE LEE, Utah

STACY SANDERS, *Majority Staff Director*
NERI MARTINEZ, *Minority Staff Director*

C O N T E N T S

	Page
Opening Statement of Senator Robert P. Casey, Jr., Chairman	1
Opening Statement of Senator Tim Scott, Ranking Member	3
PANEL OF WITNESSES	
Lois Greisman, Associate Director, Bureau of Consumer Protection, Federal Trade Commission, Washington, D.C.	5
Odette Williamson, Staff Attorney, National Consumer Law Center, Boston, Massachusetts	7
Kate Kleinert, Scan Survivor, Glenolden, Pennsylvania	8
Vee Daniel, President and CEO, Better Business Bureau Serving Upstate South Carolina, Greenville, South Carolina	10
CLOSING STATEMENTS FOR THE RECORD	
Closing Statement of Senator Robert P. Casey, Jr., Chairman	24
Closing Statement of Senator Tim Scott, Ranking Member	24
APPENDIX	
PREPARED WITNESS STATEMENTS	
Lois Greisman, Associate Director, Bureau of Consumer Protection, Federal Trade Commission, Washington, D.C.	31
Odette Williamson, Staff Attorney, National Consumer Law Center, Boston, Massachusetts	48
Kate Kleinert, Scan Survivor, Glenolden, Pennsylvania	60
Vee Daniel, President and CEO, Better Business Bureau Serving Upstate South Carolina, Greenville, South Carolina	64
QUESTIONS AND RESPONSES FOR THE RECORD	
Lois Greisman, Associate Director, Bureau of Consumer Protection, Federal Trade Commission, Washington, D.C.	69
Odette Williamson, Staff Attorney, National Consumer Law Center, Boston, Massachusetts	85
Kate Kleinert, Scan Survivor, Glenolden, Pennsylvania	91
ADDITIONAL STATEMENTS FOR THE RECORD	
AARP Government Affairs, Bill Sweeney, Senior Vice President	95
AARP Government Affairs, Stop Senior Scams Act Letter of Support, Bill Sweeney, Senior Vice President	97
ASOP Global, John B. Hertig, Board President	98

FRAUDS, SCAMS AND COVID-19: HOW CON ARTISTS HAVE TARGETED OLDER AMERICANS DURING THE PANDEMIC

THURSDAY, SEPTEMBER 23, 2021

U.S. SENATE,
SPECIAL COMMITTEE ON AGING,
Washington, DC.

The Committee met, pursuant to notice, at 9:30 a.m., via Webex, Hon. Robert P. Casey, Jr., Chairman of the Committee, presiding.

Present: Senators Casey, Gillibrand, Blumenthal, Rosen, Kelly, Warnock, Tim Scott, Collins, Braun, and Rick Scott.

OPENING STATEMENT OF SENATOR ROBERT P. CASEY, JR., CHAIRMAN

Chairman CASEY. Good morning, everyone. The Senate Special Committee on Aging will come to order. Today, the Committee convenes a hearing to learn about how COVID-19 left older Americans more vulnerable to frauds and scams.

In the early days of the pandemic, many seniors isolated themselves in an effort to avoid contracting the virus but in the process were cutoff from family and friends. Fraudsters saw an opportunity, and they pounced. They preyed on the fear and the uncertainty surrounding the disease as well as the loneliness and isolation that resulted from the pandemic. People were longing for human contact, and a friendly voice on the phone or a beckoning message on Facebook, that became harder to turn away from, all of that. At the same time, without regular contact with friends and family, it was easier for small scams to balloon into big scams.

Still today, 18 months into the pandemic, Federal agencies, State governments, and advocates warn of con artists who will do all of the following: Number one, peddle fake cures for the Coronavirus, Number two, charge outrageous prices for protective equipment, and third, seek to steal stimulus checks and unemployment benefits. These types of scenarios, which are exacerbated by the pandemic, are not hypothetical.

Today, the Committee will hear testimony from Kate Kleinert. Kate is a resident of Glenolden, Pennsylvania, in Delaware County, southeastern Pennsylvania. Last year, Kate survived a scam in which a con artist defrauded her of tens of thousands of dollars.

I want to thank Kate for being with us today. I will introduce her later, more formally. Also, I want to say to Kate and to so many others who come here to Congress to testify about something

that has happened to them personally, that is an act of courage and sharing her story will help others.

The Federal Trade Commission's data shows that Kate was not alone in the experience that she endured. A theme we will hear from Kate and our other witnesses today is the importance of education in stopping frauds and scams before they start.

Stories like Kate's are why I reintroduced the bipartisan Stop Senior Scams Act with Senator Moran, Senate Bill 337. I want to thank Ranking Member Scott for cosponsoring the bill and others who are working with us. This bill will create an advisory committee to ensure that banks and other businesses have the information and tools they need to train their employees to spot, and to speak up about, possible senior scams.

I was also pleased that the American Rescue Plan that was passed by Democrats in March of this year included funding for the Elder Justice Act to support programs to combat elder abuse, enhance adult protective services, and more. This is one of the many programs that serve as frontline defenses against elder financial exploitation and abuse.

In addition, the Aging Committee's annual Fraud Book, here is the book I am referring to. This is this year's edition. This provides tips on how older Americans can avoid being scammed. This Fraud Book also provides lists of consumer watch dogs and law enforcement agencies that can help people who believe they or someone they love may have been scammed. Starting today, this 2021 Fraud Book—the Committee's 2021, I should say, Fraud Book, will be available for download on the Aging Committee's website, at www.Aging.Senate.gov.

In 2013, the Aging Committee started its toll-free Fraud Hotline with the goal of making it easier for seniors to report fraud and to seek assistance. Since that time, since 2013, the Committee has received thousands of calls, and the hope is that the hotline provides the caller with helpful advice, but it also helps the Committee keep a pulse on the types of threats that older Americans are facing. For people listening at home, the Fraud Hotline toll-free number is 1-855-303-9470. I will say that again, 1-855-303-9470.

This hotline would not be possible without the efforts of frontline staff receiving these calls and providing advice, which is hard and often heartbreaking work. To that end, I would like to thank Jose and Jasmine on my staff for their efforts to keep the Fraud Hotline up and running.

This the first time that Ranking Member Scott and I have released the Fraud Book together, and I think I can say on his behalf that we are proud to do that and proud to join those who have worked on this on the Committee for many years.

One final point, today's hearing will include Senators participating both virtually and in person, and I guess it is the second time we have done that. We also have votes coming up. We are hoping to get through at least opening statements by witnesses after Ranking Member Scott's statement, and then we will see where we are with voting and determine whether we should take a brief recess so we can vote and then come back and continue the hearing.

I want to thank our witnesses and others who made this hearing possible, and with that, I will yield and turn to our Ranking Member, Senator Tim Scott.

**OPENING STATEMENT OF SENATOR
TIM SCOTT, RANKING MEMBER**

Senator TIM SCOTT. Thank you, Mr. Chairman. Thank you for holding such an important hearing. There is no doubt about it that during a pandemic the last thing you want to hear about are frauds and scams, especially fraudsters, scammers who focus on our senior population in their golden years. It is just disgusting and heartbreaking to hear so many stories from so many seniors who have had to deal with the challenges of fraud.

I thank you for your bipartisan leadership. Often people look around our country and wonder if anything works in Washington in a bipartisan fashion. I would say that with your leadership we are not working in a bipartisan fashion; we are just working in an American fashion. We are putting the priorities of Americans before anything else.

When it comes to our seniors, I think it is really important for us to continue to focus on ways to make sure that our seniors appreciate the fact that the leadership here are servant leaders, focusing on how we make sure that the fraudsters and the scammers that are taking advantage of too many of our seniors, that stops and that there are ways for us to deal with those challenges.

I do appreciate the fact that we have a Fraud Hotline that I think everyone should hear once again. It is 855-303-9470. I say that because so many times, and there are so many situations and scenarios, where our seniors face scams. The older you get, the more isolated sometimes too many of our seniors become and the more they face the challenges of scammers.

There are a couple of ones that I want to point out. One is the romance scam. Just deplorable, frankly, from my perspective. I know that so many people in their golden years lose a loved one or become widows or widowers, and they are faced with something called the romance scam. In 2020, romance scams reached \$304 million in losses, a 50 percent increase from 2019. What is in common is the fact that in the middle of the pandemic seniors were isolated and lonely and maybe more susceptible to this type of fraud and this type of scam.

Congress can do its part to help, and I thank again Chairman Casey for the bill, the Stop the Senior Scams Act. It creates an advisory group to educate industry employees on how to identify and prevent scams targeting our seniors.

Forced isolation because of COVID makes our seniors so much more vulnerable. I think of one in particular in South Carolina. The romance fraud claimed 250 victims, who suffered losses in excess of \$4 million in 2020. A lovely lady, Judy, 66 years old, in South Carolina, a widow, began a relationship with a man over social media. He slowly gained her trust and then swindled her out of her resources. Ten thousand dollars, a senior on a fixed income lost to this scam.

Today, we are releasing, as the Chairman noted, the 2021 Fraud Book. This is such an important guide that could help our seniors avoid such challenging situations.

In 2020, the FBI Internet Crime Complaint Center received over 791,000 complaints; 28 percent of the victims were over the age of 60. This resulted in approximately \$1 billion in losses to our seniors.

A constituent of mine from Columbia, South Carolina, shared that she received a phone call from someone pretending to be her grandson. She did what most grandmothers would do. She called her grandson back and tried to verify that it was him. This car accident that supposedly he was in, that required an immediate wire of money, \$5,012. She wired the criminal scammers when she could not get in touch with her grandson. Unfortunately, these types of fraud, are very common. In 2020, the grandparent scam was the fifth most reported type to our Committee's Fraud Hotline.

Education and greater awareness are the best ways to make seniors informed consumers. That is why I am proud of what we have in South Carolina called Project Hope, helping our precious and elderly. Based in Richland County, South Carolina, Project Hope partners retired law enforcement volunteers with our seniors. They check in on a weekly basis, and they make sure that they are very aware of the potential scammers out there and making sure that they create a firewall between the scammers and our seniors. I am so thankful that there are dedicated men and women of our law enforcement community, the men and women of blue, who retire and still have a passion for people, find a new way to serve their communities in Richland, South Carolina.

I am also thankful to the Chairman and for the National Senior Fraud Awareness Day, which this year was May 13, 2021. This day will continue to help raise awareness about the increasing number of scams targeting our seniors.

Finally, let me just say to the former Chairwoman of this Committee, Susan Collins, who has been a strong leader on this issue of fraud and scams, I thank her for her leadership.

I look forward to hearing the testimonies from our witnesses today. I want to thank each and every one of you for participating in this critical and very important meeting.

I yield back, Mr. Chairman.

Chairman CASEY. Thank you, Ranking Member Scott. I want to acknowledge, as we will throughout the hearing, members as they appear. For those seeing this on television or listening, we have members of the Committee in the room, but the witnesses are remote, and wanted to acknowledge first Senator Rosen who has joined us virtually.

Let's move now to our witnesses. Our first witness is Ms. Lois Greisman. Ms. Greisman is the Associate Director of the Bureau of Consumer Protection at the Federal Trade Commission, where she heads the Agency's Division of Marketing Practices. Ms. Greisman has dedicated much of her professional career to combating fraud and working within the Federal Trade Commission to hold these scammers accountable. Today, Ms. Greisman leads the Commission's law enforcement initiatives tackling frauds and scams. She also serves the Commission's Elder Justice Coordinator.

Our second witness is Ms. Odette Williamson. Ms. Williamson's career has been dedicated to protecting consumers and combating elder abuse. She currently works as a staff attorney at the National Consumer Law Center in Boston, Massachusetts, where she works on issues of consumer justice and economic security. Previously, Ms. Williamson served as the Assistant Attorney General in the Massachusetts Office of the Attorney General of the State, where she enforced consumer protection laws and served on the Elder Law Advocates Strike Force.

Next, I will turn to Ranking Member Scott to introduce our next witness, Mrs. Vee Daniel.

Senator TIM SCOTT. Thank you, Mr. Chairman.

It is my pleasure to introduce Mrs. Vee Daniel from Spartanburg, South Carolina. Mrs. Daniel has been President and CEO of the Better Business Bureau serving the upper State of South Carolina since 2011. The Better Business Bureau is a non-profit serving 10 counties in the upper part of the State. They work with the public, including military service members and seniors, to help consumers find businesses they can trust. They also investigate and call out substandard marketplace behavior.

During the COVID-19 pandemic, their senior hotline received calls asking about various COVID-related products and claims. The Better Business Bureau was able to inform callers of the scams.

During Mrs. Daniel's tenure, the BBB also created and implemented programs to help seniors better protect themselves against frauds and scams. I look forward to hearing about this program and the great work the Better Business Bureau does to support seniors.

Mrs. Daniel, we thank you for your passion, your commitment, and your service to seniors. Thank you for taking the time to talk with us today, and I look forward to hearing your whole testimony.

Thank you, Mr. Chairman.

Chairman CASEY. Thank you, Ranking Member Scott.

Finally, I am pleased to introduce Ms. Kate Kleinert,

Kate, who is a resident of Glenolden, Pennsylvania. That is, as I mentioned, Delaware County, in the southeastern corner of our State. Kate retired from her career as an executive secretary for various businesses to take care of her late husband, Bernie, and currently manages public relations for a local author. Over the pandemic, Kate became a survivor of a scam and is now sharing her story to help others understand the emotional and financial toll the scams can take.

Let us now move to the witness statements. We will begin with Ms. Greisman.

Ms. Greisman, you may begin.

**STATEMENT OF LOIS GREISMAN, ASSOCIATE DIRECTOR,
BUREAU OF CONSUMER PROTECTION,
FEDERAL TRADE COMMISSION, WASHINGTON, D.C.**

Ms. GREISMAN. I am Lois Greisman. I appreciate the opportunity to discuss the FTC's initiatives to protect older adults. As always, my oral remarks and responses to any question reflect my own views and do not necessarily reflect those of the Commission or any individual commissioner.

Protecting older adults is a core element of the FTC's work. We know older adults are targeted and adversely affected by a wide range of scams. As many have mentioned, the pandemic has exacerbated that deceptive and unfair marketing and has had a particularly devastating impact on the health and finances of older communities. I want to touch on three areas: data trends, law enforcement, and education.

Starting with data trends, in 2020, the FTC's Consumer Sentinel Network logged nearly 5 million reports from consumers. Older adult reporting trends are based upon reports about fraud from consumers who voluntarily identify themselves as over age 60.

Three observations: First, as a general matter, younger adults, age 20 to 59, are more likely to report losing money to fraud than older adults, but quite disturbing is that older adults reported much higher individual median losses than did younger adults, and in fact, people age 80 and above reported the largest median losses.

Second, we observed that older adults are more likely than younger adults to lose money to certain types of scams, mainly technical support scams, prize and sweepstakes scams, and family and friend impersonation scams. That last category includes the grandparent scam.

Third, the data indicate what types of scams are causing the greatest dollar loss to older adults. One has already been mentioned by you, romance scams, followed by prize/sweepstakes scams and followed by business impersonator scams. The economic harm is enormous, more than \$600 million reported by older adults in 2020, and we know this is just the tip of the iceberg. Notably, reported losses to romance scams have increased significantly in the years, and this trend has only accelerated during the pandemic.

Shifting now to law enforcement, looking at the past year, we have filed at least 13 cases that have a notable impact on older adults. These range from investment scams to products to treat or prevent COVID-19, to products to treat or prevent cognitive decline.

When we file a case, we have two immediate goals: stop the ongoing harm and preserve assets so that we can return money to defrauded consumers. Over the years, the FTC has successfully returned billions of dollars to consumers. For this year, we have returned money to consumers or conducted the claims process in at least 11 cases where we have seen older adults impacted.

A recent Supreme Court decision, however, AMG, eliminated the FTC's ability to obtain monetary relief for defrauded consumers. Under Section 13(b) of the FTC Act. I cannot underscore enough how vital this tool, Section 13(b), has been to put money back into people's pockets. The economic impact of the pandemic has been devastating, particularly so on older adults who may be on fixed incomes. As a law enforcement agency, we are committed to providing redress to defrauded consumers, but to do so effectively and efficiently we need a fixed 13(b).

Finally, the FTC devotes considerable resources engaging in outreach and education for older adults. Since 2014, Pass It On has been the FTC's signature fraud prevention education campaign for older adults. It is a robust compendium of resources to enable people to understand scams and to literally pass on information about

them to friends and family. In addition, the FTC has continued to reach communities during the pandemic, conducting nearly 100 pandemic-related outreach events with partners in Fiscal Year 2021.

To sum up, I hope it is clear that protecting older adults is a priority for the FTC. The devastating impact of the pandemic on older adults has only emboldened its work. Finally, restoring the FTC's ability to obtain monetary relief under 13(b) is critical to enable the Agency to continue to provide redress to all those harmed by unfair and deceptive acts and practices.

Thank you very much, and I look forward to your questions.

Chairman CASEY. Thank you, Ms. Greisman, for your statement. We will now turn to Ms. Williamson. You may begin.

**STATEMENT OF ODETTE WILLIAMSON, STAFF ATTORNEY,
NATIONAL CONSUMER LAW CENTER,
BOSTON, MASSACHUSETTS**

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

The National Consumer Law Center uses its expertise on consumer law and energy policy to work for consumer justice and economic security for low-income people. At NCLC, I focus on issues impacting older consumers, provide training through the National Center on Law and Elder Rights, and direct our racial justice initiative.

All consumers are vulnerable to frauds and scams, but widespread illness and death, combined with the social isolation brought on by the pandemic, created fertile ground for the proliferation of scams aimed at older adults. This includes bogus treatment and cures for COVID-19, romance scams, government imposter scams, and fake charities. The list is endless. Scammers are constantly developing new and creative ways to steal money from consumers.

Scammers target older adults, whom they suspect are lonely, isolated, confused, or financially distressed. Low-income older adults, including those facing eviction, unemployment, and economic uncertainty, are especially at risk as they search for government programs or financial assistance.

Older adults in communities that are racially, ethnically, or linguistically isolated face a special challenge. An FTC fraud survey, for example, found that Latinos experience higher rates of fraud than other populations. Scammers purchase ads on Spanish language radio and exploit misinformation and confusion regarding COVID-19 treatments, vaccines, and the availability of financial assistance. Given the disproportionate impact of the pandemic on communities of color, we expect to see further uptick in frauds and scams aimed at these communities.

The impact of frauds and scams on older adults is simply devastating. Depending on the amount of money or assets taken, older adults can fall into poverty or homelessness. Scams also impact the emotional and physical health of victims as they struggle to live on

fewer resources for food, medicine, and other basic necessities. The financial strain and embarrassment may cause older victims to become fearful, depressed, and even suicidal.

The options to recover the money or assets stolen are few. Many scams are not discovered early, and consumers' attempts to stop or reverse payment is often too late or not possible. Scammers are known for the speed with which they redeem gift cards and pick up money wired to them, and consumers are rarely able to retrieve funds sent through these mechanisms.

More protections are needed to give consumers a fighting chance to recover money transferred to scammers. New payment systems, such as the peer-to-peer, or P2P, payment platforms—Venmo, Cash App, and others—are being used to facilitate scams. The warnings provided by the payment apps are simply not enough to protect consumers. Rather, Congress should modernize the Federal law, the Electronic Funds Transfer Act, to add protections for fraudulently induced payments and consumer errors.

Finally, the Federal Reserve Board is in the middle of developing a new P2P payment system called FedNow. However, recently proposed rules for the FedNow program duplicate the problems of existing P2P payment systems by failing to provide consumers with protections against fraud and consumer errors. Financial institutions and payment providers have a responsibility to prevent accounts from being used for scams and other illegal purposes. The Fed must make FedNow a model for other payment systems and must not value speed and convenience at the expense of safety.

Older consumers who have suffered the devastating health and economic consequences of the COVID-19 pandemic deserve the highest level of protection from frauds and scams.

I thank you for the opportunity to testify today and look forward to your questions.

Chairman CASEY. Thank you, Ms. Williamson, for your opening statement.

Mrs. Daniel, you may begin.

I know we had some connection issues.

Senator TIM SCOTT. Yes. I think she may still be suffering through the technology issues there.

Chairman CASEY. Maybe we will move to our next witness, and we can come back to Mrs. Daniel. We will move now to Kate Kleinert.

STATEMENT OF KATE KLEINERT, SCAM SURVIVOR, GLENOLDEN, PENNSYLVANIA

Ms. KLEINERT. Good morning, Chairman Casey, Ranking Member Scott, and members of the Aging Committee. My name is Kate Kleinert, and I am scam survivor. I am from Glenolden, Pennsylvania, and I have been widowed for 12 years. My husband, Bernie, passed away in 2009. Since then, I have never looked for any new romance in my life because I still felt married to my husband. I was not interested in finding another love.

Last summer, in August 2020, I received a friend request on Facebook that caught my eye. It was, unfortunately, the one in a million that I decided to accept and become friends with. His name is Tony. Well, that is what he told me. We exchanged messages for

a number of days, and he told me that he was interested in the same things that he saw on my Facebook page, like dogs and gardening. I thought that was wonderful.

We started talking on the phone through an app he had me download. He told me he was a surgeon working in Iraq through a contract with the United Nations and that he has two children, a little boy and a girl.

Tony became romantic much more quickly than I did, and I kept trying to put him off, saying we did not know each other. Tony had the kids get in touch with me through e-mail, and they started calling me "mom," which is my Achilles heel because I did not have children of my own. That put me head over heels.

The first request for money came from the girl who needed some feminine supplies but was embarrassed to ask her father. I sent her a gift card. I would go to any store, buy a gift card, take a picture of the front, the back, and the receipt, and send her that information through e-mail, and she could use it to make purchases. From then, there was always some kind of an emergency or some urgent need for money.

Things became more serious between Tony and I. He wanted to get married. He even asked if I would go out and start looking at houses. I was constantly sending him gift cards even though now I was using up the last of my husband's life insurance. My savings were gone. I was living on my credit cards, and he was getting what I took from Social Security and my pension. In all this time, only one person, an employee at a drugstore, ever asked me if I knew who I was sending these gift cards to. I kept doing this because he swore to me he would repay me the minute he got back to the States and even sent me his passwords to his account at Bank of America so I could see his balance, which was a little over \$2 million.

When he was finally allowed vacation, Tony was going to fly to Philadelphia on December 10th, and I was going to pick him up at the airport. I was so excited. I got all dressed up. My hair was done. My nails were done. I waited all night long. He never called. Even at this point, I never considered that it was a scam. I was just worried about him.

Then the next morning I got a call from a man who said he was Tony's lawyer and said that in Iraq someone had slipped drugs into Tony's bag and he knew nothing about it but was arrested at the airport and now needed money for bail. He asked me for \$20,000. The lawyer told me to do whatever I could, take out a second mortgage on my home, borrow it from my family, do whatever I could, but I was not able to do that.

I became suspicious when I asked to meet Tony in person, but the lawyer said that he had been transferred to Oklahoma. I became even more suspicious when Tony started calling me himself five or six times a day from prison, asking for more gift cards to buy better food. Something was not right.

By now, I had sent him a total of \$39,000, which to some people is not much, but to someone in my position it is a great deal. I am still paying for that today because I cannot get things repaired at the house. I have had no air conditioning this summer. My refrigerator is off, and my stove is off. I have been leaning on my sisters

and a few friends to get me through this. The loss that hurts the most was losing his love and losing the family I thought I was going to have and what my new future was going to be. That is much harder to deal with than losing the money.

I have since come to find out that all those pictures he sent me of himself were actually a doctor in Spain. I tried to report this to the police but could not get anyone to listen to me. I also called AARP's fraud number that was in their magazine and got a retired detective who was supportive and encouraged me to share my story. I have been frustrated at the lack of options to recover the money that I have lost or the ability to hold him responsible for these damages.

Even though this experience is painful to speak about, I want to be an ambassador for this cause because it is so devastating and many people have been through this but not spoken about it. They continue to carry this heavy burden alone. In my case, I got pulled in because I had forgotten how good it felt to be loved. Thank you.

Chairman CASEY. Kate, thank you for sharing your personal story. It was a moving story when I read it but even more so when we hear it from you. We are just grateful you are here with us.

I think we are going to try Mrs. Daniel again to see if she is connected.

Ms. DANIEL. Yes. Sorry about that.

Chairman CASEY. Great.

**STATEMENT OF VEE DANIEL, PRESIDENT AND CEO, BETTER
BUSINESS BUREAU SERVING UPSTATE SOUTH CAROLINA,
GREENVILLE, SOUTH CAROLINA**

Ms. DANIEL. Chairman Casey, Ranking Member Tim Scott, and distinguished members of the Committee, thank you for the opportunity to testify today on a topic of "Fraud, Scams, and COVID-19: How Con Artists Have Targeted Older Americans During the Pandemic."

My name is Vee Daniel. I am a college communications major graduate, mother of an early childhood teacher, an intern architect, and a new grandmother. I will be celebrating my 30th wedding anniversary this year.

I serve as President and CEO of the Better Business Bureau of the Upstate and the Better Business Bureau Education Foundation, a position I have held since 2011. BBB is a nonprofit promoting trust between consumers and businesses and the marketplace and has been around for more than 100 years.

When I was first offered the position, I was intrigued. I grew up with a father who was a huge advocate for the BBB. When his friends needed assistance with customer service issues, my dad would always say, call the BBB.

After a few weeks on the job, I received an invitation to speak to a senior group about the latest scams. I will never forget that day I spoke to those seniors and listened to their scam stories. It was heartbreaking. I learned to speak louder, ask questions, listen, and the most important part was realizing education is the key to fighting senior fraud. That is when I knew this role with the BBB was the perfect fit for me. Since that day, I never turn down an opportunity to speak to educate seniors. In 2015, we dubbed the

program “Savvy Seniors” because that is what we wanted to achieve.

During the pandemic, we witnessed new scams that involved masks, non-FDA-approved medical supplies, immunity—boosting products, and equipment through online purchases related to COVID-19. We have also seen fake websites, phishing e-mails that involve stimulus checks, price gouging, scammers impersonating government agencies like Medicare, and promoting fake vaccines. We have also seen an increase in romance scams during COVID-19.

BBBs across the country rallied together to put out fraud prevention messages, and we did thousands of media interviews to try to warn consumers about all COVID-related scams we were seeing. Senior groups were not able to meet during COVID-19, so we partnered with our local Appalachian Council of Governments Greenville office and Meals and Wheels to provide 1,000 BBB Savvy Senior packets that included education information on fraud and scams.

As part of a larger national effort, the BBB of the Upstate has hosted Secure Your ID Day since 2009. Local BBBs from all across the United States and Canada join in on the event designed to protect consumers from the growing threat of identity theft and provide education. Consumers and businesses are encouraged to attend the free community service event and properly shred and destroy sensitive documents. In 2018, BBB Upstate partnered with AARP-South Carolina, and from that partnership we have increased our shred events from 4 to now 8 events a year. Last week, we held two events, one in Greenville and one in Anderson, with two happening in October in Spartanburg and Simpsonville in our area. About 90 percent of attendees are seniors.

BBB Scam Tracker is an online platform that enables consumers and businesses to report scams and suspicious activities. The data is analyzed, and reports are made available to the general public, thus empowering consumers to avoid losing money to scammers. The website features a searchable heat map, so users can view the number, types, and details about scammers, scams reported in their communities. BBB Scam Tracker data enables local BBBs to educate consumers and stop fraudsters by leveraging the power of technology and our network of BBBs serving communities through North America and Canada.

Using data from the BBB Scam Tracker, our foundation, the BBB Institute for Marketplace Trust, released a report on the rise of online scams during the COVID-19. The BBB Risk Index is a formula that looks at scams in a different way: the volume of each type of scam reported to BBB Scam Tracker; the susceptibility rate, that is, how people who exposed to the scam actually lose money; and the dollar loss. That formula shows us which scams are the riskiest, and it may not be for the scam with the most reports. For instance, romance scams were the riskiest for ages 55 through 64, followed by online purchases and investment scams. Travel, vacation, timeshare scams were the riskiest for ages 65-plus, followed by online purchases and romance scams.

Since BBB began tracking scams in this way in 2016, we have seen a clear pattern. Although seniors are pretty savvy and tend

to fall for scams less frequently than the younger demographic groups, they lose more money. This is partly because the type of scams that target seniors—romance scams, investment scams, family emergency scams—tend to be the higher dollar amounts.

Although many seniors have gotten the message and are more cautious than in the past, too many are still falling victim to unscrupulous criminals. BBB is proud of the role we play in educating seniors and all the consumers, but there is much more that can be done, and we appreciate the attention this issue is getting.

Thank you for the opportunity to be a witness today on a relevant topic of how con artists have targeted older Americans during the pandemic.

Chairman CASEY. Mrs. Daniel, thanks so much for your testimony.

I want to acknowledge two members of the Committee who are here, or one who has been here and will be back, I guess. Senator Collins is here with us.

Ranking Member Scott made reference, Senator Collins, to the years when you were Chairman and producing the fraud and scams book that the Committee has been using for so many years. We thank you for being here.

Senator Braun was with us earlier, and I want to acknowledge Senator Braun's attendance at the hearing, and maybe he will be back here.

So we will take a brief recess now to vote, at least so that Ranking Member Scott and I can vote, and then we will come back and resume the hearing.

[Recess.]

Chairman CASEY. Okay. The hearing will resume, and I wanted to start by acknowledging that Senator Gillibrand and Senator Warnock, have joined us via Webex. I will start with my questions and then turn to Ranking Member Scott.

I want to start with Kate Kleinert. Kate, as I mentioned, your story is so powerful, and unfortunately, for America it is not unique. I think every member of the Committee was moved by what you said. As I said, your written testimony was powerful enough, but hearing it directly from you had a big impact on me and I know other members. We are grateful you are here, and we are grateful that your story can help other seniors when there are scammers out there and perpetrators of fraud trying to rip people off.

I wanted to focus on one part of your story and the story of many others, Kate. You said that, or you know, I should say, that social isolation is not something new for seniors, but for many people the pandemic made this terrible isolation that much worse. Do you believe the pandemic left you more susceptible to being scammed?

Ms. KLEINERT. I really do. When I think back to the beginning of the pandemic, when we were first locked down and it was so strange to be home without any physical contact with other folks, not seeing your family, it was very hard and upsetting to be by yourself. I think when this man was kind to me on the Facebook that I did react to it more than I would have at any other time.

Chairman CASEY. Yes, I think that is understandable. I thought it was noteworthy among many things you said that as much as

you lost a significant dollar amount, some \$39,000—I was just recounting that to some reporters in the hallway as we went out to vote. I was struck as well by what you said on page three of your testimony, where you said “The loss that hurts the most was losing his love and losing the family I thought I was going to have and what my new future was going to be.” That tells us so much about how devastating these scams can be.

So, Kate, we are grateful for your testimony, and I may be able to come back to you later with some other questions.

This question I will direct to Ms. Williamson and Mrs. Daniel together, and it does not matter who answers first.

As we just made reference to Kate’s testimony, she shared that only one person, an employee at a retail store, warned her that she might be a victim or might be a target of a scam. Businesses and financial institutions are, of course, uniquely situated to respond to these attempts to rip people off, but often the employees of those institutions are not trained to detect fraud or to speak in a sensitive and effective manner to the consumer, to give them a heads-up based upon their experience and their training.

As I mentioned, our bill, the bipartisan Stop Senior Scams Act, would fill in these gaps in both knowledge and training so that we have more instances so it is not just in Kate’s case, one person, but more than one person giving people a heads-up.

So in your view—and I guess maybe I will start with Mrs. Daniel just to go in order. In your view, would this legislation help reduce the risk . . . the risk of older Americans being defrauded?

Ms. DANIEL. Yes, I would think that it would. You know, any—you know, there is lots of reports out there about, you know, with education and everything. I mean, I think it is very important that with the education and with the risk that we are talking about—you know, I think it would definitely help. You know, I think that during COVID-19, you know, it was more risky, and it still is because COVID is still going on. I would say, definitely, I think it is.

Chairman CASEY. Ms. Williamson?

Ms. WILLIAMSON. I would also support the legislation. I think we need more tools to prevent, to fight these scams up front. Simply, the retail employees are first line of defense. They are in these stores day in and day out. They know their customers. If they have more training and more information on these scams, they can simply warn the victims not to complete this transaction.

It is simply better to not have the elder transfer away that money than to try to get that money back on the back end. There are just fewer options to retrieve that money once it is transferred away.

Chairman CASEY. Well, thank you very much. Just as you were answering the question, I am reminded of a story from years ago in this Committee where we heard the story about someone who was a target of a scam, and it was not until he was in the parking lot of the bank where he was about to transfer money that he got someone to interrupt and say you have got to think about this before you go into the bank. The more people that can provide that warning, the better.

I will turn next to Ranking Member Scott.

Senator TIM SCOTT. Mr. Chairman, I will defer my opening questions to my brother from another mother, Senator Scott from Florida.

Senator RICK SCOTT. Thank you, Senator Scott.
[Inaudible.]

Chairman CASEY. I think we need a microphone.

Senator RICK SCOTT. You worry about them every day, whether somebody is going to try to take advantage of them. When you hear the story of somebody that acts romantically interested and takes somebody's life savings, it devastates you because it is very difficult for law enforcement to find these people and to track them down and to be able to prosecute them, and it is so large. Your heart goes out to people that this happens to.

My first question is for Ms. Greisman. First, I want to thank you for your hard work to protect our seniors and everything you do to bring justice to the criminals who take advantage of our older Americans. Are there any additional resources or authorities you and your team need to carry out your mission?

Ms. GREISMAN. Senator Scott, I appreciate the question. The main tool we need back is our ability to obtain, effectively and efficiently obtain, monetary relief under Section 13(b) of the Federal Trade Commission Act. A remedy to fix that is what truly needed so that we can put money back in people's pockets, money back to people who are defrauded.

Senator RICK SCOTT. We have put out information out of our office to give to seniors to try to get them to do it.

Ms. Kleinert, first off, I just want to tell you that it is disgusting that this happened. It is disgusting that this individual took your money and also disgusting that he gave you hope when he should not have. Criminals are just like this, they are despicable.

What advice do you give others to make sure this does not, you know, happen to them? Is there anything when you look back that you can say, gosh, I should have—there was a red flag I did not see, that maybe somebody else will say they see your testimony and they will not make—the same thing will not happen to them?

Ms. KLEINERT. I have really been astonished at the amount of information that has been said today, the things that are out there, programs that are out there, and I knew nothing about them. I think there is a gap between what is being done and the senior citizens, and we need to close that somehow.

I am not so sure the education of the retail personnel is the way to go. If I am in the line at a drugstore, buying a gift card, and there is a 19-year-old kid behind the cash register with a Santa hat on, I do not think I am going to listen to him about the dangers of buying that gift card.

I think there needs to be some kind of a pamphlet, a brochure that has statistics, warning signs, and where to go, not sitting at the cash register to take one if you want one, not being handed to you by the cashier if he says, "Would you like to have this," but to be automatically put in the bag when you are purchasing a gift card. Just put it in the bag. People will go home. A lot of them will throw it away, but many more, when they are by themselves, will sit and read this and take it to heart.

There has to be more education out there, and it has to be more visible to the senior citizens. Get commercials on the television. Show scenarios of scams and how they come about. Tell people that you are not dumb for falling for it, that these people are so sophisticated and so good what they do that you are not being stupid or making bad decisions by being taken in by these people. They are smarter than you are.

Senator RICK SCOTT. Have you gotten much media attention? Has the media been interested in your story?

Ms. KLEINERT. I have been interviewed for a newspaper article earlier in the spring, and AARP asked me to do a podcast. I have done two podcasts, but that has been it.

Senator RICK SCOTT. Okay. Mrs. Vee Daniel, I want to thank you for the work you have done. Do you think that local businesses have the resources they need to educate their staff on potential fraudulent activity, and is there anything else that you think that we ought to be doing to help our small businesses to do a better job to stop this?

Ms. DANIEL. I think—well, thank you, Senator Scott.

Great question. I think there is definitely more education that could be done. As I mentioned, most of our Savvy Seniors are groups, and we do small business webinars actually to our accredited businesses and non-accredited businesses. I think there is definitely more education that we can do with small businesses to, you know, alert them, the small business owners and their staffs, of the, you know, prevention tips and what to look out for.

So I definitely—you know, in our area, we cover 10 counties. We are a staff of nine, and you know, we try to do the best that we can. I think definitely with more collaboration just like we did with AARP this past year, and more collaboration with government agencies, to be able to provide more education.

Senator RICK SCOTT. Thank you.

Thank you, Chairman.

Chairman CASEY. Senator Scott, thanks very much.

I will next turn to Ranking Member Scott.

Senator TIM SCOTT. Thank you, Mr. Chairman.

I will direct my first question to Mrs. Daniel. Mrs. Daniel, under your leadership, the Better Business Bureau is really making a difference in the lives of our fellow South Carolinians. The Savvy Senior program provides tips on how to spot the latest scams. Have you heard from golden Americans who utilized the lessons they learn from the program and applied it to their lives?

Ms. DANIEL. Yes. That is the rewarding part. I mean, the rewarding part is, you know, when you hear someone that says that, you know, our prevention tips or red flags helped them stop from becoming the next victim. It is very rewarding.

I can tell a little bit of a story we had, a short story. I had an executive. He was a retired executive of a very large business here in the Greenville area that came into the office, and he wanted to talk because he had a new employment job that he was starting to feel a little—you know, he was not sure whether it was a scam or not. He came in and talked to us, and you know, he said that basically what he was doing was he had someone contact him about a job opportunity which was offering a lot of money. What

he started doing was packaging up items that were shipped to him by his employer and then he would reship them to someone else. As soon as he said that—because we have seen that before. It is called employment scam. We just immediately told him, you need to stop. What you are doing is wrong. It is—you know, you should not be making that much money. Then he says, well, I have not even been paid. He had been doing it for a while. Then I said, you need to stop. He agreed. He agreed. About a couple weeks later, we heard back from him, and he told me that he got a call from the Mall of America, an investigator from Mall of America, and that what he was doing was wrong because what he was shipping was actually bought from stolen credit cards.

Senator TIM SCOTT. Wow. Wow.

Ms. DANIEL. He called me, and he asked me if I would reach out to the guy from Mall of America, the investigator, and so I did. I let him know the guy was very up and up. He is a very up and up leader. He was a leader in our community, and you know, he just got intertwined with something that he thought was right, was wrong.

There was no charges or anything, and actually they worked with him later on. We do not really know all the specifics there. You know, without him coming into the office and talking to us, my worry is he could have been indicted or he could be in jail.

Senator TIM SCOTT. I guess.

Ms. DANIEL. You know, that is just one example, but thank you.

Senator TIM SCOTT. That is a very good example. Thank God for your hard work and your dedication on such an important issue.

Let me ask you one other question before I turn to Ms. Greisman. Given your background and extensive experience with the Better Business Bureau, can you help us understand how to help our seniors who live in rural America? Sometimes they do not get the same level of information and they are not perhaps as connected to broadband. They may not have broadband connections. They may not have the same access to information as folks who live in more suburban areas. Is there a way that the Savvy Senior program helps to encourage and inform our rural golden Americans?

Ms. DANIEL. Yes, the Savvy Senior program does. It is just short, very short. Basically, the program over the years has presented to senior groups in all parts of our 10 counties that we cover, even rural areas. What I say is, whether we drive 10 miles or 100, we never say no to presenting education to seniors about scams and fraud.

Senator TIM SCOTT. Excellent. Thank you very much.

Ms. Greisman, thank you for your work and certainly your expertise. I am certainly proud to co-sponsor with Chairman Casey Senate Bill 337, the Stop Senior Scams Act, which creates an advisory group with industry stakeholders, and leading and regulatory bodies, to identify opportunities for consumers, companies, policymakers, and law enforcement to protect our aging community.

In light of your work with the Commission, could you please speak to how this new advisory group can serve to optimize the Commission's current practices without duplicating work that has already been done at the Federal level?

Ms. GREISMAN. Thank you, Senator Scott. Look, we are keen to work with you and your staff on any type of legislation that will enhance and improve our ability to serve older adults and to do so more efficiently. We look forward to working with you on that.

Senator TIM SCOTT. Thank you, ma'am.

Mr. Chairman.

Chairman CASEY. Ranking Member Scott, thanks very much.

We are awaiting some other Senators. I wanted to continue the question period with one that I had, and I will pick up where the Ranking Member left off with regard to the witness, in this case, Ms. Greisman.

We have heard Kate's story earlier that I made reference to, and you heard Kate Kleinert's testimony. In particular, of course, what she has identified is a particular kind of scam, a romance scam. We know that she is not alone. Unfortunately, this is one of the areas where there is an awful lot of increase or growth in that kind of a scam. In fact, the Federal Trade Commission reported a significant increase in reports of these scams between 2019 and 2020 as Americans became more isolated.

I just looked in your testimony, Ms. Greisman. I am looking at page four. It says, "For older adults, reported losses to romance scams increased from near \$84 million to about \$139 million in 2020." So, 84 to 139. There are millions of dollars. Every time it moves up the scale, millions of dollars. Then it goes on to say, or your testimony, I should say, goes on to say, "Among older adults, hardest hit were the 60–69 and 70–79 age groups." Basically everybody over 60, between basically 60 and 80, "which reported \$129 million of the 2020 losses," meaning \$129 of the \$139 million in losses were reported by that age group, "making romance scams the category of highest reported losses for both groups." Obviously, a lot of money and a big cohort of Americans being affected by this.

Ms. Greisman, here is my question. Based on this uptick in romance scams and all the dollars lost because of it during the pandemic, what work is the Commission doing to both educate consumers and to prevent, or help consumers prevent, themselves from being preyed upon by these so-called romance scammers?

Ms. GREISMAN. Thank you, Chairman. First of all, let me say that Ms. Kleinert is indeed a compelling Ambassador, and her testimony is courageous, and it highlights how sophisticated romance scammers are and how they work hard to build trust and cause enormous harm.

One of the main payment systems that romance scammers use are money transfers, and the FTC in recent years has sued both major—each of the major money transfer networks, MoneyGram and Western Union. MoneyGram recently failed to live up to the requirements of a prior order and crack down on fraudulent transfers across its network, and Western Union facilitated fraudulent—allegedly, facilitated fraudulent transfers on its system. I think that type of law enforcement work goes a long way toward minimizing the harm that is caused by wire transfers in connection with romance scams.

On the education front, Pass It On, again, is our signature education campaign. What we have seen, and I think what Ms. Kleinert's testimony underscores, is how important it is that people

have the knowledge of scams, and that is a primary goal of the FTC: to educate; push out information; to do it at local, State, and Federal levels; work with our partners like the Better Business Bureaus, consumer groups, AARP. Getting information out there so that people are aware of the type of scam, we know from research, makes it less likely they will fall prey to that scam.

Chairman CASEY. Well, thanks very much.

I am going to concede the rest of my time and turn to Senator Gillibrand, who is, I think, connected for her questions.

Senator GILLIBRAND. Yes. Thank you, Mr. Chairman.

Thank you, Ms. Greisman, for your testimony and the answer to the Chairman's last question. I just have a follow-up question. How can the FTC do more to get information out to seniors in all of their communities so they can recognize this fraud more?

I have been to assisted living facilities across New York, and I have heard story after story. Stealing life savings. The grandchild scam. You know, all the different kinds of ways. The IRS scam. It does not end.

We know that a lot of these artists are—scam artists are criminals, criminal networks. I know we arrested a criminal network from India, one from Russia. The FBI works to subvert these kinds of frauds.

I feel that the FTC needs to work in perhaps a different way to make financial institutions more aware, to make sure seniors are more aware, to make sure places where seniors go, assisted living facilities are more aware. What can you do to help solve this problem?

Ms. GREISMAN. Senator, maximizing our outreach, maximizing our ability to reach in the communities is just a top priority, and it is a challenge. It is especially more so—it is a special challenge in a pandemic. I assure you our outreach efforts are constantly being rethought, re—evaluated. It is our goal to reach into the communities at the grassroots levels, through local organizations like the public libraries, through legal services. We have a tremendous network of contacts, and we are constantly tapping them both to push out information, so that they have access to the resources we have and can use in their communities, and also to receive information from them to inform our law enforcement work and our education and outreach.

Senator GILLIBRAND. Is your outreach including sort of this urgency, that if they are a scam that they are going to report these scams? Obviously, if we do not give the FBI the information and law enforcement the information to go after them, they will have less data and information to be successful.

Ms. GREISMAN. A core piece of information that is indispensable to all of our outreach is to report what they are hearing. Go to www.reportfraud.ftc.gov. It is absolutely, incredibly important that we receive that information so that we know what is going on and we can be proactive in our enforcement.

Senator GILLIBRAND. Are you asking the institutions to do the reporting? I can promise you no senior that has been scammed is going to want to go to a website and report the scam. If they are not willing to go to the police in the first place, they are not going

to go to a website. Are you asking the assisted living facilities and the financial institutions to do the reporting?

Ms. GREISMAN. We do receive data from certain contributors in the private sector such as MoneyGram, Western Union, Better Business Bureaus. I am not aware that any financial institutions report directly to us, but that is certainly something that we will give thought to. Appreciate it.

Senator GILLIBRAND. Ms. Kleinert, thank you so much for sharing your story. I know it is a horrible, horrible thing. You are very courageous, and you can prevent what happened to you from happening to other people. Can you tell us what you wish was available for you or how would you have been able to be warned more effectively? What would have worked for you, and what type of interventions or resources would be helpful for you and your friends?

Ms. KLEINERT. I think we need to get more of this information out to the people. I had no idea where to go. I tried reporting my problem to the police but could not get them to listen to me. That was very discouraging, and I was giving up at that point.

I did call the AARP fraud line and got a very nice man. That is important, too, to have someone who is compassionate and not speaking down to you, not talking to you like you are senile and cannot make good decisions because that is not true. That is—you already feel that way anyway by yourself. You do not need someone else reinforcing that.

Senator GILLIBRAND. To be honest, Ms. Kleinert, these are highly sophisticated criminals. This criminal enterprise of senior fraud is worth hundreds of billions of dollars every year. It is not a small thing. You guys are their primary targets because seniors together have over a trillion dollars of assets, you are a ripe, very rich target for these criminal networks.

I guess what you are saying is you would like law enforcement to be better informed so they could have put you in touch with the right people. Police departments.

Ms. KLEINERT. Yes.

Senator GILLIBRAND. That might be a way, Ms. Greisman. To reach out to law enforcement so that the FTC can actually brief every police department in America, you know, over the next several years would be great because, you know, if Ms. Kleinert has an instinct to report this to the police, and the police make fun of her or do not take her seriously or say, well, you are stupid, then not only does Ms. Kleinert not get justice or does not get to effectively report, but it is going to make her feel that it was her fault. That is exactly the opposite of the nature of these crimes. They are highly sophisticated adversaries, who are doing everything they can to steal resources. Is that something the FTC can do, Ms. Greisman?

Ms. GREISMAN. We do work closely with local police offices and have—

Senator GILLIBRAND. You put together a training for them, like even just a deck of slides for police departments to use to train all police officers?

Ms. GREISMAN. I do not know that we have specifically done a training for police officers. We do have a tool kit actually on stop-

ping gift card scams, and the driving force of it, the message, is that gift cards are for gifts. That tool kit is targeted toward retailers, and it gives them information they can display in their stores, interact with customers.

Senator GILLIBRAND. That is super helpful. Well, maybe then—I mean, on this Committee, we will have recommendations because that is what our committees do, but just from this hearing alone I hope that you will take some of the information you learned here and implement it.

Chairman CASEY. Well, thanks very much, Senator.

Senator GILLIBRAND. Thank you, Mr. Chairman.

Chairman CASEY. Thanks, Senator Gillibrand.

We will turn to Senator Blumenthal.

Senator BLUMENTHAL. Thank you, Mr. Chairman, and thank you to you and Senator Scott for having this hearing.

I would like to talk about robocalls which are a bane of all of our existence but most especially, I think, for seniors. I hear from them all the time. In 2019, I supported the passage of the Telephone Robocall Abuse Criminal Enforcement and Deterrence Act, known as the TRACE Act, which directed the FCC to establish standards to protect consumers from unauthenticated numbers and to work with providers to verify the legitimacy of incoming calls.

This law has worked in part, not an ultimate answer, but now nearly 95 percent of high-risk robocalls do not originate from the 6 largest carriers.

Unfortunately, smaller internet-based providers, who have until 2023 to work within the FCC's requirements, now account for the majority of these robocalls. They continue to prey on our seniors. They do so especially in these times of pandemic, when seniors and all of us are particularly vulnerable to these pitches.

Let me ask you, Ms. Williamson, how effective are robocallers in reaching consumers, particularly older Americans?

Ms. WILLIAMSON. Thank you for your question. Scams aimed at older adults are primarily perpetrated over the telephone. The protections that you mentioned are critical to helping older adults avoid these types of scams, and we certainly thank you for your efforts on that. We also believe that their protections should be enhanced to further clarify that with respect to the TCPA, that solicitation—the prohibition against solicitations does apply to scam calls. We need further protections against spoof calls. We absolutely support the FCC's efforts on that end to date. We also need to tamp down on other loopholes, such as the fake charity scams, and make sure that when consumers, when older adults are being requested to put their hard-earned money to help others, that those charities are actually legitimate.

Senator BLUMENTHAL. Taking that point, I think it is an important point about charity scams. How much have you seen arise in those charity scams during the pandemic? Is there an increase? What would you say about charity scams?

Ms. WILLIAMSON. Certainly we do not have data on the charity scams. We just have information that we have heard from consumers and advocates. What we have heard is that there is indeed an uptick in these types of fake charity scams, that older adults at home, isolated, wanting to help in some way, are being victimized

by these types of scams. We are looking to put more protections in place to help avoid those types of scams.

Senator BLUMENTHAL. Do you find that seniors are particularly vulnerable to these scams, as we have found when I was Attorney General of Connecticut, during times of crisis, in cases of natural disaster, whether it is hurricanes, floods? We have seen a lot of both and other weather events. Is there an increased vulnerability because of those natural disasters?

Ms. WILLIAMSON. Oh, absolutely. Scammers read the headlines. They follow what is happening, especially if they are outside the United States. They follow what is happening in terms of disasters, in terms of other issues coming up in the news, and they tailor their scams to fit those details. If there is a natural disaster, if there is a fire, flood in an area, they are targeting consumers in those areas. They are targeting older adults. They are targeting people who they know to be sympathetic, who they know to be charitable, to get them to turn over their hard-earned money to them.

Senator BLUMENTHAL. What I have advised seniors is that they should contribute and be generous but make sure they know that the organization that they are supporting is in fact the one that they really want to support. In other words, Americares, the Red Cross, these organizations are established. They do good work. Would you agree?

Ms. WILLIAMSON. Absolutely would agree that there are ways to research the charity and make sure that it is legitimate, make sure that it will help the people you intend—that your money will help the people you intend your money to be directed toward. There are so many ways to absolutely find out about the background of an organization.

We always advise for consumers to be wary, that if they are being solicited over the phone to research the organization through other means, and to really give their money to reputable charities.

Senator BLUMENTHAL. Thank you very much, Ms. Williamson.

Thanks, Mr. Chairman.

Chairman CASEY. Thanks very much, Senator Blumenthal.

The second vote just started, almost about 10 minutes into the vote, so we have got to hustle. We will hear from Senator Rosen who rejoined us, then Senator Kelly, and then we will close. Senator Rosen.

Senator ROSEN. Thank you. I have already voted. I was presiding in the Chair. Thank you, Chairman Casey, of course, Ranking Member Scott. This is a really important hearing, Chairman. Scams against seniors are nothing new, and they are only increasing in scope and severity. I appreciate your holding this important hearing and for all the witnesses here today for the important work that you do. Of course, Nevada is no different than some of the other states or most other states, and we have a lot of challenges in health scams, particularly now of course with the pandemic. You know, one of the challenges throughout the pandemic has just been the unchecked spread of misinformation, disinformation, of course, resulting in an increase in scams, especially those targeted at seniors.

In fact, according to the Federal Trade Commission, in 2020, Nevadans over the age of 60 lost more than \$36.5 million to scams. That is a lot of money. Some of the most common COVID-19 scams in Nevada related to those involving the creation and distribution of fake vaccine cards and contact tracing scams in which scammers pose as health department officials asking for sensitive personal information, such as your Medicare or Social Security number.

Fortunately, our attorney general, his office has compiled a list of COVID-19-related scams and tips on how to avoid falling victim. People have resources, where to check if they are able. As elected officials, I believe we have to do as much as we can to get the word out about these scams.

Ms. Greisman, for the record, I want to really clear the air for Nevada seniors and get this out everywhere I can. Would a legitimate tax department official ever ask for a senior's personal information, like their Medicare or Social Security number, with the contact tracing for COVID-19?

Ms. GREISMAN. No, no. No legitimate entity would make an unsolicited request for that kind of personal information.

Senator ROSEN. Thank you. I am going to reiterate that; no legitimate entity would make a request for that personal information. Thank you.

I know you have been speaking about this, but for those who do fall victim and they do give their sensitive personal information and they fall victim to now a COVID-related scam, can you talk about, Ms. Williamson, some of the resources available to the senior or someone who is helping them, maybe another family member or a caregiver, to help recover that information and reverse potential damage?

Ms. WILLIAMSON. Sure. There are many resources available to older adults who have fallen victim to scams and frauds. I think the first line of defense is for the older adult and his or her advocate to really audit all of their financial accounts. Call their banks. Call the credit card company. Make sure that they reach out to law enforcement organizations. Of course, the FTC has a great part of their website that will help victims as well. I would refer folks to that as well.

What is also important is to reach out to the IRS or the Social Security Administration if there has been a disclosure of personally identifiable financial information. Just make sure those organizations as well know that you have been victimized by this scam.

It is also important really to reach out to a legal services organization or to another lawyer to make sure that you protect your whatever money or assets you have remaining because if the fraudsters really have your financial information they could be wrecking—doing damage to not only your credit report but also trying to seek other assets that you may have.

Senator ROSEN. Thank you. We have been really proud because our U.S. attorney in Nevada appointed a COVID-19 fraud coordinator to lead investigations, to help with just the kinds of things you are talking about, and our attorney general did announce the creation of a COVID-19 task force to help protect Nevadans, all of Nevadans, not just seniors, who may fall victim.

It is a whole-of-government approach that we are trying in my home State. It is a response with 15 agencies—FBI, Secret Service, SBA, our small business office, inspector general, the post office, the police departments. We are really trying to pull together to protect people, because we did this, Nevada ranked first amongst all states for the reported number of total fraud reports in 2020, with a whopping number of over 35,000 fraud reports, and so now 18 months into this pandemic, what can you—what lessons have we learned from these types of task forces that we can report to other states to help protect people?

Chairman CASEY. Just for the information of the Senator, because we have got a vote, I just want to make sure we—

Senator ROSEN. Okay. We will take it off the record. Thank you.

Chairman CASEY. If we can do that in writing, that would be better.

Senator ROSEN. Thank you.

Chairman CASEY. Thank you, Senator Rosen, for coming back to the hearing and being with us. Now Senator Kelly.

Senator KELLY. Thank you, Mr. Chairman.

Ms. Greisman, I wanted to follow-up on Senator Blumenthal's question about robocalls. Arizona ranked first in complaints to the FTC about the Do Not Call Registry or the Do Not Call List. Arizonans are getting these calls all hours of the day. Some folks are getting hundreds of calls in a week. Nobody can blame Arizonans for being frustrated about this. I think we all are.

There has been a fair amount of activity in the courts this year related to the TCPA, the Telephone Consumer Protection Act. Could you give us an update where things stand, penalties, maybe an example of a specific case, and what Congress can or should do in order to better our constituents?

Ms. GREISMAN. Senator Kelly, obviously, robocalls, unwanted calls, whether live or prerecorded, are a significant consumer protection issue. Each month, the FTC is receiving some 450,000 complaints from consumers about unwanted calls. Typically, 68 percent of them relate to robocalls.

FTC has a vital, vibrant law enforcement program combating unwanted telemarketing calls. We recently settled with a cruise line, Grand Bahamas, just earlier this week, involving millions and millions of unwanted calls. We brought some 150 law enforcement actions and coordinated with all of our State partners, including Arizona. Both in terms of law enforcement and consumer outreach, it is a significant part of the work that we do.

Senator KELLY. Do you know, what is the rate of robocalls? The number that consumers are receiving, has it been lately trending up or down?

Ms. GREISMAN. In what has been reported to us, it has held pretty stable at about 450,000 a month. What we are seeing are the call-blocking technologies are working. Recently, STIR/SHAKEN been deployed among the larger carriers. Senator Blumenthal mentioned this; it took effect just in June of this year. Obviously, a lot of issues remain with the smaller VoIP service providers that Senator Blumenthal also talked about.

We sued a number of them. Our State partners sued a number of them. Our DOJ has sued them. There is significant law enforcement work to tamp down on these unwanted calls.

We are not there. There is no question about that. I assure you we are hard on the issue.

Senator KELLY. Well, please let us know if there is anything you need from Congress here to make your job easier.

Thank you, and I yield back the remainder of my time.

Chairman CASEY. Thank you, Senator Kelly.

In light of the fact the vote is now into overtime, I think we have to close right now, but I will be submitting a statement for the record as I understand Ranking Member Scott will as well.

Chairman CASEY. Let me just say this for the record, two things: Number one, we want to thank our witnesses for the testimony they brought to us today on these terrible scams and ways we can prevent them. For the record, if any Senator has additional questions for witnesses or statements to be added, the hearing record will be open for seven days until Thursday, September 30.

Chairman CASEY. Thank you all for being here. We are adjourned.

[Whereupon, at 11:20 a.m., the Committee was adjourned.]

**CLOSING STATEMENT OF SENATOR
ROBERT P. CASEY, JR., CHAIRMAN**

Thank you to all the witnesses for testifying today. A special thank you to Ms. Kleinert for sharing your experience with us. Your powerful story is a reminder that we must keep fighting to prevent these predatory schemes and bring these criminals to justice.

No one should have to go through what Ms. Kleinert has been through. No one should experience the shame and loss that comes with having been exploited by a criminal. In Congress, we have a sacred duty to protect seniors against these criminals.

Again, I am pleased that today the Aging Committee is releasing our 2021 Fraud Book, which will arm older Americans with the information they need to protect themselves from scammers.

We know even more work needs to be done. That starts with putting the bipartisan Stop Senior Scams Act, S. 337, on President Biden's desk. I'll keep fighting to pass this important bill.

Thank you.

**CLOSING STATEMENT OF SENATOR
TIM SCOTT, RANKING MEMBER**

Thank you Chairman Casey. Thank you to our witnesses. Being aware and staying vigilant is the best way to protect yourself from frauds and scams. One way to protect the seniors in your life is to check in on them. Stay connected to your parents, grandparents, aunts, uncles, neighbors, and friends, especially during COVID lockdowns.

In 2020, more than 1,300 South Carolinians aged 60 and older fell victim to frauds, losing nearly \$10 million. By working together, we can help older Americans make informed decisions. COVID-19 has made it harder to stay connected.

Now, more than ever, we have got to support one another. We know that in-person meetings allow friends and family members to see changes in a person's behavior that serve as red flags.

I want to thank Vee Daniel for her time today, her powerful testimony, and her service in supporting seniors across South Carolina. The Better Business Bureau Serving Upstate South Carolina is positively influencing the lives of so many seniors and their loved ones. Perceptive seniors are informed consumers who can spot and stop con artists. It is vital that we continue to raise awareness of these scams and advocate on behalf of our seniors.

Thank you Chairman Casey. It has been such a long-standing tradition of the Aging Committee to highlight ways to fight against frauds and scams, and I'm humbled to do this work with you.

I yield back.

APPENDIX

Prepared Witness Statements

**PREPARED STATEMENT FROM LOIS GREISMAN OF THE
FEDERAL TRADE COMMISSION**

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

**Before the
UNITED STATES SENATE
SPECIAL COMMITTEE ON AGING**

**UNITED STATES SENATE
WASHINGTON, D.C.
SEPTEMBER 23, 2021**

Chairman Casey, Ranking Member Scott, and members of the Committee, I am Lois Greisman, Associate Director of the Division of Marketing Practices, Bureau of Consumer Protection at the Federal Trade Commission (“Commission” or “FTC”).¹ I also serve as the Elder Justice Coordinator for the FTC. I appreciate the opportunity to appear before you today to discuss the Commission’s initiatives to protect older adults.²

Protecting older adults in the marketplace is one of the FTC’s top priorities. For the past 18 months and continuing each day, the global pandemic has challenged the entire country, and hit the health and finances of older communities particularly hard. Older adults continue to be targeted by a wide range of scams and the unfair and deceptive marketing of products and services, which has been exacerbated by the pandemic. To protect older consumers, the FTC has implemented a multi-faceted approach that includes strategic research and data analysis initiatives, robust law enforcement, and vigorous consumer education and outreach. I am pleased to present highlights from each of these facets of our work.

I. Older Adult Consumer Reporting Trends

The FTC collects and analyzes consumer report information through its Consumer Sentinel Network (“Sentinel”) to inform its consumer protection mission. Sentinel is a secure online database that provides federal, state, and local law enforcement agencies with access to reports about fraud and other consumer problems. Government agencies and other organizations³ contribute consumer reports to the database, which is searchable by criteria such as the type of fraud or problem and the name, address, and telephone number of the reported entity. Using Sentinel, the FTC and its law enforcement partners can analyze reports filed by older adults to

¹ The views expressed in this statement represent the views of the Commission. My oral presentation and responses are my own and do not necessarily reflect the views of the Commission or any individual Commissioner.

² I am referring to persons 60 and older when using the terms “older adults” or “older consumers.”

³ Data contributors are listed at <https://www.ftc.gov/enforcement/consumer-sentinel-network/data-contributors>.

look for patterns and trends, identify problematic business practices and enforcement targets, and develop cases against targets under investigation.

During calendar year 2020, Sentinel took in more than 4.8 million reports, both directly and through its data contributors, about problems consumers experienced in the market. Of that number, nearly 2.3 million reports were about fraud, nearly 1.4 million were about identity theft, and more than 1.2 million were about other consumer problems.⁴ Consumers reported losing over \$3.4 billion to fraud in 2020. About 45% of fraud reports filed in 2020 included age information. Consumers who said they were 60 and older filed 334,411 fraud reports with reported losses of more than \$600 million. Because the vast majority of frauds are not reported to the government, these numbers represent only a fraction of the older adults harmed by fraud.⁵

Older adults (ages 60 and over) are good reporters of their experiences with scammers. They file reports about frauds they have spotted but have not lost money to at a higher rate than younger adults (ages 20-59). Contrary to what many people may believe, younger adults are **more** likely to report losing money to fraud than older adults. The disturbing trend in the reporting data is that older adults in 2020 reported much higher individual median dollar losses than younger adults (ages 20-59). The disparity in reported losses was particularly large among people 80-plus, who reported the largest median losses of \$1,300.

⁴ See generally FTC, *FTC Consumer Sentinel Network* (July 29, 2021 update), available at <https://public.tableau.com/profile/federal.trade.commission>. Figures do not include reports about unwanted calls. Sentinel data is self-reported and not a survey. As such, individuals decide whether to file a report and decide what information, if any, to provide. Not all consumers who file a report provide their age, payment method, amount of dollar loss, and other data. As referenced in the text above, “other consumer problems” includes various categories of reports not classified as fraud, such as auto-related reports and reports about cable and satellite TV.

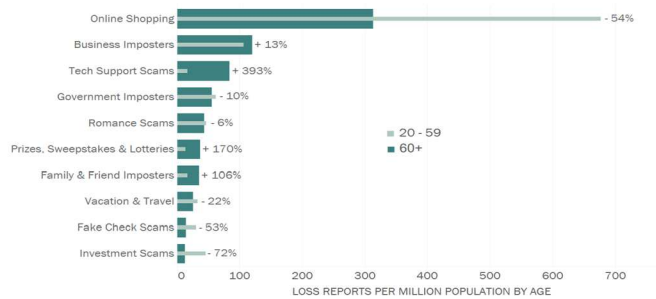
⁵ See Anderson, K. B., *To Whom Do Victims of Mass-Market Consumer Fraud Complain?* at 1 (May 2021), available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3852323 (study showed only 4.8% of people who experienced mass-market consumer fraud complained to a Better Business Bureau (“BBB”) or a government entity).

Reports Show Older Americans were Disproportionately Affected in Certain Scams

Online shopping fraud, which has been on the rise during the pandemic, was the most commonly reported category of fraud in which people of all ages indicated they lost money. However, older adults were **less** likely to report losing money to online shopping fraud than younger adults.⁶ Older adults continued to be much **more** likely than younger people to report losing money on tech support scams,⁷ prize, sweepstakes and lottery scams, and family and friend impersonation scams.⁸ Figure 1 shows the number of reports by fraud type and age group.

FIGURE 1: 2020 LOSS REPORTS BY AGE AND FRAUD TYPE

Older and younger consumers differ on loss reporting rates by fraud type. Percentages indicate the difference in the loss reporting rates for each fraud type by older adults as compared to consumers ages 20 - 59.



Fraud types ranked by the number of loss reports filed by consumers 60 and over. Sentinel fraud types classified as "unspecified" are excluded. Reports provided by the Internet Crimes Complaint Center are excluded due to differences in the report categorization. Figures are normalized using U.S. Census Bureau data for population by age. See U.S. Census Bureau, Annual Estimates of the Resident Population for Selected Age Groups by Sex for the United States (June 2020).

⁶ Reports of online shopping fraud increased sharply in the second quarter of 2020 as online marketers failed to deliver masks and other scarce items needed during the COVID-19 pandemic. Overall, reports of losses to online shopping fraud by older adults more than doubled in 2020, and the numbers continued to be far higher than pre-pandemic levels in the first half of 2021. The reported median individual dollar loss to online shopping fraud by older adults in 2020 was \$95. While substantial for many, it is on the lower end of losses, relative to other fraud categories.

⁷ These scammers impersonate well-known technology companies and computer repair companies to convince consumers there is something wrong with their computer and they must pay for the repair.

⁸ These scammers impersonate friends and family members including grandchildren, convincing the consumer to send money to save a loved one in a dire situation such as jail, or a hospitalization following a car accident.

Romance scams;⁹ prize, sweepstakes and lottery scams; and business impersonator scams caused the highest aggregate reported losses to older adults. Analysis of total dollars reported lost by older adults by fraud type, shown in Figure 2, highlights the immense financial harm caused by these scams. Reported losses to romance scams have increased significantly in recent years, and this trend accelerated during the COVID-19 pandemic.¹⁰ For older adults, reported losses to romance scams increased from nearly \$84 million in 2019 to about \$139 million in 2020. Among older adults, hardest hit were the 60-69 and 70-79 age groups, which reported \$129 million of the 2020 reported losses, making romance scams the category of highest reported losses for both groups. Prize, sweepstakes, and lottery scams ranked next, taking \$69 million from adults 60 and over in 2020. Over \$31 million of the reported losses on prize, sweepstakes, and lottery scams were reported by adults 80 and over, far higher than any other fraud category for this age group.¹¹ Reported losses by older adults from business imposter scams increased from \$34 million in 2019 to \$65 million in 2020.¹² Reported losses to government imposter scams by older adults showed modest decline in 2020 as compared to 2019.¹³ Notably, aggregate reported dollar losses by older adults on investment scams nearly

⁹ These scammers use fake dating profiles to impersonate people supposedly looking for romantic relationships online. They ultimately convince their love interests to send them money.

¹⁰ FTC Consumer Protection Data Spotlight, *Romance scams take record dollars in 2020* (Feb. 10, 2021), available at <https://www.ftc.gov/news-events/blogs/data-spotlight/2021/02/romance-scams-take-record-dollars-2020>.

¹¹ Government imposter scams, with \$11 million reported lost, ranked second to prize, sweepstakes, and lottery on aggregate reported dollar losses by adults 80 and older in 2020.

¹² This increase is due, in part, to a sharp increase in reports of losses to scammers posing as Amazon, who reportedly contact consumers with false claims about compromised accounts or unauthorized purchases.

¹³ Older adults filed more loss reports about Social Security Administration (“SSA”) impersonation scams in both 2019 and 2020 than about any other government imposter scam, but the numbers of loss reports by older adults to SSA impersonators declined from 1,838 in 2019 to 971 in 2020.

doubled in 2020, and reports of losses on phony cryptocurrency investment opportunities by older adults increased nearly fivefold in the fourth quarter.¹⁴

FIGURE 2: 2020 TOP FRAUD TYPES BY TOTAL DOLLARS LOST (AGES 60 AND OVER)

Aggregate reported losses by older adults increased in 2020 on all top frauds with the exception of government imposter scams.



Percent change from 2019 is shown in parenthesis. Sentinel fraud types classified as "unspecified" are excluded. The Art, Gems & Rare Coin Investments, Investment Seminars and Advice, Stocks & Commodity Futures Trading, and Miscellaneous Investments fraud types are grouped as "Investments" for this visualization. Reports provided by the Internet Crimes Complaint Center are excluded due to differences in report categorization.

Top Contact Methods Reported Show Rise in Online Contacts

Reports by older adults of losses to frauds initiated online were the most frequent, but reported median individual losses were highest for frauds that started with a phone call. Reports to Sentinel suggest online contact methods are increasingly used to defraud older adults. Understandably, this trend became more pronounced with the COVID-19 pandemic. In 2020, the tremendous volume of loss reports about online shopping fraud combined with loss reports about other online frauds eclipsed phone fraud for the first time. Notably, people 80 and over were an exception in that this age group continued to report losses to phone frauds far more frequently

¹⁴ See FTC Consumer Protection Data Spotlight, *Cryptocurrency buzz drives record investment scam losses* (May 17, 2021), available at <https://www.ftc.gov/news-events/blogs/data-spotlight/2021/05/cryptocurrency-buzz-drives-record-investment-scam-losses>.

than online fraud.¹⁵ Also noteworthy is the increase in scams that started on social media.

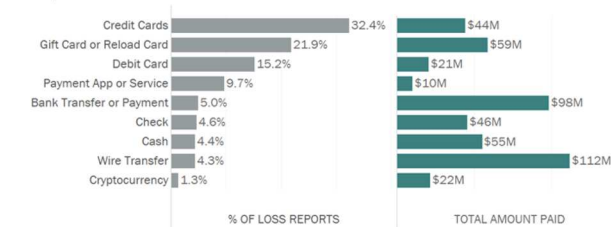
Reports indicating a loss to frauds that reached older adults via social media more than doubled, from 1,955 reports in 2019 to 5,169 reports in 2020, and 5,998 such reports were submitted in the first half of 2021 alone.¹⁶

Top Payment Methods Tell a Familiar Story but Cryptocurrency Payments Grow

People reporting fraud frequently indicate the payment method they used. The first column in Figure 3 shows that, in 2020, older adults most often reported paying scammers with credit cards, followed by gift cards or reload cards. The second column in Figure 3 shows the aggregate dollar losses that older adults reported for the payment methods shown. Aggregate losses reported by older adults were highest on wire transfers.

FIGURE 3: 2020 PAYMENT METHODS AND TOTAL AMOUNT PAID (AGES 60 AND OVER)

Credit cards were the most frequently reported payment method, but wire transfers were highest on total reported dollar losses.



Percentage calculations based on 58,173 loss reports directly to FTC by consumers ages 60+ indicating a payment method. Wire transfer companies MoneyGram International and Western Union, and reload card provider Green Dot, contribute a significant number of reports to Sentinel each year. To avoid distorting the number of reports indicating certain payment methods, data provided by data contributors are excluded.

¹⁵ In 2020, 48% of reports indicating a dollar loss by adults 80 and over were phone frauds and 23% were online frauds. By comparison, 22% of reports indicating a dollar loss by adults 60 to 79 were phone frauds and 38% were online frauds. These percentage calculations exclude reports that did not indicate a method of contact. Moreover, the median individual reported loss to phone fraud was \$3,000 for people 80 and over compared to \$1,500 for people ages 69 to 79.

¹⁶ See FTC Consumer Protection Data Spotlight, *Scams starting on social media proliferate in early 2020* (Oct. 21, 2020), available at <https://www.ftc.gov/news-events/blogs/data-spotlight/2020/10/scams-starting-social-media-proliferate-early-2020>.

As Figure 3 shows, gift cards and reload cards were the second most frequently reported payment method by older adults in 2020. Gift cards and reload cards were the top payment method older adults reported using on impersonator scams. After a year of modest declines, these reports surged to record levels in the second half of 2020. This resurgence was related to a sharp increase in reports of scammers posing as well-known businesses. Further, compared to 2019, reports of bank transfers and payments by older adults more than doubled in 2020, and reports of cryptocurrency payments more than tripled. The growth in reports of romance scam by older adults was an important driver of these increases. Bank transfers and payments accounted for nearly a third of reported romance scam losses by older adults at \$31 million, and romance scammers reportedly took another \$12 million in cryptocurrency. Another \$4 million were reported lost on cryptocurrency investment scams. Finally, older adults increasingly reported using payment apps or services such as PayPal. Those reports more than tripled in 2020 compared to 2019.

Pandemic-Related Fraud Reports Show Substantial Losses

In response to the pandemic, the FTC launched interactive dashboards to provide aggregate data about reports of frauds associated with COVID-19 and related stimulus money offers.¹⁷ Looking at this discrete set of data for 2020, older adults submitted over 26,518 fraud reports related to COVID-19 in 2020 with \$104 million in reported losses. The median individual reported loss for these reports was \$308, but, for adults ages 80 and over, the reported median individual loss was \$798. Pandemic-related online shopping frauds and government

¹⁷ This data is a subset of the 2020 fraud reports in Figures 1-3. COVID-19 related reports are reports that mention COVID, stimulus, N95 and related terms, along with those in which the consumer specifically flagged the report as related to COVID-19. These interactive dashboards, which are regularly updated, are available at <https://public.tableau.com/profile/federal.trade.commission#!/vizhome/COVID-19andStimulusReports/Map>. Nearly 100,000 people have viewed the dashboards to date.

impersonator scams were the most frequently reported by older adults in 2020. However, pandemic-related romance scams were highest on reported aggregate dollar losses.¹⁸ Many people reported that romance scammers used the pandemic to explain requests for money or their inability to meet in person.

II. Law Enforcement Actions to Protect Older Adults

Aggressive law enforcement is a vital component in the FTC's efforts to protect older adults.¹⁹ For many years, the FTC's anti-fraud program has combatted a range of the pernicious frauds affecting older consumers. While nearly all FTC enforcement actions involve consumers of all ages, the agency brought at least thirteen new actions in the past year that had a notable impact on older adults. Here are a few highlights from recent years of significant actions affecting older adults:

In *RagingBull.com*, the FTC alleged that the defendants fraudulently marketed investment-related services that they claimed would enable people to make consistent profits and beat the market.²⁰ Instead, the FTC alleged, consumers—including retirees, older adults, and immigrants—lost more than \$197 million in this scheme in only the last three years. The defendants claimed that people did not need a lot of time, money, or experience to make a substantial income. And the FTC alleged that, during 2020, the defendants employed additional marketing tactics based on the pandemic's impact on the stock market and the nationwide economic uncertainty. In March 2021, the court entered an order prohibiting misleading earnings claims and appointing a compliance monitor while the litigation is ongoing.

¹⁸ Reported losses by older adults on romance scams related to COVID-19 totaled \$10.5 million.

¹⁹ See, e.g., FTC, *Protecting Older Consumers 2019-2020* (Oct. 2019), available at <https://www.ftc.gov/reports/protecting-older-consumers-2019-2020-report-federal-trade-commission>.

²⁰ *FTC v. RagingBull.com, LLC*, No. 1:20-cv-3538 (D. Md. filed Dec. 7, 2020), available at <https://www.ftc.gov/enforcement/cases-proceedings/2023073/ragingbullcom>.

In *Quickwork*, the FTC alleged that the respondents deceptively marketed “Wellness Warrior” products as scientifically proven to treat or prevent COVID-19.²¹ According to the complaint, filed by the U.S. Department of Justice (“DOJ”) on the FTC’s behalf, the respondents baselessly claimed that Wellness Warrior products containing Vitamin D and zinc treat or prevent COVID-19, are scientifically proven to work, and are more effective at preventing the disease than approved vaccines. In May 2021, the court entered a stipulated preliminary injunction, prohibiting the respondents from continuing to deceptively market these products. The court also required them to remove all links containing deceptive claims from all websites, social media accounts, and other domains under their control. Litigation is ongoing.

Complementing law enforcement actions, the FTC has sent hundreds of cease and desist letters, more than 80 since October 2020, about potentially false or deceptive marketing related to the pandemic.²² COVID-19 obviously has had and continues to have a particularly devastating impact on older Americans.²³ Overwhelmingly, companies that received the FTC’s letters quickly removed the misleading COVID-19 claims from their advertising. However, when a cease and desist letter would not work or would not be appropriate given the conduct at issue, the FTC has pursued law enforcement. In *FTC v. Golden Sunrise Nutraceutical*, the Commission sued a company that failed to heed a warning urging removal of deceptive claims that its products were scientifically proven to treat COVID-19, and obtained a court order barring the defendants from making unsubstantiated health claims and requiring them to refund defrauded

²¹ *United States v. Quickwork, LLC*, No. 4:21-cv-00437 (E.D. Mo. filed Apr. 15, 2021), available at <https://www.ftc.gov/enforcement/cases-proceedings/202-3188/quickwork-llc-eric-nepute>.

²² Information about these letters can be found at <https://www.ftc.gov/coronavirus/enforcement/warning-letters>.

²³ Not only are older adults more likely to get sick from COVID, they are also more likely to face drastic health-related consequences as a result. See Center for Disease Control and Prevention Guidance (updated Aug. 2, 2021), available at <https://www.cdc.gov/coronavirus/2019-ncov/need-extra-precautions/older-adults.html>.

consumers.²⁴ *United States v. Quickwork, LLC*, mentioned above, is another case stemming from the failure to heed an FTC letter demanding cessation of deceptive COVID-19 treatment and prevention claims.

More generally, both before and during the pandemic, the FTC has brought actions halting a variety of scams, including those identified through our data analysis as scams harming older adults, such as impersonation and romance scams. One approach has been to sue providers who facilitate or play a role in such schemes. Here are some recent examples:

In the past few years the FTC has sued Voice over Internet Protocol (“VoIP”) providers for their role in facilitating illegal calls. For example, in *Alcazar Networks*, the FTC settled with the VoIP provider for allegedly facilitating tens of millions of illegal telemarketing calls, including calls that impersonated SSA and displayed spoofed caller ID numbers, such as “911.”²⁵

Perpetrators of many different types of scams — including those that especially affect older adults, such as prize and sweepstakes schemes, romance scams, grandparent and other impersonator scams — rely on money transfer systems to obtain money from consumers.²⁶ The FTC has sued both of the major U.S. providers. In November 2018, *MoneyGram* agreed to settle allegations that the company failed to take steps required under a prior FTC order to crack down on fraudulent money transfers that cost U.S. consumers millions of dollars.²⁷ In February 2021,

²⁴ *FTC v. Golden Sunrise Nutraceutical, Inc.*, No. 1:20-at-00540 (E.D. Cal. filed July 30, 2020), available at <https://www.ftc.gov/enforcement/cases-proceedings/202-3146-x200051/golden-sunrise-nutraceutical-inc>.

²⁵ *FTC v. Alcazar Networks, Inc.*, No. 6:20-cv-2200 (M.D. Fla. filed Dec. 3, 2020), available at <https://www.ftc.gov/enforcement/cases-proceedings/1923259/alcazar-networks-inc>.

²⁶ Scammers know that money sent through money transfer systems can be picked up quickly and anonymously at locations all over the world—and once the money is paid out, it is all but impossible for people to get their money back. See, e.g., *Before You Wire Money*, FTC Consumer Information, available at <https://www.consumer.ftc.gov/articles/before-you-wire-money> (last visited Sept. 20, 2021).

²⁷ *FTC v. MoneyGram Intl, Inc.*, No. 09-cv-6576 (N.D. Ill. filed Oct. 20, 2009), available at <https://www.ftc.gov/enforcement/cases-proceedings/062-3187/moneygram-international-inc>.

the claims process began to eventually deliver nearly \$125 million in redress to people allegedly defrauded by scammers who were aided by MoneyGram. In January 2017, *Western Union* entered into an agreement with the FTC, DOJ, and others to resolve charges related to its role in fraudulent money transfers on its system.²⁸ The FTC's complaint alleged that, for many years, Western Union was aware that fraudsters used the company's system to bilk consumers, and that some Western Union agents were complicit in the frauds. The complaint listed some of the frauds such as lottery and prize scams, emergency scams including grandparent scams, and romance scams. In March and September 2020, affected consumers received refunds resulting from the actions, amounting to over \$300 million, which reflected 100 percent of their verified losses.

Online dating services often are used to find and contact potential romance scam victims. Fraudsters create fake profiles, establish trusting relationships, and then trick consumers into giving or loaning them money. In 2019, the FTC sued online dating service *Match*, alleging that the company used fake love interest advertisements to trick hundreds of thousands of consumers into purchasing paid subscriptions.²⁹ The FTC alleged that Match unfairly exposed consumers to the risk of fraud by encouraging people to pay for subscriptions via messages the company knew were from scammers. Litigation is ongoing.

In pursuing law enforcement actions that have the largest possible impact, the FTC also coordinates with federal, state, local, and international agencies, including those with criminal authority, leveraging resources to track down fraudsters and build actions to stop them. With the DOJ, the FTC organizes and participates in the Global Anti-fraud Enforcement Network, a

²⁸ *FTC v. The Western Union Company*, No. 1:17-cv-00110-CCC (M.D. Pa. filed Jan. 19, 2017), available at <https://www.ftc.gov/enforcement/cases-proceedings/122-3208/western-union-company>.

²⁹ *FTC v. Match Group, Inc.*, No. 3:19-02281 (N.D. Tex. filed Sept. 25, 2019), available at <https://www.ftc.gov/enforcement/cases-proceedings/172-3013/match-group-inc>.

multilateral network of agencies that enforces laws prohibiting mass marketing fraud. The Network has been pivotal in enforcement actions against entities that have defrauded millions of older consumers. Further, the FTC has continued to be an active member of the Elder Justice Coordinating Council, a multi-agency federal entity charged with identifying and proposing solutions to elder abuse, neglect, and financial exploitation.

III. Returning Money to Older Americans Harmed by Scams

Returning money to consumers harmed by scammers has been a cornerstone of the FTC's law enforcement actions. These cases have resulted in redress totaling more than \$358 million to consumers of all ages so far during Fiscal Year 2021. These payments provide people some recompense for losses from illegal conduct.³⁰ Thus far this year, the agency has distributed funds to consumers or conducted the claims process in at least eleven cases that notably affected older consumers.³¹

The FTC's ability to obtain monetary relief pursuant to Section 13(b) of the FTC Act is now substantially limited following the Supreme Court's decision in *AMG Capital Mgmt., LLC v. FTC*, 141 S. Ct. 1341 (Apr. 2021). Restoring this critical tool to redress consumers is vital to the FTC's mission to safeguard the American public.³² The FTC's authority to obtain monetary

³⁰ The FTC provides updated statistics about where refunds were sent, the dollar amounts refunded, and the number of people who benefited from FTC refund programs at

https://public.tableau.com/app/profile/federal.trade.commission/viz/Refunds_15797958402020/RefundsbyCase.

³¹ See, e.g., Press Release, FTC, *Federal Trade Commission Sending Refunds to More than 31,000 Consumers Allegedly Defrauded by Online Training Academy* (Aug. 16, 2021), available at <https://www.ftc.gov/news-events/press-releases/2021/08/federal-trade-commission-sending-refunds-more-31000-consumers>; Press Release, FTC, *FTC Returns Almost \$775,000 to Consumers Who Purchased Deceptively Advertised Arthritis and Joint Pain Relief Supplement Synovia from A.S. Research, LLC* (Dec. 1, 2020), available at <https://www.ftc.gov/news-events/press-releases/2020/12/ftc-returns-almost-775000-consumers-who-purchased-deceptively>; Press Release, FTC, *FTC Sending Refund Checks Totaling Almost \$149,000 to Consumers Who Bought Rejuvenation "Anti-Aging" Pill* (June 1, 2020), available at <https://www.ftc.gov/news-events/press-releases/2020/06/ftc-sending-refund-checks-totaling-almost-149000-consumers-who>.

³² The FTC is urging Congress to pass a legislative fix. See Press Release, FTC, *FTC Asks Congress to Pass Legislation Reviving the Agency's Authority to Return Money to Consumers Harmed by Law Violations and Keep Illegal Conduct from Reoccurring* (Apr. 27, 2021), available at <https://www.ftc.gov/news-events/press-releases/2021/04/ftc-asks-congress-pass-legislation-reviving-agencys-authority>.

relief has always been a powerful tool for making wronged consumers whole, but has been even more critical during the pandemic when so many Americans are struggling. This is particularly true for older adults who may be retired or on fixed incomes and cannot afford to lose money to fraud

IV. Outreach and Education Activities

Pass It On is the FTC’s ongoing fraud prevention education campaign for older adults. Campaign materials show respect for the readers’ life experience and accumulated knowledge, and supply them with resources to read and “pass on” to family and friends to start conversations about fraud. The factsheets, bookmarks, videos, presentations, and other materials refresh and add to readers’ knowledge by briefly explaining how certain scams work and what a reader can do in response. Since the *Pass It On* campaign began in 2014, its print and online material has expanded, based in part on community partners’ requests, to address many common frauds.³³ The FTC has distributed 15.6 million *Pass It On* items since the campaign began, including more than 920,000 items in Fiscal Year 2021. The free English and Spanish material is available at ftc.gov/PassItOn, ftc.gov/pasalo (Spanish), and ftc.gov/bulkorder.

The FTC emails Consumer Alerts about many of the topics covered by *Pass It On* and other topics of interest to older adults. The FTC emails the Alerts in English and Spanish to nearly 385,000 subscribers, which include individuals, community groups, advocates, national and local news media outlets, and other stakeholders. The FTC also posts these Alerts and materials on its consumer website, consumer.ftc.gov, so the public can read, link to, and share

³³ These include: Identity Theft; Tech Support Scams; Home Repair Scams; Imposter Scams; Grandkid Scams; Work-at-Home Scams; Charity Fraud; Online Dating Scams; Money Mule Scams; Health Care Scams; IRS Imposter Scams; “You’ve Won” Scams; and Unwanted Calls.

the prevention messages.³⁴ In honor of Older Americans Month in May 2021, the FTC published a series of Alerts focused on scams that harm older adults,³⁵ and the agency has issued more than 160 Alerts on pandemic-related topics, including COVID-19 vaccines, stimulus payments, health and treatment claims, government imposter scams, and privacy issues. The FTC published a Consumer Alert about what to do if a nursing home or care facility wrongfully took someone's stimulus check,³⁶ and a related Business Alert, warning nursing facilities that having residents sign over their check to the facility contradicts the law.³⁷

The FTC collaborates with many organizations across the country to share its consumer education messages and inform the public about its work. In the past year, FTC staff in Washington, DC and eight regional offices have presented, exhibited, or participated in more than 280 outreach events with the public, other law enforcement agencies, and stakeholders focused on protecting members of a wide range of communities from scams. At least 120 outreach events served older adults and the people who work with them or engaged partner organizations in discussions about issues that affect older adults. During this time, a large part of the FTC's outreach and education work focused on issues related to the coronavirus pandemic.

In the past year, FTC staff participated in events for older adults together with local, state, and federal organizations, including the BBB, Senior Medicare Patrols, public libraries, consumer organizations, legal services providers, as well as attorneys general offices and federal agencies like the Consumer Financial Protection Bureau and the Federal Emergency Management Agency. Staff joined in more than a dozen events with AARP, including

³⁴ Information about subscribing to the FTC's Consumer Alerts is available at www.ftc.gov/subscribe.

³⁵ Consumer Alert, FTC, *Celebrating Older Americans Month* (May 10, 2021), available at <https://www.consumer.ftc.gov/blog/2021/05/celebrating-older-americans-month-0>.

³⁶ Consumer Alert, FTC, *Stimulus payments for people, not nursing homes* (Jan. 4, 2021), available at <https://www.consumer.ftc.gov/blog/2021/01/stimulus-payments-people-not-nursing-homes>.

³⁷ Business Blog, FTC, *Nursing Homes: Stimulus payments are for residents* (Jan 4, 2021), available at <https://www.ftc.gov/news-events/blogs/business-blog/2021/01/nursing-homes-stimulus-payments-are-residents>.

nationwide Facebook Live conversations in English and Spanish about COVID-19 scams, identity theft, and cyberscams, and national tele-town halls. Staff also discussed scams that affect older adults at several conferences, including events organized by the American Bar Association's Commission on Law and Aging, ADvancing States, and the American Society on Aging. The FTC's outreach partnerships with groups and communities throughout the country provide opportunities to share important prevention messages, and foster communication lines so the FTC learns in real-time about scams and other consumer problems affecting the public. This, in turn, can generate ideas for policy and education initiatives, as well as new case leads.

Shortly after the coronavirus pandemic began, the FTC developed a multi-media campaign with consumer and business advice to respond to people's needs, all available at [ftc.gov/coronavirus](https://www.ftc.gov/coronavirus). This webpage, available in English and Spanish, serves as a one-stop directory of the FTC's coronavirus education resources for consumers and businesses. It also contains links to information about FTC enforcement actions related to the pandemic, and connects to the FTC's fraud-reporting system. Visitors have collectively viewed approximately 7.8 million pages of the FTC's coronavirus-related material.

During FY 2021, FTC staff conducted nearly 100 pandemic-related local and national outreach events with partners. The agency engaged with ethnic media, community organizations, community advocates, and many others through webinars, tele-town halls, Twitter chats, Facebook Live events, and interviews with local, state, and national media.

As the pandemic has continued, new consumer financial issues have emerged and others worsened. To ensure it is responding to the issues people are facing, the FTC staff coordinated a series of virtual listening sessions across the country. Session participants included representatives from elder justice centers, departments of aging, legal services, social services,

housing counselors, faith-based groups, the BBB, and the offices of state attorneys general who shared their knowledge and concerns about the pandemic's effects in their communities. Based on stakeholders' comments, the FTC is working to enhance and expand its COVID-19 financial recovery and resiliency campaign, and to create a web-based toolkit in multiple languages.

V. Conclusion

The FTC remains firmly committed to protecting older adults through aggressive law enforcement and effective consumer education and outreach. Research, law enforcement experience, and input from stakeholders will continue to be critical as the Commission innovates in using its resources to protect older adults in the years ahead.

The FTC is grateful to this Committee and others for the work you are doing to ensure our work to protect older consumers can continue. Of particular importance is the work to restore the FTC's ability to secure monetary relief from those that violate the law. Until the Supreme Court's decision in *AMG*, the FTC relied on Section 13(b) of the FTC Act to return billions of dollars to defrauded consumers, and to ensure that lawbreaking companies could not pocket their ill-gotten gains. Unless the agency has clear authority to obtain monetary relief, this decision will continue to impede our ability to provide refunds to people harmed by deceptive, unfair, or anticompetitive conduct.

I look forward to your questions.



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](https://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 Stim/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's²⁹ 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.

Kate Kleinert: Written Testimony*Glenolden, Pennsylvania*

Chairman Casey, Ranking Member Scott, and members of the Aging Committee, my name is Kate Kleinert and I am a scam survivor. I am from Glenolden, Pennsylvania, and I have been widowed for 12 years. My husband Bernie passed away in 2009. Since then, I've never looked for any new romance in my life because I still feel married to my husband. I was not interested in finding another love.

But last summer, in August 2020, I received a friend request on Facebook that caught my eye. It was unfortunately the one in a million that I decided to accept and become friends with. His name is Tony – well, that's what he told me. We exchanged messages for a number of days and he told me that he was interested in the same things that he saw on my Facebook page, like dogs and gardening. I thought that was wonderful.

We started talking on the phone through an App he had me download. He told me he was a surgeon working in Iraq through a contract with the United Nations and that he has two children, a little boy and a girl. Tony became romantic much more quickly than I did and I kept trying to put him off, saying we didn't know each other. But Tony had the kids get in touch with me through email and they started calling me

mom, which is my Achilles' heel, because I didn't have children of my own. That put me head over heels.

The first request for money came from the girl who needed some feminine supplies but was embarrassed to ask her father. I sent her a gift card. I would go to any store, buy a gift card, take a picture of the front, the back, and the receipt, and send her that information and she could use it to make purchase. From then, there was always some kind of an emergency or some urgent need for money.

Things also became more serious between us. Tony wanted to get married. He even asked if I wanted to go out and start looking at houses. I was constantly sending him gift cards, even though now I was using up the last of my husband's life insurance. My savings were gone. I was living on my credit cards and he was getting what I took from Social Security and my pension. And all this time, only one person, an employee at a drug store, ever asked me if I knew who I was sending these gift cards to. I kept doing this because he swore to me he would repay me the minute he got back to the states and even sent me his passwords to his account at Bank of America so I could see his balance, which was a little over 2 million dollars.

When he was finally allowed vacation, Tony was going to fly to Philadelphia on December 10 and I was going to go pick him up. I was so excited. I got all dressed up, my hair was done, and my nails were done. I waited all night long. He never called and, even at this point, I never considered that it was a scam, I was just worried

about him. Then, the next morning, I got a phone call from a man who said he was Tony's lawyer, who said that in Iraq, someone slipped drugs into Tony's bag and he knew nothing about it, but now he needed money for bail. He asked me for \$20,000. The lawyer told me to do whatever I could – put a mortgage on my house, borrow it from someone in my family. I couldn't do it.

I became suspicious when I asked to meet Tony in-person but the lawyer said that he had been transferred to Oklahoma. I became even more suspicious when Tony started calling me himself five or six times a day from prison, asking for more gift cards to buy better food in prison. Something was not right. By now, I had sent him a total of \$39,000, which to some people is not much but someone in my position it's a great deal. I am still paying for that today because I can't get things repaired at the house. I've had no air-conditioning this summer, my refrigerator is off and my stove is off. I have been leaning on my family, my sisters especially, to get me through this. But the loss that hurts the most was losing his love and losing the family I thought I was going to have and what my new future was going to be. That is much harder to deal with than losing the money.

I have since come to find out that all these pictures he sent me of himself were actually of a doctor in Spain. I tried to report this to the police but could not get anyone to listen to me. I also called AARP's fraud number that I found in their magazine, and got a retired detective who was supportive and encouraged me to share

my story. But I have been frustrated at the lack of options to recover the money I've lost or the ability to hold him responsible for these damages. But even though this experience is painful to speak about, I want to be an ambassador to this experience because it's so devastating and many people have been through this but not spoken about it. They continue to carry this weight around. But in my case, I got pulled in because I had forgotten how good it felt to be loved.

Thank you.

Testimony of Vee Daniel

President / CEO, Better Business Bureau Serving Upstate South Carolina

“Fraud, Scams and COVID-19: How con artists have targeted older Americans during the pandemic”

United States Senate Special Committee on Aging

September 24, 2021

Chairman Casey, Ranking Member Tim Scott, and distinguished members of the Committee, thank you for the opportunity to testify today on the topic of, “Fraud Scams and COVID-19: How con artists have targeted older Americans during the pandemic.”

My name is Vee Daniel, I’m a Catawba College Communication Major graduate, mother of an early childhood teacher, intern architect, and a new grandmother. I’ll be celebrating my 30th wedding anniversary this year.

I serve as president and CEO of the Better Business Bureau of the Upstate and Better Business Bureau Education Foundation, a position I’ve held since 2011. BBB is a nonprofit promoting trust between consumers and businesses in the marketplace and has been around for more than 100 years. When I first was offered the job, I was intrigued. I grew up with a father who was a huge advocate for BBB. When his friends needed assistance with customer service issues, he would always say “call the BBB.”

With a few weeks on the job, I received an invitation to speak to a senior church group about the latest scams. I will never forget the day I spoke to those seniors and listened to their scam stories. It was heartbreaking. I learned to speak louder, ask questions, listen, and the most important part was realizing **education** is the key to fighting senior fraud. That’s when I knew this role with the BBB was the perfect fit for me. Since that day, I’ve never turned down an opportunity to speak to educate seniors. In 2015, we dubbed the program “Savvy Seniors,” because that’s what we want to achieve.

During the pandemic, we witnessed new scams that involved masks, non-FDA approved medical supplies, immunity boosting products, and equipment through online purchase scams relating to COVID-19. We have also seen fake websites, phishing emails that involved stimulus checks, price gouging, scammers impersonating government agencies like Medicare, and promoting fake vaccines. We have also seen an increase in romance scams during COVID-19.

The BBBs across the country rallied together to put out fraud prevention messages and we did thousands of media interviews to try to warn consumers about all the COVID-related scams we were seeing.

Senior groups were not able to meet during COVID-19, so we partnered with our local Appalachian Council of Governments Greenville office and Meals on Wheels to distribute 1,000 BBB Savvy Senior packets that included educational information on fraud and scams.

As part of a larger national effort, BBB of the Upstate has hosted Secure Your ID Day since 2008. Local BBBs from all across the United States and Canada join in on the event designed to protect consumers from the growing threat of identity theft and provide education. Consumers and businesses are encouraged to attend the free community service events and properly shred and destroy sensitive documents. In 2018, BBB of the Upstate partnered with AARP South Carolina and from that partnership we have increased our shred events from 4 to now 8 events a year. Last week, we held two events, one

in Greenville and one in Anderson, with two happening in October in Spartanburg and Simpsonville. About 90% of the attendees are seniors.

[BBB Scam Tracker](#) is an online platform that enables consumers and businesses to report scams and suspicious activities. The data is analyzed and reports are then made available to the general public, thus empowering consumers to avoid losing money to scammers. The website features a searchable "heat map" so users can view the number, types, and details about scams reported in their communities. BBB Scam Tracker data enables local BBBs to educate consumers and stop fraudsters by leveraging the power of technology and our network of BBBs serving communities throughout North America and Canada.

[Using data from BBB Scam Tracker](#), our foundation, the BBB Institute for Marketplace Trust released a report on the rise of online scams during the Covid-19 pandemic. The BBB Risk Index is a formula that looks at scams in a different way: the volume of each type of scam reported to BBB Scam Tracker, the susceptibility rate (that is, how many people who are exposed to the scam actually lose money), and the dollar loss. That formula shows us which scams are the riskiest, and it may not be for the scam with the most reports. For instance, romance scams were the riskiest for ages 55 through 64, followed by online purchase scams and investments scams. Travel/vacation/timeshare scams were the riskiest for ages 65+, followed by online purchase scams and romance scams.

Since BBB began tracking scams in this way in 2016, we've seen a clear pattern: although seniors are pretty savvy and tend to fall for scams less frequently than younger demographic groups, they lose more money. This is partly because the type of scams that target seniors -- romance scams, investment scams, family emergency scams -- tend to be higher dollar amounts. Although many seniors have gotten the message and are more cautious than in the past, too many are still falling victim to unscrupulous criminals. BBB is proud of the role we play in educating seniors and all consumers, but there is much more that can be done and we appreciate the attention this issue is getting.

Thank you for this opportunity to be a witness today on this relevant topic of how con artists have targeted older Americans during the pandemic.

Questions and Responses for the Record

**Questions for the Record for Lois Greisman
From Senator Robert P. Casey, Jr.**

Question:

- 1) Your testimony noted that the scammers have increasingly used peer-to-peer (P2P) payment methods such as Venmo, Zelle, CashApp to older adults, which has been reflected by growing reports of fraud to the FTC.
 - a. What factors do you attributed to the increased use of P2P platforms to target seniors for frauds and scams?

Response:

My testimony noted an increase in the number of reports filed with the FTC's Consumer Sentinel System ("Sentinel") in 2020 by older adults who stated they lost money using a payment service or app. This amounted to 9.7% of the reports from older adults that included a payment method, and accounted for approximately \$10 million of loss in 2020. As with other trends on consumer reporting, it is difficult to discern the specific factors that account for the rise in these types of reports. As more people use payment services and apps, it is likely we will see increased numbers of consumer reports about their use in fraud. We know that fraudsters prefer payment methods that are easy to cash out and offer more anonymity than other methods.

- b. Are there risk factors that the FTC has identified that make a person more susceptible to a P2P scam?

The FTC has not identified any risk factors unique to P2P payment methods that are not also present with other methods. As with other payment methods, the ease with which consumers may make payments to individuals they have never met on P2P platforms facilitates quick purchasing decisions. Scammers are very good at what they do and seek out payment methods where they can gain access to funds quickly, and remain as anonymous as possible, making it difficult to track them down.

- c. Is there any evidence that P2P scams target specific populations disproportionately?

The FTC does not have evidence of specific targeting of certain populations for P2P scams. However, see the information below about FTC Sentinel reporting data with regard to age and demographic reporting trends.

Question:

- 2) Please provide additional data regarding these issues of P2P payment scams, including but not limited to:
- Patterns and trends associated with these payment methods;
 - The types of scams they tend to be associated with;
 - Any available demographic information including age, geography, economic status and ethnicity; and
 - The average and median dollar amounts lost by scam survivors.

Response:

The information below includes consumers reporting data from the FTC's Consumer Sentinel Network from 2017 through September 2021. The data show an increase in reports that indicate the consumer's experience involved a payment service or app. Note that the FTC has seen an increase in reports overall each year listed.

Number of Reports with Payment Services and Apps as the method of payment

	2021	2020	2019	2018	2017
Total Reports	41,914	49,170	15,715	8,573	5,883
Median amounts lost	\$395.96	\$220.00	\$240.00	\$200.00	\$165.00

Top 5 Report Categories

Report Subcategory	2021	2020	2019	2018	2017
Online Shopping	24,903	31,191	8,944	4,572	3,442
Business Imposters	4,643	3,921	1,108	813	429
Romance Scams	1,928	1,455	384	151	52
Miscellaneous Investments	1,818	1,085	122	66	41
Fake Check Scams	1,686	1,891	631	195	78

Demographics: People filing reports may provide their age if they wish, but the FTC does not collect race, ethnicity, or income level.

Consumer Age

	2021	2020	2019	2018	2017
19 and Under	3,018	3,550	1,136	407	252
20 - 29	11,005	11,862	3,941	1,861	1,163
30 - 39	8,358	9,496	3,058	1,657	1,246
40 - 49	6,513	7,465	2,137	1,199	899
50 - 59	4,949	5,382	1,528	916	634
60 - 69	3,485	3,648	1,041	688	439
70 - 79	1,410	1,354	420	279	167
80 and Over	193	195	68	60	37

Recent analysis of the Sentinel reports received in 2020 by an FTC economist provides some relevant information. Dr. Devesh Raval matched the zip code information voluntarily provided when people filed Sentinel reports in 2020 to the U.S. Census Bureau's demographics information for those zip code areas. Analyzing the aggregate information, Dr. Raval could draw inferences as to the likely demographics of the consumers filing reports and provide insight into the reporting trends for majority Black, Latino, and White communities. That research showed that people living in majority Black communities filed more reports indicating the payment method was a payment service or app than people living in Latino and White communities.¹

Question:

- 3) What, if any, engagement has the FTC had with P2P companies, industry associations or other related entities to address the increasing use of these platforms for scam payments? To the extent that FTC has engaged such companies, associations or entities, please provide information about how they have been engaged, and any commitments they have made to address these issues.

Response:

The FTC frequently engages with consumers, advocates, and industry regarding consumer protection issues and has conducted workshops on fintech issues that have involved engagement with the industry. In 2016, the agency conducted a forum on P2P payment methods that brought together government, industry participants, consumer advocates, and other stakeholders to discuss frauds and scams that could target these platforms, dispute resolution best practices, privacy and security concerns, as well as fee disclosures.² The FTC does not typically obtain commitments from an industry. Following this forum, the FTC publicized advice for companies that included developing clear policies regarding unauthorized payments and explaining those policies up front, so consumers understand what to expect if there is a dispute.³

¹ *Serving Communities of Color*, FTC Staff Report, (Oct. 15, 2021) available at <https://www.ftc.gov/reports/serving-communities-color-staff-report-federal-trade-commissions-efforts-address-fraud>.

² Information about the FinTech Forum: A closer look at peer-to-peer payment systems and crowdfunding platforms is available at <https://www.ftc.gov/news-events/events-calendar/2016/10/fintech-series-crowdfunding-peer-peer-payments>.

³ FTC Business Blog, *FinTech Forum: A closer look at peer-to-peer payment systems and crowdfunding platforms* (Mar. 7, 2021) available at <https://www.ftc.gov/news-events/blogs/business-blog/2017/03/fintech-forum-closer-look-peer-peer-payment-systems>.

Question:

- 4) How is the FTC seeking to address the rise in scams on P2P platforms? The FTC is actively monitoring consumer reports for fraud on all payment systems. Given the rise in consumers' use of this payment method, staff is watching for potential targets and welcomes information from those who have experienced fraud using a P2P app. They can report this at reportfraud.ftc.gov.

Response:

Education is essential. The FTC has developed an important education piece, *Mobile Payment Apps: How To Avoid a Scam When You Use One*, that explains how these apps work, provides tips for how to avoid sending money to a scammer, and what to do if you sent money to a scammer using one of these services.⁴ This information, available in English and Spanish, is on the FTC's website. The agency has also issued consumer alerts on this topic, including an alert from February 2020 that provides tips for using peer to peer payment systems and apps, such as CashApp, Venmo, and Zelle.⁵ These alerts are sent out to over 330,000 subscribers, including consumer advocates and members of the media who share these messages more broadly.

Question:

- 5) Social media platforms play an increasing role in exposing older adults to romance and online purchases scammers. Companies like the Facebook allow users of their platforms to report suspicious profiles, posts or advertisements. Are these companies sharing information about scams with the FTC?

Response:

None of the social media companies is a data contributor to the Consumer Sentinel Network. Nevertheless, the FTC received a large number of reports about scams consumers encounter on social media. In 2020, the FTC received over 70,000 reports indicating that social media was the contact method. Last fall, the FTC issued a data spotlight, *Scams starting on social media proliferate in early 2020*, noting the increase in reports about scams starting on social media and describing a robust picture of a growing trend.⁶

⁴ FTC Article, *Mobile Payment Apps: How To Avoid a Scam When You Use One* (Dec. 2019) available at <https://www.consumer.ftc.gov/articles/mobile-payment-apps-how-avoid-scam-when-you-use-one>.

⁵ FTC Consumer Alert, *Making mobile payments? Protect yourself from scams* (Feb. 4, 2020) available at <https://www.consumer.ftc.gov/blog/2020/02/making-mobile-payments-protect-yourself-scams>; FTC Consumer Alert, *Tips for using peer-to-peer payment systems and apps* (Feb. 27, 2018) available at <https://www.consumer.ftc.gov/blog/2018/02/tips-using-peer-peer-payment-systems-and-apps>.

⁶ FTC Data Spotlight, *Scams starting on social media proliferate in early 2020* (Oct. 21, 2020) available at <https://www.ftc.gov/news-events/blogs/data-spotlight/2020/10/scams-starting-social-media-proliferate-early-2020>.

Question:

- 6) During the hearing, Ms. Kate Kleinert spoke about the need for effective educational interventions that are sensitive, timely and appropriate. What are effectiveness of its educational materials? If such research is taking place, is the FTC sharing the lessons with other Federal agencies, and state and local entities?

Response:

The bilingual [Pass It On Campaign](#) is the FTC's research-based fraud prevention education campaign designed for, and with input from, older adults. From the outset, the FTC sought the advice of older adults and those who work with them: from testing the hypothesis of the campaign approach, to getting input on the delivery of materials, to getting feedback on the actual content and design of the resources. Once launched, the FTC – through a contracted researcher – held interviews with individuals who had ordered and used Pass It On materials. The feedback from that research is consistent with the ongoing response of the aging network, law enforcement, librarians, federal and state government officials, and others who use Pass It On: these resources meet an important need in a timely way; explanations are clear, engaging, and not alarming; and it avoids condescension while respecting the life experience of the older adult.

The FTC has regularly shared with state and federal partners, organizations, and consumer advocates its knowledge about older adults, including communicating with older audiences about fraud, their interest in fraud prevention information, and their preference for plain language communication. For example, staff have presented at FTC events, to members of the Elder Justice Working Group, the American Society on Aging, Adult Protective Services, National Sheriffs' Association, International Association of Chiefs of Police, and AARP.

Question:

- 7) During the hearing, Ms. Kate Kleinert spoke about the need for greater efforts disseminate information about scams. How is the FTC ensuring that its educational resources are reaching older adults in their communities? What specific steps is the FTC taking to reach older adults who face challenges to access the FTC materials such as lack of Internet access or limited English proficiency?

Response:

The FTC proactively works to reach older adults where they are – in their own communities and through trusted partners. In FY2021, the FTC staff in Washington, DC and eight regional offices have presented, exhibited, or participated in at least 120 outreach events, working together with organizations that serve older adults to disseminate information about scams affecting their community. Events have ranged from national webinars and tele-town halls with groups like AARP and Village to Village Network; to outreach and webinars to local and grassroots organizations, SAGE, an advocacy and service organization for LGBTQ elders; and small and rural libraries that are members of the Association of Bookmobile and Outreach Services.

Recognizing the need to connect with older adults in hard-to-reach areas or those without internet access, the FTC mailed out information on avoiding scams to over 5,000 rural and urban community health clinics. The FTC's Pass It On resources are available for free in print form at ftc.gov/bulkorder (15.6 million campaign materials distributed so far). These, and other educational materials, are often ordered by nonprofit, state, and local organizations that serve older adults.

To ensure the FTC's materials are accessible to those with limited English proficiency, the Pass It On campaign uses simple, plain language in a short, easy-to-understand format. These resources, and many others, are translated into Spanish, which can be accessed at ftc.gov/pasalo.

**Questions for the Record for Lois Greisman
From Senator Rev. Raphael Warnock**

Question:

- 1) Can you discuss how Congress can help ensure that the FTC has the tools it needs to protect some of America's most vulnerable citizens against fraud and abuse?

Response:

The most important thing Congress can do right now to help the Commission continue its work in protecting seniors and other vulnerable consumers is to amend Section 13(b) of the FTC Act to restore the Commission's ability to obtain court orders requiring violators to pay monetary relief that the Commission can use to provide refunds to consumers who lost money as a result of frauds, scams, and other unlawful conduct.

As indicated in my testimony, the Supreme Court recently ruled in *AMG Capital Mgmt., LLC v. FTC*,⁷ that courts can no longer award the Commission monetary relief under Section 13(b) of the FTC Act. This ruling struck a huge blow to the Commission's ability to provide refunds to consumers who lost money due to unfair, deceptive, or anticompetitive practices. For four decades prior to the *AMG* decision, every federal court of appeals to consider the question concluded that the language in Section 13(b) and longstanding Supreme Court precedent authorized district courts to award equitable monetary relief such as refunds and disgorgement of ill-gotten gains. Based on this unanimous authority, district courts ordered defendants who engaged in deceptive, unfair, or anticompetitive conduct to pay the Commission monetary relief that the Commission distributed as refunds to harmed consumers. Over the past forty years, the Commission used the monetary relief courts awarded under Section 13(b) to provide billions of dollars in refunds to consumers. Many of the consumers who received refunds were seniors and other vulnerable Americans who lost money due to unlawful conduct that disproportionately impacts those groups. Such conduct includes the host of scams and frauds outlined in the Commission's testimony (tech support scams; prize, sweepstakes, and lottery scams; business opportunity scams; impersonation scams) as well as anticompetitive conduct that kept drug prices higher and caused consumers to pay more for medications.

⁷ 141 S. Ct. 1341 (2021).

After *AMG*, however, the Commission can no longer obtain any monetary relief under Section 13(b), which eliminates the Commission's strongest tool in protecting seniors and other vulnerable groups. Congress should act promptly to restore this tool, as the Supreme Court invited Congress to do in *AMG*.⁸ The House recently passed a bill (H.R. 2668) that would do just that, and the Commission has called for swift enactment of legislation to restore this critical authority to the FTC.

**Questions for the Record for Lois Greisman
From Senator Marco Rubio**

Question:

- 1) In your testimony, you mentioned that criminals are increasingly making contact with older Americans online, as opposed to over the phone. What is the Federal Trade Commission doing to make it easier to report online and social media scams?

Response:

In October 2020, the FTC announced a new fraud reporting platform, ReportFraud.ftc.gov (Report Fraud), for consumers to submit reports about fraud and other consumer problems. Report Fraud is both streamlined and user-friendly, giving consumers an easier way to report issues as they encounter them. A new feature provides people who file a report with customized next steps based on the details of their experiences. To reflect marketplace changes, updates were made to report categorization with the launch of Report Fraud, and more detailed information is now collected about the contact methods and payment methods used to perpetrate fraud. Reporting data suggest that Report Fraud has significantly increased reporting by all ages, including older adults.

Question:

- 2) You mentioned that cryptocurrency has been used to steal millions of dollars from older Americans. How can we help prevent cryptocurrencies from being used to target elderly Americans to fund international illicit activity, while also being careful not to stifle innovation in the crypto industry? What efforts are underway to more effectively track where these funds are going?

⁸ See *AMG Capital Mgmt., LLC v. FTC*, 141 S. Ct. 1341, 1352 (2021); see also Tr. of Oral Arg. at 54, *AMG Capital Mgmt. LLC v. FTC*, 141 S. Ct. 1341 (2021) (No. 19-508) (Kavanaugh, J.) (“[W]hy isn't the answer here, for the agency to seek this new authority from Congress . . . ?”)
(https://www.supremecourt.gov/oral_arguments/argument_transcripts/2020/19-508_3f14.pdf).

Response:

My testimony mentioned cryptocurrencies in two main contexts: (1) investment scams where the scammer is making false statements to convince the victim to invest in cryptocurrencies, and (2) in other scams in which cryptocurrency is the method of payment (as opposed to, for example, credit cards, gift cards, or wire transfers). In this way, many cryptocurrency-related scams are simply new incarnations of the same type of scams that the FTC has investigated and shut down for decades, and we will continue our enforcement efforts.

The FTC employs teams of experienced investigators who, among other things, are trained to identify scammers and trace how they send money throughout the financial system. We also coordinate with other law enforcement entities to stay up to date with the latest technology in new and evolving financial products. These scammers are very good at deceiving people and hiding their tracks, and as with other payment methods, it can be very difficult to track them down and retrieve their ill-gotten gains.

The FTC continues to work to educate consumers to identify the red flags of cryptocurrency scams. We have issued press releases and consumer education blog posts with detailed information, and our attorneys have spoken with national and local media about how to avoid scams involving cryptocurrency. And we have made more specific outreach efforts to older Americans and the other groups that serve that population. Given that we are dealing with scams—and not lawful consumer products—we do not expect that education, paired with our long-standing law enforcement against scammers, will stifle innovation in the crypto industry.

Question:

- 3) What are your recommendations to more effectively track the source of these scams to hold the perpetrators accountable through law enforcement?

Response:

We engage in several techniques to identify the source of these scams and refine these techniques as scammers switch tactics. One method we use is determining the operators of websites and telephone numbers for scams perpetrated online or through the telephone, by issuing pre-complaint subpoenas to domain registrars and telecommunications providers. We also trace the flow of money by examining where consumer funds are going and sending pre-complaint subpoenas to banks to find out which entities are associated with the receiving bank accounts. As scammers become more sophisticated and hide behind mazes of entities, uncovering their identities often requires multiple rounds of subpoenas. The reality, though, is that there are more scammers than there are investigators to shut down every scam. That is why the FTC emphasizes not only traditional law enforcement, but also consumer education—arming consumers with knowledge so that they can avoid becoming victims in the first place.

**Questions for the Record for Lois Greisman
From Senator Mike Lee**

Question:

Ms. Greisman, in your testimony, you note: “The FTC’s ability to obtain monetary relief pursuant to Section 13(b) of the FTC Act is now substantially limited following the Supreme Court’s decision in *AMG Capital Mgmt., LLC v. FTC*, 141 S. Ct. 1341 (Apr. 2021). Restoring this critical tool to redress consumers is vital to the FTC’s mission to safeguard the American public.”

- 1) In the AMG decision, the Supreme Court unanimously found that Section 13(b) “does not grant the Commission authority to obtain equitable monetary relief.” In other words, Congress has never granted you this authority in 13(b). Are you asking Congress to “restore” a tool that the Supreme Court unanimously agreed that you never were legally empowered to possess?

Response:

For four decades prior to the Supreme Court’s decision in *AMG Capital Management, LLC v. FTC* (“*AMG*”),⁹ courts unanimously interpreted the language of Section 13(b) to authorize monetary relief. Seven of the federal courts of appeals to consider the question all agreed that, based on longstanding Supreme Court precedent, the language in Section 13(b) authorized district courts to award the full panoply of equitable remedies necessary to provide complete relief for consumers, including monetary relief such as refunds and disgorgement of ill-gotten gains. For decades, no court held to the contrary.

Moreover, in 1994, Congress directly ratified the FTC’s reliance on Section 13(b) by expanding its venue and service of process provisions without placing any limitations on the types of relief to which Section 13(b) applies. It did so knowing that the Commission had relied on Section 13(b) to obtain monetary remedies, as the legislative history of the 1994 amendments make clear.¹⁰

Thus, the Commission is asking Congress to take action that will restore Section 13(b) to the way it operated based on the well-accepted interpretation of the statute that existed for four decades prior to *AMG*.

⁹ *AMG Capital Mgmt., LLC v. FTC*, 141 S. Ct. 1341 (2021).

¹⁰ See S. Rep. No. 103-130, at 15-16 (1993) (noting under Section 13(b), the Commission could “go into court ex parte to obtain an order freezing assets, and . . . obtain consumer redress” and that the amendments would “assist the FTC in its overall efforts” at enforcement).

Question:

Ms. Greisman, In *AMG Capital Mgmt., LLC v. FTC*, 141 S. Ct. 1341 (Apr. 2021), the Supreme Court noted: “Nothing we say today, however, prohibits the Commission from using its authority under §5 and §19 to obtain restitution on behalf of consumers.” In your testimony you note, “Unless the agency has clear authority to obtain monetary relief, this decision will continue to impede our ability to provide refunds to people harmed by deceptive, unfair, or anticompetitive conduct.” Your testimony makes it appear that restitution for consumers is nearly (if not completely) out of reach without the authority to seek monetary relief under 13(b).

- 2) Is the Supreme Court incorrect that you cannot currently use Section 5 and Section 19 to obtain restitution?

FOLLOW UP: Assuming the Supreme Court is correct that you can use Section 19 to pursue restitution. Why, in your opinion, is the Section 19 process insufficient to provide monetary relief for consumers who have been subject to deceptive or unfair trade practices?

Nothing in the *AMG* decision limits or impacts the Commission’s ability to obtain monetary relief under Section 19 or civil penalties under Section 5. Nonetheless, those pathways have significant limitations that make them insufficient for replacing the lost ability under Section 13(b) to provide monetary relief for harmed consumers.

Any civil penalties obtained under Section 5 of the FTC Act cannot be returned to harmed consumers. By law, civil penalties that the Commission collects under Section 5 of the FTC Act must be deposited in the U.S. Treasury.

Although Section 19 of the FTC Act does allow courts to order violators to pay certain monetary relief that the Commission can use to seek refunds for harmed consumers, it has several limitations that make it an insufficient replacement for the loss of the Commission’s 13(b) monetary relief authority.

First, in cases that do not involve alleged violations of FTC rules, Section 19 allows federal court lawsuits only after the Commission has completed an entire administrative proceeding, including through all levels of appeal. That process involves multiple steps and can take many years. An FTC administrative law judge must first conduct an adjudicative hearing and then issue a decision, which is appealable to the Commission. Then, if the Commission enters a final order, the respondent can appeal it to a federal court of appeals, followed by Supreme Court review. At the conclusion of those proceedings, the Commission must then initiate a new action in federal district court to obtain an order requiring the defendant to pay monetary relief. After that proceeding is complete (including all appeals), only then can the Commission begin distributing the monetary relief as refunds to harmed consumers. In past cases in which the Commission has utilized this pathway, the process has taken a decade or longer.¹¹

¹¹ In the Commission’s action against Figgie International, it took more than 12 years from the initiation of the Commission’s administrative action to send refund checks to harmed consumers. See *FTC v. Figgie Int’l, Inc.*, 994 F.2d 595 (9th Cir. 1993), *cert. denied*, 114 S. Ct. 1051 (1994); *In re Figgie Int’l, Inc.*, 107 F.T.C. 313 (1986).

Second, the inefficiencies of Section 19 are even worse in non-rule violation cases involving hardcore frauds and scams. Defendants in such cases are highly likely to dissipate assets¹² or destroy evidence¹³ once they learn that the Commission has undertaken an enforcement action against them. As a result, the most effective way to preserve assets for consumer redress and evidence necessary to show a violation is for the court to impose a receivership and an asset freeze. Under Section 19, however, the Commission will first have to seek an asset freeze and appointment of a receiver in federal court because the Commission cannot grant such relief administratively. If the court grants the Commission's request, the Commission will next file and litigate the merits of its complaint in an administrative proceeding (including all appeals) after which the Commission will return to federal district court to seek monetary relief under Section 19(a)(2). This trifurcated process is highly inefficient—the Commission and defendants will be mired in years of litigation, consumers will have to endure even longer waits to get refunds, and a district court judge (assuming preliminary relief is granted) will spend years overseeing an asset freeze and receivership for a case in which the merits will be litigated in an administrative forum. Given these inefficiencies, judges likely will be wary of granting the Commission's requests for asset freezes and receiverships. If such relief is not granted, the assets needed to provide refunds will be long gone by the time the court issues a monetary judgment.

Third, Section 19 is not available for every case that the Commission can bring under Section 13(b). Significantly, Section 19 does not apply to antitrust violations and therefore cannot be used to provide redress to consumers that have been harmed solely by unfair methods of competition. Prior to *AMG*, the Commission had obtained monetary relief awards under Section 13(b) in several cases involving anticompetitive practices in the pharmaceutical industry that led to higher drug prices for consumers.¹⁴

(complaint filed May 17, 1983), *aff'd sub nom Figgie Int'l v. FTC*, 817 F.2d 102 (4th Cir. 1987); Press Release, Federal Trade Commission, *Figgie International, Inc.* (June 9, 1995), <https://www.ftc.gov/news-events/press-releases/1995/06/figgie-international-inc>.

It took 10 years for the Commission to obtain monetary relief against Koskot Interplanetary, an unlawful multi-level marketing scheme. See *FTC v. Turner*, No. 79-474-Orl-Civ-R, 1982 WL 1947 (Dec. 29, 1982); *In re Koskot Interplanetary*, 86 F.T.C. 1106 (1975) (complaint filed May 24, 1972), *aff'd sub nom Turner v. FTC*, 580 F.2d 701 (D.C. Cir. 1978).

¹² See, e.g., *FTC v. Am. Fin. Benefits Ctr.*, No. 4:18-cv-00806-SBA (N.D. Cal. 2018) (within hours of receiving notice of the FTC's action, individual defendant transferred \$400,000 from corporate bank accounts to himself, his family, and one of his attorneys); *FTC v. E.M.A. Nationwide, Inc.*, No. 1:12-CV-2394 (N.D. Ohio 2012) (after FTC request for an asset freeze was denied and individual defendants received notice of the FTC's complaint, they withdrew more than \$152,000 from a corporate bank account); *FTC v. Lakhany*, No. 8:12-337-CJC (C.D. Cal. 2012) (individual defendant withdrew \$204,000 from corporate bank accounts in violation of the asset freeze).

¹³ See, e.g., *FTC v. Elite IT Partners, Inc.*, No. 2:19-cv-125-RJS (D. Utah 2019) (after receiving notice of the FTC's action, defendant secretly removed a hard drive from the premises that contained evidence inculcating the defendant and his companies in scam); *FTC v. Dayton Family Productions, Inc.*, No. 2:97-cv-00750 (D. Nev. 2013) (within hours of receiving notice of FTC action, employee permanently erased a computer hard drive); *FTC v. Asia Pacific Telecom, Inc.*, No. 10-cv-3168 (N.D. Ill. 2010) (after receiving notice of the FTC's action, defendant deleted an email account used to conduct many of the illegal practices at issue in the FTC's complaint).

¹⁴ See, e.g., Press Release, Federal Trade Commission, *Reckitt Benckiser Group plc to Pay \$50 Million to Consumers, Settling FTC Charges that the Company Illegally Maintained a Monopoly over the Opioid Addiction*

Fourth, even in certain consumer protection cases under Section 19, a court can award monetary relief only if the Commission establishes that the unfair or deceptive conduct at issue is conduct that a “reasonable man would have known under the circumstances was dishonest or fraudulent.”¹⁵ The Commission will not be able to meet this heightened requirement in every case where monetary relief is warranted. In such cases, a defendant who has been adjudicated by a court as having violated the law will get to keep the money earned from the violations, and the consumers who lost money will get nothing.

Finally, Section 19 has a three-year statute of limitations that is far too short to effectively protect consumers. Many Commission actions involve schemes that have been operating undetected for many years because many consumers do not initially realize that they have been defrauded and many FTC defendants take steps to conceal their identity and location from law enforcement. As a result, it often takes several years for such schemes to come to the Commission’s attention and for the Commission to identify the perpetrator. In such cases, by the time the Commission commences and completes its investigation and files suit, more than three years have elapsed from when the unlawful conduct first began. A three-year limitation period for monetary relief leads to inequitable outcomes because it prevents consumers who lost money in the early days of a scheme from recovering anything at all, even though they suffered the same harm as consumers who lost money more recently.¹⁶

Treatment Suboxone (July 11, 2019), <https://www.ftc.gov/news-events/press-releases/2019/07/reckitt-benckiser-group-plc-pay-50-million-consumers-settling-ftc>; Press Release, Federal Trade Commission, *Mallinckrodt Will Pay \$100 Million to Settle FTC, State Charges It Illegally Maintained its Monopoly of Specialty Drug Used to Treat Infants* (Jan. 19, 2017), <https://www.ftc.gov/news-events/press-releases/2017/01/mallinckrodt-will-pay-100-million-settle-ftc-state-charges-it>; Press Release, Federal Trade Commission, *FTC Settlement of Cephalon Pay for Delay Case Ensures \$1.2 Billion in Ill-Gotten Gains Relinquished; Refunds Will Go To Purchasers Affected By Anticompetitive Tactics* (May 28, 2015), <https://www.ftc.gov/news-events/press-releases/2015/05/ftc-settlement-cephalon-pay-delay-case-ensures-12-billion-ill>; Press Release, Federal Trade Commission, *Generic Drug Marketers Settle FTC Charges* (Aug. 12, 2004), <https://www.ftc.gov/news-events/press-releases/2004/08/generic-drug-marketers-settle-ftc-charges> (generic manufacturers agreed to disgorge \$6.25M in illegal profits).

¹⁵ 15 U.S.C. § 57b(a)(2).

¹⁶ A good example of the shortcomings of a three-year statute of limitation for monetary relief is the Commission’s 2016 case against Volkswagen (VW). The FTC alleged that, from 2008 to 2015, VW sold “clean” diesel vehicles that the company claimed had been shown in government tests to have reduced emissions. In reality, the vehicles did not have lower emissions because they were equipped with a defeat device that could detect government testing and artificially lower emissions in response. VW stopped using defeat devices in 2015 after the EPA and California began investigating. The FTC brought suit shortly thereafter in 2016, securing nearly \$10 billion in compensation in the form of vehicle buy-backs or repairs for consumers who purchased “clean” diesel vehicles that had lost significant value due to the defeat devices. If a three-year statute of limitation applied, however, the FTC only would have been able to secure only a fraction of this relief.

Question:

Ms. Greisman, as I've already noted, the Supreme Court unanimously ruled in *AMG Capital Mgmt., LLC v. FTC*, 141 S. Ct. 1341 (Apr. 2021), that the Commission Lacked the authority under Section 13(b) to obtain monetary relief.

- 3) If Congress were to consider amending 13(b) to provide the Commission with the ability to obtain monetary relief, would you agree that Congress is perfectly justified in instituting appropriate guardrails around the Commission's use of 13(b) in order to prevent this prior abuse of authority found by the Supreme Court? Or would you recommend Congress simply provide this authority with no limits?

Response:

Prior to *AMG*, courts had developed several guardrails governing monetary relief under Section 13(b). For example:

- The FTC was required to make several evidentiary showings to establish a causal connection between the defendant's unlawful conduct and consumer losses to obtain a monetary relief award under Section 13(b).
- To obtain monetary relief under Section 13(b) for deceptive misrepresentations, the FTC had to demonstrate that: (1) the defendant made "material" misrepresentations (i.e., representations that a reasonably prudent consumer would rely upon); (2) the misrepresentations were "widely disseminated"; and (3) consumers actually purchased the defendant's products.¹⁷
- To calculate the amount of monetary relief under Section 13(b), the FTC was required to provide evidence to support a "reasonable approximation" of the amount of losses caused by the defendant's unlawful conduct.¹⁸ Once the FTC provided a reasonable approximation supported by evidence, the defendant had the opportunity to contest the approximation by providing evidence that the FTC's calculation was inaccurate or unreasonable.¹⁹

Moreover, it is important to note that Section 13(b) only authorized the court, not the Commission, to award monetary relief. So another guardrail built into the language of Section 13(b) itself was that a neutral federal court judge always made the final decision whether to impose monetary relief under Section 13(b) and, if so, how much.

In short, prior to *AMG*, courts already had imposed significant guardrails to prevent the Commission from abusing its Section 13(b) monetary relief authority. Proposals for amending Section 13(b), such as the recently passed House bill (H.R. 2668), would retain all those existing guardrails.

¹⁷ See, e.g., *FTC v. BlueHippo Funding*, 762 F.3d 238, 244 (2d Cir. 2014).

¹⁸ See *FTC v. Bronson Partners, LLC*, 654 F.3d 359, 368 (2d Cir. 2011).

¹⁹ *Id.*

Finally, I note that the House bill does impose one new guardrail that did not previously exist under Section 13(b) case law. Historically there has been no statute of limitation applicable to claims brought under Section 13(b). As such, in theory the Commission could have sought monetary relief under Section 13(b) for violations no matter how long ago they occurred. The House bill, however, limits the Commission from seeking, and courts from awarding, monetary relief under Section 13(b) for violations that occurred more than 10 years before the Commission files suit. This 10-year guardrail provides an additional protection against the Commission potentially abusing Section 13(b) by seeking monetary relief for extremely old and stale violations.²⁰

FOLLOW UP: In order to seek restitution under the Section 19 process, the Commission has to prove that a “reasonable person” would have known that his conduct was dishonest or fraudulent. If Congress were to consider a process under 13(b) for the Commission to obtain equitable monetary relief, should Congress minimally model it off of these evidence requirements in Section 19?

Limiting monetary relief under Section 13(b) to violations that a “reasonable person” would have known were “dishonest or fraudulent” is problematic for two reasons.

First, such a limitation will prevent the Commission from obtaining monetary relief in cases where a court has concluded that the defendant broke the law by engaging in unfair, deceptive, or anticompetitive conduct, but where there is insufficient evidence to establish that a reasonable person would have known the defendant’s conduct was dishonest or fraudulent. In particular, it will be difficult, if not impossible, to meet that standard in many cases involving unfair or anticompetitive conduct. If the Commission cannot prove that the defendant’s law violations were objectively “dishonest” or “fraudulent,” the court will not be able to award any monetary relief. The end result will be that consumers in such cases will not recover their losses, and the defendant will get to keep the money earned from breaking the law. Such a result fails to sufficiently protect consumers and allows lawbreakers to profit from their violations.

Second, adding a “reasonable person” standard to Section 13(b) monetary relief is not necessary in consumer protection cases because “reasonableness” is already incorporated in the elements of deception and unfairness. Conduct is deceptive only if the Commission can prove that it was likely to mislead consumers acting reasonably under the circumstances.²¹ Conduct is unfair only if it causes substantial injury that consumers could not reasonably avoid.²² Adding another objective standard on top of these already existing objective standards is unnecessary,

²⁰ Note that we have not uncovered any historical evidence of such abuse. We have been unable to identify any case that the Commission has brought since Section 13(b) was enacted in 1973 in which the Commission sought monetary relief for violations that were more than ten years old. Furthermore, an analysis of recent cases in which courts awarded monetary relief under Section 13(b) shows that only a few involved refunds for consumer losses suffered eight years prior to the filing of the FTC complaint; most sought monetary relief for losses suffered within five years of the FTC’s enforcement action.

²¹ FTC Policy Statement on Deception, 103 F.T.C. 110, 174 (1984).

²² 15 U.S.C. § 45(n).

particularly when doing so will allow some violators to keep the money they wrongfully took from victims.

Question:

- 4) Ms. Greisman, if Congress were to amend 13(b), should the amount of “equitable monetary relief” to be obtained be based solely on relief to make the consumer whole? Or would you request that Congress permit the Commission to seek “monetary relief” beyond consumer losses?

Response:

Congress should amend Section 13(b) to make clear that courts can award all monetary remedies traditionally available in equity. Historic equitable monetary remedies include restitution and disgorgement. Restitution is measured by the amount of consumer losses that resulted from the defendant’s violation of the law. Disgorgement is measured by the amount of unjust gains the defendant earned by breaking the law. Prior to the *AMG* decision, courts calculated monetary relief awards under Section 13(b) as restitution or disgorgement depending on the particular facts and circumstances of the case.

The Commission typically has sought restitution under Section 13(b) with the goal of providing full refunds to harmed consumers. In some Section 13(b) cases, however, calculating monetary relief based on consumer losses is not practical or possible. In such cases, courts have awarded disgorgement—a long-standing form of equitable monetary relief that the Supreme Court reaffirmed in its recent ruling in *Liu v. SEC*, 140 S. Ct. 1936 (2020). As the Supreme Court explained in *Liu*, disgorgement of unjust gains is a traditional form of equitable monetary relief based on the foundational principle that it is inequitable for a wrongdoer to profit from his wrongdoing. *Id.* at 1943.

In short, Congress should amend Section 13(b) to restore courts’ ability to award *all* forms of equitable monetary relief, which includes both restitution designed to make harmed consumers whole as well as disgorgement of unjust gains designed to ensure that wrongdoers do not profit from their wrongdoing.²³

FOLLOW UP: If Congress were to permit the FTC to use 13(b) to obtain monetary relief, does the FTC believe such 13(b) authority should be granted retroactively? And what are the due process implications of retroactive application of new 13(b) authorities?

Congress should restore courts’ ability to award equitable monetary relief under Section 13(b) and make such amendment applicable to all pending cases. H.R. 2668 includes a provision that does this,²⁴ and I cannot think of any principled reason why Congress would

²³ Although the Commission has never asked courts to use Section 13(b) to order a defendant to pay both full restitution and disgorgement of all unjust gains, H.R. 2668 nonetheless includes language that would require the amount of any disgorgement be subtracted from the amount of any restitution. H.R. 2668, Sec. 2(a)(2).

²⁴ H.R. 2668, Sec. 2(c) (“The amendments made by this section shall apply with respect to any action or proceeding

want to deny refunds to consumers who suffered losses based on conduct at issue in our pending cases.

At the time the *AMG* decision was issued, the Commission had roughly two dozen cases pending in federal courts that involved well over \$2 billion in consumer harm and for which Section 13(b) was the only viable pathway for monetary relief (in other words, the Commission could not obtain monetary relief in those cases under Section 19). If amendments to Section 13(b) are not made applicable to pending cases, the potential monetary relief in our pending enforcement actions will be permanently lost. Consumers who suffered losses will get nothing due to the pure happenstance that the Commission's enforcement action was pending at the time that *AMG* was decided, whereas consumers who lost money in cases that were fully resolved before *AMG* was decided and consumers who lost money in cases filed after Congress amends Section 13(b) will get relief. Such a result is grossly unfair to the thousands of consumers who suffered losses due to the unlawful conduct alleged in our pending cases.

As to the due process concerns, it is important to note that the pending cases provision in H.R. 2668 would not allow the Commission to alter or re-litigate any final judgments already entered. The language in H.R. 2668 only makes amendments to Section 13(b) applicable to any unresolved case that is pending at the time the amendments take effect, as well as to any new cases subsequently filed. Provisions that make statutory changes applicable to pending cases are common in federal civil legislation and have long been recognized as constitutionally permissible. Moreover, defendants in pending cases will get due process because those cases are still being litigated in court and they will have the opportunity to contest any award of equitable monetary relief.

Finally, the pending cases provision in H.R. 2668 is not unusual or unique. The provision in H.R. 2668 is nearly identical to Section 6501(b) of the 2021 National Defense Authorization Act,²⁵ which made a statutory fix Congress gave to the SEC applicable to all pending SEC cases. In short, there is very recent congressional precedent for a statutory fix that is made applicable to pending cases.

that is pending on, or commenced on or after, the date of the enactment of this Act.”).

²⁵ National Defense Authorization Act for Fiscal Year 2021, Pub. L. No. 116-283, § 6501(b) (“The amendments made by subsection (a) shall apply with respect to any action or proceeding that is pending on, or commenced on or after, the date of enactment of this Act.”)

**Questions for the Record for Odette Williamson
From Senator Robert P. Casey, Jr.**

Question:

- 1) Your testimony highlighted that peer-to-peer (P2P) payment fraud has been increasing alongside the rise of digital apps and websites that allow users to easily transfer money from one person's account to another. Testimony from the Federal Trade Commission further substantiated this issue, noting older adults reporting scams to the agency "increasingly reported using payment apps or services such as PayPal," and that "those reports more than tripled in 2020 compared to 2019."
 - a. Please provide additional information about how the provisions of the Electronic Fund Transfer Act (EFTA) can be updated to better address the evolving issues related to peer-to-peer payment fraud.

Response:

Scammers are increasingly using peer-to-peer (P2P) payment platforms to defraud older adults. Yet most payment providers and financial institutions are taking the position that there is no protection under the EFTA for a consumer who is fraudulently induced to send a payment to a scammer. Some providers will ask the financial institution or scammer that received the funds to voluntarily return them, and some will not even do that. The payment platform may also provide a warning that a consumer should be careful to send funds only to people they know, but that is not adequate to protect older adults from losses. More than half of consumers surveyed by AARP incorrectly assumed that their payments would be protected if there was an error or fraud associated with the transaction.¹

There are two problems with the EFTA's protections. First, the definition of "unauthorized transfer" excludes transfers initiated by the consumer. Second, financial institutions and payment providers incorrectly take the position that consumer errors are not "errors" covered by the EFTA's error resolution provisions. Either Congress or the CFPB could update and clarify the EFTA to address both of these issues. Key steps include:

- Expand the definition of "unauthorized electronic fund transfer" to cover fraudulently induced payments, with liability resting with the institution that received the fraudulent payment;
- Require that P2P platforms investigate and correct errors and fraud, even in cases where the consumer sent the payment erroneously or as a result of fraud in the inducement;
- Prioritize fraud prevention and remediation as part of financial institutions' know-your-customer duties; and
- Require P2P platforms to provide and display a customer service telephone number and respond to customer service inquiries in a timely manner.

¹ AARP, *AARP Survey Finds Majority of Americans Using Payment Apps Unaware of Danger Posed by Scammers*, May 12, 2020, available at <https://press.aarp.org/2020-5-12-AARP-Survey-Finds-Majority-of-Americans-Using-Payment-Apps-Unaware-of-Danger-Posed-by-Scammers>.

The institutions that develop and implement payment platforms should be accountable for fraudulent conduct on their platforms. These institutions, not consumers, are best able to prevent scams by designing robust fraud and error prevention systems to stop scammers in their track.

- b. Please provide additional information about how the Federal Reserve's Regulation E can be improved to better address peer-to-peer payment fraud.

The Consumer Financial Protection Bureau has authority over Regulation E under the EFTA. That issue is addressed above.

Separately from Regulation E, the Federal Reserve Board ("FRB") is developing a new payment system called FedNow, which will be similar to Zelle. The FRB has proposed amendments to Regulation J to cover that system. The FRB should not wait for the CFPB to update Regulation E and must on its own make sure that FedNow will be safe for consumers. Advocates have significant concerns that FedNow, under recently proposed Regulation J, will not be safe for consumers or other small users, and will replicate the problems of existing payments systems by failing to provide protection against fraud and errors. A wide variety of stakeholders filed comments with the Fed pointing out the concerns about the lack of protections from fraud and limited ability to reverse fraudulent payments, among other concerns, and provided a slate of recommended improvements.² The recommendations to improve fraud protections under proposed Regulation J include:

- The rules must protect consumers and small businesses against fraud in the inducement and impose liability on the institution that received the fraudulent payment. Liability for the receiving institution is consistent with their obligations under existing know-your-customer and anti-money laundering obligations to ensure that accounts are not opened with fraudulent identities and that an institution's customers are not using an account for illegal purposes.
- Rules that protect consumers and small businesses will give providers an incentive to develop and improve anti-fraud measures. Reports of fraud should be collected, analyzed to detect patterns, and followed up on. The FRB, as a key part of its faster payment system, must develop tools to aggregate and quickly share this information.
- The FedNow system must also prevent and resolve costly errors. In aggregating and sharing information the FRB could, for example, develop a central directory of end users to check the consistency of the information provided and enable payors to verify the recipient.³ A directory would help to ensure that consumers are sending funds to the correct person, and might also be used to ensure that an email, cell phone, or other identifier are not linked to the wrong account or an imposter account.

² 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.

³ This activity should be conducted with consideration of consumers' privacy. Institutions should only be able to access to the consumer data needed for each real time payment transaction and should not be able to use the directory for debt collection, marketing or other purposes.

The FRB has a responsibility to ensure that its system is safe, especially for those users for whom fraud or errors can be devastating. The FRB can be a model for other systems developed by private companies that do not have the same public accountability. The FRB should work with the Consumer Financial Protection Bureau to ensure that FedNow is safe for participants. The two agencies should identify issues – and make recommendations to Congress if necessary -- to develop a comprehensive set of proposed regulations that both facilitates faster payments and protects consumers and small businesses.

Question:

- 2) In your written testimony, you describe how frauds and scams disproportionately impact communities of color. How can existing consumer protection and education programs be updated to better serve the communities being disproportionately affected by frauds and scams?

Response:

Fraudulent practices and scams impact every community. A recent Federal Trade Commission (FTC) report highlighted how government imposter scams, bogus offers of assistance and financial relief, and abusive financial products impact Native American, Black, Asian and Latinx communities.⁴ These vicious scams drained the resources and wealth of communities already reeling from the health and financial consequences of the pandemic. While governments and organizations can step up outreach, education and law enforcement, more protections are necessary to protect older adults, especially limited English proficient (LEP) elders from scams.

Older adults in communities that are linguistically isolated are particularly at risk. According to the FTC, marketers capitalized on the health concerns of consumers during the pandemic to push unproven products and services to prevent, cure or treat COVID-19, including products advertised in Korean, Vietnamese and Spanish.⁵ Others pushed bogus business opportunities, pyramid schemes, and deceptive financial products to unbanked and underbanked LEP consumers.⁶ Scammers purchase ads in ethnic media outlets to exploit misinformation and confusion regarding COVID-19 and programs designed to ameliorate the pandemic's economic impact.

Limited English proficient consumers are exposed to scams in their own language, and lack in-language information from reputable sources.⁷ To avoid the lure of scammers peddling predatory financial products and schemes LEP consumers need information in their own language regarding mainstream products and services. Households where only Spanish is spoken, for example, are unbanked at five times the rate of households where Spanish is not the only language spoken.⁸ While some marketing of financial products may occur in a consumer's preferred language, often the transaction documents and any subsequent contact (oral or written) is English-only. LEP consumers must rely on friends and family members, and sometimes children, to convey and transmit sensitive financial information, putting them at risk of identity theft.

⁴ Federal Trade Commission, *Serving Communities of Color: A Staff Report on the Federal Trade Commission's Efforts to Address Fraud and Consumer Issues Affecting Communities of Color*, October 2021.

⁵ *Id.* at 2.

⁶ *Id.* at 12.

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 Consumer Fin. Prot. Bureau, Spotlight on Serving Limited English Proficient Consumers (Nov. 2017), at 13.

The financial marketplace can do a much better job of serving the needs of LEP consumers and protecting them from fraud. Regulators can take steps to have financial institutions bring LEP consumers into the financial mainstream to make them less vulnerable to scams. The Consumer Financial Protection Bureau has started this conversation by encouraging financial institutions to better serve LEP communities.⁹ This is especially important as financial services move online or are provided through mobile applications that do not give consumers the option of visiting a brick and mortar location.

Regulators should ensure that financial institutions take the following steps to expand access for LEP consumers:

- Ensure that webs portals and mobile apps are accessible in languages other than English, beginning with Spanish and continuing to expand to the most prevalent LEP languages;
- Communicate with customers in languages other than English (orally and in writing);
- Include mechanisms for collecting and retaining customers' language preference in the customer's electronic and paper file;
- Transfer language preference information to assignees, servicers, collectors, or other relevant parties;
- Allow customers to fill out applications and provide supporting documentation in languages other than English; and
- Provide oral interpretation through multi-lingual staff or third-party vendors.

Moreover, LEP consumers who are victims of a scam may be pursued aggressively by debt collectors as they struggle to live on diminished resources. Assistance for these consumers should not be overlooked. New York City for example recently adopted rules requiring that debt collectors ask about language preference, track consumers' language preference, inform consumers of any available translation services, and point consumers to a glossary of debt-related terms available on the city's website.¹⁰

Congress can encourage regulators to promote inclusion by emphasizing language access standards for all financial institutions across the range of products and services they provide. This not only brings LEP consumers into the financial mainstream to avoid some types of scams, but may aid in know-your-customer efforts that help in the detection of fraudulent activity. Older consumers in particular have benefitted from financial institutions spotting suspicious activity, filing reports, and when possible warning customers of a possible scam or the risk of being defrauded. Protecting consumer's money and assets against known scams is one layer of protection financial institutions can make available to all consumers.

⁹ Consumer Fin. Prot. Bureau, Spotlight on Serving Limited English Proficient Consumers (Nov. 2017), https://files.consumerfinance.gov/f/documents/cfpb_spotlight-serving-lep-consumers_112017.pdf; Consumer Fin. Prot. Bureau, Supervisory Highlights (Oct. 2016) at 20-25, https://files.consumerfinance.gov/f/documents/Supervisory_Highlights_Issue_13_Final_10.31.16.pdf.

¹⁰ NYC Dep't of Consumer Affairs, Notice of Adoption (June 11, 2020), available at <https://rules.cityofnewyork.us/content/notice-adoption-debt-collectors>.

**Questions for The Record for Odette Williamson
From Senator Marco Rubio**

Question:

- 1) In your testimony, you mentioned mortgage-related, and other equity-theft scams that targeted older homeowners in financial distress reached a historic high during the COVID-19 pandemic. How can the Federal Housing Administration and the Department of Housing and Urban Development educate and spread awareness to help prevent these scams?

Response:

The U.S. Department of Housing and Urban Development (HUD) can take a number of measures to help older homeowners targeted by scammers. The frequency and type of foreclosure rescue scam or mortgage-related scam varies with changes in the real estate market.¹¹ 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 are at risk for equity theft scams if they are facing a loss of income due to the pandemic, and unable to afford the mortgage or other home-related expenses, and have a lot of equity in the home. For FHA-insured loans, HUD can take steps to further strengthen the foreclosure avoidance options offered to homeowners. Moreover, some of the COVID-specific options should be made permanent as many older homeowners may struggle with the residual economic impact of the pandemic in the years to come.
- Older homeowners in financial distress 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. This assistance is available free through a HUD-approved housing counseling organization. In addition, once states establish their Homeowner Assistance Fund, scammers will most likely trick consumers into paying for such free assistance. To get ahead of these scams HUD should provide more funding, technical support and assistance to HUD-approved housing counseling organizations, especially those located in communities hit hard by the pandemic. Moreover, HUD should encourage collaboration between housing counseling and legal services or fair housing organizations to provide a quick referral for victims of fraud and discrimination.
- As mentioned above, scammers often use affinity marketing to target their audience based on racial, ethnic, or religious affiliation.¹² Older adults and non-English speaking homeowners are

¹¹ 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).

¹² See *Reed v. Zak (In re Zak)*, 573 B.R. 13, 20 (Bankr. D. Mass. 2017) (quoting testimony that loan modification company sought out agents from different ethnic backgrounds to target communities that were particularly hard hit, particularly Latinx and Haitian communities); Lawyers' Committee for Civil Rights Under Law, *A Practical Guide for Identifying, Investigating, and Bringing Suit Against Consumer Financial Scams: Lessons Learned and Tips Developed From Combatting Loan Modification Scams* at 7 (approx. Dec. 2015) (describing efforts of scammers to

particularly likely to be targeted.¹³ HUD should provide the resources necessary to assist HUD-approved housing counseling organizations in building the capacity to serve such populations, including LEP homeowners located in the community the organization serves.

- Often older homeowners need small dollar loans to repair their homes. This makes them vulnerable to home improvement scams, and scams related to utilities and energy-efficiency upgrades. HUD should explore expanding grant programs aimed at helping older adults make repairs to their homes. Moreover, HUD should explore the creation of a FHA-insured small dollar loan program for those homeowners who need funding for more extensive repair or rehabilitation of their homes.
- HUD must coordinate closely with state and local government, legal services advocates, elder advocates and law enforcement to share information to disrupt the activity of known equity-scammers. The IRS and Social Security Administration, for example, will publicize information about existing scams; other agencies may create consumer fact sheets, videos and other consumer facing information to warn older adults and other consumers about the scam. The agencies can coordinate on law enforcement activity to stop the scammers.

Foreclosure rescue and equity theft scams deprive older adults of the ability to age in place and benefit from wealth built through homeownership. Low-income older homeowners are particularly at risk, as scammers target homeowners who are financially distressed and struggling to meet basic expenses. HUD can provide the resources and support need to assist homeowners through targeted programs to prevent foreclosure, and stabilize housing. Housing counseling organizations provide valuable outreach and assistance to vulnerable homeowners. Older adults who fall victim to a scam will also need the support of legal services organization to fight foreclosure or win back title to the property, if possible, from an equity scammer. More resources to legal services and other organizations to provide such assistance would benefit scam victims.

Question:

- 2) What, if anything, can HUD's local and regional field offices be doing to help prevent equity-theft scams?

Response:

HUD's local and regional field offices can monitor local real estate markets for equity-theft and other home-related scams, and provide this information to law enforcement and other officials. 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. Scammers often mimic government organizations, including HUD, in correspondence and mailings to win the trust of consumers. HUD grantees, working directly with consumers, may uncover a pattern of fraudulent activity first and bring it to the attention of the agency. To the extent these practices are brought to the attention of HUD's local office, including the government imposter scams that reference HUD's programs, local and regional offices can work closely with law enforcement and government officials to stamp out the fraud. Moreover, they can alert local housing counseling organizations regarding the pattern of fraudulent activity in a particular area so the organization can alert vulnerable community members.

focus on certain ethnic or language communities), available at <https://web.archive.org>.

¹³ Federal Reserve Bank of Atlanta, Foreclosure Rescue Scams: Real Estate Fraud Prevention and Awareness, <https://www.atlantafed.org/-/media/documents/community-development/data/foreclosure-resource-center/foreclosure-rescue-scams-real-estate-fraud-prevention-and-awareness.pdf>.

**Questions for the Record for Kate Kleinert
From Senator Rev. Raphael Warnock**

Question:

- 1) You are a survivor of a scam much worse than \$2,500. You suffered the tremendous loss of your husband and then the loss of your bank account, which totaled to a financial loss of \$39,000. Can you talk about the emotional toll this scam has had on you, and how that toll affects victims' comfort with reporting these scams?

Response:

Thank you for your kind question. As devastating as the money loss is, the emotional toll is far greater. I mourn for the loss of this new love that entered my life and feel betrayed. The emotions that follow are shame, embarrassment, and a sense of feeling stupid and worthless. Who wants to share that with anyone? The worst part was not knowing who to call or where to get help. We have to close the gap between where the help and information is and the people who need it.

Question:

- 2) Can you talk more about what we can do to ensure people feel comfortable reporting these types of scams earlier so we can prevent further harm?

Response:

In my case, I called the State Police and had a female officer answer. I was so relieved. When I started relaying my story, she stopped me and said "Why are you calling here? There's no crime here." There is no way to duplicate in writing how sarcastic her tone of voice was. I felt like a rape victim who is told 'you were asking for it'.

The people who are dealing with the victims need to understand the emotional frailty that comes with being through this kind of crime. So many of these scams are successful because they prey on your emotions and vulnerability. The senior citizens in their later years are frightened that their adult children will find out and come to the conclusion that Mom isn't making good decisions anymore and shouldn't be living alone.

I truly believe that the fastest and most effective way to change peoples' thinking is through ad campaigns. In the first 30 seconds of a one minute commercial, show (realistically) how these scammers persuade people to send money. Then have a sympathetic person give some statistics on how often this is happening and most importantly, where to go for help in the last 30 seconds.

In this type of campaign, not only will the seniors see it, but also their families who might understand the situation more sympathetically.

Additional Statements for the Record



September 23, 2021

The Honorable Robert P. Casey, Jr.
Chair
U.S. Senate Special Committee on Aging
G41 Dirksen Senate Office Building
Washington, DC 20510

The Honorable Tim Scott
Ranking Member
U.S. Senate Special Committee on Aging 628
Hart Senate Office Building
Washington, DC 20510

Dear Chair Casey and Ranking Member Scott:

On behalf of our nearly 38 million members and all older adults nationwide, AARP would like to thank you and the members of the Special Committee on Aging for holding today's important hearing on "Fraud, Scams and COVID-19: How Con Artists Have Targeted Older Americans During the Pandemic." AARP is also appreciative of the testimony from Kate Kleinert, who first shared her story of experiencing a devastating online romance scam in [episode 97 and 98](#) of the AARP podcast, *The Perfect Scam*.

The pandemic and related economic upheaval gave scammers ample opportunities to follow the headlines into consumers' bank accounts. Criminal scammers often look for current events and trends that facilitate stealing money and sensitive information from unsuspecting targets. Scams have varied throughout the pandemic, from selling fake personal protective gear, impersonator schemes promising accelerated economic impact payments, and jump-the-line offers for early vaccines. However, it is not only pandemic-related scams that have flourished; all scams have been on the rise.

While the Federal Trade Commission's Consumer Sentinel Network [2020 Data Book](#) accounts for 4.8 million fraud reports and losses of \$3.4 billion, we know many scams are never reported. The annual Javelin Strategy & Research identity fraud [study](#) uncovered a total of \$56 billion in identity fraud losses in 2020, \$43 billion of which was from identity fraud scams. These figures only reflect scams involving the loss of sensitive personal information and we know the landscape of the fraud industry goes further.

Whether a crime is violent, affects property, or is financial, one thing is constant – the criminal bears responsibility for the criminal act. However, when it comes to scams, the tendency is to find fault with the victim. The language widely used tends to focus on the victim being "duped," "swindled" or "falling for it." That is why AARP has begun a three-year campaign focused on changing the narrative of how we talk about victims. By encouraging awareness and empathy, victims may not feel shame in reporting the crimes against them and public policy can catch up to the rampant crime in this space.

When older adults experience a scam, their financial losses tend to be far more significant than younger victims. This makes the work of the AARP Fraud Watch Network that much more important. The [AARP Fraud Watch Network](#) equips consumers with reliable and up-to-date insights and alerts, and a fraud helpline to support victims and their families. AARP's Fraud Watch Network Helpline manages an average of 500 calls each day, on track to hit 150,000 calls this year, and average call time in 2020 was 22 minutes. Earlier this year, we launched a [pilot victim support program](#) in partnership with Volunteers of America (VOA), based on their successful programs for returning military and frontline health workers. The AARP VOA ReST program (ReST stands for Resilience, Strength, Time) offers peer-trained support via one-hour group Zoom sessions to help victims recover emotionally from their fraud experience. Reaction from participants has been so profound that we are now working to extend the program for a year, hoping to make it a permanent offering.

AARP is grateful to the committee for its continued focus on scams and fraud. The issue is only getting worse, and older adults will continue to be the most affected by the sheer losses they incur. We thank the committee for seeking solutions to this critical problem. If you have any questions, please feel free to contact me or have your staff contact Dawit Kahsai of our Government Affairs staff at dkahsai@aarp.org or (202) 434-3761.

Sincerely,



Bill Sweeney
Senior Vice President
AARP Government Affairs



September 23, 2021

The Honorable Robert P. Casey, Jr.
United States Senate
393 Russell Senate Office Building
Washington, D.C. 20510

The Honorable Jerry Moran
United States Senate
521 Dirksen Senate Office Building
Washington, D.C. 20510

Dear Senators Casey and Moran:

AARP, on behalf of our 38 million members and all older Americans nationwide, is writing to thank you for reintroducing the Stop Senior Scams Act. AARP appreciates your commitment to establish a Senior Scams Prevention Advisory Council that would collect and publish educational materials and information on model programs that may be used by retailers, financial services, and wire-transfer companies as a guide to prevent scams that target senior citizens.

AARP has a long history of fighting for protections for older Americans and has been on the forefront of advocacy in support of federal and state laws and regulations that prevent financial exploitation and scams targeting seniors. Through the AARP Fraud Watch Network, we empower consumers to protect themselves, their families, and their communities from fraud and scams, and provide tips to spot and avoid scams like identity theft, investment fraud, and holiday scams.

Scammers steal billions of dollars from unsuspecting consumers every year. The effect on victims and their families can be financially and emotionally devastating, especially for older Americans. That is why AARP is pleased to endorse your bill, and we call on Congress to swiftly pass this legislation to protect older Americans from fraud.

Thank you again for your steadfast leadership and commitment to protecting seniors from financial exploitation. If you have any questions or need additional information, please feel free to contact me or Dawit Kahsai at dkahsai@aarp.org.

Sincerely,

A handwritten signature in purple ink that reads "Bill Sweeney".

Bill Sweeney
Senior Vice President
Government Affairs



September 23, 2021

Chairman Bob Casey
Senate Special Committee on Aging
393 Russell Senate Office Building
Washington, DC 20510

Ranking Member Tim Scott
Senate Special Committee on Aging
104 Hart Senate Office Building
Washington, DC 20510

Dear Chairman Casey and Ranking Member Scott:

On behalf of the [Alliance for Safe Online Pharmacies \(ASOP Global\)](https://www.asopglobal.org/), thank you for holding the hearing entitled "Frauds, Scams and COVID-19: How Con Artists Have Targeted Older Americans During the Pandemic" on Thursday, September 23, 2021. ASOP Global is a nonprofit organization dedicated to public health and requests that you consider raising the dangers of the illegal sale of drugs online, a public health threat that compromises the safety of older Americans.

ASOP Global is headquartered in Washington, D.C., with activities in the United States, Canada, Europe, Latin America, and Asia and is dedicated to protecting consumers, ensuring safe online access to medications, and combating illegal online drug sellers. With more than 75 participating organizations around the world, ASOP Global prioritizes efforts to better promote a safe and legitimate online environment for patients, caregivers, and healthcare providers.

It was recently reported that 90 percent of older Americans rely on one prescription medication on a regular basis; as many as 40 percent use five or more weekly; and 12 percent take at least ten drugs per day.¹ Nearly half of Americans—including seniors—are obtaining their drugs online.² However, at any given time, roughly 95 percent of the over 35,000 online pharmacies worldwide operate illegally, selling medicines without a prescription and peddling fake and dangerous medicinal alternatives in violation of state and federal law as well as pharmacy practice standards.³ Unfortunately, the vast majority of Americans erroneously believe that all of these websites offering drugs are approved by the FDA. To make matters worse, most consumers accept the potential dangers of illegal online pharmacies in exchange for greater convenience and cost savings.⁴

¹ <https://www.merckmanuals.com/home/older-people%E2%80%99s-health-issues/aging-and-drugs/aging-and-drugs>

² https://asopfoundation.pharmacy/wp-content/uploads/2021/07/ASOP-Global-Foundation-2021-Consumer-Behavior-Survey-Key-Findings_Final-7.9.2021.pdf

³ <https://nabp.pharmacy/wp-content/uploads/2018/09/Internet-Drug-Outlet-Report-September-2018.pdf>

⁴ https://buysafesrx.pharmacy/wp-content/uploads/2021/07/ASOP-Global-Foundation-2021-Consumer-Behavior-Survey-Key-Findings_Final-7.9.2021.pdf

Alliance for Safe Online Pharmacies (ASOP)

www.BuySafeRx.pharmacy



Senior citizens lost almost \$1 billion in scams in 2020, according to the Federal Bureau of Investigation.⁵ According to FTC data, 60- to 69-year-olds reported losses of more than \$56 million to coronavirus frauds.⁶ The pandemic has driven more consumers to the internet and created global demand for COVID-19 cures and treatments. This surge in demand has led to an explosion of thousands of new, malicious websites designed to defraud patients. During March 2020 alone, at least 100,000 new domain names were registered containing terms like "covid," "corona," and "virus," with thousands confirmed as malicious COVID-19-related domains.⁷ Phony online shopping websites and COVID-19 vaccine cards ranked third and second in AARP's top scams targeting older Americans in 2021.⁸

ASOP Global has advocated for policies that put online patient safety first, including [increasing internet accountability](#) through targeted reforms to Section 230 of the Communications Decency Act, safeguarding online transparency by restoring access to accurate WHOIS data, and stopping domain name registries and registrars from facilitating online crime by requiring them to [lock and suspend suspicious sites](#). We welcome the opportunity to visit with you and your staff about these and other policies that Congress can consider to help protect seniors as they look for medications on the internet.

Thank you for your continued leadership on behalf of America's seniors. As you continue to investigate fraud, we ask that you consider the harms associated with rogue online pharmacies and that you submit this letter to the hearing record. Should you or your staff have any questions related to illegal drug sales online, please consider ASOP Global a resource. We look forward to working with you to advance public health and patient safety.

Respectfully,

A handwritten signature in black ink, which appears to read "John B. Hertig".

John B. Hertig, PharmD, MS, CPPS, FASHP
 Board President, ASOP Global Board of Directors
 Vice-Chair and Associate Professor, Department of Pharmacy Practice
 Butler University College of Pharmacy and Health Sciences
jhertig@butler.edu

⁵ <https://abcnews.go.com/Politics/senior-citizens-lost-billion-scams-year-fbi/story?id=78356859>

⁶ https://www.axios.com/scammers-seize-on-covid-confusion-b40cca88-c288-4d94-9f5a-1df19ac01812.html?utm_source=newsletter&utm_medium=email&utm_campaign=newsletter_axiosam&stream=top

⁷ Don't Panic: COVID-19 Cyber Threats." Palo Alto Networks Unit 42 blog, 24 March 2020, at: <https://unit42.paloaltonetworks.com/covid19-cyber-threats/>

⁸ <https://www.aarp.org/money/scams-fraud/info-2021/schemes-targeting-older-adults.html>

Alliance for Safe Online Pharmacies (ASOP)
www.BuySafeRx.pharmacy