Written Testimony of Amanda Senn

Alabama Securities Commission Chief Deputy Director and NASAA Cybersecurity Committee Chair

On behalf of

The North American Securities Administrators Association

June 16, 2020

United State House of Representatives

Committee on Financial Services

Subcommittee on National Security, International Development and Monetary Policy

"Cybercriminals and Fraudsters: How Bad Actors Are Exploiting the Financial System During the COVID-19 Pandemic"

I. Introduction

Good Morning, Chairman Cleaver, Ranking Member Hill, and members of the Subcommittee. My name is Amanda Senn, and I am the Chief Deputy Director of the Alabama Securities Commission and Chair of the Cybersecurity Committee for the North American Securities Administrators Association ("NASAA").[1] I am honored to testify before the Subcommittee today on behalf of NASAA about how cybercriminals and fraudsters are exploiting the financial system amid the COVID-19 pandemic.

In the United States, state securities regulators have protected Main Street investors for more than 100 years, longer than any other securities regulator. As the regulators closest to your constituents, with an office in every state, we are on the frontline of investor protection. My colleagues and I are responsible for enforcing state securities laws, including investigating complaints, examining broker-dealers and investment advisers, registering certain securities offerings, and providing investor education programs to your constituents.

States are leaders in civil and administrative enforcement actions, as well as criminal prosecutions of securities violators. Our most recently compiled enforcement statistics reflect that in 2018 alone, state securities regulators conducted 5,320 investigations, leading to more than 2,000 enforcement actions, including 218 criminal actions. In 2018, NASAA members reported enforcement actions involving 758 senior victims. Older Americans are a major target of fraudsters and are particularly vulnerable during this crisis due to the nature of the COVID-19 pandemic.

States also continue to serve a vital gatekeeper function for our capital markets by screening out bad actors before they have a chance to conduct business with unsuspecting investors. In 2018, a total of 4,551 securities license applications were withdrawn because of state action, and an additional 1,032 licenses were either denied, revoked, suspended, or conditioned.

Our focus is on protecting retail investors and history has shown us that opportunistic fraudsters will use COVID-19, as much as they have used other crises, to fleece mom and pop investors. Moreover, state securities regulators have a long history of not only working together with one another but also working alongside our federal counterparts and industry self-regulatory organizations to stop frauds and educate investors.

As I will detail in my testimony, acting within the framework of NASAA, state securities regulators are undertaking decisive action aimed at anticipating and shutting down frauds related to the COVID-19 pandemic and the resulting economic uncertainty. Specifically, NASAA has formed a COVID-19 Enforcement Task Force ("Task Force"), consisting of state and provincial securities regulators, to identify and stop potential threats to investors that arise from the COVID-19 crisis. This initiative is being led by NASAA's Enforcement Section Committee and includes more than 100 investigators from the vast majority of member jurisdictions. The Task Force is using online investigative techniques to identify websites and social media posts that may be offering or promoting fraudulent offerings, investment frauds, and unregistered regulated activities.

II. State Securities Regulators and the Protection of Retail Investors from Fraud

State securities regulators routinely take aggressive actions against a wide variety of actors. From fraudsters engaged in Ponzi or pyramid schemes to companies who mislead investors our

[1] The oldest international organization devoted to investor protection, NASAA was organized in 1919. Its membership consists of the securities administrators in the 50 states, the District of Columbia, Canada, Mexico, Puerto Rico and the U.S. Virgin Islands. NASAA is the voice of securities agencies responsible for grass-roots investor protection and efficient capital formation.

message is simple – if you rip off or defraud investors, we will act. Whether acting independently or collaboratively, such as through the NASAA enforcement framework or in conjunction with our federal regulatory partners, state securities agencies have a long history of pursuing enforcement actions that affect not only the residents of our individual states, but also the citizens of our nation as a whole. Moreover, state securities regulators are uniquely well positioned to protect investors by undertaking proactive measures, in addition to reactive measures, to police the securities markets.

Enforcement and Investor Protection

State securities agencies are usually more nimble than our federal counterparts. Upon identifying a problem, we can move quickly to halt ongoing investment frauds using a range of civil and administrative remedies. The cases we bring can involve localized conduct to practices that harm investors across the country. Notable examples of some of the enforcement actions where the states have led the way to address violative conduct involving a large number of investors and large losses include: the securities fraud investigation of Prudential Bache Securities in the 1980s; the 2003 investigation of sell-side research analysts' conflicts of interest; abusive market timing practices by mutual fund investment advisers, which gave an unfair and illegal advantage to hedge funds and other large entities at the expense of retail investors; and the post-2008 financial crises cases involving subprime mortgage-backed securities and auction rate securities, which resulted in billions of dollars being returned to investors as a result of wrongful conduct.[2]

As pointed out in the preceding examples, states have been and will continue to be active in a broad range of cases, especially those involving investors in our communities. Indeed, while our mission aligns with that of our federal counterparts, the primary focus of state securities enforcement is on the needs of *retail* investors. State securities regulators are well-suited for this mission because of our geographical and societal nexus to the individuals we serve. Moreover, state securities regulators are able to cultivate relationships and partnerships with local criminal authorities and are often able to achieve justice through criminal channels in cases that U.S. Attorneys may be unable to bring due to limitations on resources and directives governing the allocation of those resources.[3] State securities regulators are highly skilled and adept at investigating and prosecuting misconduct. They capably represent the public they serve, and no complaint is too small.

Moreover, in Alabama our office has criminal authority and can work criminal cases from start to finish to ensure fraudsters are swiftly and appropriately punished. Financial crimes can be devastating and having the authority to seek justice on behalf of victims is an honor and a privilege that I have never taken for granted. Too often, smaller cases are overlooked, passed over, or fall through the cracks. But in our local offices, we are better able to serve your constituents because they are our friends and our neighbors. And what may be considered a small loss to some is a devastating loss to the person suffering it. Thus, it is oftentimes in these cases that the state securities regulator discovers true meaning in his or her work, for the victim has nowhere else to turn.

Protecting Investors in the Digital Age

[2] In Alabama alone, the repurchase of auction rate securities resulting from this action totaled $1.3 billion, saving Alabamians from defaulting on home loans, ruining their credit, and allowing them to pay their bills.

[3] Likewise, FINRA is a national self-regulatory organization where decisions are not necessarily made at the grass roots level but through a hierarchy where the focus is often on systematic issues rather than individual violations. Moreover, FINRA's jurisdiction does not extend to unlicensed individuals. While state securities regulators often partner with the SEC and FINRA, and achieve great results, many cases are outside the jurisdiction of or do not meet the threshold criteria for evaluation from either organization.

The proliferation of technology has changed much about the ways in which we are solicited for investments, manage those investments, and communicate with the companies and individuals who handle those investments. Unfortunately, fraudsters are evolving with technology, and the methods by which they prey on investors are rapidly increasing. The digital world presents numerous and complex obstacles to investigations and prosecutions – from the growing number of actors and schemes, to challenges in identifying online perpetrators and collecting evidence in a forensically sound manner. These challenges pose significant hurdles for regulators who must adapt quickly to the ever-changing landscape of online fraud.

For example, in early June my office received three separate reports pursuant to Alabama's Protection of Vulnerable Adults from Financial Exploitation law, a NASAA model law enacted in Alabama in 2016, which indicated individuals were victims of an online financial fraud scheme. According to the three reports detailing the scheme, the victims had visited the webpage of a reputable online broker to review or access their accounts and discovered that they were unable to login. Upon their attempts, they received a screen with a "help" button. The individuals each reported that they clicked on the button and were instructed to call a "1-800" number. The victims called the number and the individual who answered the phone told the victims that the broker's website was down because "5G towers were being placed in California." That person then instructed the caller to log into his account with information that was provided by the suspect. The victims logged in as instructed and shortly after the victims reported that wire transfers were initiated from their accounts to various banking institutions, some overseas. During an interview with the firm last Friday, our case agent learned that attempted wires from the brokerage accounts held by the firm exceeding $2.6 million had been initiated by the fraudsters and that $1.2 million had already been stolen. At this time, it is believed that malware was responsible for redirecting the victims from the legitimate webpage of the broker-dealer to a fraudulent knock-off site. To date, 84 victims nationwide have been impacted, but the numbers are rising. Our interview confirmed that the majority of these victims were ages 60 or older.

At one time, this crime would have been likely perpetrated by a person that local authorities could readily identify, such as a person that the victim may have trusted and/or known in the community. Records could have been obtained memorializing any agreement between the two regarding the investment, subpoenas and/or search warrants could have been issued to gather documents that were not readily available, and the identity of the suspect most likely would have been known or could have easily been discovered. In other words, physical evidence of the crime, sufficient to prosecute, could have been collected with relative ease. In the digital age, prosecutors are confronted with numerous evidentiary challenges which, given limited resources, make it exceedingly difficult to investigate, much less, prosecute, these cases. Cyber criminals have an obvious advantage in that they can remain concealed and anonymous.

NASAA members recognize the constraints on investigating and prosecuting cybercrimes and, moreover, the reality that victims may never recover their losses. Thus, states are dedicating resources to more proactive measures. Here, the goal is to stop the fraudsters from victimizing our residents by identifying emerging risks to deter, reduce, and fight them before they become problems.

The COVID-19 Pandemic has Baited the Hook for Fraudsters

Predicting the latest fraud is sometimes simple; just look at the issues of the day. Fraudsters trade on natural disasters, economic crises, and tragedies to push their schemes. They exploit systemic issues at times when investors are most susceptible to fears such as outliving their money or missing out on the next big investment opportunity. This pattern is familiar to regulators as we have seen plenty

of examples such as the waves of fraud during the dot.com bubble of the 1990s, the post-2008 financial crisis, and the creation and evolution of cryptocurrencies. Today, of course, we have COVID-19.

The pandemic coupled with dramatic volatility in the markets has brought loneliness due to social isolation and concerns for financial security. This is likely the reason that my colleagues and I have seen a significant uptick in the number of financial exploitation cases over the past two months.

To date, dozens of reports of fraud related to the Pandemic have come across my desk. From investments purporting to develop vaccines and other pharmaceutical treatments, to investments with a charitable component falsely claiming to help those affected by COVID-19, these frauds are myriad and run the gamut.

Elderly Investors May be Especially Vulnerable Targets

Sadly, and especially during the COVID-19 pandemic, many seniors are spending time in isolation to protect themselves from infection. Friends and family who may have visited regularly are unable to spend time with them. Many seniors have turned to the Internet as a social outlet and have become heavily reliant on online services for shopping, banking, and the initiation of electronic payments that may have otherwise been paid in person. With many seniors in isolation, friends and family are unable to physically check in and are not able to notice the sometimes small but important changes in behavior that could indicate a person is susceptible to fraud or worse, is being victimized.

In January 2016, NASAA created and approved the Model Act to Protect Vulnerable Adults from Financial Exploitation, or "Model Act," which provides for reporting of suspected financial exploitation to regulatory agencies and allows firms and advisers to enlist the assistance of state securities regulators to review potential red flags of fraud.[4] In this area, in particular, state securities regulators have partnered with the industry to help protect seniors from being financially exploited. The Model Act has been enacted in 27 jurisdictions, with more considering legislation. As a result of this law, states have seen increased reports of financial exploitation, many of which might not have otherwise been brought to light. In the past several months, I can report that in Alabama these cases have tripled and most of the reports allege that a cybercriminal is the suspect.

NASAA's COVID-19 Enforcement Task Force

On April 28, 2020, NASAA announced the formation of the COVID-19 Enforcement Task Force ("Task Force"), consisting of state and provincial securities regulators, to identify and stop potential threats to investors stemming from the COVID-19 pandemic.[5] Modeled after NASAA's successful Operation Cryptosweep,[6] the new initiative is being led by NASAA's Enforcement Section Committee.

The objective of the Task Force is to disrupt, discourage and deter fraudulent or illegal activities which pose threats to investors before significant losses occur. With these goals in mind, the NASAA membership quickly organized and coordinated this large-scale effort. Instructional webcasts

[4] Additional information about the NASAA Model Act, including legislative commentary for the 2020 State legislative session, is accessible at: http://serveourseniors.org/wp-content/uploads/2020/01/NASAA-Model-Act-Updated-Commentary-for-2020-Session-012820.pdf.

[5] *See:* https://www.nasaa.org/54844/nasaa-forms-covid-19-enforcement-task-force/?qoid=current-headlines.

[6] In April 2018, NASAA organized a task force of its member state and provincial securities regulators to begin a coordinated series of investigations into ICOs and cryptocurrency-related investment products. As part of its work, the task force identified many cryptocurrency-related products and hundreds of ICOs in the final stages of preparation before being launched to the public. These pending ICOs were advertised and listed on ICO aggregation sites to attract investor interest. The work of the task force yielded hundreds of investigations and scores of enforcement actions. Additional information about Operation Crypto sweep is accessible at: https://www.nasaa.org/policy/enforcement/operation-cryptosweep/.

and tutorials on the details of the operation and logistics were provided to participating jurisdictions. Members share resources and assign tasks according to areas of expertise. The Task Force is presently using online investigative techniques to identify websites and social media posts that may be offering or promoting fraudulent offerings, investment frauds, and unregistered regulated activities.

Importantly, the emphasis of the Task Force is on *proactively* protecting investors against fraud through the broad dissemination of enforcement orders, notices, and warnings. By preemptively identifying and uncovering fraudulent conduct that could result in investor losses, the Task Force can expose or discredit the perpetrator to prevent the public from becoming a victim of fraud. In cases where it is discovered that victims have already fallen prey to the fraud, enforcement actions have and will continue to be instituted, and through coordination with internet service providers and/or social media platforms, websites, posts, threads, and advertisements are being dismantled or removed. In other words, not only are we "poisoning the well," we are also able to shutter it and prevent the broad solicitation of their fraudulent offerings. During the project, as fraudulent activity and conduct is identified, NASAA members throughout the United States, Canada, and Mexico are engaged in media campaigns to promote public awareness of the schemes and investor education.

Currently, 111 participants from 44 NASAA jurisdictions in the United States, Canada and Mexico are leveraging their experience and using their unique tools to stop schemes and enjoin promoters. At the time of formation, the Task Force had identified over 200,000 coronavirus-related domains, either active or reserved. The matters are classified as either investment-related or non-investment related.

To date, 91 investment-related matters have been identified as potentially fraudulent, and there are 54 active and open investigations. Over a dozen of these investigations have resulted in an administrative action, and 26 financially-related referrals have been made to either third parties, law-enforcement, or other regulatory agencies. In addition, the Task Force has identified 39 other "non-investment related" matters and has made at least 12 referrals, with additional referrals forthcoming.

Schemes Identified by NASAA's COVID-19 Enforcement Task Force

While the schemes observed by the Task Force are manifold, many involve a cryptocurrency or promote investments that are outside the stock market – perhaps due to recent market volatility. In cases involving digital assets, we generally see promoters holding themselves out as cryptocurrency traders and offering investments in schemes promising lucrative profits. Some are more sophisticated than others. In some cases, there is a charitable component related to coronavirus efforts. Other investment opportunities include oil and gas ventures, real estate, penny stocks, precious metals, and investments in the foreign exchange markets. Based on the solicitations and placements of offers, suspects appear to be targeting seniors and persons with portfolios that are losing or have lost value due to current economic conditions.

For example, Alabama and Texas have enforcement actions against an outfit operating under the name "Ultra Mining LLC" that offered investments related to cryptocurrency mining operations.[7] To induce investors to purchase the "mining plans," the company claimed that it donated $100,000 to UNICEF to fight the coronavirus. Other examples of recent enforcement targets include:

- A promoter using social media and online advertisements to recruit victims into an illegal cryptocurrency scheme by fraudulently claiming he can make lucrative profits by trading cryptocurrency.[8]

[7] Alabama CD No. 2020-0007 and Texas ENF-20-CDO-1801
[8] Texas ENF 20-CDO-1804

- A self-described oilman who broadly targets victims through online advertisements and social media, fraudulently claiming he has "developed a process for making money drilling oil even after the crash of the oil markets."[9]

- A company allegedly based in Los Angeles, California, SwiftTradings, advertised on Instagram and communicated with investors about investment opportunities. The company concocted account statements, promised significant returns, and failed to disclose its preposterous fee schedule, which the company claimed were being assessed due to the COVID-19 pandemic.[10]

- An investment advertised through Craigslist that encouraged investors to invest their COVID-19 stimulus checks in his scheme. The ads targeted at least 49 states and 2 countries.[11]

- A promoter who targets retirees and investors who need supplemental income "due to crash in the economy," touting his ability to capitalize on volatility in the markets to make lucrative guaranteed returns.[12]

- An advertisement posted on Craigslist that encourages prospective clients to "exploit the current coronavirus crises by trading penny stocks from the pharmaceutical and biotechnology industry whose stocks are experiencing significant price fluctuations due to the pandemic."[13]

This is merely a snapshot of the investment-related cases that are being reviewed by the Task Force. In addition to investment-related schemes, the Task Force is seeing countless other online frauds, which are being referred to the National Center for Disaster Fraud.[14] For example:

- *Stimulus check fraud.* The Task Force has identified advertisements and notices that appear official and claim that "in order to expediate stimulus checks" individuals should fill out their census form. A link is provided to what appears to be an official census form, which solicits the personal information contained on a census form and gives the fraudsters all of the Personal Identifying Information that they need to steal the victim's identity.

- *Business identity fraud.* The Task Force has seen the names of legitimate non-profits are being used to solicit donations for coronavirus related medical studies.

- *Theft of personal information.* The Task Force recently discovered a company dedicated to "remembering those who lost their lives in the 1st pandemic of the third millennium of the Gregorian Calendar," whose website creates the appearance that it is a memorial for deceased persons. Users are asked to enter personal information to access the directory.

[9] Texas ENF 20-CDO-1802
[10] Alabama CD No. 2020-0010
[11] Alabama CD No. 2020-0008; Washington State S-20-2879-20-FC01
[12] Texas ENF-20-CDO-1800
[13] Alabama CD No. 2020-0009
[14] The National Center for Disaster Fraud is a national coordinating agency within the Department of Justice's Criminal Division dedicated to improving the detection, prevention, investigation, and prosecution of criminal conduct related to natural and man-made disasters and emergencies, including the COVID-19 pandemic.

- *Personal protective equipment fraud*. The Task Force has found numerous companies fraudulently claiming to sell personal protective equipment, sanitizers, and other products.

The list goes on, as does the work of the Task Force. We believe the Task Force's efforts have prevented and will continue to prevent many from being victimized and from becoming another restitution statistic in our respective agencies. In my experience, these enforcement efforts are effective deterrents to fraud, and the long reach of the Task Force's collective jurisdictions enable it to accomplish it on a large scale.

III. NASAA's Activities and Perspective Relating to Cybersecurity

The egregious character of financial crime is enhanced by technology and our growing dependence on online services. As a result, cyber criminals are on the rise and the financial sector remains a top target. Retail investors and small firms feel the impact, and thus cybersecurity is an area where NASAA proactively acts to protect registrants and investors. Indeed, NASAA members serve not only as regulators but also as resource to small firms in their respective jurisdictions.

NASAA Cybersecurity Initiatives and Partnerships

NASAA's Cybersecurity Committee coordinates and facilitates information sharing between NASAA members, industry participants, and state registrants to evaluate how NASAA can best address cybersecurity. The Committee also organizes and holds a cybersecurity roundtable each year in which experts discuss relevant and trending topics in cybersecurity. The roundtable is available for live streaming to the public, including to state-registered investment advisers.

In addition, NASAA's Investment Adviser Cybersecurity and Technology Project Group develops resources for registrants to assist them in protecting their firms and the personally identifiable information ("PII") they maintain on behalf of their clients. These resources include NASAA's Cybersecurity Checklist for Investment Advisers provided in 2018 and a resource guide for cybersecurity practices. These tools are available free of charge to firms and can be used to help state-registered investment advisers identify, protect, and detect cybersecurity vulnerabilities and to respond to and recover from cyber events. Earlier this year, NASAA updated the checklist and issued detailed guidance on steps state-registered investment advisers could take to better protect client information. To further protect investor PII, and in response to consistently identified cybersecurity deficiencies, on May 21, 2019, NASAA members adopted the Investment Adviser Information Security Model Rule Package.[15]

Cybersecurity Examinations of State-Registered Investment Advisers

Cybersecurity is a priority for state securities examiners. Smaller companies are the low hanging fruit for cybercriminals, and when you consider that more than three-fourths of the nearly 18,000 state-registered investment advisers are 1-to 2-person shops it is clear how important cybersecurity should be for these small businesses as well.

In their examinations of state-registered investment advisers in 41 U.S. jurisdictions between January and June 2019, state examiners found deficiencies relating to cybersecurity in more than one-quarter (26%) of their examinations, up from 23% during the last series of coordinated examinations in 2017. The top five cybersecurity-related deficiencies included: no testing of cybersecurity vulnerabilities; a

[15] *See:* https://www.nasaa.org/48065/nasaa-members-adopt-investment-adviser-information-security-model-rule-package/

lack of procedures regarding securing or limiting access to devices; a lack of procedures related to internet connectivity; weak or infrequently changed passwords; and inadequate cybersecurity insurance.[16] As noted above, these findings have spurred NASAA members to continue to focus on the importance of enhanced cybersecurity resources for state-registered advisers.

Cybersecurity Collaboration with Federal Authorities

Finally, NASAA members work closely with the federal government and other federal law enforcement agencies regarding cybersecurity. For example, since 2001, NASAA has served as a member of the Financial and Banking Information Infrastructure Committee (FBIIC).[17] Since state securities regulators are the primary regulators for state-registered investment advisers and co-regulators with the SEC for the broker-dealer community, NASAA's engagement with the FBIIC allows for facilitation of the sharing of information regarding emergency planning and preparedness.

Through monthly meetings and, when needed, daily reports and phone calls, staff from FBIIC member organizations work on operational and tactical issues related to critical infrastructure matters, including cybersecurity within the financial services industry and ultimately the effect on retail investors in the marketplace. From cyber safety and education, protecting networks from ransomware, and security of payment networks, to alerts on "hacktivist" threats, conducting tabletop exercises and disaster and recovery tracking and alerts, NASAA provides a central information source for its state members and provides input to the FBIIC on ground level events.

The senior leaders of FBIIC are the principals from each member organization who meet to provide strategic, policy-level direction to the work being done by FBIIC. Topics range from removing information-sharing impediments and enhancing incident-response planning, to examining financial firms to identify best practices around cybersecurity controls. Our office in Alabama is honored to be the NASAA representative to the FBIIC and the designated member to the FBIIC Principals Group.

IV. NASAA's Perspective on Proffered Legislative Proposals

The Committee has invited NASAA to share its views regarding several legislative proposals that have been posted in connection with today's hearing. Accordingly, I am pleased to express strong support for draft legislation entitled, "Senior Investor Pandemic and Fraud Protection Act" (also known as the "Empowering States to Protect Seniors from Bad Actors Act"), and draft legislation entitled "COVID-19 Restitution Assistance Fund for Victims of Securities Violations Act." I will address them in turn.

1. The Senior Investor Pandemic and Fraud Protection Act

The Senior Investor Pandemic and Fraud Protection Act would implement the Senior Investor Protection Grant Program, originally established and authorized by Section 989(A) of the

[16] *See:* https://www.nasaa.org/52507/state-investment-adviser-examinations-find-rising-cybersecurity-deficiencies/.
[17] Chartered under the President's Working Group on Financial Markets, the Financial and Banking Information Infrastructure Committee (FBIIC) is charged with improving coordination and communication among financial regulators, promoting public-private partnerships within the financial sector, and enhancing the resiliency of the financial sector overall. Additional information about the FBIIC is accessible at https://www.fbiic.gov.

Dodd-Frank Act, but never put into effect.[18] The bill would also expand the scope of the grants to explicitly include fraud related to COVID-19. Under the bill, qualifying states and state regulators would be able to apply for up to $500,000 annually in grant funding to combat financial fraud of seniors and vulnerable adults, including cases related to the pandemic, for a maximum of two consecutive years, for a total of $1 million.[19] The grant funds could be used for such purposes as: hiring staff to investigate cases involving fraudulent marketing related to the pandemic; funding technology, equipment, and training for prosecutors to increase the prosecution of salespersons who target seniors and vulnerable adults; and providing educational materials to seniors and vulnerable adults to raise awareness of misleading or fraudulent marketing.

NASAA strongly supports the Senior Investor Pandemic and Fraud Protection Act.[20] Indeed, such legislation is one of state securities regulators' highest priorities for the 116th Congress.[21]

Evidence suggests that as many as one out of every five citizens over the age of 65 has been victimized by financial fraud.[22] According to research published by the Consumer Financial Protection Bureau ("CFPB"), financial institutions have reported over 180,000 suspicious activities targeting older Americans since 2013. While the total financial loss is hard to determine, the estimated losses of older adults due to exploitation ranges from $2.9 billion to $36.5 billion annually.

Moreover, Congress has repeatedly recognized that seniors are especially susceptible to fraud and agreed on a bipartisan basis regarding the importance of supplementing state resources to educate and protect senior investors. Amid the COVID-19 pandemic, Congress should assist state regulators in securing resources to combat financial exploitation against those most vulnerable in this crisis. [23]

2. The COVID-19 Restitution Assistance Fund for Victims of Securities Violations Act

The COVID-19 Restitution Assistance Fund for Victims of Securities Violations Act would create a fund at the Securities and Exchange Commission to provide restitution payments for

---

[18] The "Senior Investor Pandemic and Fraud Protection Act" is directly modelled on precursor legislation that also aimed to make the necessary technical corrections to Section 989A, entitled the "The Empowering States to Protect Seniors from Bad Actors Act of 2019," which was proffered by the House Financial Services Committee in connection with a hearing on Consumer Financial Protection Bureau oversight in September 2019. The legislation is supported by a diverse coalition of organizations, including The Consumer Federation of America, The Insured Retirement Institute, The American Council of Life Insurers, The National Association of Insurance Financial Advisors, The American Association of Life Underwriters, The Financial Services Institute, The National Conference of Insurance Legislators, The Financial Planners Association, National Association of Personal Financial Planners, and The Certified Financial Planners-Board of Standards.

[19] Among the entities that would be eligible to apply for the Senior Investor Protection grants established by the bill are state securities regulators, state insurance regulators, and certain state consumer financial product regulators.

[20] The legislation is also supported by the National Association of Insurance Commissioners ("NAIC").

[21] *See:* NASAA's Legislative Agenda for the 116th Congress (April, 2019), accessible at https://www.nasaa.org/wp-content/uploads/2019/03/NASAA-Legislative-Agenda-for-116th-Congress.pdf.

[22] Almost one in five Americans over the age of 65, which is nearly seven million seniors, have "been taken advantage of financially in terms of an inappropriate investment, unreasonably high fees for financial services, or outright fraud," according to a major survey conducted by Public Policy Polling (PPP) and the Investor Protection Trust (ITP). Additional information on the Elder Investment Fraud and Financial Exploitation Survey is accessible at: http://www.investorprotection.org/downloads/EIFFE_Survey_Report.pdf.

[23] The CFPB has stated the failure to implement Section 989A as directed is due to ambiguity regarding the Bureau's authority to fund the grants. *See* Letter from CFPB Director Richard Cordray to Senator Collins (August 14, 2014). ("While Section 989A(h) authorizes…there has been no appropriation made for these grants to date.")

individuals in connection with securities fraud related to coronavirus if they do not otherwise receive full payment of restitution.

NASAA wholeheartedly shares Congress's interest in the potential establishment of a nationwide investor restitution fund to help victims of investment fraud recover a portion of what they lost when full restitution is not possible. In many cases of investment fraud, some or all the money defrauded from investors may be already gone by the time the scam artist is caught and prosecuted. All too often, the victims of these investment scams are senior citizens who do not have the time and resources to recover from the losses that have been inflicted upon them. The establishment of a restitution fund to help qualifying investors recover a portion of their losses is a common-sense tool that can provide critical assistance to harmed investors, while also contributing to investor confidence broadly.

In fact, some states have already enacted and successfully implemented this type of legislation. Indiana and Montana have reported that their restitution assistance programs are successful. Since the inception of their funds, Indiana has paid approximately $1 million in restitution assistance awards to 102 claimants, and Montana has paid $1.6 million to 118 claimants. The average recipient was 64 years old in Indiana, and 82% of recipients were over 60 years old in Montana.

V. Conclusion

State securities regulators are standing on the front lines in the fight against the criminals and opportunists looking to abuse America's investing public. The pandemic has sadly heightened their vigor, as bad actors attempt to exploit a pandemic and the present economic disruption. NASAA and Congress share a compelling interest in protecting investors, punishing fraudsters, and contributing to a robust economic recovery.

Thank you for the opportunity to testify before the Subcommittee. I will be pleased to answer any questions you may have.