NASAA 2022

Enforcement Report

Based on an Analysis of 2021 Data

Introduction: The Past, the Present and the Future of Investment Fraud

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. NASAA members have protected Main Street investors from investment schemes for more than 100 years. They continue to serve as the first, and often the last, line of defense against white-collar crime and financial misconduct targeting the investing public.

This report provides an overview of recent securities enforcement efforts in the United States. The report summarizes these efforts using information compiled from NASAA's most recent annual survey of U.S. members (also referred to in this report as state securities regulators). This year, the responses reported by state securities regulators in 48 jurisdictions generally covered their 2021 fiscal and calendar years. The NASAA Enforcement Section coordinated the reporting of these responses and then analyzed the measures to identify new trends, current market developments and emerging public threats. The analysis clearly shows that state securities regulators are leaders in protecting the public from illegal and fraudulent investment schemes.

Despite new and ongoing challenges derived from the pandemic, state securities regulators continued to serve on the front lines of the fight against financial fraud. In 2021, they investigated 7,029 cases and reported 1,661 enforcement actions, including 196 criminal actions, 80 civil actions, and 1,284 administrative actions. Although the pandemic may have limited access to courts and restricted their ability to pursue other investigatory tactics, NASAA's U.S. members nevertheless secured $312,097,734 in restitution and $145,567,334 in fines. They also successfully secured justice for victims of white-collar investment crimes, reporting 6,594 months in prison sentences and 2,237 months of supervised release.

Their work demonstrates that state securities regulators are uniquely positioned to act swiftly to protect all investors - including retirees, senior citizens and other vulnerable victims. Despite recent challenges, NASAA's U.S. members took decisive action aimed at frauds targeting senior investors , opening 605 investigations and securing 304 enforcement actions involving older Americans. These cases involved a variety of tactics and products, ranging from traditional sales of unregistered securities to an increasing number of illegal promotions tied to precious metals, frauds perpetrated through social media and the internet, romance scams and other schemes designed to exploit older investors.

In additional to summarizing important measures, this report also highlights key administrative, civil and criminal cases from the 2021 fiscal and calendar years. These enforcement actions include complex theft and misapplication cases, bad actors touting recent changes in the markets for real estate and energy, and high-tech schemes involving cryptocurrency depository accounts, non-fungible tokens and the metaverse. In many ways, these enforcement actions illustrate the dangers posed by scams that leverage established tactics, contemporary socioeconomic developments and futuristic products. This report, therefore, presents an opportunity to consider recent state enforcement efforts through the lens of the past, the perspective of the present and the vision of the future.

State securities regulators have been, are and will continue to work to protect investors from threats derived from the past, the present and the future. Simply put, our mission is an important today as it was more than a century ago and will be a century from now.

Sincerely,

Joseph P. Borg, NASAA 2021-2022 Enforcement Section Chair, Director, Alabama Securities Commission

Joseph Rotunda, NASAA Enforcement Section Vice-Chair, Director of Enforcement, Texas State Securities Board

SECTION COMMITTEE: Joseph P. Borg (AL), Co-Chair; Christopher Gerold (NJ), Co-Chair (9/21 to 6/22); Joseph Rotunda (TX), Vice-Chair; William Carrigan (VT) (9/21 to 11/21); Wendy Coy (AZ); Ricky Locklar (AL); David Minnick (MO) (9/21 to 7/22); Mary Ann Smith (CA); Lori Chambers (BC), Canadian Liaison; Dylan White, NASAA Liaison

Enforcement Report Overview

The responses to the enforcement survey again demonstrate the critical role that state and territorial securities regulators continue to serve in protecting investors and holding securities law violators accountable for the damage that they cause to individual investors and the capital markets.

KEY STATISTICS

6634
Tips and complaints

7029
Total investigations

1661
Enforcement actions

6014
Licensing sanctions

$312,097,734
Restitution

8,831 months
Prison/probation

ENFORCEMENT ACTIONS

1284 Administrative Enforcement Actions

80 Civil Enforcement Actions

196 Criminal Enforcement Actions

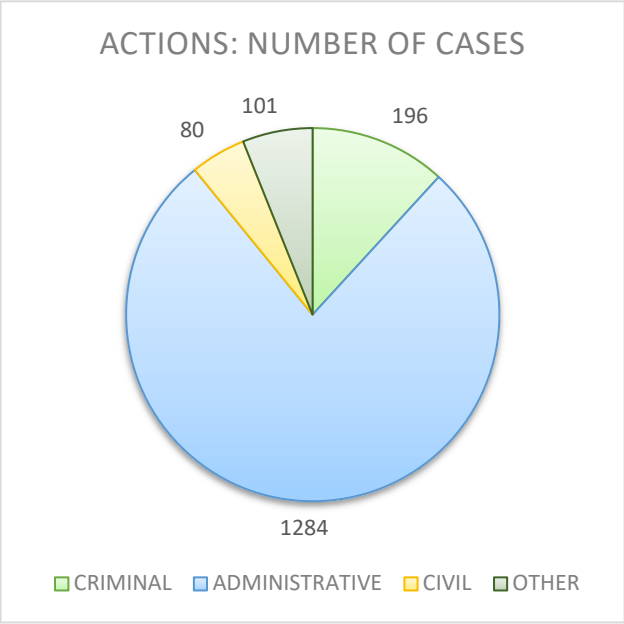
Key Data – Investigations and Enforcement Actions

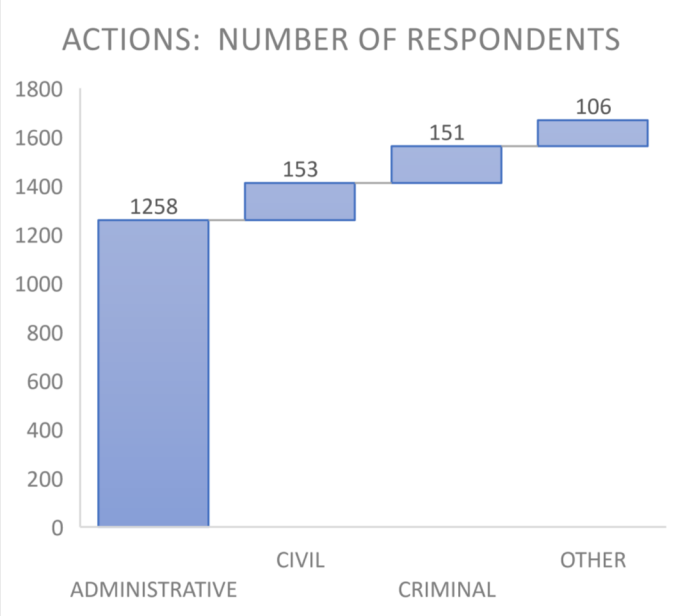
U.S. NASAA members are uniquely close to their constituents and routinely field tips and complaints from investors residing in their jurisdictions. Responding members reported receipt of 6,643 tips and complaints during their 2021 calendar and fiscal years – a 34% increase in tips and complaints from the previous year. These tips and complaints can provide invaluable intelligence and often serve as the spark that leads to the opening of investigations and the filing of enforcement actions.

In 2021, state and territorial securities regulators opened 5,337 new investigations. These investigations are often complex and, depending on the volume of evidence and number of investors, may require months and, in some cases, years to resolve. Accounting for both new and ongoing investigations, U.S. NASAA members worked on 7,029 investigations during the 2021 calendar and fiscal years.

State and territorial regulators opened 5,337 new investigations and continued investigating an additional 1,692 ongoing cases. Their formal investigatory work is supplemented by extensive efforts to resolve matters and achieve compliance through informal means. Many informal resolutions are not easily quantified, and as such the scope of enforcement is even more robust than reflected in data.

State and territorial regulators reported more than 1,661 enforcement actions against 1,668 respondents, including 1,284 administrative actions, 80 civil actions and 196 criminal actions. These actions vary from scheme to scheme and case to case and different types of actions may be brought against the same parties to obtain comprehensive relief. These types of actions include cease and desist orders, licensing sanctions, orders assessing administrative fines, other admin actions, civil receivership and injunctive actions, criminal prosecutions and enforcement actions that resulted in monetary relief for victims of misconduct.



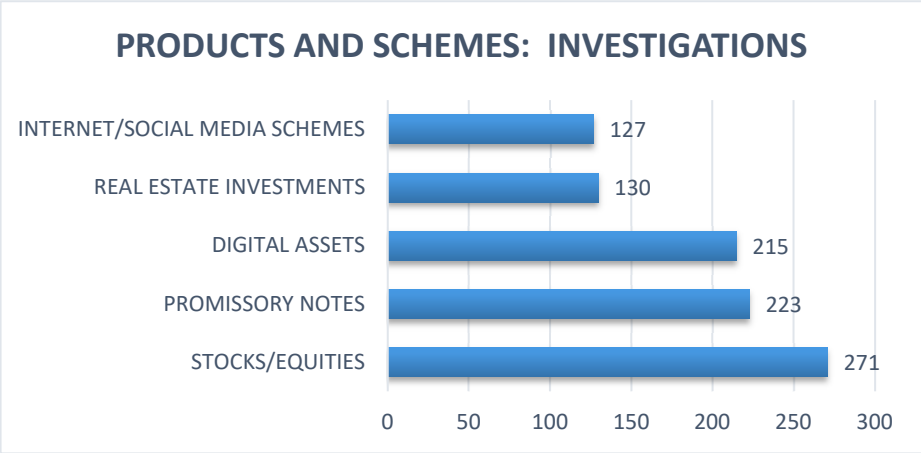


Key Data – Products and Schemes

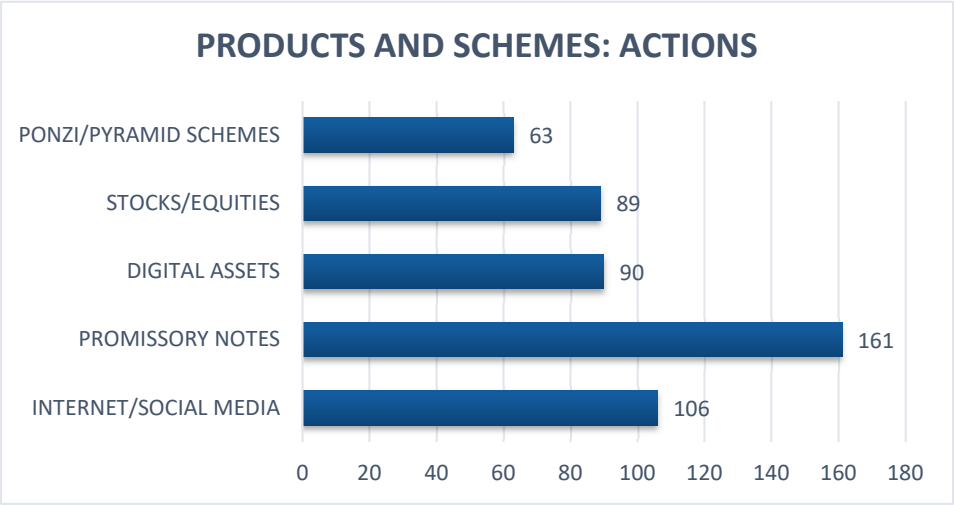
State securities regulators continue to police the market to protect the public. They frequently uncover suspect securities offerings and then conduct investigations and file enforcement actions that typically stop ongoing schemes, secure monetary relief for victims and assess monetary fines against perpetrators. They also often refer cases for the prosecution by local, state or federal prosecutors.

The responses to the latest enforcement survey reflect recent changes in the market. These recent changes include the increasing use of the internet and social media to illegally market products and the leveraging of widespread interest in digital assets to harm the public. This year, members also reported an increase in investigations involving real estate schemes – which may be attributable to economic changes in the markets for land, housing and other real estate.

U.S. members are increasingly investigating suspect securities tied to digital assets. They reported an increase of approximately 70% in their investigations of suspect securities schemes tied to digital assets than the previous year.



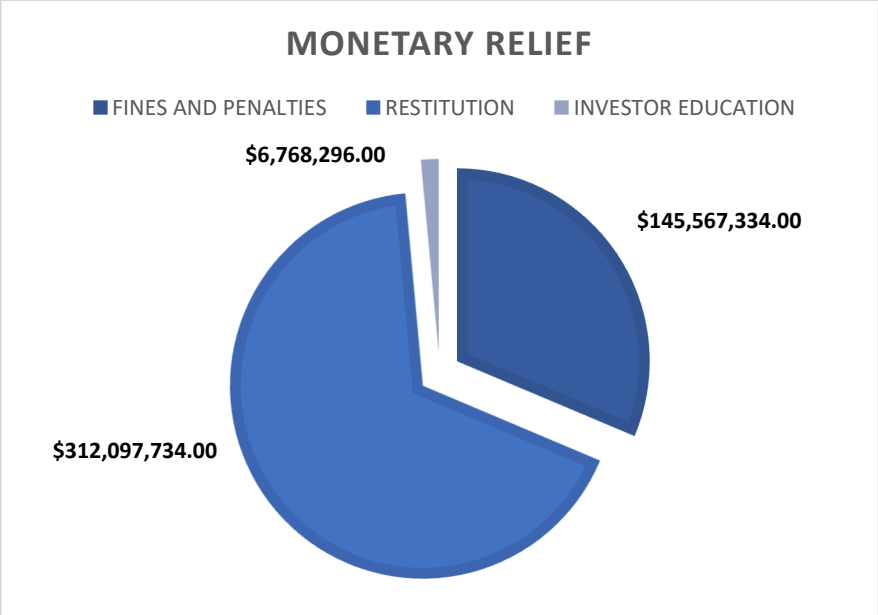
Despite new and ongoing challenges presented by the pandemic, state securities regulators continued to pursue enforcement actions to stop ongoing offerings, prosecute white-collar criminals and protect the public from financial fraud and misconduct. Although these actions involve a variety of products and varying tactics, U.S. members reported more cases involving promissory notes than any other instrument. Promissory notes and other debt instruments that purport to pay a certain return by or before a specified date are often appealing to retail investors as they portray certainty during uncertain times.



U.S. members reported more enforcement actions involving promissory notes than any other products – and it was not even close. Securities regulators also identified schemes incorporating promissory notes as a top threat to retail investors for 2023.

Key Data – Monetary Relief

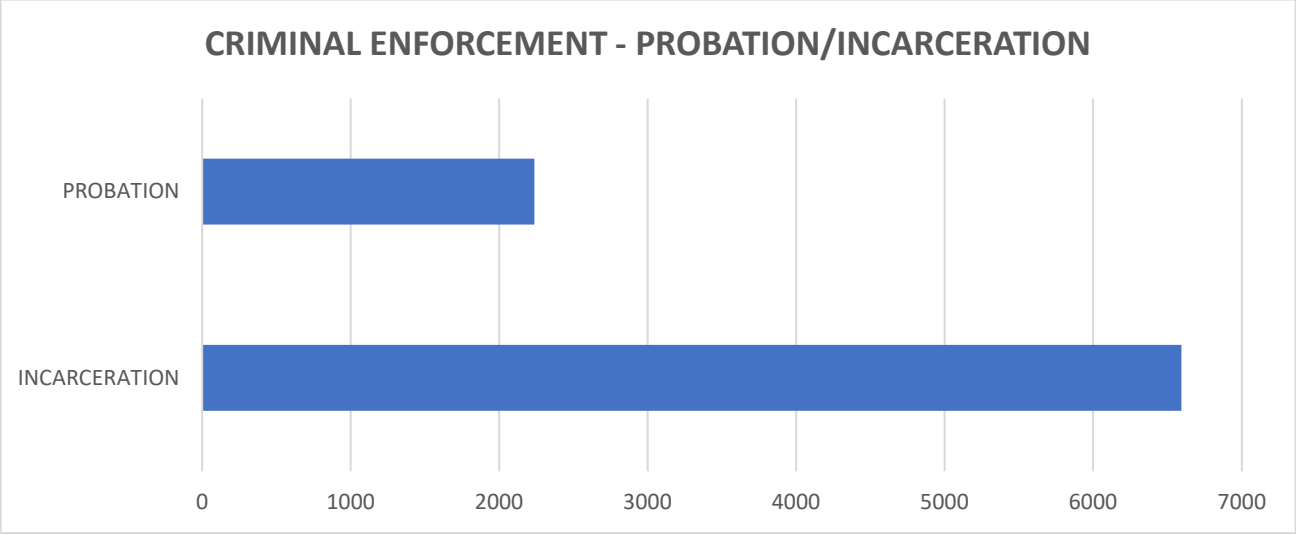
The pandemic limited many traditional investigatory tactics including access to courts and administrative hearings offices. Despite these challenges, state securities regulators were able to obtain restitution and significant monetary relief for victims of financial misconduct and, where appropriate, assessed appropriate fines against parties violating state securities laws and regulations. Their actions also resulted in monetary relief that can be used to cover costs associated with investor education and outreach programs.



Despite challenges stemming from the pandemic, state securities regulators were highly successful in obtaining monetary relief. They obtained more than $145 million in fines – an increase of 313% from the previous year – nearly $312 million in restitution – a slight increase over the previous year – and approximately $4 million for investor education efforts – an increase of more than 50% from the previous year.

Key Data – Criminal Prosecutions

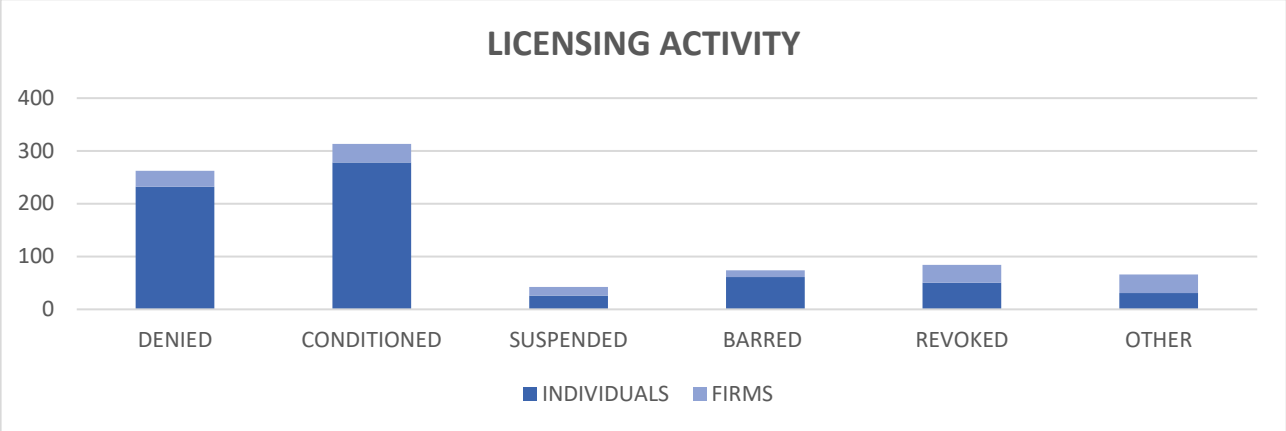
State securities regulators continued to pursue justice for crime victims and hold white-collar criminals accountable for their offenses. Their referrals and prosecutions resulted in dispositions totaling more than 8,831 months (approximately than 735 years), including 6,594 months (approximately 550 years) of incarceration and 2,237 months (approximately 186 years) of community supervision.



Licensing Activity

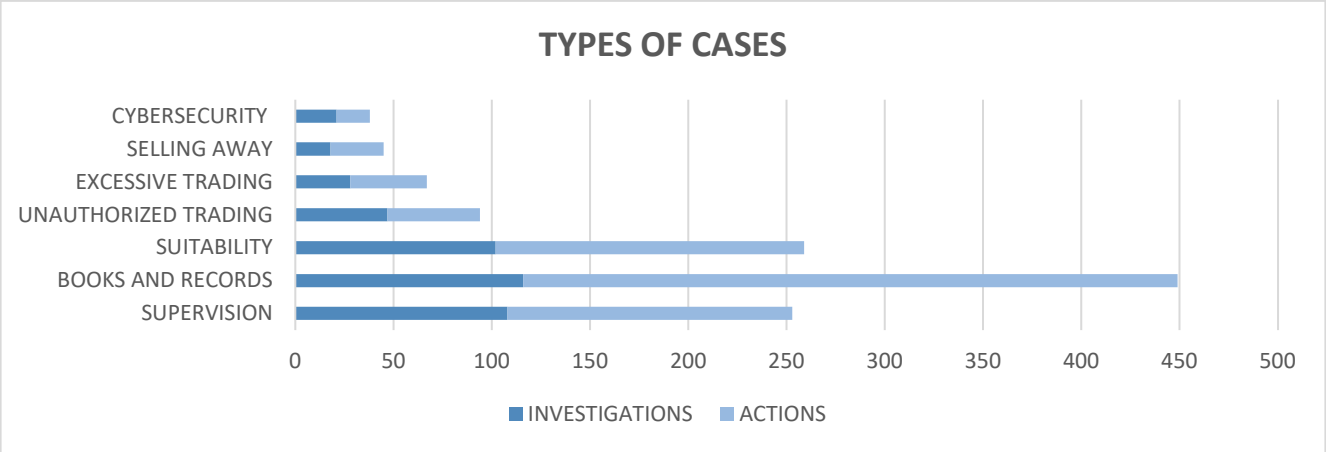
U.S. members are responsible for regulating securities firms and professionals conducting business in their states and with their constituents. They perform a critical gatekeeping function – such as preventing bad actors from entering the industry and barring and revoking licenses for securities professionals engaging in significant misconduct.

In 2021, U.S. members were highly successful in fulfilling their gatekeeper role. They denied 232 applications for licensure (an increase of 76% from 2020), conditioned the approval of 278 applications (an increase of 67% from 2020) and suspended 26 securities professionals (an increase of 13% from 2020). They also revoked licenses of 50 securities professionals and barred 61 individuals from the industry.



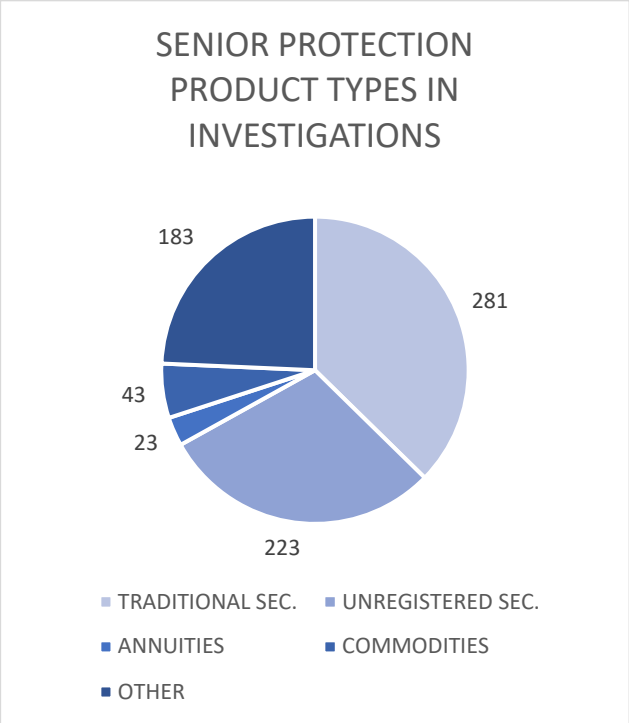
In many cases, applicants withdraw or abandon their applications when confronted with evidence from investigations or to avoid to consequences of enforcement actions. In 2021, 4,880 individuals withdrew their applications – an increase of 53 percent when compared to 2020.

State securities regulators continue to promote compliance by registered firms by taking appropriate steps to identify, investigate and address violations. In 2021, they opened 678 investigations and filed 140 enforcement actions against broker-dealers and agents and opened 478 investigations and filed 267 enforcement actions against investment advisers and representatives. They opened their investigations and filed these actions to address a variety of matters, including 63 actions tied to supervision, 48 actions tied to books and records, 48 actions tied to suitability and 25 actions tied to unauthorized or excessive trading.



Proactively Protecting Older Investors

White-collar criminals and other bad actors often promote investment scams that target older adults. In 2016, NASAA adopted a model law to give states the ability to uncover schemes preying on these investors. The model law, commonly referred to as the NASAA Model Act to Protect Vulnerable Adults from Financial Exploitation, generally requires certain financial services professionals to notify state securities regulators and adult protective agencies whenever they form a reasonable belief of the attempted or actual exploitation of an elderly or vulnerable client. To date, 34 states have adopted some version of the model law.



The NASAA Model Act to Protect Vulnerable Adults from Financial Exploitation quickly proved to be a critical component of senior protection. In 2021, for example, U.S. members reported the receipt of 1,428 reports of suspected exploitation – an increase of 35% from 2020 and 118 percent from 2019 – and opened 356 investigations – an increase of 57% from 2020 and an increase of 98% from 2019. They also filed 54 enforcement actions based on the information provided from financial services professionals.

STATE REGULATOR SECURES RESTITUTION FOR ELDERLY VICTIMS

In 2021, after a contested hearing, Missouri Securities Commissioner David M. Minnick issued an administrative hearing order against Retire Happy, LLC, Julie A. Minuskin and Joshua P. Stoll. It found Retire Happy, Minuskin and Stoll influenced and assisted investors to facilitate rollovers of their retirement accounts from well-known, well-established financial institutions to a relatively unknown and unconventional custodian. Once the rollovers were completed and the investors' retirement account had been liquidated to cash, investors were solicited to reinvest their savings into highly illiquid and highly risky, so-called alternative investments. These were principally unsecured and unregistered promissory notes in fledgling companies. In the end, Missouri investors lost more than $700,000 of their retirement savings in these alternative investments while Minuskin and Stoll pocketed tens of thousands of dollars of investor money through undisclosed commissions and fees. Missouri Commissioner Minnick ordered Retire Happy LLC, Minuskin and Stoll to pay $6.21 Million in civil penalties, in excess of $700,000 in restitution with interest and more than $52,000 in costs.

State securities regulators continued to develop other evidence of investment fraud perpetrated on older investors. In 2021, they fielded 1,320 tips and complaints, opened 605 investigations and filed 304 enforcement actions relating to senior fraud. These statistics also represent an increase in efforts to protect older investors when compared to the information reported for each of the previous two years.

Recent Enforcement Activity – Through the Lens of the Past

On March 10, 1911, Kansas enacted the first state blue sky law. For more than 100 years, state securities regulators have protected investors from illegal and fraudulent investment schemes. Many of the scams that percolated during the early years of securities regulators continue to threaten retail investors. These historic schemes provide context for considering many key recent enforcement efforts.

Through the Lens of the Past – White Collar Crime

Charles Ponzi is synonymous with financial fraud. In fact, one of the most dangerous and prolific scams even bears his name. In 1920, Ponzi began scheming to steal from the public. The actual mechanics of his fraud were rooted in turn-of-the-century economics. Ponzi began raising capital from the public, telling them he was purchasing postal reply coupons in other countries and redeeming them at face value in the U.S. The returns were purportedly lucrative – investors expected a profit of 50% within 45 days or 100% within 90 days. Ponzi, however, was not generating profits through dealings with postal reply coupons and instead paid existing investors with principal obtained from new clients.

In 2021, U.S. members referred 291 cases to state or local law enforcement agencies, an increase of 43% from 2020 and 63% from 2019. They also referred 79 cases to federal law enforcement agencies, an increase of 68% from 2020 and 41% from 2019.

Ponzi was charged, pleaded guilty and sentenced to serve 5 years in federal prison. More than a century after his release, white-collar criminals continue to threaten retail investors. Although their schemes have evolved throughout the years, the key underlying elements remain the same: say whatever needs to be said to separate victims from their money.

SIXTEEN YEAR SENTENCE FOR FRAUDSTER TARGETING ELDERLY, VULNERABLE

Kent Maerki, a 78 year-old resident of Scottsdale, Arizona, was the founder of Dental Support Plus Franchise, LLC, and Janus Spectrum, LLC. He was sentenced to 16 years in prison for his participation in a nationwide investment fraud conspiracy that cost victims over $23 million in total losses. Many of the victims targeted in this scheme were elderly. Unsuspecting investors cashed out 401K retirement plans and other retirement accounts to invest in companies founded by Maerki, without knowledge that significant portions of their principal were being transferred to other companies controlled by members of the conspiracy. As a result, some individual investors - including investors who were blind, disabled, or otherwise unable to return to work - lost hundreds of thousands of dollars from their retirement savings. The total amount of victim losses from this scheme exceeded $23 million, and over $4 million of those fraudulently obtained funds went to Maerki.

U.S. members continue to aggressively investigate and pursue the prosecution of white-collar criminals that steal from retail investors. Some state securities agencies employ sworn peace officers, and a considerable number of regulators are prosecuting securities fraud either through inherent prosecutorial authority or pursuant to appointment from an elected district attorney. In 2021, state securities regulators reported 196 criminal enforcement actions involving 151 defendants, and criminal cases were resolved with aggregate prison sentences of 6,594 years and 2,237 months of community supervision.

Through the Lens of the Past – Promissory Notes

Ponzi was neither the first nor the last con artist to entice victims with the promise of certainty – the payment of fixed returns on or before a fixed date. Although more recent products may vary from instrument to instrument and scheme to scheme, promoters selling illegal or fraudulent promissory notes to investors continue to threaten the public. In 2021 alone, state securities regulators opened 223 investigations involving suspect promissory note offerings and brought 161 enforcement actions involving promissory note schemes that violated state law – and more enforcement actions involved promissory notes than any other type of product. State securities regulators also named promissory notes as a top threat to the public in each of the past three years – and a top overall threat to retail investors in 2023.

Why do fraudsters gravitate to promissory notes? A number of factors are in play, not the least of which is certainty. Promissory notes purport to pay fixed returns to investors on a fixed date – typically independent of volatility in the traditional stock market and changes in the economy – and as such they

RESTITUTION IN REAL ESTATE NOTE SCAM

The Arizona Corporation Commission found Premier Asset Management Group, LLC and multiple individuals defrauded investors with a real estate investment scheme involving unregistered promissory notes. The Commission found Premier Asset Management Group, LLC bought high-end real estate properties to fix up and rent out or sell, funded with notes purchased by investors. The Commission ordered respondents Michael Barry Eckerman, Bernardine Ann Michalik (Shields), Venessa Sandoval, their spouses, and Premier Asset Management Group LLC to pay restitution amounts ranging from $1,460,259 to $4,495,136 and to pay administrative penalties of up to $400,000.

can be attractive to retirees or older investors that prioritize the preservation of their wealth. These elements are as relevant today as they were a generation ago, because in uncertain times, certainty sells.

Through the Lens of the Past – Energy Scams

Long before someone coined the term "Bitcoin millionaire," promoters of energy scams weaved enticing tales of early retail investors obtaining unimaginable returns from energy deals. They played on the intersection of "black gold" and the "blue sky," claiming they were affording retail investors the opportunity to secure their financial futures by participating in lucrative ventures typically reserved for the elite. And they are still conjuring these images, pitching not only traditional oil and gas investments but also products tied to solar power, electric vehicles and other uses of green energy.

Recent Enforcement Activity – The Perspective of the Present

For more than a century, U.S. members have worked to protect the investing public from fraud and deceit. Their efforts are increasingly challenged by bad actors that are now able to leverage advances in technology to conceal financial misconduct and broadly perpetrate fraudulent schemes. These powerful tools now fuel new scams while also increasing the scope and gravity of traditional frauds.

OIL PROMOTER SENTENCED TO 121 MONTHS IN FEDERAL PRISON

Former registrant and oil promoter Brian Keith Alfaro was sanctioned by regulators and expelled from the industry. He was also sued by defrauded investors and later put his oil investment company in bankruptcy. Despite the bankruptcy filing, the victims later won a judgment of approximately $8 million against him

Following an investigation by the Texas State Securities Board and the FBI, Brian Alfaro was indicted and tried in federal court. The jury found him guilty of seven counts of mail fraud in connection with defrauding investors in an oil and gas investment scheme. The evidence showed Brian Alfaro used their funds to further an extravagant lifestyle – including the purchase of a Lamborghini and season tickets for the San Antonio Spurs. He was recently sentenced to serve 121 months in federal prison.

Within days of the sentence, the Texas Securities Commissioner entered an emergency cease and desist order to stop Kristi Alfaro and their children, accusing them of promoting investments in an illegal and fraudulent wildlife breeding and development program to elderly investors.

The Perspective of the Present – Internet and Social Media Schemes

For many decades, scammers have used various forms of media to broadly market financial frauds to new victims. Historically, they relied on advertisements carried in newspapers and magazines, promotions broadcast on local radio stations, pamphlets sent through the mail and unsolicited telephone calls. Although bad actors used these marketing tactics to reach many potential clients, their efforts were ultimately limited by costs associated with marketing, the scope of distribution, the range of broadcast and various technological barriers that restricted the breadth of their promotions.

In 2021, state and territorial regulators opened 127 investigations of suspect securities offerings marketed through the internet and social media. They also filed 106 enforcement actions against promoters using the internet and social media to market scams – an increase of 22% from 2020 and 74% from 2019.

Advances in technology have removed many of these barriers and changed the way scams are marketed to the public. Financial fraudsters no longer need to rely on print media, radio promotions and cold calls to fraudulently market securities. Instead, they are capitalizing on the rapid growth in technology including expanded access to the internet, development of smartphones, proliferation of social media, and availability of inexpensive voice and text messaging platforms. They can now shatter geographic boundaries and broadly reach many different demographics - from Baby Boomers and Generation X-ers connecting on Facebook and watching videos on YouTube to Millennials and Generation Z-ers scrolling through TikTok and communicating through Snapchat.

Although the internet and social media provide a new pathway for perpetrating scams, bad actors are also using new technologies to create more immersive and realistic frauds. They are able to readily spoof email addresses, easily create professional websites that foster legitimacy, and profit from the use of malicious applications.

ONLINE DATING APPLICATIONS

It's not just traditional social media – dating applications have led to a rise in romance schemes. For example, the Oregon Division of Financial Regulation recently entered a cease-and-desist order against Abiodun Ogundipe, DBA Focus Automobile, and Bunsunad LLC for serving as intermediaries in a securities fraud case. The order accused them of meeting an elderly widow through an online dating application and accused them of persuading the victim to invest $126,000 in an offshore mining scheme. According to the order, the scheme incorporated "money mule" aspects, whereby parties concealed the flow of funds and used principal to purchase unrelated goods and foreign currency.

The Perspective of the Present – Impersonation Schemes

State securities regulators have also recognized a rise in schemes where promoters use tactics to falsely assume the identity of a bona fide registered securities professional. These cases are on the rise. In 2021, state and territorial regulators opened 20 investigations of impersonation schemes – up 15% from the 13 cases opened in 2020 – and filed 6 enforcement actions against these scams.

Many recent impersonation schemes incorporate Central Registration Depository (CRD) Numbers. CRD Numbers are unique identifiers assigned to securities firms and professionals. These identifiers are important for securities regulation and are also commonly used by investors to conduct due diligence. For example, investors can use a CRD Number to query an online platform such as BrokerCheck to check the background of an investment professional. The platform associates the CRD Number with a real person, and it can thereafter confirm whether the person is registered to sell securities and provide any disciplinary actions brought against the person.

STATE STOPS CRYPTO IMPERSONATION SCHEME

The AZ Corporation Commission ordered Abuchi Okoye of Nigeria and his affiliated company Coininvest to pay $2,500 in restitution and a $25,000 administrative penalty for committing securities fraud in connection with cryptocurrency and other alternative investments.

In its default order, the Corporation Commission found Okoye and Coininvest sold the cryptocurrency and other alternative investments under the pretense of being Arcadia Capital, LLC and Arque Capital, LTD, two Arizona securities dealers registered with the Commission's Securities Division. The actual Arizona businesses have no relationship with or connection to Okoye and Coininvest.

State and territorial regulators are increasingly investigating cases where these bad actors are also incorporating the CRD Number of a real person in their schemes. They are providing investors with real CRD Numbers assigned to unaffiliated registered agents, and investors are using these real CRD Numbers to conduct due diligence. Their independent research will likely reveal the CRD Number is assigned to a person who is, in fact, registered to sell securities. An investor who does not learn the CRD Number is assigned to a registered agent unassociated with the scammer may incorrectly conclude the scammer is actually licensed and has not been subject to discipline.

The Perspective of the Present – Precious Metals Schemes

Bad actors are using contemporary macroeconomic factors – such as volatility in the markets and federal monetary policy – as a tool to more effectively market traditional scams. For example, in recent precious metals scams, many promoters have been using deception and emotion to prey on financial fear. They often use headlines to stoke further fear and concern over the potential adverse impact on retirement savings. On

The tactics have proven effective. In 2021, state and territorial regulators opened 95 cases involving suspect precious metals schemes, a 12% increase from 2020 and an 84% increase from 2019. They also filed 14 enforcement actions against promoters of precious metals schemes – an increase of 4% from 2020 and 133 percent from 2019.

the other hand, they have been using deception and emotion to sell hope, claiming concerned investors can prevent wholesale losses by liquidating equities and using the proceeds to purchase precious metals.

U.S. members are working together, coordinating their efforts to shut down nationwide scams and address significant misconduct. They are also joining with the Commodity Futures Trading Commission (CFTC) and filing joint enforcement actions to ensure the protection of investors throughout the nation. In 2020, for example, 30 state securities regulators and the CFTC obtained injunctive relief and a receivership against TMTE Inc. aka Metals.com in the Northern District of Texas. The complaint pleaded grave facts - the company and affiliated defendants used traditional and social media marketing to lure more than 1,600 investors, including at least 1,300 elderly victims, in a scheme that involved more than $140 million in retirement savings. It also alleged virtually every investor lost the majority of their funds.

More recently, in 2021, state securities regulators began investigating Safeguard Metals LLC and Jeffrey Santulan, its principal. Earlier this year, the California Department of Financial Protection and Innovation, along with 26 state securities regulators and the CFTC, filed a federal lawsuit against Safeguard, Santulan and related parties in the Central District of California. The complaint alleged the firm preyed on fear, creating a sense of urgency and encouraging prospective clients to remove their savings from the stock market to avoid significant loss. It also allegedly advised clients to liquidate their traditional retirement accounts and transfer the proceeds into self-directed IRAs to purchase coins that were marked-up as much as 71 percent. More than 450 mostly elderly retail investors were victimized by the scheme, according to court filings.

Recent Enforcement Activity – The Vision of the Future

Science fiction and popular culture once created visions of utopian societies free of crime and war, with humans conquering poverty and famine and residing in lavish homes in futuristic cities. Having already mass-produced hoverboards and flying cars, fantasy tropes revealed a future where civilization turned its eyes to the next frontier: traveling through space and building new cities on distant planets. These achievements were often fueled by technological advances that made the impossible seem inevitable.

Although many of these concepts have yet to materialize, remarkable advances in technology are quickly adding futuristic elements in the financial markets. The future, it seems, is now.

The Vision of the Future – Digital Assets Tied to Securities

In late 2008, an anonymous person or group of persons acting under the pseudonym Satoshi Nakamoto published a white paper introducing Bitcoin – the first and arguably most popular modern cryptocurrency. Although Bitcoin and other cryptocurrencies initially traded in relative obscurity, state regulators quickly recognized that white collar criminals and other bad actors could leverage cryptocurrencies to perpetrate high-tech fraudulent securities schemes.

Although many legitimate firms are adopting blockchain technology, bad actors are increasingly using investments tied to digital assets to threaten the public. Based on inquiries, complaints and investigations from state and territorial securities regulators, digital assets ranked 9th among threats in 2019, 2nd in 2020 and 1st in 2021. State regulators also identified scams tied to cryptocurrencies and digital assets as the top threat to investors in 2022.

Nearly a decade ago, NASAA began warning investors about cryptocurrency investment scams. In 2017, as the market for initial coin offerings caught fire, state securities regulators filed their first enforcement action to stop an illegal digital asset investment scheme. The next year, NASAA launched Operation CryptoSweep, an international task force consisting of members from more than 40 US and Canadian agencies. The task force worked to uncover and stop fraudulent investment schemes tied to cryptocurrencies – acting proactively, before firms were broadly able to recruit investors. Operation CryptoSweep resulted in more than 330 inquiries and investigations and led to the filing of more than 85 enforcement actions.

Despite the complexity of the products and unique investigatory challenges, state securities regulators have been leaders in taking on the biggest and most dangerous cryptocurrency investment frauds. For example, in 2017, state regulators began investigating BitConnect, a promoter of an international cryptocurrency trading and staking scheme. BitConnect employed multilevel marketing tactics to fuel an aggressive sales program that broadly recruited many retail investors. Its marketing tactics proved highly effective, as increasing demand drove the price of BitConnect's native token from around $0.17 per coin at the beginning of 2017 to more than $463.00 per coin in late 2017 and the firm's market capitalization skyrocketed to more than $2.6 billion. State securities regulators – again acting proactively prior to receiving complaints from victims – began investigating BitConnect and quickly uncovered evidence proving BitConnect was perpetrating a massive fraud. In early 2018, they coordinated their filing of enforcement actions to stop the scam and prevent the firm from recruiting new victims. The enforcement actions proved highly effective – within days the scheme collapsed and shortly thereafter the native token became virtually worthless. In late 2021, nearly four years after states filed their cases, the SEC filed its enforcement action against BitConnect and in early 2022 the DOJ indicted the founder of the scheme.

More recently, state securities regulators began coordinating their investigations of unregistered firms offering investments similar to traditional depository accounts promoted by regulated banks. However, instead of tendering fiat currency, investors transfer digital assets to the depository account. The issuers thereafter use the digital assets to generate revenue from various transactions, such as lending the digital assets to third-party borrowers. The revenue is then used to pay interest to depositors upon withdrawal of their tokens. The promised rates of interest are typically significantly greater than yields earned through accounts maintained at regulated banks – often as high as 10 or 15 percent or more per annum.

In 2020, a coordinated team of state regulators began investigating BlockFi Lending LLC, and parties affiliated with the company. The investigation revealed that BlockFi was promoting digital asset interest accounts. It also revealed that as many as 570,000 investors – including nearly 400,000 investors from the United States – may have invested more than $10 billion in the firm's cryptocurrency depository accounts. State regulators ultimately filed coordinated enforcement actions against BlockFi, alleging the investments in the depository accounts constituted securities, the firm was not registered to sell securities and it had not registered its depository account program with state agencies. State regulators also accused the firm of violating registration statutes and failing to provide critical information to investors relating to the risks associated with the depository account program.

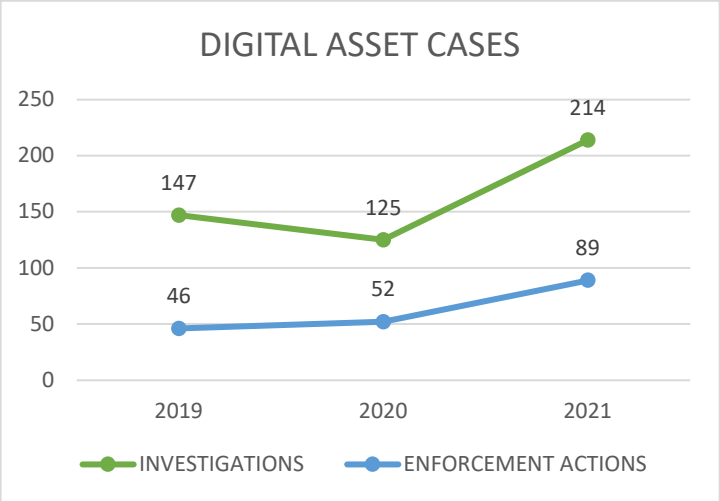
In 2022, state regulators settled the case with BlockFi. The settlement required compliance with applicable securities laws while ensuring the protection of investors. BlockFi immediately stopped offering unregistered depository accounts to the public, represented it intended to comply with state and federal registration requirements, and agreed to pay a fine of $50 million to state agencies. The SEC joined state regulators and also secured a settlement on similar terms with BlockFi.

Investor protection relating to digital asset depository accounts did not end with the settlement with BlockFi. State regulators have been and are continuing to coordinate their efforts to address misconduct by other firms accused of illegally promoting similar unregistered digital asset depository accounts. For example, state regulators have been coordinating investigations and enforcement actions against Voyager Digital LTD, Celsius Network, Inc., and various parties affiliated these firms. Both cases involve highly complex transactions and allegations of widespread misconduct – state regulators accused Voyager of receiving more than $5 billion for more than 1.5 million unregistered depository accounts and Celsius of raising more than $12.5 billion from more than 350,000 domestic and international clients. Although Voyager and Celsius recently filed for protection under federal bankruptcy statutes, states are continuing to advocate for investors in the bankruptcy proceedings and working to address the illegal activity.

UNSTABLE STABLECOINS

Stablecoins are purportedly "stable" cryptocurrencies because they are supposed to maintain a real-dollar value. However, the New York Office of the Attorney General accused iFinex — the operator of Bitfinex — and Tether of making false statements about the backing of the "tether" stablecoin. The statements allegedly related, at least in part, to overstating reserves and hiding approximately $850 million in losses. In February 2021, the NY AG settled the claims with iFinex, Tether and related entities. The agreement required them to cease trading activity with residents of New York, pay $18.5 million in penalties and take steps to increase transparency.

Source: Attorney General James Ends Virtual Currency Trading Platform Bitfinex's Illegal Activity in New York, Press Release, New York State Office of the Attorney General, February 23, 2021.



Digital asset depository accounts represent only one of many new products tied to digital assets. The market for investments incorporating cryptocurrencies continues to evolve, and state securities regulators are working to promote confidence in this new market while ensuring legitimate firms embracing blockchain technology can lawfully raise capital from the public. At the same time, state securities regulators are serving as the first, and often the last, line of defense for protecting retail investor from illegal and fraudulent schemes tied to cryptocurrencies.

The importance and sheer volume of the work cannot be understated – in the most recent reporting year, state regulators opened 215 investigations of parties suspected of illegally or fraudulently offering securities relating to digital assets, an increase of around 70 percent from the previous reporting year. They also filed 89 enforcement actions against firms accused of misconduct involving products incorporating digital assets, an increase of 43 percent over the past year and 100 percent over the past two years.

The Vision of the Future – The Metaverse

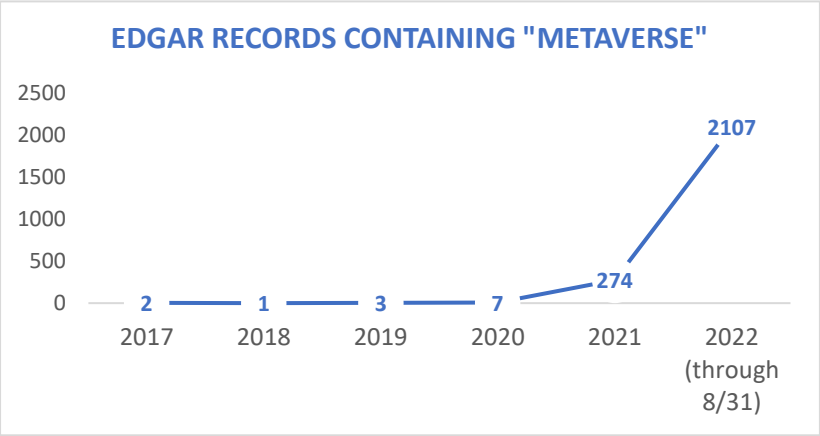
Science fiction introduced concepts of flying cars, jet packs, hover boards, teleportation devices, time travel and spaceships that permit interstellar travel to strange new worlds. Although technology advances at a rapid pace, consumers still typically commute on paved roads, hover boards have not replaced skateboards, time travel has not defeated the passage of time and teleportation is largely limited to movies, comic books or movies adapted from comic books. Now, however, we can instantaneously travel to strange new worlds thanks to the metaverse.

What is the metaverse? The term, first coined in 1992 by science fiction author Neal Stephenson in the novel *Snow Crash*, generally refers to one or more interconnected virtual worlds that promote interactivity, entertainment and commerce. Users can now readily access these virtual worlds with minimal technical expertise and standard office equipment such as a computer, keyboard, mouse and internet connection.

What happens after entering the metaverse? Users do not physically enter metaverses. Instead, they interact through digital representations of themselves, referred to as avatars, and socialize with others, play games, shop for digital assets, attend concerts, drive virtual cars or even work in artificial environments. Metaverses are becoming increasingly popular as corporations continue to invest in augmented realities and new technologies increasingly intersect with movies, video games, and popular culture.

> *"Wherever there is excitement around a new industry or technology, fraudsters are bound to flock. The metaverse is no different. The lack of regulation in the metaverse and the ability to operate from anywhere in the world make it easy for fraudsters to hide their schemes. In addition, security lapses on developing platforms and the ability to build fake metaverse experiences can lead to hacks, fraud, or the theft of users' funds."*
>
> *- NASAA Informed Investor Advisory: The Metaverse, August 2022*

State securities regulators are uniquely positioned to identify changes in the markets that impact retail investors, and as such they were able to quickly recognize the securities markets are beginning to embrace the concept of the metaverse. For example, many legitimate, established companies are developing virtual storefronts, creating interoperable assets and designing hardware and applications tied to the metaverse. Financial services firms – including registered dealers and accounting firms – are no exception. These financial service firms have been purchasing plots of virtual land and constructing virtual offices, and they are now promoting services in the metaverse and creating products that afford investors the opportunity to increase financial exposure to the metaverse. As demonstrated through securities filings, the embracement of the metaverse is a very new, very recent phenomenon. Over the past five years, parties have filed 2,391 records with the SEC referring to the metaverse. More than 2,100 of these 2,391 records were filed in 2022, meaning that almost all of these securities filings referring to the metaverse were submitted within the nine months preceding this report.



Although many legitimate firms are involved in the development of the metaverse, bad actors may be able to use the new technology to more effectively conceal their identities, launder money, market and sell illegal goods and impersonate trustworthy parties. Moreover, fraudsters are now leveraging widespread interest in the metaverse to promote illegal securities offerings and deceive retail investors.

State regulators are leading efforts to stop financial misconduct tied to the metaverse. In April 2022, for example, members coordinated and filed the first securities actions to stop a fraudulent metaverse securities offering. The case was filed against Sand Vegas Casino Club, an issuer of unregistered NFTs that allegedly served as high-tech digital equivalents of traditional equities. The NFTs purportedly provided purchasers with an ownership interest in a metaverse casino and the right to share in the profits of the metaverse casino – including profits derived from virtual gambling and the sale of digital assets representing drinks and cigarettes. The profits were purportedly lucrative, as the respondents allegedly represented purchasers of NFTs could earn between $102 and $6,750 per NFT per month or $1,224 to $81,000 per NFT per year. The state actions accused the firm of violating state registration requirements and concealing material information from purchasers.


FROM FLAMINGO CASINO CLUB

State regulators later filed enforcement actions to stop Flamingo Casino Club from illegally and fraudulently offering securitized NFTs to the public. The actions alleged the NFTs provided purchasers with ownership of a different metaverse casino and the right to share in profits from this metaverse casino. The actions also accused Flamingo Casino Club of engaging in a complex scheme to conceal the true nature of its operation – that the issuer was secretly operating from Moscow and that it originated the scheme around the time Russia invaded Ukraine.

Although international digital asset schemes are inherently complex, states effectively shut down Flamingo Casino Club's fraudulent offering and protected the public from further harm. At the time of the state actions, Flamingo Casino Club was offering 11,111 securitized NFTs to the public. States brought their actions on May 11, 2022, and at that time the issuer had already sold around 42 NFTs to around 33 purchasers. Since the entry of the state actions, Flamingo Casino Club has not sold any of the remaining 11,069 NFTs.

Canadian Enforcement

NASAA's Canadian members recently issued the Canadian Securities Administrators' (CSA) 2021-2022 Enforcement Report. The CSA report highlights the work of provincial securities regulators and their actions to detect, disrupt and deter wrongdoing and hold securities law violators accountable. The report is accessible at the CSA website, and the following table summarizes key data from the report.