Gen™

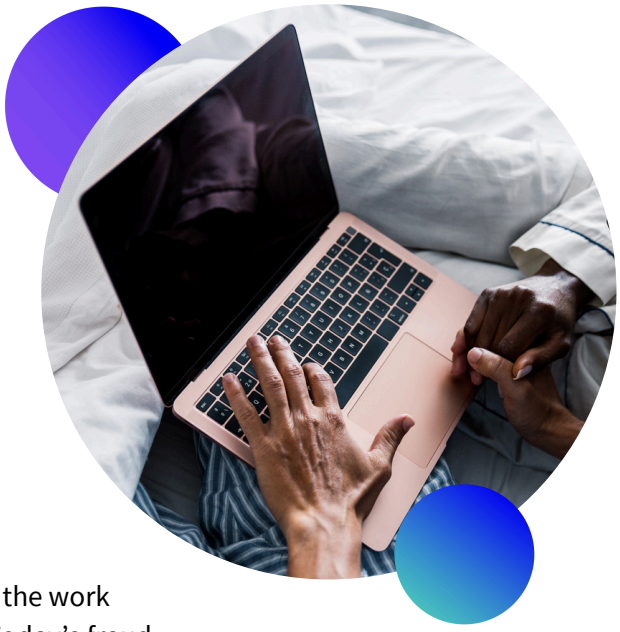
2025

Gen Position Paper:

Protecting Americans from Online Scams:

A Policy Roadmap for Smarter Digital Safety in the AI Era

norton™ Avast™ LifeLock™ by norton MoneyLion®



Executive Summary

Online scams have become a national crisis that is evolving faster than our current defenses can keep up with. In 2024 alone, U.S. consumers lost **$16.6 billion** to scams, a staggering **33% increase** over the previous year. According to a 2025 Gen survey, **35% of Americans** have already been targeted and nearly three-quarters of them have suffered financial harm, with an average loss of $**3,858 per victim.**

This crisis is simultaneously growing and transforming. What was once the work of isolated hackers has matured into a sophisticated, global industry. Today's fraud networks operate like professional businesses, complete with call centers, scripts, and AI-powered tools that enable highly personalized, profitable, and persuasive scams. In Gen's Q3 Threat Report, we reported that we blocked over 140,000 scam websites developed with AI generators, a new type of threat called VibeScams. The previous quarter we identified FunkSec, a new player in the fraud scene and the first instance of ransomware operators using generative AI and large language models (LLMs). Across the cyber safety landscape, malicious actors are using LLMs and AI to build, expand and better target their threats.

This paper outlines essential policy actions that lawmakers can take to protect Americans from the rising tide of AI-powered scams. Addressing these recommendations will be vital for the US government to effectively mitigate the rapidly evolving threat posed by AI-driven online scams.

State of Play

A New Era of Fraud

Scammers today are more targeted and manipulative than ever before. According to Gen data, over 90% of all threats to individuals that we block are scams and social engineering, those that rely on psychological manipulation and prey on people's vulnerabilities for success. The subject of these scams and the groups they target vary, and there are nearly endless combinations of "how" and "who". The Federal Trade Commission found that investment scams cost Americans **$5.7 billion** in 2024 and imposter scams drained another **$2.95 billion.** Seniors are frequently targeted by these criminals, with **59% of Americans** saying an older loved one has been scammed. Young adults face risks too, as their digital exposure and online data make them appealing targets for personalized AI-driven scams. Romance scams and pig butchering schemes (cases when a victim is contacted via dating apps or social media and encouraged to make increasing financial contributions via cryptocurrencies over a long period), also exploit relationships and trust, often leaving victims devastated both financially and emotionally.

These are not abstract numbers. They represent seniors who lose their life savings, young adults whose financial reputations are damaged before they even begin their careers, and hardworking families blindsided. Fraud has become a tax on trust, undermining both financial security and personal confidence in the digital economy.

How AI and Data Are Driving the Threat

In the hands of criminals, AI is enabling flawless phishing messages, cloned voices, and synthetic videos that impersonate real people. When combined with data from breaches and brokered sources, AI allows scammers to launch highly targeted, convincing attacks. The number of Social Security Numbers exposed in data breaches and sold on the dark web has increased from 8 milion before 2024 to over 300 million. This flood of personal data, coupled with generative AI, has made fraud scalable and harder to detect than ever before.

Gen's Strategy

Gen believes the best defense is a comprehensive one. Criminals use AI to build more complex networks and capabilities, but these advanced technologies also serve as a powerful means of protection. At Gen, we are investing in AI-driven tools for real-time scam and deepfake detection, identity restoration, and consumer education. We take a layered approach that combines cutting-edge technology, human insight, and recovery resources. We combine:

- **Detection and defense:** Gen tools like the Norton AI-powered Scam Assistant and Deepfake Protection catch scams before they cause harm.
- **Education and recovery:** We provide education to people online through our products, website as well as invest in nonprofit partnerships and training programs to help consumers, schools, and families recognize and resist scams and fraud.
- **Threat intelligence at scale:** We draw on billions of data points from over 500 million global users to act fast across platforms.

We support consumers not just at the point of attack, but across every stage of their digital lives.

Policy Recommendations for U.S. Lawmakers

Fraud prevention is a bipartisan issue and must remain a national priority. Lawmakers on both sides of the aisle understand that protecting Americans from digital scams is urgent, achievable, and in the public interest. We urge Congress to take the following actions:

1. Empower Consumers

- Authorize a national scam awareness campaign through agencies like the Federal Trade Commission or Department of Homeland Security.
- Fund digital safety education programs for seniors, parents and students.

2. Crack Down on Data Exploitation

- Enact stronger regulations on data brokers to limit how personal information is collected and sold.
- Create a centralized public database of data breaches to accelerate notification and response.

3. Strengthen Law Enforcement Capabilities

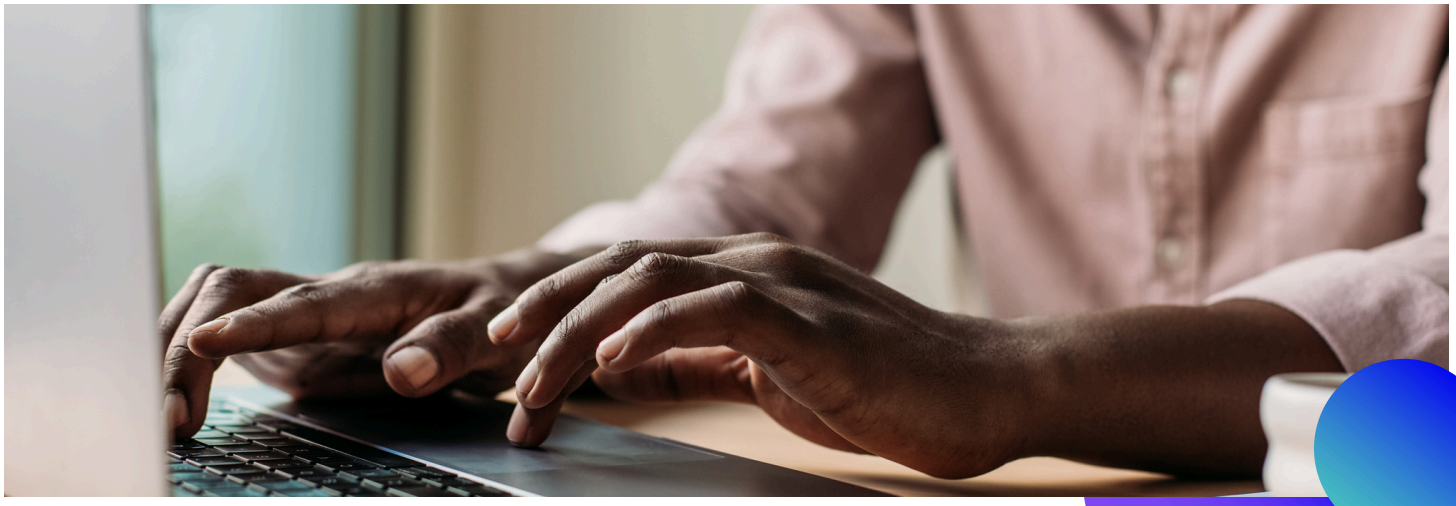
- Increase federal funding for local and state cybercrime units.
- Improve coordination across jurisdictions to disrupt international scam networks.

4. Empower Consumers Across the Digital Ecosystem

- Promote consumer choice and encourage operating systems, digital platforms and service providers to present consumers with options, including third-party antivirus and cybersecurity solutions, during initial device setup or installation.
- Foster fair competition and ensure that these systems are designed for seamless integration and interoperability with a wide range of third-party cybersecurity tools, including anti-malware, anti-scam, and anti-fraud solutions.

Conclusion

At Gen, our mission is to protect and empower consumers across every stage of their digital lives. We are proud to contribute our technology, threat intelligence, and expertise to support smarter policies and stronger protections for people.



About Gen

At Gen (NASDAQ: GEN), our mission is to create innovative and easy-to-use technology solutions that help people grow, manage, and secure their digital and financial lives. Dual headquartered in Tempe, Arizona and Prague, Czech Republic, Gen is a global company dedicated to powering Digital Freedom through its trusted brands including Norton, Avast, LifeLock, MoneyLion and more.

Our family of consumer brands is rooted in providing financial empowerment and cyber safety for the first digital generations. Today, Gen empowers people to live their digital lives safely, privately and confidently for generations to come. Gen brings award-winning products and services in cybersecurity, online privacy, identity protection and financial wellness to nearly 500 million users in more than 150 countries. This scale gives us unparalleled, real-time data on the evolving threat landscape and positions our solutions as a critical preventive layer in the fight against cross-platform online scams.

For further information please contact:
Kim Allman
Head of Corporate Responsibility & Government Affairs
Kim.Allman@GenDigital.com
Transparency Register number: *083146048556-68*

Washington, DC, December 2025

[1] Read Ian Bednowitz Testimony in front of the US House Financial Services Committee from September 2025: https://docs.house.gov/meetings/BA/BA09/20250918/118624/HHRG-119-BA09-Wstate-BednowitzI-20250918.pdf
[2] For more information and examples, check Gen Digital's latest threat reports (Q3/2025, Q1/2025, Q4/2024)