NASAA

NORTH AMERICAN SECURITIES ADMINISTRATORS ASSOCIATION

ENFORCEMENT REPORT

2025 EDITION

INTRODUCTION

The North American Securities Administrators Association ("NASAA") is an international association of state, provincial, and territorial securities regulators in the United States, Canada, and Mexico. These regulators continue to serve as the first, and often the last, line of defense against fraud, theft and other misconduct targeting the investing public.

As consumers turn to the internet and social media for their investing, banking, and even social needs, bad actors have adapted and excelled at taking advantage of these new targets and platforms to promote fraudulent schemes. Similarly, bad actors have continued to exploit the ever-increasing hype and excitement surrounding digital assets and the underlying technology to obtain money from investors, resulting in 463 new investigations and 122 enforcement actions reported to involve these products. Rapid advancements in the capability and accessibility of artificial intelligence tools, along with increasing reliance on social media, have coincided with the continued proliferation of impersonation and pig butchering scams. The international and anonymous nature of many of these schemes frequently makes them difficult to prosecute. State and provincial regulators have responded by using technology and other methods to disrupt and promote awareness of fraudulent schemes.

While cases involving technology and digital assets continue to be an important area of focus, state securities regulators are still conducting investigations, and seeking penalties where appropriate, in cases involving conventional securities products and violations. The most common violations reported by state securities regulators in 2024 were securities fraud and registration violations. Familiar products and schemes like stocks and equities, promissory notes, real estate investments, and Ponzi and pyramid schemes were among those most commonly reported in 2024. State securities regulators also continued to take action to address violations by broker-dealers, agents, investment advisers, and investment adviser representatives, and to take steps to prevent bad actors from participating in the industry.

This year's report reflects the responses of securities regulators in 49 U.S. states and territories covering the 2024 fiscal and calendar years, as well as summary data from securities regulators in the Canadian provinces. In 2024, state securities regulators investigated 8,833 cases and initiated 1,183 enforcement actions, including 145 criminal actions, 69 civil actions, and 853 administrative actions. States also secured more than $190 million in restitution and more than $69 million in fines, as well as approximately 3,458 months in prison sentences and 3,044 months of probation and deferred adjudication. This data highlights the continued vigilance of NASAA's members as fraud fighters and the local "cops on the beat." As technology continues to advance, the underlying principles of state securities laws, and the important role of securities regulators, remain relevant. The fraudulent schemes might look different or reach investors through different means. However, existing and time-tested regulatory tools and legal frameworks, such as the established "investment contract" analysis and the regulation of market intermediaries, continue to be effective to protect investors and maintain the integrity of our capital markets.

In addition to providing enforcement statistics, this report will highlight several of the investment schemes commonly seen throughout NASAA membership, as well as key enforcement cases from the 2024 fiscal and calendar years. The data also show that state securities regulators remain proactive in investigating and filing enforcement actions to prevent or stop senior financial exploitation and punish those responsible. On behalf of the Enforcement Section, thank you for taking an interest in this report. NASAA members are in a unique, and often unfortunate, position to witness conduct in our own "backyards," often impacting our friends, families, and neighbors. The challenges facing investors are many and evolving, and NASAA and its members will continue working to ensure that all investors are treated fairly.

Sincerely,

Amanda Senn
Former Enforcement Section Chair (2024-2025)
Director, Alabama Securities Commission

NASAA Enforcement Section Committee

Anthony R. Leone (MA), Chair	Jonathan Williams (SC), Vice-Chair
Wendy Coy (AZ)	Eric Forcier (NH)
Chad Harlan (KY)	Andrew Hartnett (IA)
Ricky Locklar (AL)	Mary Ann Smith (CA)
Shamiso Maswoswe (NY), Liaison	Lori Chambers, CPA, CA, CFF (BC), Canadian Liaison

*Amanda Senn (AL), Former Chair (September 2024 – September 2025)

ONGOING THREATS AND EVOLVING TRENDS

Securities regulators are dedicated to safeguarding the public by actively addressing persistent risks and adapting to emerging fraud trends. For the third consecutive year, digital assets and cryptocurrencies have ranked as the leading threat to investors, with so-called pig butchering scams—schemes where fraudsters build trust with victims before luring them into bogus investment opportunities—coming in close behind.

As in previous years, scams involving promissory notes, Ponzi schemes, and pyramid schemes remain top threats. These schemes typically involve unregistered offerings. Additionally, investment frauds connected to social media usage have been identified as significant dangers, as regulators note that scammers continue to exploit platforms such as Facebook, Twitter/X.com, WhatsApp, and others to target and reach unsuspecting investors. Securities regulators have also identified real estate investments as a top threat in 2024. With the evolution of artificial intelligence and blockchain technology, fraudulent schemes are becoming increasingly more sophisticated and infinitely more challenging to investigate. Securities regulators continue to explore tools to aid their efforts in this expansive digital era.

In some cases, multiple threats such as social media manipulation, unregistered offerings, and Ponzi schemes may be combined within a single securities offering, amplifying the risks to the investing public.

Affinity Fraud, Real Estate Ponzi Scheme

On August 20, 2024, Jesse Wayne Harris, a 36-year-old man living in Sedgwick County, Kansas, received a 30-month prison sentence from the District Court. His conviction involved three level-four felonies related to securities fraud, a serious offense that demonstrates a deliberate breach of trust and legal standards in financial dealings.

Beginning in 2016, Harris engaged in the sale of securities to generate investment capital for the acquisition of real estate intended for resale or operational profit, as well as for the purported purchase and resale of concrete. Contrary to his representations to investors, mostly fellow church members, Harris misappropriated a substantial majority of the funds, diverting them for personal expenses and to compensate other investors. In June 2018, the Securities Commissioner of Kansas was appointed as the receiver for Harris and his entity, Harris Custom Projects LLC. This receivership has successfully resulted in the restitution of over $536,000 to the affected investors. The investigation of this matter was conducted by the Securities Division of the Kansas Department of Insurance, while the prosecution was handled by the Kansas Attorney General's Office.

As technology evolves and fraudsters continue to employ artificial intelligence, NASAA members anticipate that the number of investigations and enforcement actions will increase in areas involving digital assets, cryptocurrency ATMs, "pig butchering" schemes, impersonation

frauds, and scams perpetrated through social media, as well as pump-and-dump schemes. Regulators are exploring ways technology can aid in the investigations of these cyber-schemes and collaborating with technology providers to disrupt fraudulent offerings by issuing investor alerts, collaborating with domain providers to shut down fraudulent websites, and partnering with blockchain analytics firms and digital asset exchange platforms to trace and seize assets obtained through fraud.

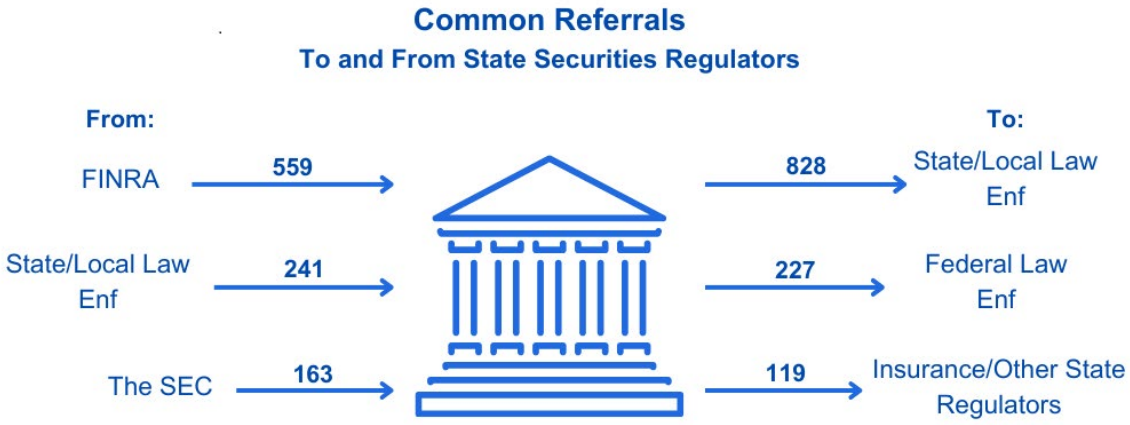
Regulators also continue their concerted efforts to promote awareness of investment fraud and bring special attention to new methods deployed by fraudsters. For example, regulators emphasize to their investing public to be extremely cautious of scams that begin with seemingly innocuous "accidental" text messages, which fraudsters use as a tactic to initiate contact and subsequently lure victims into fraudulent investment opportunities. These proactive warnings and education reflect an ongoing response to the rapid evolution and diversification of fraud schemes targeting retail investors in the digital age.

KEY INDICATORS AND BENCHMARKS

INTAKE AND INVESTIGATIONS

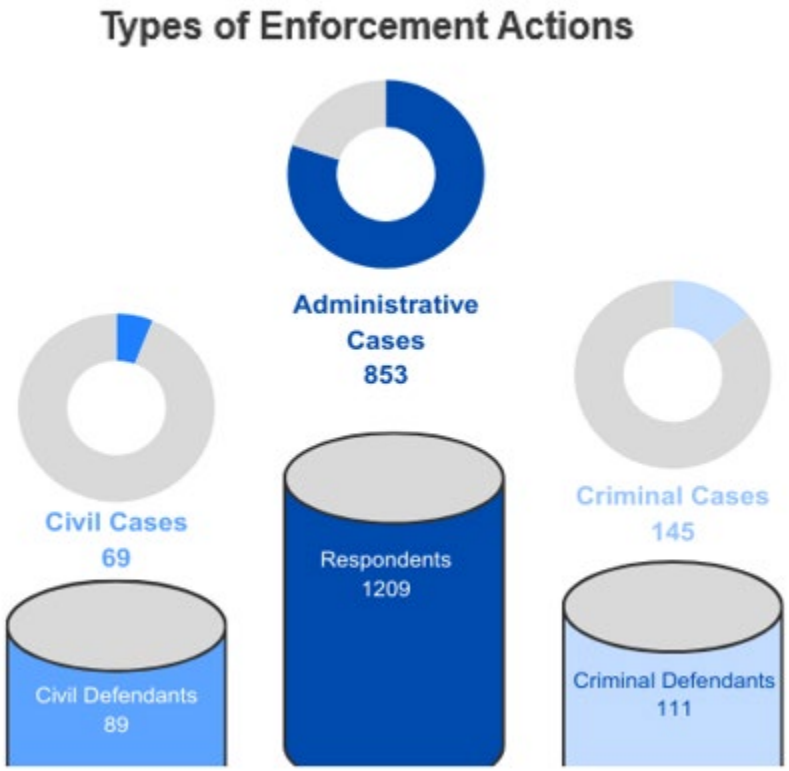
In 2024, state and provincial securities regulators continued their mission to protect investors from financial harm through robust enforcement efforts. Regulators in the United States received 8,309 tips and complaints from the public, reflecting a year-over-year increase, along with 1,685 referrals from external agencies. The largest sources of referrals included the Financial Industry Regulatory Authority ("FINRA") (559), state and local law enforcement and prosecutorial agencies (241), and the U.S. Securities & Exchange Commission ("SEC") (163).

State securities regulators opened 4,937 new investigations into suspected securities law violations. Due to the complexity of many cases, 3,896 previously opened investigations remained active. This resulted in a total caseload of 8,833 ongoing investigations in 2024, underlining the sustained efforts of state securities regulators to uphold market integrity and investor protection.



ENFORCEMENT ACTIONS

Securities regulators actively pursue enforcement actions to protect investors from a broad spectrum of financial fraud and misconduct. Their authority extends to cases involving unregistered securities, unregistered investment advice, unsuitable products, and outright fraud. As fraudulent schemes grow more sophisticated—often involving cryptocurrency, social media, and international actors—state regulators remain on the front lines. They work to disrupt illegal activity, secure restitution for harmed investors, impose financial penalties, and deliver justice to victims.



Securities regulators work to protect investors by investigating possible violations of securities laws and issuing actions when a violation has been found. In 2024, state securities regulators initiated 1,183 enforcement actions against 1,514 individuals and entities to combat a wide range of financial fraud and misconduct. These actions included 853 administrative proceedings involving 1,209 respondents, 69 civil cases against 89 defendants, and 145 criminal prosecutions targeting 111 reported defendants.[1]

COMMON VIOLATIONS, PRODUCTS, AND SCHEMES

The investigations that securities regulators initiate, and the actions that they take, can provide useful insight into the areas that may pose the most risk for investors. Consistent with previous years, the most common violations reported by NASAA's U.S. members in 2024 were

[1] Some NASAA members tracked prosecutions, but not the number of defendants.

securities fraud (980 investigations and 298 actions), the offer and sale of unregistered securities (497 investigations and 223 actions), and the offer or sale of securities or investment advice by unregistered parties ("unregistered activity") (650 investigations and 312 actions). Also consistent with previous years, stocks and equities (177 investigations and 51 actions), promissory notes (112 investigations and 65 actions), private placements (152 investigations and 47 actions involving offerings relying on SEC Rule 506(b)), real estate investments (70 investigations and 27 actions), and Ponzi and pyramid schemes (75 investigations and 36 actions) were among the products and schemes most commonly reported by state securities regulators in 2024. Further, state securities regulators reported opening 64 investigations and initiating 27 enforcement actions involving precious metals, indicating that scams involving these products are on NASAA members' radar and remain a threat to investors amidst uncertainty and volatility in the markets.

Affinity Fraud, Promissory Note Scheme

In November 2024, the Maryland Securities Division entered into a Final Judgment and Consent Order for Permanent Injunction with Prosperity Partners, Inc. and related respondents. Respondents sold promissory notes and equity shares issued by Prosperity Partners, Inc. and Prosperity Medical and Health System, LLC to at least 585 unsophisticated, nonaccredited investors from the Nigerian and Cameroonian immigrant communities totaling at least $25 million.

Respondents were unregistered and did not disclose any risks or the payments to themselves and for personal use. Despite promising a 6% monthly return, Respondents made no investments that could produce such returns and refused, or were unable, to pay the promised interest or principal owed to investors. Respondents recruited many investors in part because they paid solicitors a referral fee or commission of 5% of the investment amount. Respondents' recruitment efforts included use of a WhatsApp forum.

Respondents were charged with the unregistered offer and sale of securities, unregistered broker-dealer or agent, employment of unregistered agents, fraud in connection with the offer or sale of securities, and violation of summary order for continuing their conduct after the Division's initial cease and desist order. Respondents filed for bankruptcy and ultimately settled the Division's administrative action for a deferred penalty of $17.2 million.

In addition to conventional violations and misconduct, state securities regulators continue to face complex schemes involving digital assets, the use of social media platforms, and international actors. NASAA members have used their authority to halt unlawful activity, disrupt ongoing frauds, seek restitution for investors, impose financial penalties, and pursue justice for victims.

Cases involving technology and digital assets continue to be a significant part of state securities regulators' caseloads. While some form of technology plays a part in just about every securities-related case, technology-related cases are those that rely on technology to remotely

communicate with investors, offer and sell the investments, or obscure the identities of those selling the investments. In 2024, state securities regulators reported opening 463 new investigations involving digital assets, 175 investigations involving social media fraud, and 81 investigations involving frauds perpetrated by impersonating legitimate securities industry firms and professionals. State securities regulators also opened investigations involving the sale of unregistered securities through smartphone apps, offerings and schemes related to blockchain-based metaverses, and other AI driven frauds.

Artificial intelligence is increasingly employed by fraudsters to reach a new level of deception. In each of the last three years, states have reported a small but consistent number of cases involving artificial intelligence. In 2024, state securities regulators reported six investigations involving artificial intelligence and two enforcement actions. These reported cases largely involved "AI washing," where the perpetrators of a scam represent that their trading tool uses artificial intelligence, or they otherwise imply that artificial intelligence is being used to improve the success of the investment. Of particular note is that the number of investigations reported to involve impersonation scams has increased significantly in recent years and nearly doubled from 2023 to 2024. This increase coincides with and appears to correlate with dramatic and rapid advancements in the capability and accessibility of artificial intelligence tools, as well as the ease with which fraudsters can reach potential victims through social media.

Impersonation of a Registered Broker-Dealer

On July 1, 2024, the New Jersey Bureau of Securities ("Bureau") issued a Summary Cease and Desist Order against a fraudulent online investment recovery scheme impersonating a registered broker-dealer to scam investors. The fraudulent website, www.almaxfinancialsolution.com, claimed to advertise the services of a "recovery intelligence firm … committed to helping you recover your money at the shortest possible time frame and with the most cost-effective approach."

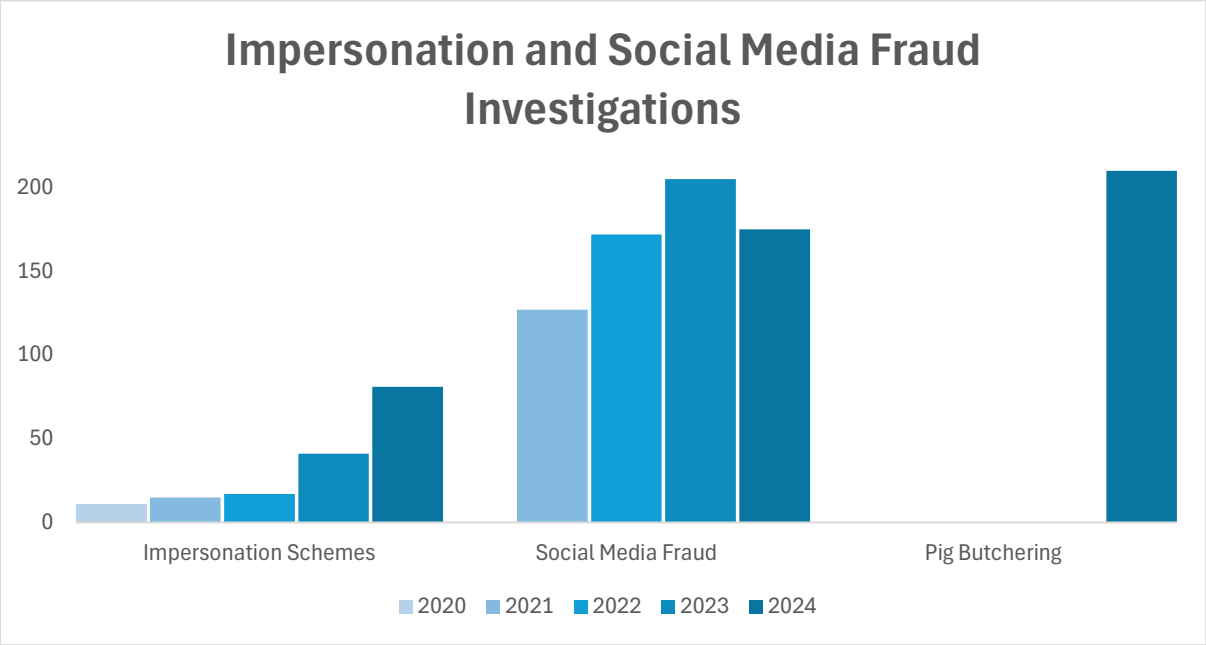
The persons behind the fraudulent website perpetrated their scheme under the assumed identity of a legitimate New Jersey-registered broker-dealer with which it had no affiliation. To further deceive investors, the website used phony testimonials from purported clients and stock photos bearing phony names and titles of purported firm leaders.

The website lured unsuspecting individuals seeking to recover lost or stolen funds and convinced them to submit their personal contact information. Once in contact with intended victims, the people behind the website made false promises and deployed deceptive tactics to pressure individuals into sending cryptocurrency as payment for recovery services and related expenses.

In April 2023, the www.almaxfinancialsolution.com website was suspended by its web host due to abusive service. The website was later registered and hosted by a different domain service before once again becoming inactive sometime after April 1, 2024. The Bureau's action ordered

the shutdown of the website and put the investment community on alert to these unlawful operations.

This year, NASAA refined its annual enforcement survey to collect specific data about NASAA members' investigations and enforcement actions related to pig butchering, including investment-, relationship-, and employment-based scams. These scams rely on relationships that the perpetrator develops with their victims, whether for the long- or short-term, and they almost always involve communicating through social media or messaging apps. States reported opening 229 new investigations that involved pig butchering and issuing 19 enforcement actions.



Technology-related cases like those discussed above often present unique challenges for investigation, and therefore enforcement. Investigations of pig butchering and similar scams are often extremely time-consuming, as they require tracing digital assets through multiple platforms and digital wallets, and they rarely result in the seizure or recovery of funds. In other cases, territorial jurisdiction can be uncertain, the respondents may be located abroad or unidentifiable, and investor funds can be nearly impossible to trace because they are quickly mixed or tumbled with other digital assets. While state securities regulators are taking actions in these cases, they are also pursuing alternative methods to address technology-related complaints and protect investors, as discussed in the Digital Assets section below.

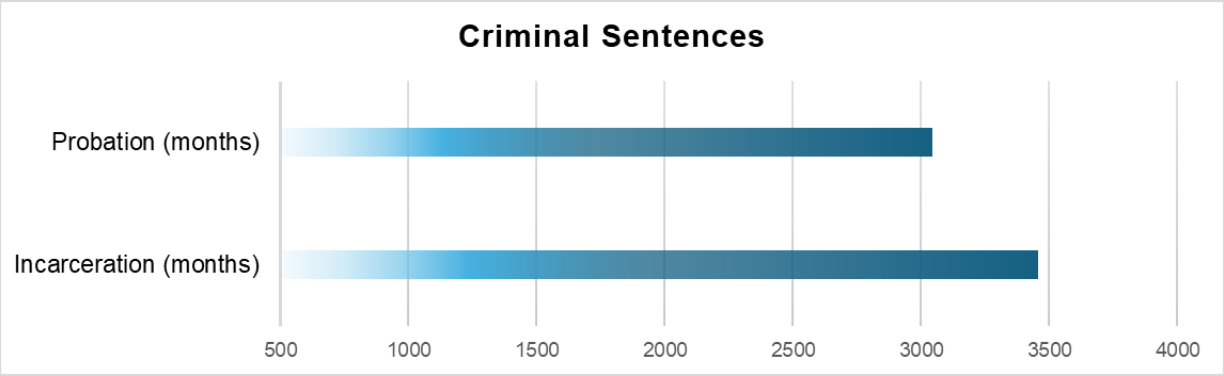
While cases involving technology and digital assets continue to be an important area of focus, state securities regulators are still conducting investigations, and taking enforcement action where appropriate, involving conventional securities products and violations. In 2024, state securities regulators reported opening 441 investigations and taking 71 enforcement

actions involving recordkeeping violations, as well as 144 investigations and 64 actions involving dishonest or unethical business practices. As discussed above, NASAA members have also continued to address wrongdoing involving familiar products like stocks and equities, promissory notes, Ponzi and pyramid schemes, real estate investments, and private placements.

CRIMINAL PROSECUTIONS

In addition to administrative and civil investigations and actions, state securities regulators often initiate criminal proceedings for securities law violations, either through inherent prosecutorial authority or appointments from district attorneys or attorneys general. They 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.

State securities regulators play a crucial role in the successful criminal prosecution of securities offenses and consider a number of sentencing options when recommending appropriate sentences in criminal matters. While probation may be appropriate in some cases, a period of incarceration is often sought to punish criminals and deter future conduct.



Last year, state securities regulators helped convict white-collar criminals that collectively were sentenced or ordered to serve 3,458 months (approximately 288 years) in prison and 3,044 months (approximately 253 years) of probation and deferred adjudication. These actions show that securities regulators are committed to the pursuit of justice for victims of financial fraud.

Securities Fraud and Theft

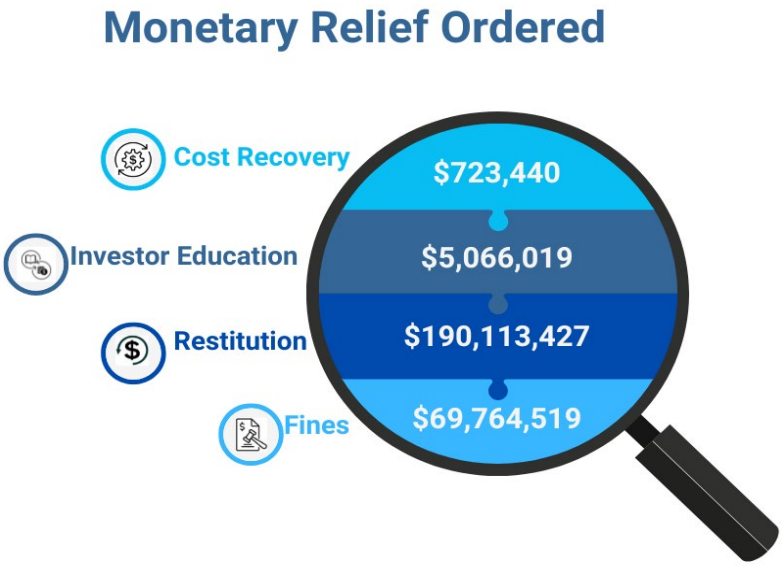
On December 30, 2024, Garry Savage, Sr. of Huron, Ohio, and his company Coast to Coast Chill, Inc., were sentenced to more than three years of incarceration, eighteen months of parole, and ordered to pay $2,909,350 in restitution to 18 Ohio investors. Savage and Coast to Coast Chill, Inc. pleaded guilty to 23 counts of securities fraud, investment adviser fraud, and theft

earlier in the year. Savage had been extradited from Florida in May 2022 after a 2021 indictment.

The funds raised by Savage and Coast to Coast Chill, Inc. were supposed to be invested into The Joseph Company International to build a facility in Youngstown, Ohio, that would manufacture self-chilling beverage cans. But funds were misappropriated and used to pay prior investors.

MONETARY RELIEF

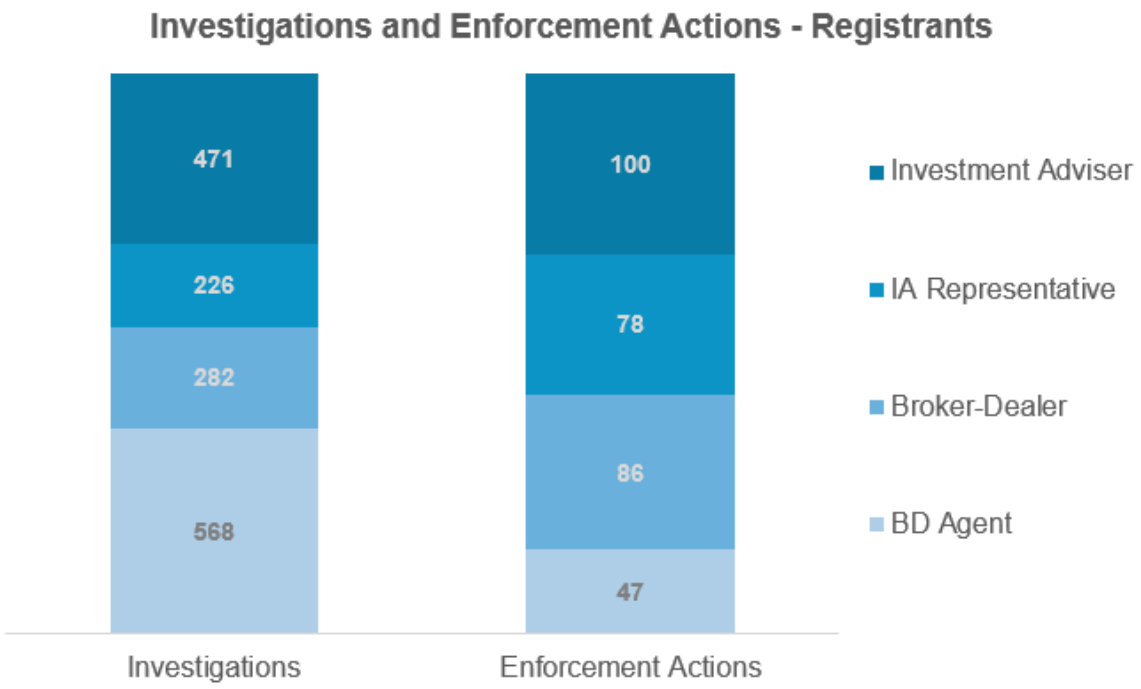
Many victims of securities fraud are left financially devastated by the illegal misconduct of bad actors. State and provincial securities agencies often seek restitution or disgorgement for victims to help repair the damages caused by securities fraud, in addition to monetary penalties. Financial penalties can serve as a substantial deterrent to future fraudulent conduct. Restitution can help to reduce or relieve the financial harm caused by fraudsters.



The sanctions imposed by state securities regulators can vary from year to year, depending on the nature of the cases pursued. In 2024, state securities regulators obtained significant monetary relief through enforcement action, including ordering over $259 million in combined monetary fines and restitution. They also reported ordering over $700,000 to reimburse investigative costs and approximately $5 million in payments to investor education programs.

REGISTERED FIRMS AND INDIVIDUALS

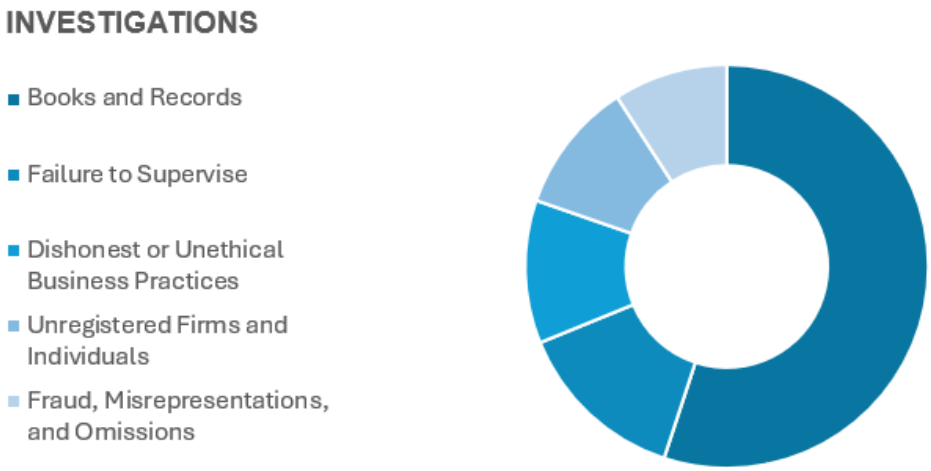
In 2024, state securities regulators reported 282 investigations involving broker-dealer firms, 568 involving agents, 471 involving investment adviser firms, and 226 involving investment adviser representatives. The reported number of investigations in each category increased from 2023. In addition, states reported 944 investigations involving unregistered individuals and 345 involving unregistered firms. While states reported opening slightly fewer investigations of unregistered firms than the previous year, the reported number of investigations involving unregistered individuals increased by more than 50%. States' investigations resulted in 86 reported enforcement actions against broker-dealer firms, 47 against agents, 100 against investment advisers, and 78 against investment adviser representatives.

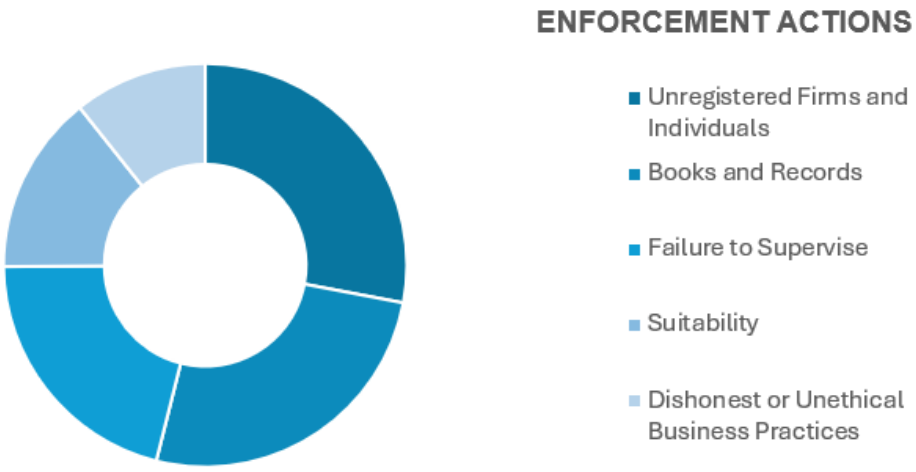


MOST COMMON VIOLATIONS

This year, NASAA further refined the enforcement survey to collect more detailed information about the violations and practices involved in NASAA members' investigations and enforcement actions against registrants. In 2024, state securities regulators reported that registrants were most commonly investigated for potential violations related to recordkeeping, supervision, dishonest or unethical business practices, unregistered activity, and securities fraud. In enforcement actions involving registrants, NASAA's U.S. members most commonly reported violations involving unregistered activity, recordkeeping violations, failure to supervise, suitability, and dishonest or unethical business practices.

TOP REGISTRANT VIOLATIONS

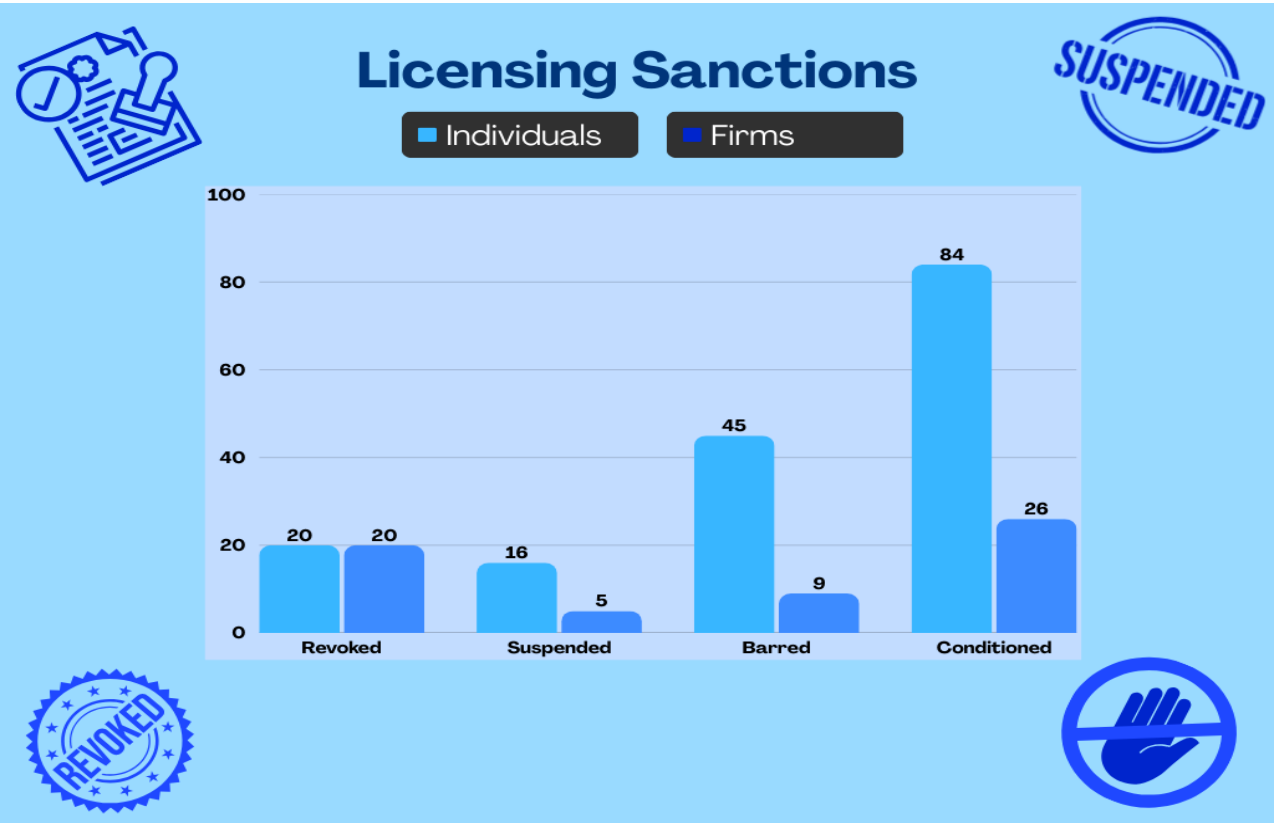




In addition to pursuing bad actors for violations of state securities laws, regulators play a critical gatekeeping role in preventing misconduct. This includes the vetting of financial professionals to ensure that they possess the required qualifications, education, and experience for registration in the securities industry. State regulators decline to allow registration to individuals without the necessary credentials, and they suspend or revoke the registration of bad actors. In addition, regulators conduct routine and for-cause examinations of broker-dealers and state-registered investment advisers.

Overall, state securities regulators continued to take strong steps to prevent bad actors and unqualified individuals and firms from participating in the securities industry. In 2024, states revoked the registration of 40 individuals and firms and barred 54 individuals and firms from the industry. State regulators also conditioned or suspended the registration of 100 individuals and 31 firms. Moreover, states denied nearly 500 individual applications for registration and more than 150 firm applications for registration. Notably, more than 4,600 applications for registration were withdrawn before states took formal action. These denials and withdrawals

underscore the strong front-end efforts of regulators to protect consumers by preventing unqualified or dishonest parties from working in the securities industry.



Unsuitable Investments for Senior Clients

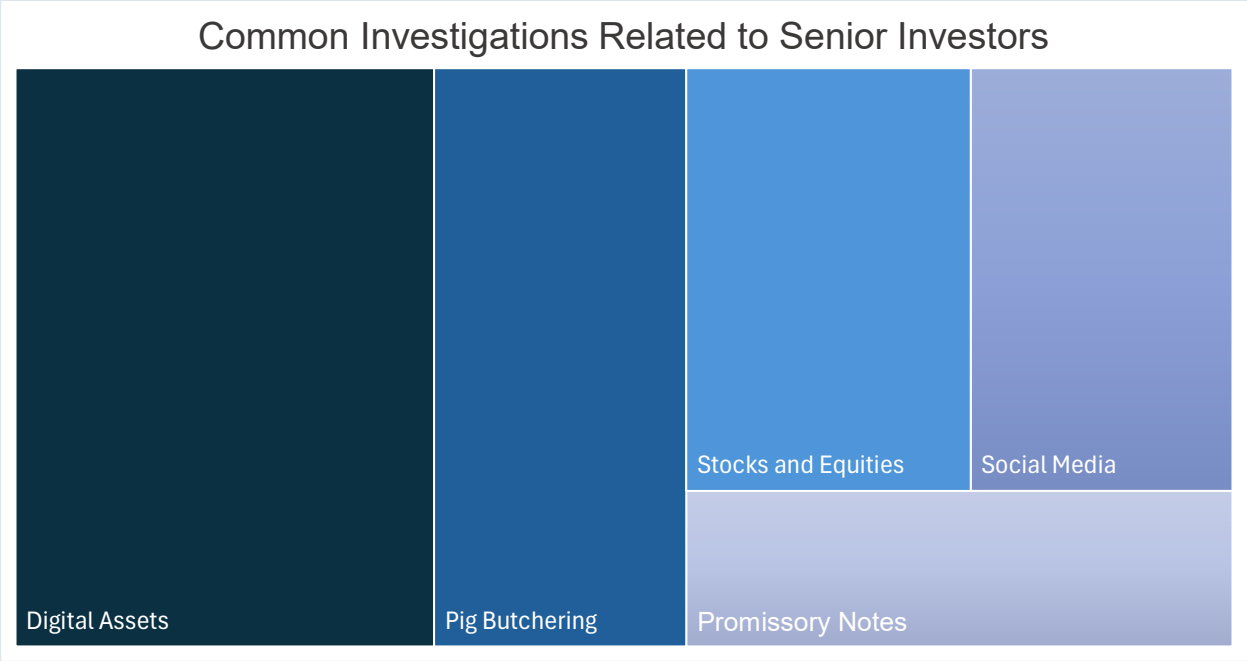
On September 30, 2024, the New Jersey Bureau of Securities found that a dually-registered broker-dealer agent and investment adviser representative, Carlos Leston, had been recommending and selling unsuitable and high-risk investments to elderly clients to their detriment and his benefit. Leston failed to disclose that his friend – who had been barred from the securities industry – was the CEO of the corporation in which he recommended his clients invest $3.65 million. Leston violated his duty to act in the best interest of his clients and instead he put his own interests ahead of theirs. As a result, the New Jersey Bureau revoked Leston's registrations as a state broker-dealer agent and a state investment adviser representative.

PROTECTING OLDER INVESTORS

Regulators have long recognized that fraudsters target older investors who may possess more wealth and may also be more vulnerable to financial scams or exploitation. Older investors may have concerns regarding their retirement income lasting throughout their extended lifespan and lack the technological sophistication to protect themselves when interacting online with strangers with ulterior motives. State securities regulators remain proactive in investigating and filing enforcement actions to prevent or stop senior financial exploitation and punish those responsible. These regulators also refer reports of such financial exploitation to other agencies, such as adult protective services or law enforcement, and connect victims with other resources when appropriate.

Older investors – those aged 65 and above – remain popular targets for financial fraudsters. In 2024, state securities regulators fielded 3,613 complaints of alleged financial misconduct against older investors. This resulted in states opening 1,652 investigations and filing 53 enforcement actions involving 676 senior victims.

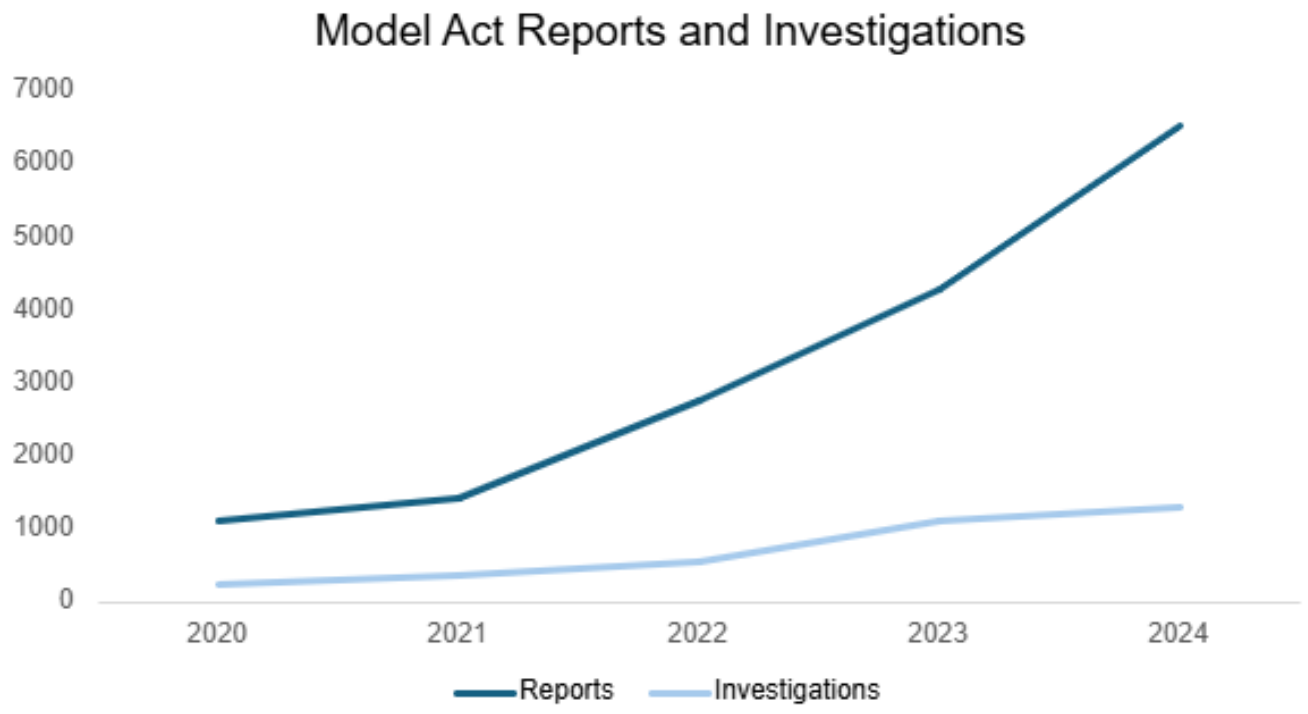
In new investigations opened in 2024 that involved senior investors, the products and schemes most commonly reported by state securities regulators were digital assets (151), pig butchering (91), stocks and similar equities (75), social media fraud (69), and promissory notes (51).



MODEL ACT TO PROTECT VULNERABLE ADULTS FROM FINANCIAL EXPLOITATION

NASAA members voted to approve the Model Act to Protect Vulnerable Adults from Financial Exploitation ("Model Act") in 2016 to better combat financial exploitation and prevent financial losses. Since its introduction, 43 U.S. states and territories have adopted and enacted it as law, or enacted similar laws. Under the Model Act, certain financial services professionals must notify state securities regulators and adult protective services agencies whenever they form a reasonable belief of the attempted or actual exploitation of an elderly or vulnerable client. The Model Act has prevented millions of dollars from leaving the accounts of senior investors, which would have otherwise been lost to fraud. Financial services professionals have played a significant role in that result by recognizing and reporting financial exploitation. Many jurisdictions continue to provide training and resources to registrants to help identify and report financial exploitation.

The Model Act provides a powerful tool in the toolbelt of state securities regulators when it comes to protecting senior investors. NASAA first began collecting data regarding the number of reports of suspected financial exploitation of vulnerable investors in 2017. That year, states reported receiving approximately 500 reports. This number has increased significantly each year since then as shown in the graph below.



States reported that they received more than 6,500 reports of suspected exploitation of vulnerable adults under the Model Act in 2024. As a result of these reports, states reported opening 1,290 investigations. Many of the matters reported include scams that cannot be

investigated because the nature of the conduct is outside securities regulators' jurisdiction. For example, many of these reports do not involve a security and instead relate to wills, trusts, other probate matters, or unlawful consumer sales practices. In such cases, state securities regulators typically refer the matter to Adult Protective Services or another governmental agency with the appropriate jurisdiction.

The number of Model Act reports received by state securities regulators in 2024 reflects a 52% increase from 2023 and a 492% change from 2020. The increase in Model Act reports demonstrates that seniors continue to be targets of financial fraud. State securities regulators remain dedicated to protecting senior investors. The number of reported cases of financial exploitation is staggering, however, and continues to rise. While securities regulators stretch their resources to prioritize financial exploitation, this is an area where increased multi-jurisdictional cooperation and additional funding is critical in order to accommodate the volume of suspected fraud that is reported.

MULTIJURISDICTIONAL AND MULTIAGENCY ACTIONS

NASAA members frequently collaborate with other members and local, federal, and foreign partners to leverage resources and combat fraud across state lines and international borders. The cases highlighted in this year's report are just a small sample of the important joint and parallel cases from 2024.

Alberta Man Who Fled to Montana Extradited to Canada

Ronald James Aitkens was found guilty of fraud and making false or misleading statements in connection with the sale of securities in a real estate investment scheme raising over $35 million from over 1,475 investors contrary to the Albera Securities Act. The Alberta Securities Commission's investigation also revealed that Aitkens misappropriated at least $10.7 million. After his conviction, in November of 2023, Aitkens failed to appear for sentencing, and a warrant was issued for his arrest. The Alberta Securities Commission worked with the U.S. Marshals Service, the U.S. Customs and Border Protection, the U.S. Border Patrol, U.S. Department of Homeland Security, Department of Justice (Canada), the Canada Border Services Agency, the Royal Canadian Mounted Police ("RCMP"), the British Columbia Sheriff Service, the Alberta RCMP Federal Policing Integrated Market Enforcement Team, the Alberta Sheriffs, and Crime Stoppers to arrest Aitkens in Montana and return Aitkens into custody in Canada. On August 15, 2024, Aitkens was sentenced to four years in jail.

NASAA Members Settle with Edward Jones

NASAA members collaborate on cases involving both registered and unregistered entities and individuals. In late 2024, state regulators reached a $17 million settlement with registered broker-dealer Edward D. Jones & Co., L.P ("Edward Jones"). An investigation into the firm found that Edward Jones charged front-load commissions on investments for some clients who sold or moved their mutual fund shares sooner than originally anticipated. The

states found gaps in Edward Jones's supervisory procedures related to this activity. Those clients then paid advisory fees on their shares in addition to the front-load commissions they already paid, resulting in clients paying higher fees to Edward Jones than they otherwise would have. All 50 states, Washington D.C., the U.S. Virgin Islands, and Puerto Rico participated in the settlement.

Florida Man Sentenced to 23 Years for Orchestrating Ponzi Scheme

Securities regulators also play an integral role in joint and parallel investigations to stop multi-million-dollar Ponzi schemes. For example, the Florida Office of Financial Regulation recently engaged in a joint investigation with the Federal Bureau of Investigation, the United States Attorney's Office, and the United States Department of Transportation into Sanjay Singh, the owner of Royal Bengal Logistics, Inc. The investigation revealed that from January 2020 until June 2023, Singh and his co-conspirators defrauded more than 1,600 investors out of $160 million through a classic Ponzi-style investment scam. Under the guise of operating a profitable trucking logistics business called Royal Bengal Logistics, Inc. ("RBL"), they offered different investment programs to investors including trucking, short-term investment, long-term investment, trailer manufacturing sponsorship, real estate, airline, and truck dealership. During the two-and-a-half-year period, Singh and his co-conspirators continuously lied to investors about the success and profitability of the company. While RBL did generate revenue from its trucking operations, none of the investment programs generated any revenue. Singh operated an affinity fraud by targeting Haitian American investors throughout the United States while using new investor money to pay earlier investors. At least $3 million of the victims' money was used to pay his co-conspirators, while the rest was used to fund Singh's personal lifestyle, including sending $6 million to a company owned by his brother-in-law and $540,000 to other relatives.

On November 6, 2024, a jury found Singh guilty of wire fraud, money laundering, and conspiracy charges. In May of 2025, the U.S. District Court for the Southern District of Florida sentenced Singh to 23 years in federal prison followed by 3 years of supervised release.

Hawaii, California, and the Commodity Futures Trading Commission Obtain Over $50 Million Dollar Judgment in Precious Metals Scam Targeting Seniors

State securities regulators are empowered not only to regulate the offer and sale of securities and oversee investment advisers and broker dealers, but also to enforce the federal Commodity Exchange Act. In April of 2024, the U.S. District Court for the Central District of California entered a consent judgment against a Southern California based precious metals dealer, Red Rock Secured, LLC, its owner, Sean Kelly, and top producing salesman, Anthony Spencer, for fraudulently misleading investors about the value of gold and silver coins and for giving unregistered investment advice by urging investors to liquidate securities in their retirement accounts to buy grossly overpriced precious metals. The judgment requires defendants to collectively pay over $38 million in restitution, disgorge $5.1 million, and pay $12.5 million in civil penalties. The judgment also permanently prohibits Defendants from

violating both federal and state laws. Additionally, Sean Kelly and Anthony Spencer are subject to commodity trading bans and are barred from working in the broker-dealer or investment adviser industries in California and Hawaii, and are also barred from offering or selling securities in Hawaii. In a parallel proceeding, the SEC secured a comparable judgment, enjoining the parties from future violations of federal securities laws and obtaining similar monetary relief.

SOCIAL MEDIA

Social media platforms have increasingly become fertile ground for fraudulent activity due to their far-spread reach, ease of anonymity, ability to manipulate trust, and ability to evade detection by regulators and law enforcement. Issuers continue to use social media and the internet to raise capital and seek new investments. Although legitimate financial services firms are using these platforms to advertise new products and engage with clientele, bad actors are also using social media to more effectively recruit victims and defraud the public.

Social Media Influencer Scheme

On May 7, 2025, A Utah businessman and social media influencer, Jeremiah Joseph Evans "The Bull," 29, of Utah County, was sentenced to 96 months in prison, three years' supervised release, and ordered to pay $19,134,150 in restitution. Evans had pleaded guilty to securities fraud and money laundering in January 2025, admitting to defrauding over 530 victims out of about $20 million. Lead sales agents Dallin Pili and Kole Brimhall were also charged and convicted of securities fraud for their role in selling the scheme.

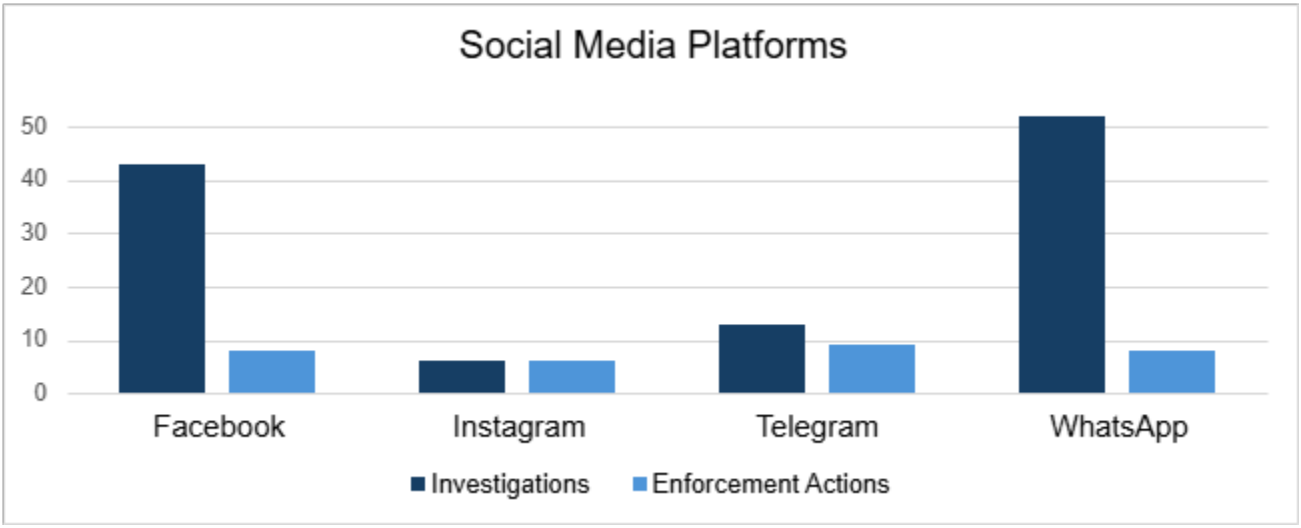
From July 2019 to July 2022, Evans fraudulently sold investments in e-commerce stores through Alpha Influence, LLC, a registered Utah corporation. Evans structured sales of e-commerce stores to purchasers as a passive investment opportunity and promised that the stores would make high, consistent, predictable, monthly returns, despite knowing this was false.

Evans primarily solicited investors through social media and webinar sales pitches on YouTube. Most notably, Evans held investment seminars and self-improvement events, including AlphaCon in 2022, influencing investors to "be great, or be nothing." He employed a team of unregistered agents, promising them high commissions and bonuses for selling the investments.

As part of the scheme to defraud, Evans and his agents lied to investors about how successful he and his company were, and how long it had been in operation. Evans failed to disclose that the majority of investor funds were distributed as commissions to those selling the fraudulent investment, and to Evans himself, with only a small portion sent to the servicer of the investors' e-commerce stores.

The survey responses show how pervasive the use of social media and the internet are in soliciting investments from the public. In 2024, state securities regulators reported that they opened 175 investigations that involved social media fraud. They also reported initiating 24 enforcement actions that involved social media fraud. These numbers decreased from last year, which could be partially due to a change in how the survey asked about technology-related cases, specifically the collection of information about pig butchering. It could also be due to several interconnected factors rooted in the global and anonymous nature of the rapid evolution of internet technology used by bad actors, making prosecution difficult.

This year, NASAA collected information about the platforms that were used by bad actors in cases involving alleged frauds and other misconduct perpetrated through social media. WhatsApp and Facebook were the platforms most commonly reported in the context of states' investigations.



DIGITAL ASSETS

NASAA members have played a pivotal role in protecting investors from emerging threats related to digital assets, including crypto staking programs, non-fungible tokens ("NFTs"), metaverse investments, and crypto interest accounts. In 2024, NASAA's U.S. members reported opening more than 460 investigations involving digital assets and initiating more than 120 enforcement actions. These enforcement actions have targeted a range of illicit activities, including fraudulent securities offerings and trading platforms, "high yield" investment programs, unregistered offerings, Ponzi and pyramid schemes, unregistered staking and yield programs, and metaverse projects. NASAA's U.S. members have taken strong action to stop localized frauds that might otherwise evade detection, while also collaborating with other local, state, federal, and international agencies to protect investors.

DISRUPTION

In today's rapidly evolving technological landscape, state securities regulators are embracing innovation by incorporating blockchain tracing software into their investigations to track the origin and movement of funds. Additionally, regulators are now using artificial intelligence tools to enhance and expedite their investigative process. As the case below highlights, some regulators are proactively taking measures to work with law enforcement and industry participants to disrupt online investment fraud.

Operation Avalanche: Disrupting "Approval Phishing"

In March of 2025, the British Columbia Securities Commission ("BCSC") led a coordinated operation to warn victims that they may have lost—or may soon lose—some of their crypto assets. Operation Avalanche united securities regulators, police agencies, crypto trading platforms, and a blockchain analysis firm to disrupt so called "approval phishing" in which fraudsters trick victims into granting them access to their wallet on the Ethereum blockchain. By granting approval, the victim – often unknowingly – allows the fraudster to withdraw crypto from their wallet. The Ethereum blockchain shows which wallets have granted such permission.

Although there can be legitimate reasons to grant access to a wallet, most of the time it's part of a long-term online investment fraud. The BCSC partnered with Chainalysis (a blockchain transaction analytics firm) to identify compromised wallets and trace where the cryptos in those wallets originated. If Chainalysis determined that the cryptocurrency for a compromised wallet came from one of the crypto trading platforms participating in Operation Avalanche, regulators notified that platform. The platform then provided contact information for the account holder to regulators and police sitting alongside them. During the operation, 89 victims were contacted by telephone or email. The blockchain addresses identified during the operation were drained of crypto assets worth an estimated $4.3 million.

Operation Avalanche – which included the Alberta Securities Commission, the Autorité des marchés financiers, the Ontario Securities Commission, the Delta Police Department, the Vancouver Police Department, the RCMP and the U.S. Secret Service – is another example of how various agencies at the local, provincial, federal level, along with agencies in other countries, are collaborating to disrupt cryptocurrency scams orchestrated by transnational organized crime. The participating crypto trading platforms, all of which are registered to operate in Canada, were Netcoins Inc., Ndax Canada Inc., Coinbase Canada Inc., Wealthsimple Investments Inc., and Shakepay Inc. Kraken and Coinsquare also provided information as part of the Operation.

As Operation Avalanche shows, regulators continue to combat high yield investment programs, pig butchering scams, Ponzi/pyramid schemes, and unlawful digital asset related offerings. In addition to issuing cease and desist orders, regulators are issuing public alerts and advisories and publishing scam trackers and caution lists.

In California, the Department of Financial Protection & Innovation uses social media and investor education in conjunction with the agency's administrative enforcement actions to inform victims before they invest by posting educational videos and alerts about the scams. The videos are shared on DFPI Facebook, Twitter, and LinkedIn, generating views on those platforms.

Some state securities regulators are sending website takedown requests to registrars and web hosts. For example, the Washington Department of Financial Institutions sends website takedown requests when it identifies a website that was apparently used to defraud investors. The requests highlight the red flags that indicate the website is involved in a scam, and they note that the conduct likely violates the registrar or web host's service agreements. These requests frequently result in the website being taken down, enabling regulators to prevent investor harm.

Securities regulators are also partnering with local, state, federal, and international authorities in an attempt to disrupt or prosecute digital asset-related scams.

Global Cryptocurrency Ponzi Scheme

Based on a joint investigation between the Florida Office of Financial Regulation, Department of Homeland Security, the New York Police Department, New York City Sheriff's Office, the Florida Department of Financial Services, and the New York Southern District Attorney's Office, on October 15, 2024, Juan Tacuri was sentenced to 240 months (20 years) in prison for his role as a senior promoter in the cryptocurrency Ponzi scheme known as Forcount (later known as Weltsys). Tacuri was one of the scheme's most successful promoters and reaped millions of dollars from his participation in the fraud, which he spent on Florida real estate and luxury goods, among other things. Forcount held itself out as a cryptocurrency mining and trading company and solicited investments globally from primarily Spanish speaking individuals. Forcount promised its investors guaranteed returns that would double within six months' time. In reality, Forcount's promoters used investor funds, in some cases hundreds of thousands of dollars, to pay for promotional expenses and personal expenditures such as luxury goods and real estate.

Investors were additionally provided with access to an online portal where they could see and monitor their purported returns. Although victims saw profits in their accounts, most were unable to withdraw their funds and were only provided with excuses and delays when they complained. Despite these complaints, Forcount's promoters, including Tacuri, continued to promote the fraudulent scheme and accept new investments. As complaints mounted, Forcount began offering a proprietary crypto token, Mindexcoin, to raise additional capital to prop up the fraud. By 2021, the scheme had imploded. In addition to his prison term, Tacuri was also ordered to pay at least $3.6 million in restitution and forfeit over $3.6 million and all right and title to a home in Florida that he purchased in part with investor funds.

Pig Butchering

The next case demonstrates that both experienced and inexperienced investors can fall for pig butchering scams.

Pig Butchering Scam

In 2024, the State of Oklahoma Department of Securities initiated an investigation into David Jerry Love, a registered agent and investment adviser representative until he was discharged in May of 2024 for allegedly violating his employer's rules of supervisory procedures. In 2023, Mr. Love met, through an online dating platform, an individual who offered him the opportunity to invest in cryptocurrency on a secondary exchange called "Coub Asgx" using options and artificial intelligence guided software. Mr. Love allegedly deposited $19,000 worth of Ethereum into a Coub wallet. He subsequently received signals telling him the product, time of day, dollar amount, and duration for a trade.

Mr. Love allegedly believed that his trading had been highly profitable, and he began recommending the investment to friends, family, and his investment advisory clients. The Department found that Mr. Love caused three of his investment advisory clients to send assets totaling approximately $989,000 (including assets from retirement funds) from their advisory accounts under his management to be pooled with the assets of others in his Coub wallet and traded using the AI signals he received from the individual he met online. Mr. Love allegedly told his clients and other investors that they would make ten percent per trade. Mr. Love was allegedly led to believe that his Coub wallet had grown in value to $51 million.

In May of 2024, Mr. Love was notified by email from the purported Coub Asgx exchange that his wallet was frozen and that he was under investigation for money laundering. At that time, he was locked out of his wallet and the website he used to open his account was no longer operating. Mr. Love, his clients, and other investors collectively lost over $1.2 million of principal through the scam. In 2025, Mr. Love was barred from registration as a broker-dealer, investment adviser, and investment adviser representative, and from relying upon an exemption from registration in those capacities.

Crypto Interest Accounts

Over the last five years, options for retail investors to participate in digital asset interest accounts surged. These accounts offer investors the chance to earn income by depositing digital assets like Bitcoin and Ether, often at higher yields than traditional investments. Companies offering these accounts, in turn, have sometimes pooled and lent out these digital assets to crypto hedge funds and other institutional investors to generate returns. However, these accounts were frequently offered without disclosure of critical information about risk of loss, capitalization, and the creditworthiness of borrowers.

In 2020, U.S. and Canadian securities regulators coordinated numerous investigations of these large, highly complex businesses that offered interest-bearing accounts to the public. In 2021, state securities regulators filed coordinated actions against a family of companies known as BlockFi, accusing BlockFi of selling unregistered securities in the form of interest-bearing accounts. In 2022, BlockFi agreed to cease and desist offering unregistered, non-exempt securities and agreed to pay a fine of $50 million to the states and $50 million to the SEC.

Regulators also filed actions against Celsius, Voyager, Abra, and Nexo, highlighting undisclosed risks and lack of transparency about firm capitalization and borrower creditworthiness. In 2022, largely as a result of the fallout from failed digital asset firms like Three Arrows Capital and FTX, Celsius, Voyager, and BlockFi froze investor accounts and filed for bankruptcy. In 2023, state securities regulators stepped in to protect investors during insolvency proceedings, working to maximize investor recoveries.

In 2024, securities regulators continued their efforts to ensure companies offering interest bearing accounts provide investors with essential disclosures and adhere to securities laws.

Unlawful Crypto Interest Earning Program

In February of 2024, a taskforce of state securities regulators and the SEC reached a $3 million settlement with TradeStation Crypto, Inc. ("TradeStation") concerning its crypto interest-earning program. The investigation found that TradeStation offered its crypto interest-earning program to investors nationwide without first complying with state securities laws. As a result, investors were sold unregistered securities and additionally did not receive material information and disclosures necessary to understand the potential risks of TradeStation's crypto interest-earning program. Under the settlement, TradeStation agreed to cease offering, selling, or renewing its crypto interest-earning program until it complied with state and federal securities laws, and paid a $3 million fine to the States and the SEC.

CANADIAN ENFORCEMENT

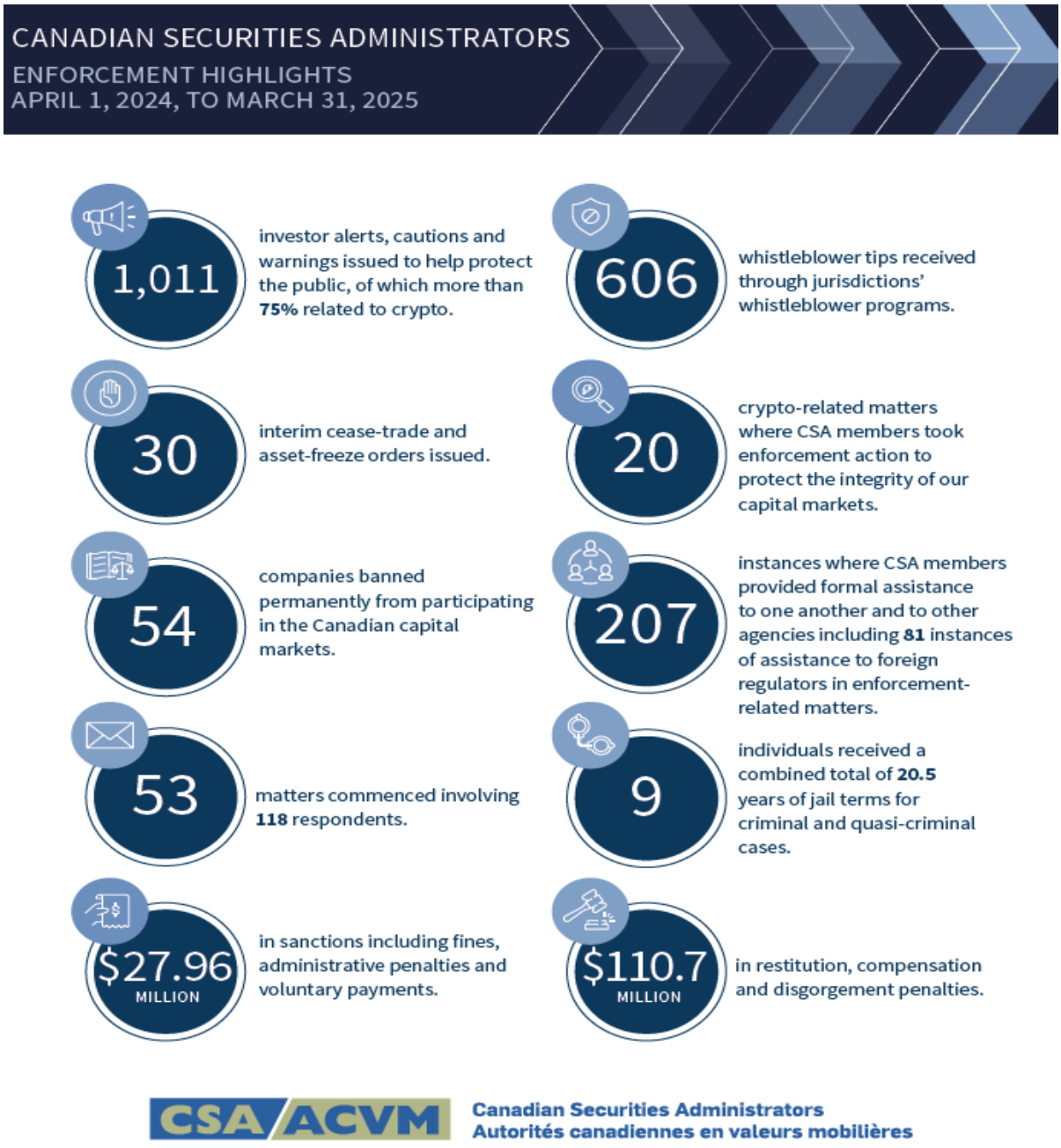
The Canadian Securities Administrators ("CSA") is made up of Canada's provincial and territorial securities regulators. Each year, it produces a Year in Review report that showcases the work of provincial and federal regulators.

As the graphic on the next page shows, from April 1, 2024 through March 31, 2025, the CSA was proactive in issuing 1,011 investor alerts, cautions, and warnings, including the BCSC's innovative and playful music video[2] reminding investors to do their due diligence and

[2] B.C. Sec. Comm., *We Are All F**ked: AI Investment Scams*, YouTube (Jan. 27, 2025), https://www.youtube.com/watch?v=1ZQwXbn_wbw. Warning: This video contains profanity

to contact the Commission with any questions before falling prey to a deep fake, impersonation, or other artificial intelligence scam. A staggering 75% of these alerts were related to digital assets.

Canadian regulators also issued 30 interim cease-trade and asset-freeze orders, banned 54 companies from participating in Canada's capital markets, and commenced 53 matters involving 118 respondents. The CSA ordered $110.7 million in restitution, compensation and disgorgement penalties, and almost $28 million in fines, administrative penalties, and voluntary payments. Additionally, nine individuals received a combined total of 20.5 years of jail terms for criminal and quasi-criminal cases.



MONEY MULES AND MONEY LAUNDERING

The BCSC recently took steps to curb the use of money mules in investment scams. The use of money mules is a frequent method of money laundering, enabling criminals to move illicit funds while hiding the identity, origin, and destination of the money. To recruit money mules, criminals employ various tactics, often enticing individuals with a portion of the transferred funds as compensation. They may misrepresent who they are, offer fake job opportunities, or initiate online friendships or romantic relationships. These criminals typically ask recruits to "process payments," "transfer funds" or "re-ship products" facilitating the movement of money obtained from investment fraud victims to the fraudsters themselves.

In some instances, individuals acting as money mules may be unaware that they are transferring funds on behalf of criminals and might themselves be victims of investment scams. They may believe they are assisting a friend, romantic partner, or fulfilling the duties of an online job. However, if money mules persist in sending or receiving funds for criminals after being warned to stop, they risk facing criminal or regulatory charges.

Securities regulators continue to be vigilant in identifying, locating, and contacting the intermediaries used to perpetrate these frauds.

BCSC Warns Money Mules of Liability

The BCSC identified suspected money mules after uncovering information that they sent or received money or cryptocurrency that was obtained from victims of investment fraud. The BCSC and the Royal Canadian Mounted Police Integrated Market Enforcement Team ("IMET") delivered warnings to suspected "money mules" to combat offshore investment fraud targeting British Columbians. During the joint operation in Metro Vancouver, IMET and BCSC investigators hand-delivered warning letters to people suspected of transferring funds on behalf of criminals. The money mules were warned that they cannot avoid liability by being willfully blind to the source of money.