RYAN A. BIZZARRO, CHAIRMAN
116 MAIN CAPITOL BUILDING
P.O. BOX 202003
HARRISBURG, PA 17120-2003
(717) 772-2297

HOUSE MAJORITY POLICY COMMITTEE
PAHOUSE.COM/POLICY
POLICY@PAHOUSE.NET
@PADEMPOLICY

HOUSE OF REPRESENTATIVES
COMMONWEALTH *of* PENNSYLVANIA

House Democratic Policy Committee Hearing

Protecting Seniors from Online Scams

Wednesday, February 25, 2025 | 12:00 p.m.

Representative Brian Munroe

OPENING REMARKS
12:00 p.m. Rep. Brian Munroe, D-Bucks

PANEL ONE
12:05 p.m. Kate Kleinert, Scam Victim
Glenolden, PA

Bill Moyer, Scam Victim
Allentown, PA

Q & A with Legislators

PANEL TWO
12:25 p.m. Mike Crossey, President
Pennsylvania Alliance for Retired Americans

Q & A with Legislators

PANEL THREE
12:40 p.m. Yosef Getachew, Senior Policy Counsel
Reset.Tech

Q & A with Legislators

Five Minute Testimony – Pennsylvania On-line Scams Informational Hearing –
Kate Kleinert

Good Afternoon Chairman Bizzarro, Representative Munroe, and members of the House Democratic Policy Committee Thank you for allowing me to speak today about my romance scam experience.

I was not looking for love in all the wrong places. I wasn't looking at all! At the time of my scam, I had been widowed for 11 years and we were in the midst of the lockdown due to COVID. I never, ever accept a friend request on Facebook from someone I do not already know. But that day I did. The request came from a very handsome man dressed in medical garb - a white coat and scrubs.

He had studied my profile on Facebook and knew a great deal about me. "Tony" asked me to download Google Hangouts chat so that we could talk. Those apps are completely untraceable. But I have to admit that it was nice just having a conversation with a man again.

Every single night, he would call and ask "How was your day, Honey?". No one had asked me that since my husband had died. In all the many conversations we had, he never used my first name. It was always Honey, Sweetheart, Babe, etc. and that is so that he didn't get my name mixed up with the other 45 or 50 women he was scamming at the same time!

Tony knew from my profile that I did not have children but took in hospice dogs. I had six of them and Tony learned all their names and could recognize them by their bark. It endeared him to me.

Tony got romantic by the second week but I was pushing back. He never asked for money until 3 or 4 months into the "relationship." By that time I was talking to him 5 or 6 times a day and trusted him.

He began by asking me for a hundred dollar gift card here, then a fifty dollar gift card there. The big request came for airfare to get him to Philly to meet me. And of course he never showed. Once I realized I was being scammed, my heart shattered. Losing the money is devastating. Losing that love, and the life I thought was going to be mine….that was more than I could handle. I cried for days and days.

Because Facebook and Google have let this stuff go on for years and years despite all their power to track what people engage with, it almost seems like they want to make it easy for people like me to be targeted for scams.

I met with resistance when I tried to report this to the police. You have no idea how much courage it takes to make those calls. I called the non-emergency number for the local police and left a message that I needed to come in for them to take a report. I never heard back from them. Then I called the State Police. A woman answered and I was so relieved because I thought it would be easier to tell a woman my story. She interrupted after a few sentences and said “Why are you calling here? There’s no crime here.” I started to cry and she said, “You willingly gave him that money, Hon.” And she hung up.

And I must be honest: I did not even know that reaching out to the social media platforms where the scam took place was an option. I did not know where to report what was happening or whether anyone would respond.

That’s where The Unbreaking Project – Kate’s Hug was born. I am crocheting afghans for victims of romance scams for them to wrap around themselves and feel supported.

The kit has a blanket – either made by me or other volunteers and in order to fill the need, we are even purchasing soft flannel throws. Also in the kit there is a list of resources the victim can contact and there is a letter that I have written to the victim. The catch is I am giving the kits to Law Enforcement – free of charge – for them to give to the victim. The Law Enforcement personnel and the victim will see each other differently after the kit is given.

I’m going to bring this to a close, but I need to quickly tell you about the second half of my story. I had no money for any repairs on my house and because of a faulty extension cord, my house burned to the ground with every blessed item I owned. I ended up in the Burn Unit at Crozer Chester Burn Center and none of my 6 hospice dogs made it out.

I share my story not to embarrass myself but to shine a light on how social media can be used by scammers to target victims and build trust. These platforms make it too easy for scammers to create convincing fake identities and find and target people like me. With just a few clicks, a

stranger could identify that I was a widow, view my interests, and learn enough about my life to craft a believable story tailored specifically to me. The same tools that help us connect with friends also enable bad actors to search for and single out older adults who may be isolated or grieving.

The damage from scams is devastating and certainly does not heal overnight. These people are tremendously good at what they do and the platforms make it even easier for them. I urge this committee to put more accountability on platforms so there are safeguards in place to prevent scammers from reaching and harming people like me.
Thank you for listening.

DRAFT Testimony of Bill Moyer

House Democratic Policy Committee Informational Hearing on Tech-Enabled Scams

February 25, 2026

Good afternoon, Chairman, and members of the Committee. My name is Bill Moyer, and I live in Allentown, Pennsylvania. I'm not a tech expert. I'm not a policy analyst. I'm just a homeowner who, for the better part of a year, had strangers showing up at my front door — crying, angry, and devastated — because they had been scammed on Facebook.

In September of 2023, my wife and I moved into a new house. Not long after we settled in, something unusual started happening. Our Ring doorbell camera caught someone walking around our property, peering at the house. Then another person showed up, pacing in our driveway on their cell phone before coming to bang on our door. When I answered, he was furious. He said he was there to pick up his puppy.

I had no idea what he was talking about. But he did. He had found a Facebook page advertising Belgian Malinois puppies for sale, run by someone calling herself "Ginger Malinois." He had paid $800 upfront. The page looked professional. The photos were convincing. The puppies had names. He had driven to Allentown expecting to bring home his dog. Instead, he found me, a stranger, at the address listed for the "breeder." There was no breeder. There was no puppy. There was only a scam.

That was not a one-time incident. Over the next eight months, it happened 12 to 14 times. People came from Michigan, Tennessee, New Jersey and elsewhere. They would book hotels, drive into town on a Saturday or Sunday morning, and pull into my driveway full of hope. I'd be out doing yard work and watch a car turn in, and my stomach would drop. I knew what was coming. My wife started telling me to go inside whenever a car slowed down in front of our house. You just never know how someone is going to react when they realize they've been scammed.

And they had been scammed. Every single one of them. What stays with me most is not only the fear, but the look on people's faces. I watched grown adults stand in my driveway and cry. I heard people say, over and over, "I should have known better." So many people had trusted what they saw on Facebook completely.

Let me be clear about how this scam worked: it ran entirely through Facebook. The fake breeder created a Facebook page, posted photos of puppies, gave them names, built a following. When someone expressed interest, they were directed off-platform to a separate website to complete payment — which is exactly how Facebook claims to escape responsibility. The transaction didn't happen on their platform, so they say it isn't their problem. But the advertising did. The recruitment of victims happened on Facebook. Without that platform, this scammer could not have reached hundreds of people across multiple states.

I reported it to Facebook. More than once. I never heard back. I went to the police; they sympathized, but told me there was nothing they could do. I filed a complaint with the FBI. Nothing came of it. I attribute the lack of response due to the fact that I was not personally financially impacted. The Better Business Bureau started sending threatening letters to my address because victims were filing complaints listing my home as the business location. I had to contact the BBB myself, repeatedly, to explain that I was the victim too.. At every turn, there was no clear path forward. No accountability. No one willing to act.

Meanwhile, that Facebook page stayed up. Weeks passed. Months passed. People kept coming to my door. It wasn't until a local news station ran a story that things finally began to slow down. Not because Facebook acted, but because media attention scared the scammer into eventually going quiet.

I have since learned that this is not unusual. I have read that Meta made $16 billion last year from scam-related activity — that it is, essentially, a line item in their budget. They have calculated it is more profitable to leave scammers on their platform and collect revenue, than to take them down. If that is true, and I believe it is, then what happened in my driveway was not an accident.

I am not here today because I personally lost money. I'm here because I watched what it did to the people who did. I stood in my own yard and witnessed the aftermath of what happens when a billion-dollar platform ignores what is happening and fails to protect trusted users. Those people who showed up at my house — hopeful, then heartbroken — they deserved better. They trusted a platform that is a household name, and that platform failed them. Facebook built this platform and let scammers run wild on it, but they left my innocent family to answer the door.

I'm grateful this Committee is holding this hearing. I hope my story helps you understand that this is not an abstract problem. It showed up at my front door, over and over, wearing the face of someone who just wanted a puppy. These are real people, and they need real protection. And so do the rest of us.

Thank you.

Pennsylvania Alliance for Retired Americans®

Good afternoon. I'm Mike Crossey, President of the Pennsylvania Alliance for Retired Americans, or PARA. We are a grassroots advocacy organization representing more than 313,000 members across the commonwealth. Together we educate, organize, and mobilize older Pennsylvanians to fight for a healthy and secure retirement — for today's retirees and for future generations of Americans.

It won't surprise anyone who has bought groceries or paid a utility bill recently that a secure retirement is becoming harder to achieve. For retirees and older Pennsylvanians — many of whom live on fixed incomes — inflation hits especially hard.

But rising costs are not the only threat to financial security. Older Americans are also being scammed at alarming and growing rates.

Fraud is not new. And older adults have long been targeted. But the scale, speed, and sophistication of scams today are unlike anything we have seen before.

Scams on social media and digital platforms, increasingly powered by artificial intelligence, are targeting older Americans at shocking rates. These scams threaten financial security, privacy, and peace of mind.

That's why the Alliance for Retired Americans and PARA have launched a year-long national Stop the Scam campaign to help older adults stay safe online, share their experiences, and demand stronger protections.

Federal data show billions of dollars are lost to fraud every year. Older Americans are disproportionately affected. In 2024 alone, older Americans reported $4.8 billion in losses from internet scams — a 43 percent increase

from the year before. Social media is now the leading contact method for fraud targeting adults aged 60 and older, both in the number of cases and the total dollars lost. These scams are not spreading by chance. They are spreading because tech platforms provide scammers with powerful tools to find and target victims at scale.

Closer to home, Attorney General Sunday says Pennsylvanians lost more than $75 million in 2025 to scammers, much of which has been fueled by artificial intelligence. And we know these numbers are only part of the story. The FBI says that many scams go unreported because victims feel embarrassed, ashamed, or unsure where to turn.

This is not abstract. It is happening in our communities right now.

One of our members, Kathy from Philadelphia, received a phone call that appeared to come from her bank. The caller told her there were suspicious purchases made in Atlanta and asked if she had made them. She had not.

The caller said he would close her account and open a new one to protect her. As part of the process, Kathy received security codes by text and was told to read them aloud — which she did.

When she later checked her account online, she discovered that $1,500 had been moved from her savings to her checking account and then sent through Zelle to someone the bank could not trace.

Kathy was fortunate. She contacted her bank quickly and was reimbursed. Bank staff later explained that scammers had spoofed the bank's phone number, making the call appear legitimate.

That story has a positive ending. Too many do not.

Kathy knew to check her account online — not everyone can or understands when they should. She reported the fraud quickly — before

additional losses occurred. And she benefited from consumer protection laws that sometimes require reimbursement.

But those same protections are not necessarily available to everyone who loses money in a tech-enabled scam.

For example, we have Alliance members who have been scammed on Facebook. They thought they were purchasing an item from a company they knew – only to realize too late that the company had been impersonated and there was no way to recover the money, and couldn't even figure out how to report the problem to Facebook.

Fighting these scams is going to take all of us.

At PARA, we're now making education a key part of our programming.

As part of the Alliance for Retired Americans, we have launched a 'Stop the Scam' campaign - an initiative designed to combat the rise of AI and social media-enabled scams targeting retirees. Educating seniors about the risks and providing tools to recognize warning signs and protect themselves is a critically important part of the campaign.

But education alone cannot solve a problem that is operating at industrial scale.

We need legislators and regulators to create stronger safeguards, stronger enforcement tools, and to demand greater accountability from the technology platforms that allow scams to spread rapidly and at scale.

We also need policymakers to listen to older adults. These harms are happening to real people, in every community across the state, and the consequences can be devastating — financially, emotionally, and psychologically.

Because protecting retirement security in the modern world requires more than helping people avoid scams.

It requires building a digital world that is safer by design — where platforms take responsibility, safeguards are strong, and all consumers are truly protected.

Thank you.

Reset • Tech

Written Testimony of

Yosef Getachew
Senior Policy Counsel
Reset Tech

Before the
House Democratic Policy Committee

Regarding

‘Protecting Seniors from Online Scams’

February 25, 2026

Introduction and Summary

Chairman Bizzarro, Representative Munroe, and Members of the House Democratic Policy Committee, my name is Yosef Getachew and I serve as Senior Policy Counsel at Reset Tech. Thank you for the opportunity to testify before your committee today. I am here to discuss a serious and rapidly escalating threat to the financial security and wellbeing of Pennsylvanians: the spread of online scams and the role of social media platforms.

Scams and fraud have been problems for decades, but over the past several years we have seen a dramatic transformation in how these schemes are conceived, disseminated, and financed. At the heart of this transformation lies the unprecedented reach and power of social media, combined with accelerating advances in artificial intelligence. Together, these technologies have helped turn scams into systemic threats that cost Pennsylvanians at a minimum hundreds of millions of dollars each year and undermine the safety and security of families across the Commonwealth.

This testimony will outline the scale of losses from online scams both nationally and in Pennsylvania, the unique role social media and AI play in enabling, spreading, and profiting from online scams, and policy recommendations that can hold platforms accountable while reducing economic and personal harms to families across the state.

The National Landscape: Online Frauds and Scams are Reaching Epic Levels

Online scams and fraud have escalated to unprecedented levels, evolving into a nationwide epidemic that is costing Americans billions of dollars annually. According to the Federal Trade Commission’s (FTC) most recent data, consumers reported losing more than $12.5 billion to

fraud in 2024, an increase of roughly 25 percent over the prior year.[1] Similarly, the Federal Bureau of Investigation's (FBI) most recent Internet Crime Complaint Center report found that victims reported over $16 billion in scam losses, representing a 33% increase from the prior year.[2]

What is particularly striking is how much of this fraud is originating on social media platforms. According to the FTC data collected since 2021, consumers have reported $2.7 billion from scams that originated on social media platforms, more than any other contact method.[3] The FTC's 2024 data paint an even starker picture: most people — 70% — reported a loss from scams when contacted on a social media platform, and those losses added up to $1.9 billion for the year alone.[4] A recent Pew survey also found that 73% of Americans have experienced some kind of online scam or attack with 33% reporting they received scam attempts on social media at least weekly.[5] The magnitude of these losses underscores that social media is a central transmission vector that has helped scammers at a scale that was previously impossible.

Nationally, these losses represent hundreds of thousands of individual victims, including retirees, working-age adults, veterans, communities of color, and young people. Each group faces a rapidly escalating variety of financial harms from schemes that range from cryptocurrency fraud and romance scams to government impersonation scams and AI-generated voice and video cloning. Further, scam losses from FTC and FBI datasets likely understate the true total because many victims never report scams[6] due to shame, embarrassment or the belief that nothing can be done.[7]

---

[1] Federal Trade Commission, *New FTC Data Show a Big Jump in Reported Losses to Fraud to $12.5 Billion in 2024* (March 10, 2025), https://www.ftc.gov/news-events/news/press-releases/2025/03/new-ftc-data-show-big-jump-reported-losses-fraud-125-billion-2024.

[2] *Federal Bureau of Investigation Internet Crime Report 2024* (April 23, 2025) at 3-4, Internet Crime Complaint Center, https://www.ic3.gov/AnnualReport/Reports/2024_IC3Report.pdf ("2025 IC3 Report").

[3] *FTC Data Shows Consumers Report Losing $2.7 Billion to Social Media Scams Since 2021* (Oct. 6, 2023),https://www.ftc.gov/news-events/news/press-releases/2023/10/ftc-data-shows-consumers-report-losing-27-billion-social-media-scams-2021.

[4] Bureau of Consumer Protection Staff, *Top Scams of 2024* (March 10, 2025), https://consumer.ftc.gov/consumer-alerts/2025/03/top-scams-2024.

[5] Jeffrey Gottfried, Eugenie Park, & Monica Anderson, *Online Scams and Attacks in America Today* (July 31, 2025), Pew Research Center, https://www.pewresearch.org/internet/2025/07/31/online-scams-and-attacks-in-america-today/.

[6] *Protecting Older Consumers 2023-2024: A Report of the Federal Trade Commission* (Oct. 2024) at 27, Federal Trade Commission, https://www.ftc.gov/system/files/ftc_gov/pdf/federal-trade-commission-protecting-older-adults-report_102024.pdf ("Estimating the true cost of fraud to older adults based on reporting data is challenging. While Sentinel provides invaluable information about the nature of fraud, the losses reported in Sentinel are the 'tip of the iceberg' as most consumers do not report.").

[7] Christina Ianzito, *Let's Stop Blaming Scam Victims, New AARP Report Says* (July 21, 2022), https://www.aarp.org/money/scams-fraud/victim-blaming/.

The Impact on Pennsylvania: High Losses and Persistent Vulnerabilities

Pennsylvanians are not immune to these trends and in many cases are impacted in ways that mirror the national picture. According to the Pennsylvania Office of Attorney General's Bureau of Consumer Protection, more than 4,000 scam-related complaints were filed in 2025, and residents lost over $76 million to scammers that year.[8] These reports capture a range of scams, including phishing, government impersonation schemes, and investment fraud.[9]

Data from the FBI also show that Pennsylvania consistently ranks among the top states for reported complaints and financial losses from scams. In fact, the most recent FBI data indicates that scam and internet crime losses in Pennsylvania have exceeded $400 million in a single year, placing the Commonwealth among the top ten states nationally for total reported losses.[10]

Beyond the immediate financial toll from losses, the economic and emotional impacts are profound. Pennsylvanians have lost live savings,[11] retirement funds,[12] and in some instances faced severe emotional distress[13] after being deceived by fraudsters exploiting social media platforms.

Social Media Platforms Enable and Spread Scams

Social media has increasingly become a playground for criminals to spread scams. Large social media platforms such as Meta (Facebook, Instagram, and WhatsApp), Google / YouTube, TikTok, Snap, and X are designed to connect millions of people instantly, amplify content, and monetize attention. Those same features have created an environment that has enabled scams – fraud can spread faster, look more legitimate, and reach more people than ever before.

Criminals are deliberately exploiting the structure of social media platforms to identify targets, build trust, and extract money on a massive scale here at home and across the nation. Below is a list of major social media design features that are used to spread and target users with scams:

- **Friend requests:** Social media platforms allow users to send unsolicited friend requests to strangers often by default. This means criminals can mass-send friend requests to

---

[8] *AG Meets with Older Residents Warning that Pennsylvanians Lost $76M to Scammers in 2025; AI Fueling More Sophisticated Swindles* (Jan. 29, 2026), Pennsylvania Office of Attorney General, https://www.attorneygeneral.gov/taking-action/ag-meets-with-older-residents-with-warning-that-pennsylvanians-lost-76m-to-scammers-in-2025-a-i-fueling-more-sophisticated-swindles/.
[9] *Id.*
[10] *See* 2025 IC3 Report at 21.
[11] Joshua Sidorowicz, *Berks County grandmother loses $220K in exploding "task job" scam*, CBS News (Feb. 16, 2026), https://www.cbsnews.com/philadelphia/news/berks-county-grandmother-loses-220k-task-job-scam/.
[12] Brett Balicki, *Pennsylvania woman loses over $50K in Facebook scam* (Jan. 25, 2025), YourErie, https://www.yourerie.com/news/crime/pennsylvania-woman-loses-over-50k-in-facebook-scam/.
[13] *Family Fights to Disentangle Father from Romance Scam, Part 1: A family tries desperately to free their father from a series of online scams*, AARP (Feb. 21, 2025), https://www.aarp.org/podcasts/the-perfect-scam/info-2025/romance-scam-wwe-wrestler-part-one.html.

potential victims, and, once the request is accepted, they can exploit the implied trust to push fraudulent content. As Ms. Kleinert testified today, she was the victim of a romance scam on Facebook after receiving and accepting an unsolicited friend request.[14] This design choice prioritizes network growth over user safety - more connections mean more engagement for platforms, which in turn drives revenue.

- **Direct messages**: Most social media platforms allow any user to send direct messages to any other user, creating an unmonitored private communication channel between strangers. Once a criminal establishes direct message contact, they can build trust, share fraudulent content, and pressure victims. Criminals often then move victims to messaging platforms such as WhatsApp or Google Hangouts, where subsequent conversations have even less oversight. Ms. Kleinert's scammer followed this playbook - after friending her on Facebook, the criminal suggested they move their communication to Google's messaging service.[15]

- **Targeted Advertising**: Social media platforms generate revenue primarily through advertising, and concerns have been raised that the financial incentive to maximize ad approvals may sometimes come at the cost of thorough vetting. As a result, criminals can purchase social media advertisements and exploit detailed platforms' audience targeting systems to push scams on specific demographics, such as seniors, jobseekers, veterans, or small business owners. For example, a Tech Transparency Project report found that scammers collectively ran more than 150,000 scam ads targeting seniors on Facebook and Instagram with fake government benefits.[16] While platforms claim to review ads, the significant volume and financial incentive to approve ads means scam content is frequently approved.

- **Algorithmic recommendations and amplification:** Platform algorithms prioritize content that generates engagement such as clicks, shares, comments, or emotional responses. Fraudulent content can perform well under these metrics because it may promise quick wealth, urgent threats, or dramatic claims.

- **Groups / community pages**: Social media groups and community pages are designed to create spaces where people with shared interests or geographic proximity can connect based on shared interests. Criminals exploit social groups in a few key ways. First, they can infiltrate legitimate groups to target potential victims with scams. Second, they can create fake groups that appear to be legitimate (e.g., charity pages, support groups, investment clubs, celebrity fan pages) but are actually scam operations. Poor

[14] NBC10 Responds, *Romance scammer steals $39,000 from widow* (Sept. 13, 2024), NBC10 Philadelphia, https://www.nbcphiladelphia.com/investigators/consumer/romance-scammer-steals-39000-from-widow/3969194/.
[15] *Id.*
[16] *Meta Awash in Deepfake Scam Ads* (Oct. 1, 2025), Tech Transparency Project, https://www.techtransparencyproject.org/articles/meta-awash-in-deepfake-scam-ads.

group and community page moderation by platforms creates an environment for these scams to spread.

- **Cloned / fake / impersonated accounts**: Social media platforms allow users to create accounts with minimal identity verification. Fraudsters routinely create fake profiles posing as military officers, celebrities, financial advisors, government officials, or even local community members. These accounts build credibility through profile photos, stolen content, and visible follower counts before initiating direct contact with victims.

Social Media Platforms Profit from Scams

These design features are not accidental. They are the direct result of business decisions that prioritize profits over user safety. Internal documents and investigative reports suggest that social media platforms – Meta in particular – have built scams right into their revenue model.

A recent Reuters investigation based on internal documents from Meta shows how scams are embedded in the economic structure of platforms. According to those documents, Meta internally projected that roughly 10 percent of its total revenue in 2024, about $16 billion, would come from ads tied to scams, fraudulent products, and prohibited goods.[17] The documents also revealed that Meta showed users an estimated 15 billion 'high risk' scam advertisements every day that led to the company generating $7 billion in revenue.[18]

What makes these statistics even more glaring is how Meta manages these scam ads. Rather than immediately removing all ads that raise fraud concerns, Meta's automated systems only ban advertisers when they are at least 95 percent certain the advertiser is a scam.[19] If the system is not that sure but still suspects fraud, the platform charges the advertiser more rather than cutting them off, effectively monetizing questionable scam activity rather than eliminating it.[20]

The internal trade-offs revealed by reporting and company documents show that the current business model, which places revenue growth and ad monetization at the center, creates economic incentives that can conflict with user safety.

Artificial Intelligence Supercharges Scams

While social media platforms play a significant role in the spread of scams and fraud, we are now confronting a new and more dangerous era in which artificial intelligence supercharges the sophistication and scale of scams. As highlighted in a recent report from the Consumer

---

[17] Jeff Horwitz, *Meta is earning a fortune on a deluge of fraudulent ads, documents show* (Nov. 6, 2025), Reuters, https://www.reuters.com/investigations/meta-is-earning-fortune-deluge-fraudulent-ads-documents-show-2025-11-06/.
[18] *Id.*
[19] *Id.*
[20] *Id.*

Federation of America, generative artificial intelligence tools on the market are creating highly convincing text, images, and even deepfake audio or video that can impersonate loved ones, trusted figures and institutions with alarming realism.[21]

Pennsylvania's Attorney General has explicitly warned that advancements in AI have made scams "more difficult to detect" and allowed criminals to deploy more convincing and complex schemes.[22] Indeed, Pennsylvania residents are already seeing the real-world consequences of this shift. In the Philadelphia region, experts have warned that AI-generated fake profiles and automated chat tools are making romance scams far more sophisticated.[23] Pennsylvanians have also been victimized by 'grandparent scams' where criminals use voice cloning technology to mimic a loved one in distress.[24]

While AI-generated scams are on the rise, it is important to note that the relationship between AI and social media is symbiotic. In many cases, social media platforms provide raw data – public profiles, photos, videos, and voice recordings – that AI tools scrape and weaponize to create deepfakes, voice clones, and other scams. Further, social media platforms have the ability to distribute AI-generated scam content at massive scale. Together, artificial intelligence and social media form a feedback loop that makes scams more believable and more widespread.

What Pennsylvania Lawmakers Should Do to Hold Platforms Accountable

Pennsylvania residents are not losing hundreds of millions of dollars to scams because they are careless. They are experiencing economic and emotional harm from scams because sophisticated fraud operations are operating at scale on powerful digital platforms that fail to properly prioritize consumer safety. State lawmakers should work with policy experts and other stakeholders to develop meaningful reforms to hold online platforms accountable for these harms.

Lawmakers should consider reforms that prioritize product safety and mitigate structural drivers of platform-enabled fraud including the following:

---

[21] Ben Winters, *Scamplified: How Unregulated AI Continues to Help Facilitate the Rise of Scams* (May 2025), Consumer Federation of America, https://consumerfed.org/wp-content/uploads/2025/05/Scampified.pdf.

[22] *AG Meets with Older Residents Warning that Pennsylvanians Lost $76M to Scammers in 2025; AI Fueling More Sophisticated Swindles* (Jan. 29, 2026), Pennsylvania Office of Attorney General, https://www.attorneygeneral.gov/taking-action/ag-meets-with-older-residents-with-warning-that-pennsylvanians-lost-76m-to-scammers-in-2025-a-i-fueling-more-sophisticated-swindles/.

[23] Joshua Sidorowicz, *AI is making romance scams harder to spot, and this Philadelphia expert has these red flags to look for*" (Feb. 11, 2026), CBS News, https://www.cbsnews.com/philadelphia/news/ai-romance-scams/.

[24] Kate Reilly and Tracy Davidson, *Family says scammers used AI to impersonate South Philly woman's granddaughter* (Aug. 14, 2025), https://www.nbcphiladelphia.com/investigators/consumer/philadelphia-grandparent-scam-ai-theft-impersonation-elder-fraud/4254278/.

- **Stronger Default Privacy Settings for Users:** Today, too much personal data is publicly accessible unless users actively change complex settings. Scammers rely on this data to impersonate victims, target their networks, send unsolicited friend requests and direct messages, and personalize fraud. Pennsylvania lawmakers should require platforms to adopt stronger privacy by default standards that would ultimately help limit user exposure to scams.

- **Advertiser Vetting Through Know Your Customer Rules:** Platforms operate some of the most sophisticated advertising systems in the world, yet fraudsters can often purchase ads with minimal safeguards in place. These companies are not start-ups. They are mature corporations running mature platforms. Their failure to protect consumers is not an accident or an oversight. It is a design choice. Pennsylvania lawmakers should consider applying Know Your Customer (KYC)-style measures, requiring platforms to verify the identity of all advertisers before approving ads.

- **Empower Users to Report Fraud:** Pennsylvania lawmakers should require platforms to provide clear, easy-to-use fraud reporting tools and ensure timely, meaningful responses, not just automated acknowledgments. When users report scam ads, fake profiles, or AI-generated impersonations, platforms should review them promptly, notify users of outcomes, and remove confirmed fraud quickly.

Conclusion

Pennsylvanians deserve social media platforms that prioritize their safety as much as engagement and profit. The cost of inaction can mean lost life savings, financial ruin, and emotional devastation. By enacting meaningful policies and ensuring platforms take responsibility for reducing the spread of scams, we can make our digital environment safer for all.

Thank you for your time, and I look forward to answering any questions you have.

national council on aging

Representative Ryan Bizzarro
Chair, House Democratic Policy Committee
Pennsylvania House of Representatives
P.O. Box 202003
Harrisburg, PA 17120-2003

Dear Chairman Bizzarro**,**

Thank you for convening this important informational hearing on the growing harm of tech-enabled scams and their impact on Pennsylvanians. Your leadership in elevating this issue comes at a critical moment, as digital fraud has rapidly expanded in scale, sophistication, and human cost—particularly for older adults across the Commonwealth.

Older adults have experienced staggering financial and emotional losses from online scams in recent years. According to the Federal Trade Commission, adults aged 60 and older reported more than $3.4 billion in losses in 2023 alone, with investment scams accounting for over **$**1.2 billion of that total and tech-support scams exceeding $600 million. The FBI's Internet Crime Complaint Center similarly reported more than **$**3 billion in losses among older adults in 2022. These figures almost certainly underestimate the true scope of harm, as many victims—especially seniors—feel too ashamed or embarrassed to report what happened to them.

Pennsylvania is among the states hardest hit. Last year, Pennsylvanians reported more than $400 million in losses to online scams, affecting seniors, veterans, young adults, and families in every region of the state. Social media platforms are now one of the most direct pathways through which scammers reach vulnerable residents. Internal documents reported by Reuters show that Meta earned $16 billion from scam and prohibited ads in 2024—representing roughly **10%** of its global revenue—and that its platforms show users an estimated 15 billion scam ads every day. These revelations underscore the urgent need for stronger accountability and consumer protections.

The consequences of these scams extend far beyond financial loss. Victims often experience deep emotional distress, including shame, anxiety, and a loss of trust in technology. Some face long-term financial instability, depleted retirement savings, or difficulty paying bills. The emotional toll can be severe, with documented cases of depression, health crises, and even suicide following major financial fraud. These harms ripple outward, affecting families, caregivers, and entire communities.

Given the scale and severity of this problem, state lawmakers have an essential role to play in advancing meaningful protections. I appreciate the opportunity to contribute to this discussion and encourage the Committee to work with policy experts and other stakeholders to develop meaningful policies to hold online platforms accountable for these

.Thank you again for your commitment to addressing this urgent issue. to develop effective, evidence-based policies that protect consumers across the Commonwealth. State lawmakers should.

Sincerely,

Natalie Zellner
Senior Director, Engagement and Strategy

ADVOCATING AGAINST
ROMANCE SCAMMERS

Written Testimony

Romance Scam Fraud in Pennsylvania: Scope, Harm, and the Need for Platform Accountability

Submitted to:
Pennsylvania House Democratic Policy Committee

Submitted by:
Advocating Against Romance Scammers (AARS)

Introduction

Chair and Members of the Committee,

Thank you for the opportunity to submit written testimony on the growing and devastating impact of romance scam fraud in the Commonwealth of Pennsylvania. Advocating Against Romance Scammers (AARS) is a survivor-founded nonprofit organization dedicated to advocacy, education, and prevention for individuals and families impacted by romance scams.

Romance scams, classified by the Federal Bureau of Investigation as **Confidence/Romance Fraud**, are not isolated incidents of deception. They are organized, repeatable crimes that inflict severe financial and psychological harm, facilitated largely through online platforms that currently operate with minimal accountability. Pennsylvania's most recent fraud data demonstrates the urgent need for legislative attention and systemic reform.

Scope of Fraud in Pennsylvania

Pennsylvania ranks among the most impacted states in the nation for fraud-related harm.

According to the latest data reported to the **FBI Internet Crime Complaint Center (IC3)**:

- Pennsylvania ranks **#5 nationally** for the number of fraud victims, with **27,838 reported victims**
- Pennsylvania ranks **#8 nationally** for total fraud-related financial loss, totaling **$400,082,312**

ADVOCATING AGAINST
ROMANCE SCAMMERS

These figures represent reported losses only. The FBI consistently notes that fraud, particularly romance scams, is significantly underreported due to victim shame, fear of judgment, emotional manipulation, and isolation.

Romance Scam (Confidence Fraud) Impact in Pennsylvania

Within the broader fraud landscape, romance scams represent one of the most financially damaging categories.

IC3 data indicates that in Pennsylvania:

- **775 victims** reported romance scam fraud
- **$30,024,229** was *stolen* through romance scams
- Among elderly victims, **$3,648,378 was taken through romance scam activity**.

Romance scams often involve prolonged manipulation, repeated financial extraction, and psychological coercion. Losses accumulate over time and frequently result in complete financial devastation.

About Advocating Against Romance Scammers (AARS)

Advocating Against Romance Scammers (AARS) was formed in response to a critical gap in victim support and systemic accountability. Survivors of romance scams are often left without meaningful resources, face skepticism when reporting crimes, and encounter systems that are not equipped to understand coercive fraud.

AARS exists to address that failure.

Our work includes:

- Survivor-centered advocacy and recovery support
- Education for law enforcement, financial institutions, and communities
- Public awareness initiatives focused on prevention
- Policy advocacy aimed at reducing harm and increasing accountability

AARS brings lived experience, professional collaboration, and evidence-based advocacy to the policy table.

ADVOCATING AGAINST
ROMANCE SCAMMERS

The Human Impact of Romance Scams

Impact on Victims

Romance scams uniquely exploit trust, intimacy, and emotional vulnerability. Victims commonly experience:

- Loss of life savings, retirement accounts, and financial security
- Accumulation of debt and long-term economic instability
- Psychological trauma consistent with coercive control and emotional abuse
- Profound shame, social withdrawal, and loss of trust
- Increased risk of depression, anxiety, and suicidal ideation

These harms persist long after financial losses occur and often require long-term recovery support.

Impact on Families and Loved Ones

The damage caused by romance scams extends beyond the individual victim. Families and loved ones frequently experience:

- Secondary trauma from witnessing financial and emotional collapse
- Fractured relationships due to scammer-induced manipulation
- Financial strain when attempting to stabilize housing, healthcare, or debt
- Conflict and withdrawal when attempting to intervene

Romance scams destabilize entire family systems and support networks.

Impact on Identity Theft Victims

Romance scams also create additional victims whose identities, images, or names are stolen and used to perpetrate fraud. These individuals face:

- Reputational harm and emotional distress
- Legal and financial complications
- Long-term damage to their digital presence

They did not consent to their identity being used as a tool of crime, yet they bear lasting consequences with limited recourse.

ADVOCATING AGAINST
ROMANCE SCAMMERS

The Role of Online Platforms

Social media and online platforms serve as the primary point of initial contact for romance scams. Fraudsters exploit:

- Fake and impersonated profiles
- Weak identity verification standards
- Algorithmic amplification
- Delayed or ineffective responses to user reports

Despite clear and repeated patterns of abuse, platforms continue to profit from engagement while the harm is externalized to victims, families, and communities.

The Role of Artificial Intelligence in the Evolution of Romance Fraud

Romance scams have evolved alongside advances in artificial intelligence. Fraud networks now use AI tools to create more convincing and scalable deception, including:

- AI-generated profile images that evade traditional reverse-image searches
- Deep-fake audio or video used to simulate real-time communication
- Automated messaging systems that adapt language and emotional tone to groom victims

These tools significantly increase both the reach and sophistication of romance scams while lowering the barrier to entry for criminal networks.

Big Tech's AI Duty of Care

The same platforms deploying artificial intelligence to drive engagement and revenue possess the technical capability to detect coordinated inauthentic behavior, impersonation, and fraud patterns. As AI becomes central to platform operations, the argument that these harms are undetectable becomes increasingly difficult to sustain.

Large technology companies should be held to a reasonable duty of care that requires them to:

- Implement safeguards against known forms of AI-enabled impersonation and fraud
- Act promptly on credible fraud reports
- Prevent repeat offenders from recreating scam accounts
- Prioritize user safety alongside growth metrics

ADVOCATING AGAINST
ROMANCE SCAMMERS

A duty of care does not regulate lawful speech. It requires reasonable steps to prevent foreseeable criminal exploitation occurring within their systems.

Unchecked AI-enabled fraud undermines public safety and consumer trust. As technology evolves, so must accountability.

Actions States Can Take Independently

States, including Pennsylvania, can take meaningful action to reduce harm, improve accountability, and protect residents, without violating federal law, by focusing on consumer protection, transparency, and harm mitigation.

1. Strengthen State Consumer Protection Enforcement

States can:

- Enforce unfair and deceptive trade practice statutes against platforms that misrepresent safety, verification, or fraud prevention measures
- Require greater transparency around how fraud reports are handled
- Investigate patterns of ignored or delayed responses to documented criminal activity

2. Mandate Fraud Reporting Transparency

States can require platforms operating within their jurisdiction to:

- Publicly disclose fraud report volumes and response times
- Report the number of romance scam-related accounts identified and removed
- Share anonymized data with state agencies to support prevention and enforcement

Transparency creates accountability without infringing on speech.

3. Establish Platform Duty-of-Care Standards

States can define reasonable duty-of-care expectations, including:

- Timely review of fraud reports
- Meaningful action against known scam accounts
- Clear pathways for victims and identity theft victims to seek remediation

Duty-of-care standards focus on conduct, not content.

ADVOCATING AGAINST
ROMANCE SCAMMERS

4. Expand Victim and Identity Theft Protections

States can:

- Fund survivor-centered recovery services for fraud victims
- Recognize identity theft victims used in scams as impacted parties entitled to support
- Improve coordination between law enforcement, financial institutions, and victim advocates

5. Support Law Enforcement Training and Resources

States can invest in:

- Specialized training on romance scams and coercive fraud
- Dedicated financial fraud units
- Partnerships with survivor advocacy organizations to improve victim outcomes

6. Advocate for Federal Reform

State legislature plays a critical role in:

- Passing resolutions urging Congress to modernize the Communication Decency Act, Section 230
- Elevating state-level data and harm trends to federal policymakers
- Ensuring survivor voices inform national policy discussions

Conclusion

The data from Pennsylvania represents more than financial loss, it represents lives disrupted, families fractured, and trust eroded. Romance scam victims are not negligent or uninformed; they are targeted through sophisticated manipulation enabled by systemic failures.

Advocating Against Romance Scammers (AARS) urges policymakers to:

- Recognize romance scams as a serious and distinct form of financial and psychological harm
- Support efforts to hold online platforms accountable
- Advance modernization of Section 230 to reflect digital crime realities
- Promote survivor-centered prevention and recovery frameworks

ADVOCATING AGAINST
ROMANCE SCAMMERS

Romance fraud is not inevitable. It is preventable. Addressing it requires legislative leadership, corporate responsibility, and a commitment to protecting Pennsylvanians from avoidable harm.

Respectfully submitted,

Kathy Waters
Co-Founder, Executive Director
Advocating Against Romance Scammers (AARS)

Chairman Bizzarro, members of the Committee, and distinguished policymakers,

Operation Shamrock appreciates the opportunity to provide testimony on the escalating crisis of technology-enabled financial scams impacting Pennsylvanians and Americans nationwide.

This is no longer just a consumer fraud problem; it is a national security issue.

Organized transnational criminal networks are exploiting digital platforms, artificial intelligence, and instant payment systems to steal billions from U.S. households while undermining trust in our financial and technological infrastructure.

These scams are not isolated incidents.
They are industrial-scale criminal enterprises operating across borders, using sophisticated psychological manipulation, AI-generated identities, and coordinated money laundering pipelines. Seniors are losing retirement savings, military families are being targeted, and small businesses are being drained, with devastating financial and emotional consequences.

A major driver of this crisis is the online ecosystem that enables scams to flourish. Criminals are purchasing targeted scam advertisements, leveraging the credibility of major platforms, and reaching victims at unprecedented scale. Big Tech companies continue to profit from ad revenue while scam content spreads faster than enforcement or consumer awareness can keep up.

This cannot remain the status quo. Protecting consumers must be treated as an urgent priority, while ensuring innovation and technology continue to grow responsibly. That requires clear accountability and coordinated action.

Operation Shamrock urges policymakers to focus on:

- **Platform accountability**, including stronger verification, faster removal of scam ads, and transparency around fraudulent promotion.
- **Cross-sector intelligence sharing** to disrupt scam networks and recover stolen assets more quickly.
- **Expanded victim support and education**, reflecting the modern sophistication of these threats.
- **Increased investigative resources** to combat organized, transnational fraud operations.

Technology should be a driver of progress, not a weapon for criminals. Without decisive action, these scam networks will continue to expand, eroding consumer trust, draining American wealth, and threatening the integrity of our digital economy.

Operation Shamrock stands ready to support Pennsylvania in taking meaningful steps to protect the public and strengthen our collective defenses.

Respectfully,
Erin West
Founder, Operation Shamrock
www.operationshamrock.org

Dear members of the House Democratic Policy Committee of Pennsylvania,

My name is Roberta Braga, founder and executive director of the Digital Democracy Institute of the Americas (DDIA). On behalf of DDIA, thank you for the opportunity to submit testimony for the February 25 informational hearing on scams and fraud. As scams continue to rise across the United States, understanding how bad actors target Latino communities that make up approximately 20% of the U.S. population and over 9% of Pennsylvania's population is critical to crafting effective consumer protections.

DDIA is a non-partisan, non-profit organization dedicated to centering Latino and Latin American experiences in conversations about digital harms, information integrity, and platform accountability. Between November 2025 and February 2026, we published a three-part investigation titled *WhatsApp Weaponized*, examining how scammers exploit Spanish-speaking U.S. Latinos through public WhatsApp groups. Our findings underscore an urgent need for stronger protections, particularly within messaging platforms with broadcast features that can take content viral behind the walls of encryption.

Our Investigation and Methodology

DDIA researchers examined more than 18,400 unique messages suspected of facilitating scams shared within 3,300 Spanish-speaking public WhatsApp groups in the United States between January 1 and September 1, 2025. We relied on two primary data sources:

- **Palver**, a social listening tool that enables us to analyze public WhatsApp groups that use Spanish as a primary language and that have at least 30% +1 phone numbers based in the United States (note, these are groups that have shared links for people to join online). Importantly, DDIA does not have access to personal user data and does not collect demographic information. We cannot see users' full names or phone numbers, only area codes.
- The **Google Fact Check API**, which aggregates fact-checks from media organizations worldwide. We reviewed and categorized 139 Spanish-language fact-checks published since 2017 that debunk various scams, allowing us to trace how fraud tactics have evolved over time.

Note: Hundreds of the scam-related messages we analyzed were labeled by Meta as "frequently forwarded," signaling rapid and wide circulation, and demonstrating how quickly deceptive content spreads in Spanish-language spaces.

Key Findings

1. **Commercial and Product Scams:** In the first chapter of our three-part investigation, DDIA documented fraudulent commercial schemes, including fake

retail promotions, counterfeit product giveaways, impersonation of major brands, and deceptive banking offers. These scams often use urgency ("limited time offer"), emotional triggers, and cultural cues to lure users into clicking links, sharing personal data, or sending money to unknown numbers. Because many of these messages circulate in WhatsApp groups that may include trusted family, church, neighborhood, or diaspora groups, they benefit from built-in credibility.

2. **Immigration, Legal, and Employment Scams:** The second chapter revealed particularly troubling patterns targeting immigrants and mixed-status families. Scammers are tailoring schemes to exploit individuals navigating complex immigration systems and economic precarity. We observed fraudulent offers related to Temporary Protected Status (TPS) deadlines, asylum procedures, legal services for status adjustment, fake job offers, questionable health-care enrollment assistance, and assistance obtaining documents such as driver's licenses or small loans. These schemes seem to weaponize hope and fear. They exploit people's urgent need for legal guidance, employment, housing stability, health coverage, and financial inclusion. For immigrants who may already distrust institutions or face language barriers, WhatsApp can be both a lifeline and a threat, one worth keeping an eye on.
3. **Cryptocurrency and Investment Scams:** The third chapter of our research series examined dubious investment and cryptocurrency schemes circulating in Spanish-language WhatsApp groups. These scams promise "guaranteed" high returns, insider crypto-trading models, and forex opportunities with little to no risk. Unlike employment scams, which target individuals seeking to earn income through work, these schemes prey on aspirations to build wealth. Because messaging apps, especially encrypted ones, are essentially opaque digital environments, exaggerated financial promises flourish, risks are minimized or concealed, and users are pressured to move funds quickly. The "too good to be true" reward, in this case, was clearly the bait that could lead to people draining savings.

Scams have become a routine part of Latinos' digital lives. According to the Global Anti-Scam Alliance (GASA), 70% of U.S. residents encountered a scam in the past year, facing an average of 377 scam attempts annually. In 2025 alone, an estimated $64.8 billion was stolen from U.S. victims.

Platforms with direct-messaging features, including WhatsApp, have become vectors for malicious activity that can lead to families potentially losing savings, workers potentially losing wages, and immigrants losing both money and hope. Spanish-language scams are not simply translations of English-language schemes. They are culturally adapted, community-specific, and, in today's fraught environment, often tied to immigration.

Detection systems, moderation practices, warning labels, and reporting tools can be improved in non-English spaces, and certainly this is the case in a space like WhatsApp. With Latinos being targeted online and offline with hate and violence, and as scammers grow more sophisticated, protections must grow equally strong in every language the United States uses.

Policy Considerations

Based on our research, we respectfully offer the committee the following considerations:

- Encourage or require greater transparency from platforms regarding scam detection and enforcement in non-English languages.
- Strengthen collaboration between Pennsylvania's state agencies, consumer protection offices, and trusted community-based organizations serving Latino and immigrant populations.
- Invest in culturally and linguistically tailored public education campaigns about common scam tactics. Work with local journalists and content creators to disseminate these campaigns where Latinos consume information.
- Support data-sharing frameworks that allow researchers to monitor scam trends while protecting user privacy.
- Examine the role of encrypted and messaging-based ecosystems in fraud proliferation, while balancing privacy rights and user safety.

Scams are not only a financial issue, they are a trust issue in a world where, per our polling research, Latinos are widely skeptical of most everything they see online. When individuals repeatedly encounter fraud in spaces they rely on for both connection and survival, trust in digital platforms, institutions, and even community networks erodes. Latinos are the fastest growing demographic group in the state of Pennsylvania. With U.S. Latinos' GDP reaching a historic $4 trillion, ranking as the 5th largest economy in the world when considered independently, protecting consumers in Pennsylvania and across the country requires recognizing that scams as a digital harm are multilingual, culturally tailored, and rapidly evolving.

DDIA stands ready to share additional research and collaborate on solutions that strengthen protections for Latino users of social media and messaging apps. Thank you again for the opportunity and for your attention to these issues.

Testimony Offered to the House Democratic Policy Committee's
Informational Hearing on Online Scams
February 25, 2026

Our associations express our deepest gratitude for the opportunity to submit this testimony on the critical issue before you today.

No sector invests more to protect Americans from fraud and scams than the financial services sector. To that end, our associations in collaboration with their regulators and national counterparts have spearheaded the development of numerous free tools and resources aimed at educating and increasing awareness about elder financial exploitation. The Safe Banking for Seniors program has been embraced by more than 1600 banks, and over 300 credit unions, which offer comprehensive materials for conducting in-person or virtual workshops, leveraging social media platforms, and engaging in one-on-one conversations to educate communities about scams and financial protection.[1]

Our industry has also teamed with the Federal Trade Commission to develop infographics addressing scams targeting seniors. These materials are freely accessible covering topics such as fake check scams, government imposter scams, and romance scams. Additional, ongoing partnerships with organizations like the National Adult Protective Services Association and National Sheriffs Association work towards enhancing communication between banks and state authorities.

The American Bankers Association promotes an acclaimed anti-phishing campaign #BanksNeverAskThat to provide real-world tips for consumers to identify and avoid falling victim to phishing attempts. The campaign covers a wide range of topics, including recognizing suspicious emails, avoiding sharing sensitive information online, and understanding how to spot fraudulent messages. Banks Never Ask That is a vital effort to promote online safety and security for consumers. This campaign was recently refreshed and relaunched earlier this month.

CrossState Credit Union Association equips credit unions with comprehensive fraud and cybersecurity resources—including a dedicated compliance hotline, phishing education, scam alerts, and practical prevention guidance—so credit unions have access to ready-made tools and expert guidance to proactively educate credit union staff and employees to strengthen their fraud prevention efforts.

In addition to providing educational resources, 99% of surveyed banks offer training on elder financial exploitation for frontline staff.[1] Financial institutions actively protect older customers by utilizing automated monitoring tools to detect unusual account activity. When exploitation is suspected, institutions promptly assign staff to review accounts and take necessary actions, such as filing suspicious activity reports or flagging and closing accounts.

[1] https://www.aba.com/news-research/analysis-guides/older-americans-benchmarkingreport#:~:text=More%20than%20half%20of%20the,offer%20such%20products%20(67%25).

Need for a Comprehensive Federal Response to Fraud

Despite their extensive efforts to educate consumers to avoid scams, the criminals committing these crimes are extremely sophisticated and resourced with advanced technology that allows them to impersonate legitimate entities. Every financial institution has faced a customer who insists that they know and trust the individual to whom they wish to transfer funds. In the end, it is the customer's money, and most Americans do not want institutions telling them what to do.

The following testimony is from a central Pennsylvanian credit union working every day to protect their credit union members, and continues to face the fight to protect them from predators:

A 77-year-old woman who was a newly established member. A personal account and business account was opened. A check deposit of $50,000.00 and $100,000 wire was deposited to her accounts, raising suspicion on the fraud team's end. She was under the impression she was speaking with a friend of hers from a few years back who is now flipping and selling homes, involved with real estate. She couldn't provide our team with a license # to look up and verify or verify much or any of the situation. She wanted to wire out money to crypto, as her friend informed her this was a good idea to do right now. Communication was via WhatsApp, social media, phone calls, texting, and email. She admitted that the crypto account was not in her name either.

It was believed that she was being utilized as a money mule and was a true victim. The $50,000.00 check came from her old account that was closed out from concerning activity at that financial institution. The Secret Service became involved as well as the local Area Agency on Aging.

Upon meeting with Secret Service and talking to our member, our thoughts became reality. The poor woman was a victim of severe criminal money mule activity and didn't even realize it. She complied with Secret Service, and we surrendered all of the funds to seize back to Secret Service.
Upon meeting with our member, she informed us she was instructed to lie to us by her friend. She also provided the ID provided by him and it was deemed fraudulent by our credit union's fraud team. The Secret Service ended up discovering that several institutions were involved: small and large. They also ended up being able to recover this money BACK to another elderly victim of financial exploitation and money mule activity.

The financial services industry needs a comprehensive national scam and fraud prevention strategy to reduce the ability of criminals to be "technologically authenticated" by impersonating legitimate businesses such as financial institutions. These efforts need to be coordinated among multiple regulators and connected to law enforcement.

If fraudulent ads continue to drive revenue for social media platforms without consequence, more must be done to protect consumers. This is why we and our national counterparts strongly support federal legislation that will protect consumers from social media scams. The bipartisan-sponsored Safeguarding Consumers from Advertising Misconduct, or SCAM, Act (S. 3774; H.R. 7548) would require social media companies to verify advertisers' identity, implement systems to detect fraudulent advertisements, and investigate and remove fake ads.

We also need a single, streamlined government reporting process by which to report suspected fraud schemes.

All sectors must see and claim their roles in protecting our critical infrastructure from criminal hijacking.

Financial Institutions Need Better Tools to Prevent and Respond to Elder Financial Exploitation (EFE)

Each year, millions of older Americans suffer billions in losses due to financial exploitation, much of which is irrecoverable. Despite its prevalence, quantifying the impact is challenging. The Federal Trade Commission FTC) reported that in 2021 it received 567,340 fraud reports involving adults 60 years of age and older, involving average losses of $820 for individuals ages 60 to 69; $800 for individuals ages 70 to 79, and $1.500 for individuals over 80 years of age.[2] The National Institute of Justice also reported that in 2017, 929,570 older adults were victims of financial fraud, and suffered total losses of $1.2 billion, or an average of $1,270 per-person.[3] With as few as 1 in 44 cases being officially reported, however, it is believed that as many as 1 in 5 Americans s may have been victims of a financial swindle.[4]

Older adults are more susceptible than younger people to certain types of frauds and swindles, especially those involving tech support; prizes, sweepstakes and lotteries; and exploitation by family members and friends.

Victims not only suffer financial harm but also endure emotional distress, facing the loss of their savings, homes, and dignity.[5] The impact extends to family caregivers and taxpayers who shoulder additional burdens to support financially devastated victims. As our nation undergoes a demographic shift, with more seniors than children projected within the next decade, the urgency to address elder financial exploitation grows.

State Legislative Opportunity to Combat Elder Financial Exploitation

While universal financial institution practices include employee fraud detection training and reporting suspicious activity to the federal government, there is room for improved collaboration between financial institutions and adult protective services. State legislatures are enacting laws to facilitate greater information sharing and allow for banks to decline to engage in suspicious transactions before irreversible disbursements occur.

Our Associations support legislation that:

- Establishes a clear legal framework for banks and credit unions to report suspected EFE to and cooperate with state authorities;
- Authorizes financial institutions to consult with an older adult's authorized contacts, guardians or other fiduciaries, and attorneys and financial advisors for assistance in addressing EFE;
- Enables financial institutions to hold, refuse or prevent suspicious transactions before irreversible or difficult to recover disbursements;
- Expands authorization for financial institutions to voluntarily provide records to area agencies on aging to investigate EFE and simplify procedures for area agencies to request additional records; and

[2] https://www.ftc.gov/system/files/ftc_gov/pdf/P144400OlderConsumersReportFY22.pdf.
[3] https://nij.ojp.gov/topics/articles/examining-financial-fraud-against-older-adults.
[4] Fed: One in five Americans victims of financial fraud, scams | ABA Banking Journal
[5] The Thief Who Knows You: The Cost of Elder Exploitation Examined (aarp.org)

- Authorizes AAAs to share information with FIs regarding investigations of EFE as necessary to protect older adults, such as whether to refuse, prevent or authorize transactions, or expand or release holds on transactions.

Such legislation would equip institutions with more proactive tools to protect our seniors.

###

Thank you for allowing us to submit this testimony. Please feel free to contact us with any questions you may have.

Common Cause
Pennsylvania
Holding Power Accountable

800 N. Third Street, Suite 401
Harrisburg, PA 17102
717.232.9951
www.commoncause.org/pa

February 13, 2026

RE: Testimony for Informational Policy Hearing on Online Scams and Fraud, February 25, 2026

Common Cause urges Pennsylvania lawmakers to hold online platforms accountable for the scam epidemic devastating families across the Commonwealth. With over $400 million in reported losses last year, Pennsylvania is one of the hardest hit states, with seniors, veterans, people of color, and young people facing disproportionate harm as scams drain savings, retirement funds, and emergency resources.

Platforms actively enable scams through their targeting, amplification, messaging, and payment systems, while pocketing billions in advertising revenue from criminals running fraudulent ads, yet they operate with virtually no transparency about how scams spread on their services or accountability for the harms they profit from. AI has supercharged this crisis, making scams faster, more personalized, and harder to detect, while social media provides the infrastructure for AI-generated fraud to spread at a massive scale.

We call on state lawmakers to work with policy experts and stakeholders to develop policies that require platforms to be transparent about scam prevalence and their business practices, and hold them accountable for the harms they enable, ensuring these powerful corporations serve the public interest rather than exploit it.

Testimony on Pennsylvania Informational Hearing on Scams

February 25, 2026

Chairman Ryan Bizzarro and Members of the House Democratic Policy Committee, thank you for the opportunity to submit written testimony on the growing harm of tech-enabled scams and their impact on Pennsylvanians.

In a nationally representative CR survey of 2,158 US adults in April 2025, close to half (46%) of Americans have personally encountered a digital scam attempt or cyberattack. Alarmingly, one in five of them—about one in ten Americans overall—say they lost money to the scam.[1]

Americans lose substantial amounts of money due to fraud and scams. In 2023, the Federal Trade Commission received fraud claims from more than 2.6 million individuals. The commission estimated that $10 billion had been lost that year alone. This figure does not include scams that victims chose not to report.[2]

Some communities are particularly vulnerable to digital scams. Consumer Reports' nationally representative survey data shows that, among those who had encountered a scam attempt, households with the lowest incomes were three times as likely to report financial losses due to scams as the highest income households (29 percent compared with 10 percent). And we found continued racial disparity in financial losses related to scams. Our data shows that 37 percent of Black Americans who encountered a

[1]Noemi Altman, Consumer Reports nationally representative American Experiences Survey of 2,158 U.S. adults, April 2025, https://article.images.consumerreports.org/image/upload/v1744212505/prod/content/dam/surveys/Consumer_Reports_AES_April_2025.pdf,

[2]Federal Trade Commission, As Nationwide Fraud Losses Top $10 Billion in 2023, FTC Steps Up Efforts to Protect the Public, February 9, 2024, https://www.ftc.gov/news-events/news/press-releases/2024/02/nationwide-fraud-losses-top-10-billion-2023-ftc-steps-efforts-protect-public

scam lost money to it, compared to only 15 percent of white Americans.[3] This echoes similar findings made by other organizations, including the Federal Trade Commission.[4]

Scammers use insidious strategies to target their victims. Not only can they easily access personal data on individuals, they are now using new methods such as voice cloning and deepfakes to impersonate CEOs, celebrities, banks, government agencies, and people their victims know and trust to get them to lower their guard and open their wallets.[5]

Text-messaging scams are surging, particularly among young people, where the share reporting these types of scam attempts roughly tripled between April 2024 and April 2025, from 13 percent to 40 percent.[6]

Bad actors are exploiting platforms people use regularly to scam and defraud them. For example, a *Reuters* investigation revealed that Meta — according to its own documents — delivered an estimated 15 billion scam ads a day to its users in 2024.[7] Meta, which operates Facebook and Instagram, failed to identify and remove most scam ads. This exposed billions of users to fraudulent e-commerce scams and investment schemes. Allowing the proliferation of these scam advertisements led to billions of dollars in profit for the corporation. Meta has refused to take remedial steps to curtail the stream of harmful ads, defunding its safety teams and only taking action against advertisers in the most extreme of circumstances.

Online scams proliferate on other platforms as well. YouTube channels have distributed malware by promoting pirated games, often bundled with keyloggers[8]. Additionally, companies have failed to implement meaningful safeguards against the use of their technology. A recent Consumer Reports assessment of AI voice cloning products found that the majority of companies assessed made it

---

[3]Noemi Altman, Consumer Reports nationally representative American Experiences Survey of 2,158 U.S. adults, April 2025, https://article.images.consumerreports.org/image/upload/v1744212505/prod/content/dam/surveys/Consumer_Reports_AES_April_2025.pdf

[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, https://www.ftc.gov/system/files/documents/reports/serving-communities-color-staff-report-federal-trade-commissions-efforts-address-fraud-consumer/ftc-communities-color-report_oct_2021-508-v2.pdf

[5]Derek Kravitz, The New Scams to Watch Out For, Consumer Reports, January 30, 2025, https://www.consumerreports.org/money/scams-fraud/new-scams-to-watch-out-for-a9334297641/

[6]Noemi Altman, Consumer Reports nationally representative American Experiences Survey of 2,158 U.S. adults, April 2025, https://article.images.consumerreports.org/image/upload/v1744212505/prod/content/dam/surveys/Consumer_Reports_AES_April_2025.pdf

[7]Jeff Horowitz, Meta is earning a fortune on a deluge of fraudulent ads, documents show, November 6, 2025, https://www.reuters.com/investigations/meta-is-earning-fortune-deluge-fraudulent-ads-documents-show-2025-11-06/

[8]Jonathan Greig, YouTube channels found using pirated video games as bait for malware campaign, April 3, 2024, https://therecord.media/youtube-infostealer-campaign-cracked-pirated-video-games

alarmingly easy to clone a voice without permission, requiring nothing more than a simple checkbox "self-attestation" to claim consent. These companies have failed to implement technical mechanisms to confirm the actual consent of speakers, or to detect and prevent the unauthorized creation of clones based on the voices of public figures, such as celebrities and politicians.[9]

This failure to prevent foreseeable abuse mirrors the Federal Trade Commission's recent case against the generative AI company Rytr, which sold a service specifically designed to generate a high volume of misleading consumer reviews based on extremely limited prompts[10]. The product was easily gameable by bad actors seeking to supercharge scams and skew public perception through the creation of deceptive reviews at scale.[11]

Online scams are a massive problem for consumers and persist as a source of significant harm due to a lack of consequences for the platforms that tolerate fraudulent ads and even benefit financially from ad fees. While policymakers should enact additional protections to clarify platform responsibilities, they should also utilize existing laws to hold them responsible for failing to take reasonable steps to protect consumers.

Under the FTC Act and many state consumer protection laws, companies are prohibited from engaging in "unfair" business practices that cause significant injury, are not reasonably avoidable by consumers, and that are not offset by countervailing benefits to consumers or competition. This includes injuries caused by third parties that a company had the capacity to stop but failed to take reasonable steps to do so. We urge enforcement agencies to hold platforms accountable for the facilitation of fraud and illegal authority, which causes substantial harm to consumers.

Companies should take commercially reasonable steps to limit the amount of fraudulent content in the advertisements on its platforms, such as

- Collecting and verifying the legal names, business entities, and physical location of advertisers along credit card information as a basic know-your-customer practice so that fraudulent ads can be traced back to specific users.

---

[9]Grace Gedye, AI Voice Cloning Report, Consumer Reports, March 10, 2025, https://innovation.consumerreports.org/AI-Voice-Cloning-Report-.pdf

[10]Note that The Federal Trace Commission recently reversed course on the Rytr settlement and dismissed it (FTC Reopens and Sets Aside Rytr Final Order in Response to the Trump Administration's AI Action Plan, December 22, 2025. https://www.ftc.gov/news-events/news/press-releases/2025/12/ftc-reopens-sets-aside-rytr-final-order-response-trump-administrations-ai-action-plan)
https://www.ftc.gov/news-events/news/press-releases/2025/12/ftc-reopens-sets-aside-rytr-final-order-response-trump-administrations-ai-action-plan

[11]Justin Brookman, Matt Schwartz, Grace Gedye, Rytr Comment to the Federal Trade Commission, November 4, 2024, https://advocacy.consumerreports.org/wp-content/uploads/2024/11/FTC-2024-0041-0007_attachment_1.pdf

- Investing in measures that could minimize harm, such as impersonation detection and mitigation programs and fraudulent ad detection systems
- Tools for consumers to report suspected fraudulent or deceptive ads, with both automated and manual support
- A timeline for investigating and responding to fraudulent complaints and removing the fraudulent or deceptive ad
- Recourse for buyers and sellers if transactions go awry due to a fraudulent ads or individuals impersonating companies

Thank you for your work on this issue. We look forward to working with you to ensure that Pennsylvania consumers have the strongest possible protections against scam and frauds.

Yael Grauer,
Program Manager, Cybersecurity Research
Consumer Reports