April 2025

Prioritize the Mitigation of the Online Scam Epidemic in the United States

- *Online scams are an increasing threat against Americans' public safety and financial health, with implications for our economy, the U.S. financial system, and national security. Criminals carry out their crimes in multiple venues—over social media, dating websites, online job boards, and robocalls—breaking down trust in our communication tools and institutions.*

- *State securities regulators have a long history of protecting Americans from scams, including investment scams. They file enforcement actions to stop senior financial exploitation and punish perpetrators of fraudulent schemes. They coordinate their work with other state agencies serving seniors, such as local offices responsible for adult protective services, to support victims.*

- *NASAA is calling for a whole-of-government approach to combating the growing online scam epidemic in the United States. Given the nature of online scams, often originating abroad and operated by international criminal organizations, state securities regulators cannot prevent or mitigate this threat to Americans' savings without extensive coordination with and support from our federal partners.*

Background on the Online Scam Epidemic

Online scams targeting the United States are on the rise. Presently, the United States has multiple agencies that track related data, preventing NASAA from providing an exact figure of the harm to Congress. The following figures are illustrative:

- According to data from the Federal Bureau of Investigation's ("FBI") Internet Crime Complaint Center ("IC3"), public financial losses from internet crime exceeded $16.6 billion in 2024. This marks a 33% increase over reported losses in 2023. Losses from investment scams, the costliest crime tracked by the IC3 in 2024, rose from $4.57 billion in 2023 to $6.57 billion in 2023, marking a year-over-year increase of 43.76%.[1]

- According to data from the FTC, consumers reported losing more than $10 billion to fraud in 2023, marking the first time that fraud losses have reached that benchmark. This marks a 14% increase over reported losses in 2022.[2] Persons aged 60 and over reported losing more than $1.6 billion to fraud in 2022. Investment scams targeting this group amounted to $404 million, up 175% from 2021 figures. Adjusted for underreporting, the FTC estimates that consumers lost as much as $158.3 billion to fraud in 2023, while older investors lost as much as $61.5 billion.[3] As in prior years, the analysis of fraud reports received by the FTC showed that older adults were substantially less likely to report losing money to fraud.[4]

---

[1] *See* FBI, Internet Crime Report 2024 (Apr. 2025).
[2] *See* FTC, As Nationwide Fraud Losses Top $10 Billion in 2024, FTC Steps Up Efforts to Protect the Public (Feb. 9, 2024).
[3] *See* FTC, Protecting Older Consumers, 2023-2024 (Oct. 18, 2024).
[4] *See* FTC, FTC Issues Annual Report to Congress on Agency's Actions to Protect Older Adults (Oct. 18, 2023).

Additionally, new threat vectors exacerbating the online scam epidemic continue to emerge. In particular, the proliferation of artificial intelligence ("AI") has demanded increased vigilance from investors and regulators alike. A 2024 report from the Stop Scams Alliance warned that AI will "turbocharge" fraud by facilitating phishing attacks and deepfakes.[5] Moreover, in 2024, NASAA, the Securities and Exchange Commission, and the Financial Industry Regulatory Authority issued a joint investor alert warning that bad actors are using the growing popularity and complexity of AI to lure victims into scams.[6] State and federal regulators and other market watchers are closely monitoring the potential consequences of bad actors using AI to commit scams.

Initial Ideas for a Whole-of-Government Approach for Online Scam Prevention

Given size and reach of the threat, the Administration should take the lead on establishing a new, collaborative approach to preventing and mitigating online scams. Neither state securities regulators nor any individual federal regulator or agency can tackle the online scam epidemic alone; to do so requires a coordinated, whole-of-government effort to protect consumers. The White House should jumpstart this effort by emphasizing that it considers the prevention of online scams a national priority and foster actionable dialogue among stakeholders to this end.

Keying off the White House's prioritization of this issue, Congress should prioritize, as a matter of financial stability and national security, the creation of a coordinated, national anti-online scam strategy. The strategy should establish a local-state-federal task force. The task force should hear from the private sector, particularly participants involved in financial services and telecommunications. The task force should consider whether to recommend to Congress that Congress create a new structure or adjust the mandate of an existing structure to focus on the threat to investors posed by online scams. Establishing new caucuses, committees, or subcommittees may be necessary. For example, the House Financial Services Committee could establish a new task force dedicated to stopping scams similar to the task forces that operated in recent years for financial technology and artificial intelligence.

As a next step, NASAA urges Congress to inform the White House that it wants the Administration to treat online scam prevention as a priority.

Key Points

- *Online scam losses are skyrocketing, and artificial intelligence is about to make online scam losses worse.*

- *Criminals are increasingly targeting Americans and U.S. financial institutions because our country lacks prevention and mitigation strategies and techniques relative to other countries.*

- *To address this threat, NASAA urges Congress to inform the White House that it wants the Administration to treat online scam prevention as a priority.*

---

[5] *See* Stop Scams Alliance, As Scams by Foreign Organized Crime Soar, Here's How America Must Respond (Dec. 2024).
[6] *See* NASAA, NASAA Investor Alert: Artificial Intelligence (AI) and Investment Fraud (Jan. 25, 2024).