Second Scams Against Older Adults Advisory Group Meeting – April 2, 2024

Monica Vaca:

Good afternoon all. I'm so pleased to be here today and I want to extend the regrets from our Bureau Director, Sam Levine, who had very much hoped to be here and is disappointed that he is unable to be here with us. My name is Monica Vaca, I am a Deputy Bureau Director in the Bureau of Consumer Protection here at the FTC. Thank you for joining us virtually for our second Scams Against Older Adults Advisory Group Meeting.

When we kicked off this project in 2022 after the passage of the Stop Senior Scams Act, I don't think we imagined the breadth of the depth of the work ahead of us or the remarkable collaboration and partnerships we're building among government agencies, consumer advocacy groups, and businesses. I'm so heartened by the enthusiasm, creativity, and expertise that we've seen and the commitment to identify and implement concrete solutions to help reduce the impact of fraud on older adults.

I cannot stress enough the importance of our efforts to protect older adults and to help them protect themselves. Unfair and deceptive practices always harm everyday consumers and honest businesses, but the consequences can be especially damaging for older consumers. For example, the Commission recently obtained an 18 and a half million dollars order against Publishers Clearinghouse resolving allegations that the company used dark patterns and other manipulative practices on its e-commerce sites. The FTC's complaint explained that the company was a recidivist that targeted older consumers with deceptive tactics, and part of the impetus behind the Commission's recent proposal to extend the telemarketing sales rules coverage to inbound telemarketing calls involving technical support services was the out-sized impact that tech support scams have on older Americans. With consumers 60 years of age and older being five times more likely to report a financial loss to such scams compared to younger adults.

Overall, reports to the FTC and its Consumer Sentinel Network tell a compelling story about what older adults are experiencing, especially because as a group, they're much better at reporting fraud than their younger counterparts. In 2023, nearly 400,000 fraud reports came from people 60 and older with reported losses of more than $1.9 billion. Most older adults who reported to the FTC didn't actually lose money. In fact, people in their 20s were far more likely to report losing money to fraud, but when older adults did lose money, they tended to report losing far more. And we know reported losses are just a fraction of the real losses to scams since the vast majority of frauds are not reported. The reports themselves often describe sophisticated scams. We hear stories that run the gamut from bogus investment offers with detailed forecasts that falsely promise financial security, to callers who are armed with consumers' personal information and report to be from government agencies or well-known companies like Amazon or Bank of America, to romance scams that lure people with despicable tactics

and pull on people's heartstrings. Online platforms provide fraudsters with a lot of opportunities, and when older adults report losing money to fraud, they most often say that the scam started online, but reports tell us that the median individual loss is far higher when scams start with phone calls, emails, and text messages. In fact, last year, older adults reported a median individual loss of $1,500 for scams that started with these three contact methods combined, compared to $250 for scams that started online.

The payment methods that scammers use also tell us a lot about the scams in play and how we can address them. Older adults report paying by gift card most often for common frauds like government impersonators or scammers pretending to be a grandchild, family or friend, but bank transfers accounted for the highest dollar losses. Older adults reported transferring more than $670 million to scammers last year. There's also been a significant uptick in losses involving cryptocurrency. Last year, older adults reported losing over $390 million through cryptocurrency payments to scammers. For both cryptocurrency and bank transfers, older adults reported that investment scams accounted for the largest share of their losses. Older adults are certainly not the only people targeted by scammers, nor are they the only group losing money to scams, but the individual losses can be staggering. Given the enormity of this issue, the FTC has been dedicated to addressing fraud that affects older adults for many years, including through our recent work with our partners on the Scams Against Older Adults Advisory Group.

At our last full advisory group meeting in September, 2022, the Group established four committees to implement the Stop Senior Scam Act's mandates. Since then, these committees have tackled several initiatives including, one, making consumer education and outreach efforts more effective. Two, identifying effective industry training on scam prevention. Three, reviewing research on effective consumer messaging to prevent scams, and four, identifying innovative or high-tech methods to detect and stop scams. This holistic approach takes into consideration the many stages in a person's experience with a scam and the various ways that intervention to stop or reduce consumer harm can be most effective.

Today you'll hear from each committee on the work that they've completed and the projects that are ongoing. And I'm pleased to announce that each committee's accomplishments are available on the Advisory Group's website at FTC. gov/olderadults.

All of this has been a tremendous amount of work. I want to thank our advisory group and committee members and everyone who has participated over the last couple of years. I look forward to hearing from our committees and subcommittees about concrete solutions they've identified, the work that's ongoing and the next steps that we can all take to best protect older adults and help them protect themselves from scams.

With that, I will turn it over to our Stop Senior Scams Act Coordinator, Patty Hsue.

Patty Hsue:

Thanks very much, Monica. I'd like to echo Monica's thanks to all of our advisory group and committee members who have worked tirelessly on the Advisory Group's various initiatives since the Stop Senior Scams Act was passed in 2022. I've worked closely with many of you and I so appreciate the dedication, ingenuity, and infectious energy that you all have brought to the table. I know that our collective efforts will result in helping not just older adults, but really all consumers to avoid the impact of fraud.

Now, I'm excited to introduce the work of our committees and give you a preview of what you'll hear about today. First, you'll get an update from our Committee on Consumer Education and Outreach. Consumer education is a keystone to protecting older adults and an invaluable part of our work. This committee approach consumer education from two angles. The Outreach Subcommittee has worked to

identify more effective ways to reach older adults, including through pilot programs to test new approaches. The Guiding Principles Subcommittee drew on a significant experience to identify how organizations can better reach and engage older adults. The work of both subcommittees went into the creation of guiding principles that can be implemented by any organization to better engage with older adults to help them spot, avoid and report fraud.

Next, you'll hear from our Industry Training Committee. This committee looked at strategies and ideas for how to effectively train frontline employees to spot and mitigate scams. The Committee was able to draw from its members' broad expertise across organizations and industries to share and identify principles of effective employee training, engagement, and intervention. As you'll hear from these two committees, government, industry and consumer advocacy groups alike devote considerable resources to consumer education and outreach as well as training. Given the resources involved, it's important for all of us to evaluate the effectiveness of different interventions and learn how to optimize them.

The Scan Prevention Research Committee took on this task by reviewing dozens of studies and existing research addressing fraud prevention messaging to help identify challenges to effective scan prevention messaging and research-backed approaches for better outcomes. This committee will report on their findings along with the work they have done to identify where more research is needed and the questions they propose for further investigation. Their work is summarized in a report that we hope will be useful to academics, government, and other organizations who are exploring these important questions. Finally, our Committee on Technology New Methods will provide an update on the work that its members are currently tackling. This committee has focused on different ways that technology can be used to protect older adults from scams such as by limiting or preventing scammers from contacting or collecting payment from consumers. They are also exploring how members can share intelligence more effectively to limit or stop scams from impacting older adults.

Now, I know that everyone is eager to hear what our committees have accomplished, so without further ado, I'd like to hand things over to the leaders of the Consumer Education and Outreach Committee to provide you with an update on their work. Please join me in welcoming Tanya McInnis from the Department of Treasury as our next speaker.

Tanya McInnis:

Great. Good afternoon. Thank you, Patty. Good afternoon and again. Welcome to the Scams Against Older Adults Advisory Group. I am Tanya McInnis, I am the Deputy Director in the Office of Consumer Policy at the US Department of the Treasury. I serve as Treasury's designee on this important work to reduce the occurrence and impact of scams and frauds against older adults.

The work of the Advisory Group aligns with Treasury's mission to maintain a strong economy and create economic and job opportunities by, for example, promoting the conditions that enable economic growth and stability and protecting the integrity of the financial system. Additionally, the work of the Advisory Group aligns with the mission of my office, Consumer Policy. The Office of Consumer Policy produces policy analysis on developments and financial services that impact consumers, including emerging products and services, payments, credit, financial technology, and related topics. OCP also coordinates and manages the Financial Literacy and Education Commission, also known as the FLEC, an interagency body chaired by the Secretary of the Treasury and dedicated to advancing financial wellbeing through education and literacy.

My office also works collaboratively with other Treasury offices and our federal partners to accomplish our mission. Treasury and Office Consumer Policy are engaged in these collaborative efforts to ensure that consumers have access to information, products and tools to meet their financial needs and to advance household financial security. As you may know, congressional appropriators have tasked

Treasury to develop a national strategy on financial inclusion to establish national objectives for financial inclusion, set benchmarks for measuring progress, and offer recommendations for how public policy, government programs, financial products and services, technology and other tools and infrastructure can advance financial inclusion. We are in the process of gathering and reviewing information that will inform our development of this strategy. Undoubtedly, identifying and mitigating frauds and scams will be included in the national strategy for financial inclusion.

With that, it is my pleasure to provide remarks on what the Consumer Education and Outreach Committee was created to do. This work is personal for me. My mother was a target of several scams. Fortunately, she would contact my siblings and me to tell us what was going on and to ask us what she should do, but I know that's not the story for many older adults. Based on personal experience and my work at Treasury on promoting financial literacy and education for all consumers, the more people are aware about scams and hear about them from others, the more likely they are to recognize the signs of scams as they are happening.

With this in mind, the Consumer Education and Outreach Committee was formed to bring leaders in this space together to learn about current issues, exchange knowledge, share experiences, test ideas, and implement pilot projects to find the right channels to reach the right people with the right messages, all with the same goal to help older adults spot, avoid and report scams. The Committee's nearly 40 members include a diverse group of federal, state, and local agencies, consumer advocates, and industry representatives. The committee is co-led by representatives from the FTC, Treasury, AmeriCorps Seniors, and Cuyahoga County Consumer Affairs.

Over the past year and a half, the primary work of the Committee has been divided into two complementary parts. Members of the Outreach Subcommittee tested new methods for getting existing consumer education materials into the hands of people trusted in communities, many engaged in pilot or test projects to identify more effective ways to reach older adults to help them protect themselves and those they care about from scams. Members of the Guiding Principles Subcommittee drew on their own experiences, those are the Outreach Subcommittee, existing materials and research to identify principles to help guide people in organizations to more effectively reach older adults with messages about scams.

Overall, the Committee members aim to produce a user-friendly streamlined reference sheet outlining messages and outreach best practices that could be used by all types of organizations, large and small, national and local, to enhance their fraud prevention communications with older adults. You'll hear more about the work of the subcommittees, including members' experiences in the subcommittee's final output next. You'll hear those things next.

I'll now hand it off to Atalaya who will share what the Committee actually did. Atalaya.

Atalaya Sergi:

Thank you, Tanya. Good afternoon everyone. I'm Atalaya Sergi, the National Director of AmeriCorps Seniors. I'd like to give you an idea of what both the Outreach and Guiding Principles subcommittees did over this past year.

Both subcommittees met monthly during 2023, bringing a lot of energy and ideas to the discussions. We met with the other committees as well as outside experts. For example, we drew lessons on approach and word choice from reframing aging and on reaching older adults from the Benjamin Rose Institute.

As Tanya mentioned, many members of the Outreach Subcommittee launched pilot outreach projects or drew lessons from ongoing projects to identify more effective ways to reach older adults and help them protect themselves from scams. For example, my own AmeriCorps office, AmeriCorps Seniors, drew

lessons from an ongoing grantee project that trains local RSVP volunteers, adults over 55, on scams and fraud. These volunteers then became a part of the Seniors vs Crime Project, where they not only helped

Atalaya Sergi:

... helped raise awareness in their communities through presentations on scams, but also they got trained as senior sleuths who helped investigate complaints from older adults and recoup their funds when possible. In Cleveland, the Scam Squad led by Cuyahoga County Consumer Affairs launched a project to push scam alerts out to residents using their county's ready Notify Emergency Alert System. In this way, people signed up for alerts, get real-time warnings about ongoing scams, how to spot them, and where to report them. Research to measure the program's effectiveness is ongoing. The American Bankers Association Foundation partnered with more than 700 banks nationwide to promote their safe banking for Seniors Campaign, reaching about 300,000 people. The campaign helps banks spread the word about scams with materials, social media, posts, videos, and infographics, and it's working. An older customer in Iowa saw the campaign video, realized he was about to be scammed and reported it to the bank.

Finally, out of its Pass It On program, the FTC created a fraud fighter pilot project, an idea spurred by conversations with consumer advocate, Stephanie Merman and her son Ted. The program held monthly trainings with FTC experts to see if they helped organizations better deliver ready-made presentations. Organizations nationwide participated, concluding that the trainings helped them more confidently present in both English and Spanish. While the Outreach Subcommittee was in the field, the Guiding Principles Subcommittee also met monthly to share their expertise. Discussions covered how we can best develop messages that resonate with targeted populations, are culturally relevant and language accessible.

They also discussed how best to work with partners who are trusted by the target audiences, both to share information and gather feedback. You've already heard about a range of participants in the group, so you can imagine the diversity of perspectives shared over the year. The group included major corporations, multinational financial institutions, large and small nonprofits, state and local consumer protection officials, adult protective services workers, city managers, and staff managing local volunteer programs. Each member brought their ideas, knowledge, successes, and missteps to the table. What we all created together is something we hope any organization can use to help older adults protect themselves and their loved ones from scams. I will now hand it over to Sheryl.

Sheryl Harris:

Hi. So from the outset, the Consumer Education and Outreach Committee had a goal, worked together to find the right channels to reach the right people with the right messages. And in our year of often impassioned discussions, we created a set of principles that will guide anybody who wants to help older adults spot, avoid and report scams. You can adapt these guidelines for your own agency and your own audience regardless of whether you work at a smaller local agency like mine or a national one, and regardless of the size of your outreach budget. We developed these principles by talking about things like word choice. Should we jettison terms like elderly and senior? And instead, maybe use a bigger umbrella term like older Americans or older adults that more people can see themselves fitting under. Should we retire victim blaming terms like duped and fell for? And the answer to that one was really hard, yes.

What tone is most helpful to people? How long can we realistically expect to have people's attention? And how do the answers does some of these questions change depending on what group we're actually talking to? If we can pop over to the next slide... That's great. So our conversations and the information

that we got from our pilot projects helped us create basic principles to guide our work, alerting older residents to scams. You'll be able to read more about all of our work and get additional information at ftc.gov/olderadults. But the boiled down version is this, know your audience. They are not monolithic. Use clear and empowering messages. Less is more really in both word and design. Offer resources in multiple languages whenever you can, get feedback on your products, and that can be informal or formal, depending on your budget. Extend your reach by partnering with people who are already trusted in the community that you're trying to reach.

You don't have to go make a bunch of new friends. There's someone out there in that group already that you can tap for help. And if we can go to the next slide for the URL. Again, this is going to be the new website where all this information is contained. Also on this webpage, we've shared information about common scam tactics and some advice that's really going to work on nearly any scam. As we all know, scams change really rapidly. Scammers are very good at making it easy for people to comply with what really are very confusing demands.

Our shared goal is to make it even easier for consumers to ignore scammers. We have simple advice like, "Hang up. If someone calls you to threaten you with arrest, it's always a scam. You never have to move your money to, quote, unquote, "protect" it. That's a scam. Don't be rushed into sending money. Slow down, check it out." At the end of the day, we are saying, focus on your audience. What do they need to know to protect themselves? What's the simplest, clearest way to say it? Who are our best allies in sharing that message? These guidelines will help you find the best answers for your audience. And with that, I'm going to hand it over to Jennifer Leach from the FTC.

Jennifer Leach:

Thank you, Sheryl. Hello, everyone. I have had the pleasure of working on this committee for the past year or so, and I want to echo something that Tanya said earlier, which is that this committee's work was personal because nearly everyone on this committee had an experience to share about an older adult who had intersected with tellers, cashiers, team members or even themselves. The older person in question might've lost money or were about to, they might've stopped themselves, or had help stopping before they lost money. Sometimes they paid the scammer even after someone intervened. But just about everyone on this committee had an experience like this, and I know it's the same for many of you. So today we have a request of you. We would ask for your help in getting these principles and this advice out into the world. We hope you'll read it and share it, invite someone from this committee to come and talk with your organization, co-brand it, translate it, or simply apply the ideas.

We hope that maybe you will take this further and adapt it for your own audiences, but let's keep this conversation going. As the work of this committee comes to a close, I wanted to highlight a few things that are important to remember, and they echo some of the themes that Tanya, Atalaya and Sheryl have already mentioned today. You might have mentioned, or you might have noticed that everyone in this group has talked about helping older adults, often helping older adults help protect themselves and others. That's because we believe that older adults are part of the solution, not the problem. They're not an object to be protected by some stronger, more powerful force. They're a subject and a powerful one who want to act in their own best interests.

These principles will help you empower them. Another reminder again, echoing my colleagues, words matter. We learn from our wise colleagues at Reframing Aging that words like elderly and seniors make people an other. We're all aging, so let's be inclusive and say, we and not they, and let's be more neutral. So we say older people or older adults instead of elderly and seniors. Reframing Aging has another important message on words like vulnerable and victim too. I believe it's our collective goal to empower people. So instead of labeling them in ways that might not be that helpful, maybe we can talk

about the social connections that might empower older adults and reduce the risk factors. Finally, it all boils down to your audience and you know them best. So how will you find them at the moment they need your information, what should your information look like so they know it's for them, and how will they be able to see those words? What language does it need to be in and who might they trust to deliver tricky messages if it's not you?

When it comes to messaging, one size never fits all, and all of us operate inside systems that give us some limits, maybe on what we say, what we can do and what we can spend, but our committee hopes that we've given you some things to think about and some tools to use the next time you want to reach older adults. With that, I will conclude by thanking the dozens of people who participated in this conversation over the last year or so. Thanks as well to their organizations for supporting the work these committee members did, and to all the FTC team members who made all of this go. Especially I want to thank my wonderful partners, Tanya, Atalaya, and Sheryl, who may or may not have known how big the lift was going to be when they agreed to be part of it. Now, I will hand over to my friend and colleague, Karen Hobbs, to talk about the work of the Industry Training Committee.

Karen Hobbs:

Thank you, Jennifer. Good afternoon. Let's move on to the next slide already. Together, Jilenne Gunther and I have been co-leading the Industry Training Committee, which is comprised of representatives of industries, government agencies, consumer groups and trade associations across many different sectors where scams against older adults intersect. Industries represented include retailers, gift card companies, money transfer services, P2P platforms, financial institutions, security brokers, and cryptocurrency companies. Our committee met regularly over the past year or so to collect examples of existing employee training materials, identify promising practices and examine effective methods for industry and other stakeholders who want to help prevent scams against older adults. By doing so, the outline of some gaps and areas for improvement also came into focus. Committee members collaborated and gained consensus on four guiding principles for what's necessary to establish and carry out effective employee training aimed at preventing scams against older adults. Next slide, please.

These four principles are intentionally broad, so they can be applied to any industry sector. A one-page version with additional explanations and examples is posted on the FTC's website together with a listing of the committee members. We are especially grateful to the volunteers who presented and submitted examples of their own training materials, or programs or ideas, and to those who contributed to the collective discussion, which was robust. The first pillar of successful employee training programs is fundamental. It is corporate support. When the commitment to employee training starts at the top with executives and leaders of industries where older adults are targeted by scams, employees are empowered to help. Committee members identify concrete ways that let leaders demonstrate a commitment to, and a prioritization of employee training and interventions against scams. For example, prioritize time for quality employee training at onboarding and throughout the year so customer-facing employees are more prepared to identify scams and practice the steps to intervene.

Demonstrate corporate support by celebrating and recognizing employee efforts to protect customers from fraud. Establish metrics from measuring scam prevention successes and improving outcomes and tracking training goals. Make proactive fraud intervention a part of your brand. Tell customers, employees, and the public about the concrete efforts being made to help spot and avoid scams both behind the scenes and in front. Distinguish a brand and increase employee engagement and trust. The next three principles speak to the elements of employee training that improve engagement, support learning and increase employees confidence in intervening with suspicious transactions. And now I'll turn it over to Jilenne to walk us through those principles. Jilenne?

Jilenne Gunther:

Thanks, Karen. My name is Jilenne Gunther. I am a director at AARP, and I oversee our business-to-business solutions to the financial industry on fraud. Before I dive into the other three principles, I wanted to take just a moment to recognize the members of the Industry Training Committee that really took the time to prepare and share some of the great work that they're doing that really helped inform the four principles that we're discussing today. Those organizations that presented what they were doing included Western Union, U.S. Bank, Money Services Round Table, SIFMA, AARP, RGCA, Republic Bank, PayPal, NASA, National Federal Retail Federation, Fidelity Investments, the FTC, FDIC, EverSafe, CFPB, the Chamber of Digital Commerce, Blackhawk Network, Best Buy, and American Portfolios Financial Services. As Karen mentioned, we have four core principles, and I'm going to talk about the last three, which are investing in types of training that actually create impact.

Next is focusing on training elements that actually empower the employees on the front line from an empathy standpoint, but also with a sense of responsibility and ownership. And lastly, effective trainings need to be coupled with the delivery of organizational processes and procedures that slow down and actually stop these suspicious transactions. So with that, I want to talk a little bit about the impact principle. Training is only as good as it's able to have that meaningful impact, so some of the things that this includes are making trainings more sticky, more memorable. So trainings should be interactive and gamified so that they're appealing to a variety of learning styles.

Secondly, they should be done in bite-sized training elements. We heard from organizations that most of them train once a year, or when an employee is onboarded. What we heard is that bite-sized training pieces are needed to be sent throughout the year so that employees keep this knowledge and skills fresh and top of mind. A great example of this came from when Fidelity Investments presented. They use bite-sized pieces to train. Their training is under 10 minutes, and they do it four times a year. There's also the reinforcement using bite-sized pieces, so this could be something as sending out screensavers, a quick tip, a success story that's happened within that organization, a customer

Jilenne Gunther:

... customer testimonial and more. The next principle is about empowerment. It's one thing to have knowledge about fraud. It's another to have the confidence and motivation to intervene. So training needs to instill this confidence through the use of videos that show real life scenarios where that frontline employee has to intervene successfully. What does that look like so they can mimic that behavior? It's also about showing videos of real life customers who have been targeted and how it's impacted their life. We saw this in the AARP Bank safe training that uses actors to do role playing in real life scenarios that have actually occurred on the front lines of this crime. This also helps the employee emulate the correct behavior.

And then in addition, hearing testimonials from real consumers who have experienced this crime helps that employee empathize with the customer that they're serving. We also heard from Blackhawk that some of their members use testimonial videos from employees who have stopped fraud as a means to instill that confidence to their peer employees so they can successfully intervene also.

Lastly, delivery. When it comes to impact, it's clear that employees need the policies, procedures, and tools that really enable them to make a difference. The keys to success identified by our working group included things like ensuring that all frontline employees know that they can and how to slow down a suspicious transaction, including delaying and refusing that transaction. It's also things like ensuring the organization have employees that understand how to escalate and report the suspicious transaction up through their organization. Particularly highlighted, we saw that escalations and reportings that

Eversafe's helpful tool is doing that provides a centralized reporting portal that financial institutions, regulators, and APS staff can use with a streamlined way to report fraud.

The trusted contact model was something else that was discussed when SIFMA presented on how their broker dealers use this. We're seeing a number of growing banks and credit unions adopt this, and it was noted by many of our people and within our work group as a critical tool that enables the company to contact that trusted family member or friend if they're suspected fraud. With that, I'll turn it back to you, Karen.

Karen Hobbs:

Thanks. So I guess the question is what's next? Our committee will meet again in June to gather input about how members have implemented these principles into their own employee training and education. The FTC will include these updates in its annual report to Congress in October with a commitment from leadership to prioritize employee training and support employee interventions when fraud is suspected. Any organization can use these principles to improve the quality of training and the outcomes for older adults. We are grateful to our committee members for the amount and the quality of the collaboration presentations and discussion, especially across such seemingly disparate industries. Now it's my pleasure to introduce Patti Posse on behalf of the Scam Prevention Research Committee.

Patti Poss:

Thanks, Karen. Hi, everyone. I'm one of the coordinators of the Scam Prevention Research Committee. We can move to the next slide. The Scam Prevention Research Committee is also made up of representatives from the government, industry and academia and as well as other entities. Emma Fletcher and I from the FTC are going to tell you a bit about what the committee accomplished, but our report is posted on the advisory committee's website that you've already been told about. We want to thank our co-leaders for this group, Mel Lanning with the Better Business Bureau, Andy Mao with the Department of Justice, Hector Ortiz from the Consumer Financial Protection Bureau, and Jerry Walsh with the Financial Industry Regulatory Authority, FINRA. Of course, we also want to thank all of the committee members who gave of their time and expertise to contribute to this project. Their names are all listed in our report and we really appreciate all of their efforts, and now I'm going to turn it over to Emma Fletcher who will share with you what the group found. Emma?

Emma Fletcher:

Thank you, Patty. Next slide please. So this committee looked for research to inform the goal of preventing the harms caused by scams. We focused on research related to scam prevention, consumer messaging specifically. We know this is an important and commonly used means to potentially disrupt scams. The committee did not conduct its own research but reviewed existing research. We identified several important takeaways, including key challenges to effective scam prevention messaging, strategies that may make consumer messaging more effective, and considerations for messaging campaigns to older adults. The committee also identified gaps in existing research and made recommendations for future research. Next slide please.

Several key challenges were identified in the research literature. First, studies have found that people often think they are less susceptible to scams than others, and this has been shown specifically in the scammed context. This so-called optimism bias can seriously hinder prevention campaigns and can be quite resistant to change. Second, scammers often use tactics that intentionally create a heightened emotional state, a state of fear, need, excitement or urgency. These can interfere with the ability to think critically, resulting in poor decision-making. Third, the research strongly suggests that there is a

significant decay factor in people's retention of prevention information. Some studies have found that information is forgotten within weeks. Finally, visual warnings that are timed or placed at the moment a risky decision may be made often fail. The research shows that people tend to become habituated to these warnings, and in the scam context, they may be coached by the scammer to ignore them. Taken together, these challenges suggest that scam prevention messaging will help some people some of the time.

We point out that consumer education cannot be the only tool to fight scams. This is a problem that must be addressed from multiple angles, and while not the focus of this committee, there is a need for research on non-messaging solutions too. Next slide, please.

The committee's review identified research-based strategies to improve the effectiveness of scam prevention messaging. First, messages can be made more memorable and actionable by design. The report describes specific strategies to help accomplish this, and the research suggests that repeat exposure to messages acts as a booster, improving memory of the message. Second, people may need to be persuaded of the value of the message. That is the benefits of heeding the message or the consequences of not doing so. Third, messages that appeal to a positive idea or a widely held value may be beneficial, and the research supports that both general and specific messages can help people avoid scams. That is knowing about specific types of scams or knowing about general tactics scammers use or both have been shown to help. And in the moment warnings, though they won't be effective all the time, they can be improved. The committee's report provides additional details and points to studies supporting each of these strategies. Next slide, please.

We also include special considerations and strategies for messaging to older adults. A major takeaway from the research is the so-called positivity effect. Older adults relative to young adults show an attention preference for positive versus negative information, and these messages may be more likely to be remembered. And the research points to the importance of user testing any messaging material, but especially with older adults. For example, physical and cognitive changes may affect how older adults respond to different designs or to unfamiliar symbols and consider preferred information sources. For example, research suggests that messages delivered to older adults by middle-aged rather than younger or older sources are better received, and the television and word of mouth are key information sources for older adults. And with that, I'm going to turn it back over to Patty.

Patti Poss:

Thanks, Emma. The next slide please. In the end, the committee concluded that more research is needed to help the government, industry, consumer groups and others develop campaigns and warnings that have the best chance at succeeding in preventing scams. The report makes several recommendations. Here's some of the key ones. First, representative studies. Many of the studies that we found were limited to a small number of participants and they lack diversity in the participant pool. Studies based on a more representative samples are needed to inform the work to create campaigns and warnings to disrupt scams affecting all members of the public. Message testing, which we've heard a few times here today. The committee recognized that it's difficult to study fraud in the wild. It's hard to expose participants to prevention messages and then test their resistance to a subsequent staged scam attempt, but it is important to test messaging with focus groups and qualitative methods.

Industry collaboration, committee members express support for collaborative research with consumer-facing entities conducting transactions. For example, there could be an embedded researcher with access to that transactional data and that they might study the effects of the warning signs and text alerts and things. The report also includes recommendations about the specific topics, all of those specific topics from the committee's research that Emma just mentioned. This includes things such as

overcoming the optimism bias, making messaging memorable, when to use general messaging versus specific messaging, et cetera. All of this research is needed. Next slide, please.

In conclusion, and of course, going forward, we encourage you to read the report, which is on the advisory group's website, to learn more about what the committee found and see those details, but also to hopefully inspire you to conduct or fund future research that's needed to disrupt scams. We commend the many researchers, the institutions and organizations that have conducted, funded, or otherwise supported this important area of research. And you'll see that the report includes seven pages of references to various articles and studies, including many that were authored by the institutions and the individuals who served on this committee. Their work is vital to the Scams Against Older Adults Advisory Group, and to others, anyone whose aim is to stop scams from harming all people.

We look forward to seeing more research on scam prevention consumer messaging to help develop new campaigns and new warnings that have the best chance of succeeding in prevention scams and preventing scams. And now we're happy to hand it off to Patty Hsue, the Stop Senior Scams Act Coordinator with the Federal Trade Commission, and one of the leaders of the Technology and New Methods Committee. Patty?

Patty Hsue:

Thanks so much, Patti, and thanks to Emma as well for presenting on the research that you've done. I am delighted to introduce the technology and new methods committee and the work that we're currently engaged in. As you've heard, it's important to provide consumers with tools to arm themselves against fraud. Education and training are important components of that tool set. The Technology and New Methods Committee is focusing on two equally important angles, providing older adults with tools to prevent scams from reaching them in the first place and stopping scammers from taking or keeping their money. Our committee has identified four projects that our members have committed to working on. The first is focused on increasing the possibility of recovering payments that consumers made to scammers through bank transfers and potentially cryptocurrency. The second is looking at making it more difficult to collect payment through gift cards. The third is exploring how to stop scam text messages from reaching or impacting older adults, and the fourth is focused on how our committee members who all come from different industries, as well as government agencies and consumer advocacy organizations, can better collaborate and share information, data, or other intelligence to stop scams from impacting consumers.

Before I turn things over to the project leads, to provide you with more details about our efforts, I'd like to thank my committee co-leads Lisa Schifferle from the Consumer Financial Protection Bureau, Andy Mao from the Department of Justice, Josh Burcu from US Telecom, and Katie Daffan from the Federal Trade Commission for their invaluable guidance and help in steering our work. With that, I'd like to invite Paul Benda from the American Bankers Association to tell you more about our first project.

Paul Benda:

Thanks, Patty. Thanks very much for having me here. I co-lead this effort with Andy Mao from the Department of Justice. We've had several members of the government community that are with us, along with those from the financial sector, including from banks in the crypto industry. And we've really been focused on ways that we can reduce these fraudulent transfers from occurring as well as if one unfortunately does occur, how can we recover those funds? So looking at reducing the effect of these transfers occurring has been focused on education and training that we can provide for bank employees so they can stop these transactions.

Unfortunately, banks don't necessarily want to be held liable if these transactions are stopped and there is a reason they should have gone forward. And so we look for those that have safe harbor legislation that is out there. And we've gathered up several states have put into place safe harbor legislation for multiple financial institutions that can, when an employee acts in good faith, stop these transactions from going forward. We think it's one great way to protect folks from having their money be sent to scammers.

We are trying to see how well have these been implemented. We're working with the conference of state banking supervisors who oversee these financial institutions to see have they seen any issues. We're working on developing a survey that we can send out these financial institutions to see how many are even aware that these laws exist. Have they used these laws? Have there been improvements or other elements that I think need to be improved to change those laws? So we're trying to see are there legislative remedies that need to be put in place to make these laws more palatable so they're used more broadly. We think it's one great way to stop the money from going out the door, although we do know that money goes out the door anyway.

And so we are working closely with the FBI's Internet Crime Complaint Center. This is one of the few places that a consumer can report to the government that they have fraudulently sent money out, and the government can actually work with banks and others to try and recover those funds. They've got a fairly good success rate when they are notified very quickly because this money moves very fast, and so we're trying to increase education and outreach of the availability of this tool for both consumers and banks.

One of the things that we find, especially for smaller banks, is they may not be aware that they can file one of these reports on the behalf of one of their customers, and we think that's a great way to go forward because banks have a lot of the information. There's not going to be errors in that report that goes forward, and hopefully they can do it much more quickly. So the idea is, can we increase knowledge and availability of these types of reports to recover those funds? Even taking it one step further, we know that the

Paul Benda:

... FBI may or may not be able to investigate every single complaint that's in there. Can we create a partnership between law enforcement and the private sector that increases the ability for us to recover those funds on the behalf of consumers? The key here is that time is of the essence, and so how do you create a capability for both the bank that's holding those funds and the bank that has sent those funds to transfer that money or hold and freeze that money as quickly as possible while protecting the interest of everyone that's involved? We're also interested in looking at other ways that we can increase information-sharing both amongst the government and the private sector, as well as between the private sector entities.

We're interested in ways that we can share when a fraudulent account has been identified, that with other financial institutions, so they can put that on what you might call a friction list. The American Bankers Association is developing a capability that'll allow banks to share this type of information. So when a bank is aware of one of the accounts on this friction list, they can do more appropriate due diligence. They might ask their customer more questions. Is this a new payee? This is an out-of-bound transaction that you normally don't send this kind of money, so they can determine whether the customer go back to them and say, "Do you really want to execute this transaction<" and try and stop people from sending money to scammers.

We're also working with the crypto industry, who has put in place ways to identify a similar thing for crypto wallets. A lot of those wallet transactions are public knowledge and they can see which wallets

have been used for illicit activity in the past. Some in the industry have actually created a list that stops transactions to those wallets that are known to be bad wallets. Can we create a set of best practices so that this gets implemented across the crypto industry, so that crypto kiosks, which are a common avenue for scammers to recover funds from folks, can be set up so they don't send money to those bad wallets? So we're looking at ways can we not only stop the funds from going out, can we recover those funds much more quickly and can we educate people the tools that are available?

So there's a lot of efforts underway. We're putting together basically our strategic plan on how we're going to implement these things. We hope to have that in place by early this summer and then start executing on those later this year. With that, I'll hand it over to my colleague, Mark, who will take it further. Thank you.

Mark Southon:

Thanks, Paul. Good afternoon. My name is Mark Southon. I currently lead the global transaction monitoring and fraud investigation function with Blackhawk Network, a global-branded payment technology company focused on rewards and incentives, payment solutions, and very importantly, gift cards.

In addition to my role at Blackhawk, a role that I find great purpose in, I also come before you today as a representative of a risk management consortium comprised of private industry, consumer advocacy groups, and government agencies, who operating under the umbrella of the Scams Against Older Adults Technology and New Methods Committee have collaborated over the past several months with the specific goal of identifying new tools and processes that can be brought to market to more effectively protect older adults from being scammed, especially when gift cards are used to facilitate that scam.

Each member of the consortium is recognized as an expert in their field, and each has been on the front line in either fighting fraud or helping to manage the customer experience when fraud does occur. Our collective experience, and notably our experience during the COVID outbreak, has helped to shape the scope of our current work product, which I'm happy to share with you now. Thus far, our work product can be summarized into two distinct deliverables. The first deliverable is a set of best practices for retailers who sell gift cards, the merchant brands represented on the gift cards being sold, integrators who help to facilitate transactions between the retailers and the merchant brands and the payment processors.

The second element of our work product is a set of data and/or information sharing standards between critical supply chain partners or actors to improve real-time, risk-based decisions. Allow me to provide a little more detail on each of these deliverables. Our best practices provide macro and tactical strategies to address fraud involving gift cards scams perpetrated against older adults at each stage of the customer journey. That includes steps that can be taken before a gift card is purchased, before it is activated, and after a gift card has been activated. For example, prior to activation, we provide indicators that retailers should look for when older adults or any customer is preparing to buy gift cards, which might suggest that fraud is involved.

From an activation perspective, we provide integrators with a list of core risk processes and technologies that should be built and extended to the retailers and merchant brands that they support. These capabilities include real-time controls that allow a retailer or an integrator to prevent card activations if there are signs of fraud. After the card is activated, we provide payment processors with a framework to profile malicious spending behaviors indicative that a scammer has accessed funds on a gift card. We plan to issue a draft version of our best practices to a select group of supply chain actors within the gift card industry for comments later this month.

The data and information-sharing standards are in the early stages of development. However, guiding principles in a business case have been created for sharing risk-based data and information for what we believe will enrich critical decisions when gift cards are activated and redeemed. We plan to issue a draft version of the data and information standards for comment this summer to a select group of industry stakeholders.

Now, as I conclude my remarks, I'd like to end where I began. I represent a company and a risk management consortium that collectively have invested time, effort, and millions of dollars in training and educating people, optimizing processes and building technologies to prevent scams against older adults and any consumer that uses gift cards. There's a reason that drives what we do and how we do it. When we strip away our work responsibilities and titles, we're left with reality of who we really are. We're sons and daughters, grandsons and granddaughters, nephews and nieces of older adults, some of whom have been scammed.

We do what we do out of a moral obligation to our families and our communities that we live and serve in and we hope that the collective and discrete changes that we make and introduce over the next coming months will have a transformational impact on the manner in which our families, our communities, our customers, and our industry are protected. Thank you for your time, and with that, I'll hand things over to Matt.

Matthew Gerst:

Thanks, Mark. My name is Matt Gerst. I'm a partner at the law firm Wilkinson Barker Knauer. I'm here today on behalf of CTIA, which is the trade association for the wireless industry in the US, where I worked for 13 years prior to joining the law firm. So I'm here today to talk to you about our working group focused on how to address text messages that are being received by older adults to mitigate spam and scam activity on those text messages.

So first, wireless text messaging is one of the most trusted and popular communication services among American consumers, including older adults. Over 2.1 trillion text messages were exchanged in 2022, and businesses relying on text messages to reach consumers continues to grow year over year. Yet, bad actors are determined to find ways to send spam and scam text messages that result in harm to consumers, including older adults. Maintaining wireless text messaging is a trusted communication medium that requires a multilayered approach that's unique to the wireless industry. These steps include upfront vetting, validation, filtering, and blocking, information-sharing based on consumer complaints, and enforcement by federal and state government agencies.

This approach is protecting consumers. Last year, wireless providers blocked an estimated 47.5 billion spam and scam text messages that never reached consumers. Our working group, made up of staff from the FTC, the FCC, Department of Justice, AARP, wireless providers, security vendors, and message senders like banks and financial institutions, we were tasked with identifying and recommending ways to enhance these protections through technologies, education and collaboration. While we are continuing to develop our specific recommendations, I'll briefly walk you through our key findings and where we are directionally going with our recommendations.

First, a little background. Text messaging can refer to many different text messaging technologies and platforms, some provided by your wireless provider and others provided by third-party applications like WhatsApp. Our working group is focused on text messages provided by wireless providers. Our working group is considering three areas that can help reduce spam and scam text messages. These include educating businesses who send text messages about following best practices like consumer consent and upfront vetting that can help ensure their legitimate messages reach consumers. We want to develop

new resources to help consumers identify suspicious text messages and sharing information to promote additional prevention tactics like blocking or enforcement actions.

For example, a brand like say, Walgreens or Chase Bank that has appropriate oversight over their messaging campaign can help identify impersonation scams for blocking by wireless providers and others throughout the messaging industry. We're also considering whether technical experts can explore solutions that could harness information about message senders to help maintain consumer confidence in text messaging.

Finally, we are considering how to encourage the development of new, collaborative information-sharing tools that can enhance industry capabilities and deliver ready-to-act packages for law enforcement. Stopping the spammers and scammers will be the most effective way to keep text messaging trusted medium. While we continue to finalize our recommendations, our working group is optimistic about harnessing public and private industry capabilities to make it harder for bad actors to harm consumers and maintain trust in text messaging. With that, I'll hand things over to Ryan.

Ryan McLaughlin:

Thanks, Matt. I'm Ryan McLaughlin. I'm the Director of Compliance Analytics and Design at Western Union, and I'll be giving an update on the information sharing project. The project is driven by members spanning a variety of sectors, both public and private. As a project team, we recognize that scams are perpetrated across many different industries with various technologies, communication channels, and financial services. This presents a unique opportunity to enhance the mitigation of scams by sharing information. The goal of our project team is to facilitate pathways for the sharing of information in order to mitigate scams more quickly on a tactical level, but also more proactively on a macro pattern-based level.

To this end, we're focusing on three initiatives, creating a library of existing regulations and legal avenues that allow sharing of information between organizations. Some of these avenues are already utilized to facilitate investigations. Next, creating a register of participating organizations with contacts at each whose focus and expertise lie in the mitigation of scams. And finally, defining the type of data and information that is valuable for mitigation activities and allowed to be shared-based on existing regulations and legal avenues.

The type of information under consideration includes general scam trending and intelligence, specific scam indicators and behaviors, analytical and investigative techniques, tactical data points and repositories, and new technologies utilized in data analytics. And with that, I will hand it back over to Patty.

Patty Hsue:

Thanks so much, Ryan, and thanks to all of our project leads for presenting here today. Our technology and Mew Methods Committee projects are ongoing, so please stay tuned for additional updates on our work that will be coming out later this year. I'd now like to turn things over to the FDC's Elder Justice Coordinator, Lois Greisman, to say a few closing remarks.

Lois Greisman:

[inaudible 01:03:13], Patty, appreciate that. Good afternoon everybody. It's been really terrific to hear about all the great work that's been done and all the exciting work that's on the horizon, all of this being done to counteract scams against older adults. I'd like to express my genuine thanks to everyone who's made this event possible, and particularly to the committee members who spoke today, the committee leads who helped facilitate conversations and collaboration, all committee members who've

participated and contributed to this important work, and also to the advisory group members who've been committed to help to reduce the impact of fraud on older adults. So we very much appreciate the significant time, energy, and creativity you've lent to these many initiatives. It's all been well worth the effort. I want to recap just briefly. So materials that the Consumer Education and Outreach Committee and its complementary Industry Training Committee have prepared, these provide a foundation for industry, consumer groups, government agencies, and private citizens to implement best practices in the way they communicate with older adults and with employees about scams. Consumer education must reach people at the right time, in the right way, and with a usable message.

At the same time, employees should receive top-notch training that will help them spot and intervene when appropriate in scams affecting older adults. Next, work that the Scam Prevention Research Committee has done directly informs our scam prevention messaging in the here and the now, and it serves as an imitation, if not an outright beckoning, for further research on how best to reach older adults and how to minimize harm from scams.

Finally, the potential technology-aided solutions teed up by the Technology and New Methods Committee, which remain the subject of ongoing work, offer much anticipation and reward. Next slide, please.

For anyone joining us virtually who wants to learn more about some of the ways that we can prevent and mitigate scams against older adults, thank you for your time. I urge everyone to take a look at the resources we've talked about today by going to FTC.gov/OlderAdults, one word, and also keep an eye out for the older adults report where we are going to provide more details and updates about the work of the advisory group and the work of the committees. The report will be issued to Congress and to the public later this year. It comes out in October. If you missed any parts of today's meeting or you'd like to listen to any part of it again, a video recording of the event will be posted on our events page.

In closing, I can say with much confidence that the work of the Scams Against Older Adults Advisory Group and its committees has deepened our understanding of prevention and protection strategies to reduce fraud impacting older adults. This work also has strengthened key connections among the many stakeholders who have a role to play in tackling this massive problem. What we've accomplished has and will continue to have tangible impacts, and there's always a but.

That said, as we gather here, older adults are losing money to fraud, millions of dollars every day. So my challenge to each of you is to commit anew to our coordinated work to fight fraud against older adults. Together we can continue to tackle fraud strategically. So once again, thanks to each and every one of you for your many contributions, your time, your energy. We look forward to working together. And with that, we are adjourned. Thank you all.