

## **State Securities Perspectives on Retail Investor Fraud in America**

NDBF Deputy Director Claire McHenry  
SEC Investor Advisory Committee Meeting  
March 6, 2025

Good afternoon. I would like to thank the SEC Investor Advisory Committee for the opportunity to discuss state securities regulatory perspectives on fraud impacting retail investors in America.

My name is Claire McHenry and I am the Deputy Director of the Securities Bureau for the Nebraska Department of Banking and Finance. I also have the honor of serving as the immediate past-president of the North American Securities Administrators Association, or NASAA, as well as co-chair of the NASAA Seniors Committee.

NASAA is an international association of securities regulators whose membership consists of the state and provincial securities regulators of the United States, Canada, and Mexico.

Because of our closeness to our local communities, state securities regulators are uniquely suited to identifying and responding to the frauds and scams impacting retail investors in America. A cornerstone of our shared mission is protecting investors from fraud and abuse.

Today I will be talking to you about what states are seeing with regards to frauds and scams impacting Americans, particularly as it impacts older Americans.

### ***NASAA 2024 Enforcement Report***

NASAA compiles statistics to report on the types of tips, complaints, investigations, and enforcement actions that state securities regulators see each year and releases it in its annual Enforcement Report. State securities regulators are often described as the “cops on the beat” when it comes to policing the capital markets and protecting the public from harm. The NASAA Enforcement report is a good indicator of what retail investors are experiencing. This year, NASAA saw a continuation of trends from the previous year – a new context for familiar schemes as bad actors turn to the internet and social media.

NASAA released its 2024 Enforcement Report in October 2024.<sup>1</sup> The information in the report is based on responses from 49 U.S. jurisdictions for enforcement activities that occurred in 2023. NASAA reported that state securities regulators conducted 8,768 active investigations, including 5,155 new and 3,613 ongoing cases, and initiated 1,186 enforcement actions. Many investigations are complex and may not be concluded in the same year. These actions led to more than \$333 million in monetary fines and restitution, and criminal relief of approximately 461 years of incarceration and 227 years of probation and deferred adjudication.

---

<sup>1</sup> *NASAA 2024 Enforcement Report*, (Oct. 21, 2024), [https://www.nasaa.org/wp-content/uploads/2024/10/FINAL\\_2024-Enforcement-Report.pdf](https://www.nasaa.org/wp-content/uploads/2024/10/FINAL_2024-Enforcement-Report.pdf).

### ***Tips, Complaints, and Referrals***

The majority of states' enforcement work comes from complaints submitted by the public or from referrals made by other agencies. In 2023, state regulators reported receiving 7,914 tips and complaints, a 14% increase over the last year.<sup>2</sup>

States received referrals from FINRA, the SEC, and state and local law enforcement. The largest source of referrals was from the SEC and FINRA, a more than 40% increase over the prior year. Likewise, state securities regulators refer matters out to the SEC, state and local law enforcement, and federal law enforcement including U.S. Attorney offices.

### ***Enforcement Actions***

State securities regulators routinely initiate enforcement actions to protect investors in their jurisdictions. State securities regulators reported initiating 1,186 enforcement actions against 2,660 parties. These actions include the sale of unregistered securities, unregistered investment advice, the sale of unsuitable products, and even fraud. Such fraud has become increasingly complex and often involves cryptocurrency, social media, and international actors.

State enforcement actions included administrative and civil matters. State securities regulators also play a crucial role in criminal prosecutions of securities offenses. States often prosecute securities law violations, either directly with inherent prosecutorial authority or appointments from district attorneys or attorneys general. They will also work in parallel with local, state, and federal law enforcement agencies to investigate complex schemes, refer cases for criminal prosecution, and testify in criminal proceedings as fact and expert witnesses.

### ***Products and Schemes***

The NASAA enforcement report provides information about the threats to retail investors. State securities regulators continue to investigate cases involving traditional products and schemes, including Ponzi and pyramid schemes, affinity fraud, and stocks and equities. States reported 692 investigations involving internet and social media and digital assets. In fact, this is a 30% increase in these types of investigations from the previous year.<sup>3</sup>

Like investigations, state securities regulators reported enforcement actions involving traditional products and schemes, including stocks and equities, Ponzi and pyramid schemes, and promissory notes. State enforcement actions also were heavily focused on technology, including digital assets and internet and social media fraud.

### ***Social Media and Internet Solicitations***

People are using social media and the internet to raise capital and seek new investments. We are seeing this being used by legitimate financial services firms using platforms to advertise and

---

<sup>2</sup> NASAA received 6,932 tips and complaints in 2022. *NASAA 2023 Enforcement Report* (Feb. 27, 2024), <https://www.nasaa.org/wp-content/uploads/2024/02/2023-Enforcement-Report-FINAL-1.pdf>.

<sup>3</sup> NASAA saw 172 internet/social media investigations and 357 digital media investigations in 2022. *Id.*

engage with clients. We are also seeing that bad actors are using these same tools and platforms to more effectively reach and recruit victims and defraud the public at an increasing rate. In 2023, we saw a 19% increase in investigations and a 12% increase in enforcement actions involving social media and internet solicitations.

Many of these social media and internet solicitations involve relationship scams, also known as pig butchering. Other panelists have aptly described how this scam works. I want to simply emphasize that states are seeing this too. Because these scammers spend so much time establishing a relationship and trust with the target, it can be incredibly difficult to combat this type of scam and break through the grip of the scammer's influence. The use of digital assets by international operations can lead to difficulties tracing assets and obtaining jurisdiction to recover funds. Often, states are simply looking to stop victims from sending more money to scammers or disrupting methods of obtaining money from targets.

### ***Digital Asset Enforcement Trends***

States continue to see a growing number of complaints, investigations, and enforcement actions involving digital assets. The complex world of digital assets has evolved since NASAA conducted Operation Cryptosweep in 2018. Investigations and enforcement actions include digital asset interest bearing account and earn products, staking, high yield investment programs, and digital asset offerings purporting to be powered by artificial intelligence. This year, the survey results showed more investigations and actions tied to digital assets than any other product or scheme. These investigations and enforcement actions have included unregistered activities and fraud.

Regarding the use of artificial intelligence, states are seeing it being used in a couple of ways. First is what has been called AI washing, the exaggerated or false claims about the use of AI technology. The promoter latches on to the hype surrounding AI to induce people to invest into bogus schemes. There will be claims that the person can offer AI trading programs in cryptocurrency to generate high returns.

State securities regulators are also seeing that AI tools are being used to make scams more believable. Some of these tools have been demonstrated here today and ultimately make traditional scams harder to spot. As AI continues to improve, we will also need to update our educational toolkit to address this. We can no longer rely on tips and tricks of asking people to ask for video chats or a phone call. Instead, we will need to emphasize media literacy – slowing down and considering what we are looking at, especially pictures, posts, videos and claims that trigger our emotions.

### ***Cryptocurrency ATM***

I think it is important to spend a few minutes talking about cryptocurrency ATMs. It may seem unusual for a securities regulator to focus on cryptocurrency ATMs, but we need to understand how investment scams are perpetrated in order to combat them. As state securities regulators, our work often involves looking at the big picture in our effort to protect investors.

We are seeing that scammers are using cryptocurrency ATMs as a payment mechanism to perpetrate their frauds. We see their use especially among Tech and Customer Support scams, Government Impersonation scams, and Confidence and Romance scams. Scammers convince targeted individuals to withdraw large sums of cash and deposit into cryptocurrency ATMs or kiosks at locations provided by the scammers. Once cash is deposited and converted into cryptocurrency, the scammer transfers it to other cryptocurrency accounts. These ATMs and kiosks are located in malls, gas stations, and private businesses.

Cryptocurrency ATMs may not be licensed as money transmitters or subject to another licensing regime in all jurisdictions, which can make it difficult to track and access information about how many and where they are located, let alone how much money is being transacted through them. We are seeing that there is confusion in the public about how these cryptocurrency ATMs work, the ability to recover money from them, and a belief that a cryptocurrency ATM is affiliated with a bank or financial institution.

Here, I have provided screenshots from someone I know who witnessed firsthand someone being scammed using a cryptocurrency ATM. He worked at this gas station and watched as a woman walked in and deposited \$10,000 into the ATM by following instructions from the scammer on her phone. He warned her that she was being scammed and she did not believe him. She later returned to the gas station and told him that she was scammed and asked if she could get her money back from the cryptocurrency ATM. There was nothing he could do. This was an incredibly frustrating, and unfortunately not a one-time, experience for him.

I will note that his experience is not limited to just Nebraska. Recently, the Iowa Attorney General announced that her office is filing lawsuits against two cryptocurrency ATM companies that cost Iowans \$20 million for violations of the Iowa Consumer Fraud Act. In the announcement, the investigation indicated that that a majority of scam victims were over the age of 60 and that 98% of the money sent through one cryptocurrency ATM company were scam transactions.<sup>4</sup>

I would also like to just take a moment to talk about the language that you see in the comments on this post – “wow”, “let her know I take donations”, and “how embarrassing”. The FINRA Foundation and AARP have written about how words matter and that we need to think about how we talk about victims of scams.<sup>5</sup> Victims of financial fraud often feel shock, confusion, guilt, and shame, which can lead to depression, anxiety, and isolation. It can also prevent people from reporting when they have been harmed or make additional mistakes and be revictimized. Using victim-blaming language can be unintentional, but harmful. We should put the blame where it belongs – on the perpetrator and not the victim – to rebuild confidence and encourage reporting.

---

<sup>4</sup> *Iowa Attorney General sues 2 crypto companies, costing Iowans \$20 million* (Feb. 27, 2025) <https://www.msn.com/en-us/money/financial-regulation/iowa-attorney-general-sues-2-crypto-companies-costing-iowans-20-million/ar-AA1zVu5T?ocid=BingNewsSerp>.

<sup>5</sup> *Blame and Shame in the Context of Financial Fraud* (June 7, 2022), <https://www.finrafoundation.org/sites/finrafoundation/files/Blame-and-Shame-in-the-Context-of-Financial-Fraud.pdf>.

## **Older Investors**

Financial scams can impact people of all ages. We have, however, spent significant resources on raising awareness of and combatting scams targeting older Americans. These investors are tempting targets as they have accumulated wealth over their lifetimes but may lack the technological savvy needed to detect and avoid scams.

Let us go back to the woman who lost \$10,000 using the cryptocurrency ATM. Assuming the woman at the ATM is still working and making \$44,000 (the median personal income for someone in the Midwest)<sup>6</sup> and has a personal savings rate of 4.6%<sup>7</sup>, it would take her almost 5 years to recover the money she just lost. That point illuminates what common sense tells us; older earners do not have the luxury of time in which to make up these losses.

In 2016, NASAA approved the NASAA Model Act to Protect Vulnerable Adults from Financial Exploitation. The model act provides tools to financial services professionals to report suspected financial exploitation of senior and vulnerable clients. The model act also provides broker-dealers and investment advisers with the ability to hold disbursement of client funds to allow for investigations in suspected exploitation, and the ability to notify certain parties. It also facilitates information sharing between the firm and the states.

To date, 43 U.S. jurisdictions have adopted a version of the model law and it remains a critical tool in states' efforts to protect older investors. Industry has been an important partner in these efforts. The NASAA Seniors Committee is working to identify practices and tools to assist states in implementing the model act to maximize beneficial outcomes for older investors.

The Enforcement Report shows that financial scammers target older investors at a high rate. States received 2,481 complaints alleging misconduct against older investors, which led to 1,305 investigations and 131 enforcement actions involving 2,869 senior victims. States also make referrals to other agencies and services.

When the Model Act was first approved, many expected that states would receive reports primarily about concerns over caregiver fraud, family members taking advantage of an older relative, or fraud involving traditional investments. We certainly have gotten those complaints. However, more and more, states are receiving reports from firms indicating that their clients are victims of scams. Consistent with some the previous points I have made about the data, the Enforcement report shows, however, that seniors are being targeted by internet and social media frauds and digital assets.

The Enforcement Report also notes that enforcement actions involving bad actors targeting older investors are preying on concerns about inflation and economic issues to perpetrate schemes related to commodities and precious metals. Older investors are particularly targeted due to their

---

<sup>6</sup> *Median Personal Income in Midwest Census Region*, St. Louis Fed (Sept. 10, 2024), <https://fred.stlouisfed.org/series/MEPAINUSMWA646N>.

<sup>7</sup> *Personal Saving Rate*, St. Louis Fed (Feb. 28, 2025), <https://fred.stlouisfed.org/series/PSAVERT>.

retirement holdings, and they often encouraged to rollover funds into unregulated self-directed IRAs to purchase the precious metals. States have worked with the CFTC to bring actions to protect investors in these circumstances.

### ***FBI Elder Fraud Report***

We are not alone in finding that older Americans are being impacted by scams. The FBI 2023 Elder Fraud Report found that elder fraud is growing and expensive at \$3.4 billion in losses. That older Americans were disproportionately impacted by scams and fraud with over 101,000 victims age 60 and over, and only 18,000 victims under age 20. While tech support scams were the most commonly reported kind of elder fraud, investment scams were the costliest with associated losses of \$1.2 billion. The FBI report also confirms what states are seeing – that scammers are using cryptocurrency as a medium or tool to facilitate scams targeting older Americans.<sup>8</sup>

### ***Challenges***

States, and many agencies, experience challenges when addressing scams, particularly relationship scams and scams originating from overseas. The international nature of many of these scams can make it difficult to investigate, obtain information and cooperation, and ultimately obtain jurisdiction over the scammer to bring an enforcement action. The anonymous nature of cryptocurrency, particularly with the use of cryptocurrency tumblers or mixers that obscure the trail of funds back to the original sources, can make it difficult to trace victim funds. Additionally, states are contending with the size and scope of these frauds, which can impact hundreds or thousands of investors nationwide. Ultimately, these issues can make it very difficult to obtain recovery for funds lost to these types of scams.

### ***Collaborative Efforts***

States are taking action to combat fraud impacting retail investors in America. First, we work collaboratively among our sister jurisdictions and federal counterparts to educate the public about how to protect themselves from frauds and scams.

Recently, NASAA issued a joint release with the SEC, CFTC, and FINRA warning investors about relationship scams. The release provided information about how the scam works, warning signs that they may be a target of the scam, steps to prevent them from becoming a victim, and links to additional information.<sup>9</sup>

NASAA issued a joint release with the SEC and FINRA to make investors aware of the increase in investment frauds involving the use of AI and other emerging technologies.<sup>10</sup>

---

<sup>8</sup> *FBI 2023 Elder Fraud Report* (Apr. 30, 2024), [https://www.ic3.gov/AnnualReport/Reports/2023\\_IC3ElderFraudReport.pdf](https://www.ic3.gov/AnnualReport/Reports/2023_IC3ElderFraudReport.pdf).

<sup>9</sup> *NASAA Investor Alert: Relationship Investment Scams* (Sept. 2024) <https://www.nasaa.org/73201/nasaa-investor-alert-relationship-investment-scams/>.

<sup>10</sup> *NASAA Investor Alert: Artificial Intelligence (AI) and Investment Fraud* (Jan. 25, 2024) <https://www.nasaa.org/70780/nasaa-investor-alert-artificial-intelligence-and-investment-fraud/>.

NASAA also partnered with the SEC and FINRA to educate the investing public about the purpose and benefits of identifying a trusted contact on your brokerage account. This is a person the client authorizes the financial firm to contact in limited circumstances. The trusted contact is an important tool that firms can use when they suspect a client may be the victim of financial exploitation or a scam.<sup>11</sup>

I was also pleased to be able to join FINRA last spring as it conducted a series of film screenings of the documentary “This is Not Financial Advice” and panel discussions at college campuses in Nebraska. The events used story telling to reach young investors and discuss the risks of investing, social media, financial influencers, and cryptocurrency.<sup>12</sup>

### ***State Efforts to Combat Retail Fraud***

In addition to these collaborative efforts, states conduct direct investor education on frauds and scams. These are boots-on-the-ground events with direct contact with constituents at senior centers, schools, and community organizations. NASAA also has an Investor Education section that develops toolkits and resources about saving, investing, and frauds, as well as providing training to investor education coordinators to deliver these resources.

NASAA provides education and public awareness on fighting fraud. Recently, NASAA has held webinars to discuss what makes someone vulnerable to relationship scams, artificial intelligence, and international approaches to stopping scams. And in March, NASAA will be holding a series of webinars from the Seniors Committee on the topic of Women, Aging and Money.

And as mentioned, states are actively involved in investigating and bringing enforcement actions and providing tools to industry to help combat financial exploitation of senior and vulnerable adults.

### ***Whole-of-Government Approach***

Combatting scams and fraud impacting Americans will take everyone acting together. On February 12, 2025, NASAA released its federal policy agenda for the 119<sup>th</sup> Congress.<sup>13</sup> In it, NASAA recognizes that investment scams are an increasing threat against our public health and safety, with implications on our economy, the U.S. financial system, and national security. NASAA therefore supports a robust, whole-of-government approach to the scam epidemic. I also recognize that this will require public and private partnership to address this issue. I look forward to collaborating with others to solve this problem.

---

<sup>11</sup> *Trusted Contact* (Nov. 2021) <https://www.nasaa.org/investor-education/investor-library/trusted-contact/>.

<sup>12</sup> *NDBF Celebrates Financial Awareness Month with Nebraska Colleges* (Apr. 9, 2024) [https://ndbf.nebraska.gov/sites/default/files/press/FINAL%20Film%20Screening%20Press%20Release%204.8.24%20\\_0.pdf](https://ndbf.nebraska.gov/sites/default/files/press/FINAL%20Film%20Screening%20Press%20Release%204.8.24%20_0.pdf).

<sup>13</sup> *NASAA Federal Policy Agenda*, (Feb. 12, 2025), <https://www.nasaa.org/wp-content/uploads/2025/02/NASAA-Federal-Policy-Agenda-for-the-119th-Congress-2.12.25-F.pdf>.

I would like to thank the Committee for the opportunity to discuss state perspectives on combating retail fraud in America. I welcome any questions you may have.