Testimony of

The Honorable Kathleen L. Kraninger

President and CEO

Florida Bankers Association

Before the

U.S. Senate

Special Committee on Aging

Hearing on

"Protecting Florida's Seniors:

Fighting Fraud and Financial Exploitation"

August 7, 2025

Miami, Florida

Introduction

Chairman Scott, on behalf of the Florida Bankers Association (FBA) and our more than 150 member banks operating in the great state of Florida, I am honored to appear before you on such a crucial topic. Banks are on the front line of the fight against fraud, working to protect our customers from scams, identity theft, and cybercrime. Fraud has become more complex and more prevalent, impacting individuals, families, businesses, and communities across Florida and the nation.

While some of the most troubling cases affect the most vulnerable among us such as older Americans who are the focus of this Committee, no one is immune from the barrage of attempts via every mode of communication in our modern society. It is a game of numbers – the sheer volume and ease of attempts means more success for the bad guys.

The FBA advocates for a national strategy that will tackle fraud and scams from all angles, including cutting off communication channels to targeted victims, bolstering public education, and ensuring prosecution of criminals. We are committed to strengthening collaboration among financial institutions, telecoms, tech companies, law enforcement, and policymakers, as well as engaging the public, to combat fraud, enhance consumer protections, and ensure criminals are held accountable.

The FBA works closely with the American Bankers Association (ABA) and the Independent Community Bankers Association, both of which offer services to banks to prevent, identify, and report fraud as well as advocate for initiatives to counter fraud and scams.

Defining the Problem: Fraud and Scams are a Pervasive Threat

Fraud is a national crisis, as documented by this Committee's annual fraud report. In 2024, the FBI's Internet Crime Complaint Center (IC3) received 859,532 complaints, with potential losses exceeding $16.6 billion. This represents a 2% decrease in complaints and a 25% increase in losses compared to 2023.[1]

[1] https://www.ic3.gov/AnnualReport/Reports/2024_IC3Report.pdf

Meanwhile, the Federal Trade Commission, received fraud reports from 2.6 million consumers last year, similar to 2023, but the percentage of people who reported losing money jumped from 27% to 38% in that same one-year period. The most commonly reported scam category was imposter scams. Losses to government imposter scams in particular increased $171 million from 2023 to a total of $789 million in 2024.

For the second consecutive year, email was the most common way that consumers reported being contacted by scammers. Phone calls were the second most commonly reported contact method for fraud in 2024, followed by text messages.[2] Fraudsters are targeting consumers through increasingly sophisticated channels, including phishing emails, robocalls, social media impersonation, and peer-to-peer payment fraud.

Furthermore, as AI and other technological advancements evolve, scams will only become more convincing and harder to identify for the average American, much less the most vulnerable among us. Older Americans are especially vulnerable—and Florida, with one of the largest senior populations in the country, is disproportionately affected. The losses reported by victims age 60+ went from $3.4 billion in 2023 to $4.8 billion in 2024 according to the IC3.

From inception, a significant number of cyber scams originate from other countries, especially from China and Southeast Asia, as found by the Center for Strategic and International Studies.[3] The analysis documents how the Covid-19 pandemic's lockdowns and strict border controls drove criminal groups to seek new sources of profit. In particular, Chinese criminal groups built cyber-scamming compounds where human trafficking victims, working under threat to their lives, are coerced to befriend and entice innocent Americans into fraudulent investment schemes.

[2] https://www.ftc.gov/news-events/news/press-releases/2025/03/new-ftc-data-show-big-jump-reported-losses-fraud-125-billion-2024
[3] https://www.csis.org/analysis/cyber-scamming-goes-global-unveiling-southeast-asias-high-tech-fraud-factories

Financial institutions are often the last line of defense in detecting suspicious activity and preventing significant loss. Our industry is heavily investing in such capabilities, yet it can be incredibly challenging for bank employees to convince customers that the activity is suspicious.

The stories are heartbreaking as they unfold in an all-too-familiar way. The below scam typologies are the most frequently seen by one of our larger institutions serving Florida. Furthermore, from this same institution's reporting, one out of every six elder financial exploitation scams they identify occurs in Florida.

1. Romance scams where the victim/client sends money to the perpetrator: The perpetrator insinuates themselves into the victim's life over time. The perpetrator exploits the victim/client's loneliness and provides constant communication and attention. These scammers can operate "in real life" but also purely online. With the aid of technology, this does not require much effort on the perpetrator's part. Even where the client/victim feels used or silly, they fear losing companionship so they send money. For the bank, it is more often than not impossible to overcome that emotional attachment.

2. Confidence investment scams where a victim/client sends increasing amounts into a phony cryptocurrency platform: The victim/client believes they are engaging with a legitimate opportunity because they "created" an account and can "see" they are making lucrative returns on their investment. How the victim/client is reeled into the scam could also involve a romantic element, which adds all the challenges noted in the first typology. Institutions can have success in overcoming this scam by getting the victim/client to perform their own research on what this scam entails and convincing them to try to withdraw their investment. This scam involves substantial losses because the withdrawal is often not possible, and then the scammer disappears.

3. Impersonation scams where bad actors pose as legitimate companies – often financial institutions – and assert the victim/client's money is not safe: The perpetrator preys on the victim/client's fear that they have already been scammed. The perpetrator will have details about the victim/client that bolster legitimacy (where you bank, what kind of car you drive, etc.). The bad actor directs the victim/client to either wire, transfer or withdraw funds to deposit into a bitcoin kiosk. Clients don't realize they were scammed until after they have sent or withdrawn money.

With respect to funds transfer and means of payment, there is not one particular method that perpetrators particularly exploit. Scammers tell the victims what to do, and victims follow that direction. Funds acquired through these scams can be transferred as cash in shoe box to a Target parking lot; by wire; by cashier's check; via gift cards purchased by the victim; via credit card payment; or when a victim sets up a digital wallet, purchases crypto, and transfers it. While different means of payment and transfer involve different opportunities for intervention, the point of payment cannot be the only opportunity. Efforts to stop these scams should start much earlier than the point of payment, rather they should start at the first communication point.

Engaging all Stakeholders in the Fight

A national strategy that attacks fraud from all angles and stakeholders is key. Where the U.S. problem continues to grow, we can take lessons from what other countries have done. Take Australia, for one example, where the government has seen a 25% decrease in losses reported and 18% decrease in scams reported in the past year, a decline that builds on the prior year's decline.[4] How did they do it?

Collaboration among financial institutions, telecoms, tech companies, law enforcement, and policymakers, as well as engaging the public, to combat fraud and scams is key. Starting with the first outreach to potential victims, telecommunications, technology, and social media companies can play a pivotal role by blocking scam communications before they reach consumers. Australia provides one example of how that could work. The

[4] https://www.nasc.gov.au/reports-and-publications/targeting-scams

government ingests reported information, investigates and sends out authoritative information that allows banks, social media, and telecoms to safely and efficiently act. In 2024, Australia's National Anti-Scam Centre referred more than 6,000 non-investment scam URLs for assessment and takedown, with 92.0% of those subsequently removed.

While it is mandated in some countries, the U.S. solution could look different. Companies could offer a "Do Not Contact" service enabling customers to opt out of calls, texts, and messages from overseas, as an example. The banking industry has urged the Federal Communications Commission (FCC) to develop a database of scam messages – i.e., the text messages that consumers report through the "report junk" feature on the iPhone and similar feature on Android devices. This database would be accessible to banks, law enforcement, and other legitimate companies, so that these companies can identify ongoing scams targeting the company's customers and take action to mitigate the impact.[5] The banking industry also has been a leading proponent of other FCC proposals to combat fraud perpetrated over our telecommunications systems, including the latest FCC proposal to require caller ID authentication solutions on non-Internet Protocol (IP) networks – i.e., providers of networks that do not rely on the IP for communication.[6]

The banking industry has invested significant resources in tools to identify and stop fraud early. These tools are necessary to support compliance with Bank Secrecy Act (BSA), anti-money laundering, countering terrorist financing, and cybersecurity responsibilities, as well as voluntary efforts to support our customers and protect our businesses. As a few examples, banks:

- Implement rigorous, risk-based BSA compliance and antifraud programs to flag when customers have started to send money in unusual patterns, including to high-risk individuals, entities, and jurisdictions.

[5] https://bankingjournal.aba.com/2024/11/stick-it-to-the-scammers/.
[6] https://www.aba.com/advocacy/policy-analysis/ABA-Urges-FCC-to-Impose-Call-Authentication-Requirement-for-NonIP-Networks.

- Submit Suspicious Activity Reports (SARs) to the Financial Crimes Enforcement Network (FinCEN) and subscribe to FinCEN's alert on fraud schemes, which offers tips for filing SARs.
- Deny institutions of primary money laundering concern access to the U.S. financial system, such as the Cambodian money laundering Huione Group, in response to section 311 actions by FinCEN.
- Ensure bank employees are trained to identify and report suspicious activity and know what actions to take to protect customers.
- Use the Treasury Department's Treasury Check Verification System to catch canceled, duplicate, or other problematic Treasury checks at the time of presentment.
- Employ National Automated Clearing House Association's (Nacha) rules intended to reduce the incidence of frauds, such as business email compromise, that make use of credit-push payments, as well as support the ACH Contact Registry.
- Utilize the ABA Check Fraud Claim Directory that maintains contact information for banks needing to file a check warranty breach claim with another financial institution.
- Deploy additional tools like real-time fraud detection analytics, voice biometrics, and identity verification platforms that are proving effective in detecting anomalous behavior and preventing fraud before money is lost.

Where permitted by law and protected from liability, banks can delay certain transactions when they suspect financial exploitation of an older or vulnerable person. In 2024, here in Florida, FBA worked with AARP to pass Senate Bill 556 (Protection of Specified Adults)[7], which authorizes Florida banks and credit unions to temporarily delay transactions reasonably believed to involve the exploitation of older and vulnerable Floridians under specified conditions. More than half (54.5%) of bank respondents in states with these "hold" laws have used them to prevent elder financial exploitation, according to a recent ABA Foundation survey.[8] Delays are helpful in bringing a family member into the conversation or giving the client the opportunity to stop and think.

[7] https://laws.flrules.org/2024/200
[8] https://www.aba.com/news-research/analysis-guides/state-hold-laws-and-elder-financial-exploitation-survey-report

However, where the client/victim wants to proceed with a transaction with their money, the financial institution ultimately has to do what the client asks.
In 2025, the FBA worked alongside AARP and others to pass SB 106[9] to permit substitute service of process in an injunction proceeding to protect vulnerable adults against financial exploitation by an "unascertainable" perpetrator who has communicated with the vulnerable adult victim by untraceable means, such as a text message or phone call. The substituted service must be made by the same manner of communication that the perpetrator used to contact the vulnerable adult victim. Upon issuance of a final injunction by the court after substituted service has been used, a 30-day freeze on any proposed transfer of funds or property is initiated.

That is why consumer education is essential to prevention of harm. Banks have invested in campaigns like the ABA's "Banks Never Ask That" and "Practice Safe Checks" initiatives. We partner with organizations like the AARP and bank regulators highlighting their messaging and campaigns. We encourage older Americans to include trusted contacts on their financial accounts so we can contact those individuals to flag suspicious activity or to intervene where a customer is being manipulated by a scammer. We host fraud prevention roundtables and events at our branches and offices, senior centers, libraries, and town halls. Talking about these issues is important as so many victims are embarrassed leading to what experts agree is underreporting of scams and losses. In fact, the FTC reported in 2024 that the estimated 2023 overall loss due to scams, adjusted to account for underreporting, was $ 158.3 billion.[10] Further, Bankrate recently found that more than one in three (34%) Americans experienced some type of financial fraud or scam in the past year (January 2024-January 2025). The survey also revealed that 68% of Americans have experienced a financial scam or fraud in their lifetime.[11]

[9] https://laws.flrules.org/2025/158
[10] https://www.ftc.gov/system/files/ftc_gov/pdf/paddle-anf-statement.pdf
[11] https://www.bankrate.com/credit-cards/news/financial-fraud-survey/

Partnering with law enforcement at the local, state, and federal levels is also critical to countering the fraud and scam crisis our nation faces. Where crimes are reported, as Miami-Dade County Sheriff Rosie Cordero-Stutz can attest, they often present as single incidences below prosecutorial thresholds. Yet, with the ability to connect dots at the state and federal levels, the ties to larger, and even transnational, criminal organizations are clear.

The FBA is working with the Florida Attorney General's office to explore establishing a Financial Crimes Intelligence Center or dedicated financial crimes task force like the one employed in Texas. This effort would build on the great work already done in Florida with the cyber fraud enforcement unit. This entity could:

- Serve as a hub for investigations of financial crimes in Florida, connecting what would otherwise be handled as local, low-level crimes to larger scam rings and organized crime.
- Provide fraud-specific data analytics to detect cross-jurisdiction patterns.
- Work with local prosecutors to secure timely convictions.
- Streamline reporting processes across federal and state agencies.
- Support law enforcement with fraud-specific training and digital forensics capabilities.

Information sharing to further criminal investigations is a two-way street. Government has comprehensive reporting, whereas each financial institution only sees its piece of the puzzle. FinCEN and law enforcement need to feed banks and other stakeholders actionable, up-to-date information on the typologies, patterns, and characteristics of the illicit financial transactions that target consumers. Improving feedback loops to banks was one of the important reforms Congress included in the Anti-Money Laundering Act. We are gratified to see the initiative just announced by Internal Revenue Service – Criminal Investigation (IRS-CI) on March 28, 2025 to provide quantifiable results to financial institutions on IRS-CI's use of SARs, which will include a pilot site in Florida.

A Call to Action

I have focused on large-scale scams and fraud perpetrated by organized crime in my testimony. This Committee, however, knows well that older Americans often fall prey to manipulation from the very trusted individuals in their lives – friends, caretakers, family members. Bankers often contend with and identify these crimes as well.

Fraud is not just a banking problem – it is a societal threat that requires coordinated action. Florida's bankers are committed to protecting our customers and communities, but we cannot do it alone. As part of a comprehensive strategy, we need action from other sectors and from the government.

We are grateful for the leadership being shown by you, Chairman Scott, and the Aging Committee members in holding this hearing and continuing to shine a light on these horrific scams. Thank you once again for the opportunity to testify. I look forward to answering your questions.