Gen™

Testimony of Ian Bednowitz,

General Manager, LifeLock

A Division of Gen Digital, Inc.

House Financial Services Committee

Subcommittee on Oversight and Investigations

Hearing entitled: “Fraud in Focus: Exposing Financial Threats to American Families”

September 18, 2025

Testimony of Ian Bednowitz

My name is Ian Bednowitz, and I serve as General Manager of LifeLock, a leading U.S.- based identity protection brand. LifeLock is part of Gen (NASDAQ: GEN), a global consumer cyber security company trusted by approximately 500 million users worldwide to keep them safer online. Alongside LifeLock, you may also recognize our other flagship brands Norton and Avast, both with decades of experience combating cyber threats and protecting consumers.

Our consumers are protected by award-winning security products backed by a team of researchers and cyber experts that block billions of threats annually. Gen was an early adopter of AI to keep up with criminals and better protect our consumers. Today, we are building tools that use AI to detect AI threats, monitoring behavioral anomalies and fraud patterns.

Fraud is escalating at an exponential pace, putting more people at risk every single day. Reports show the number of Social Security Numbers (SSNs) exposed in data breaches and sold on the dark web has increased from 8 million before 2024 to over 300 million. In addition, last year, the IRS flagged nearly 2 million tax returns for possible identity fraud. Our own stats show that LifeLock sent more than 81 million Identity Theft Protection alerts and notifications in 2024 alone.

Recently the Global Anti Scam Alliance (GASA), reported that fraud and scams are now the fastest-growing consumer crime globally and in the United States, overwhelming enforcement systems and undermining trust in digital services. According to the FBI's Internet Crime Complaint Center C3 report Internet Crime Complaint Center, Americans reported $16.6 billion in fraud losses in 2024, a 33% increase from 2023, with over 850,000 complaints filed.

As staggering as those numbers are, we are seeing a seismic shift in the fraud landscape. Deepfake technology is now being used to steal even more money from people. Fraud is being industrialized through AI tools that exploit public trust and institutional weakness. Criminals that work in fraud and scams are building international networks that can operate as effectively as professionally run and structured businesses. The organized frameworks allow for scalability and cross jurisdictional operations that are difficult for law enforcement to address.

It is no longer what we used to think was a lone actor in a sweatshirt on a laptop in their basement. They have grown to become international crime rings. An alert from FinCEN in late 2023 shows how sophisticated networks engaged in scams and social engineering and the growing threat of "Pig Butchering" are operating around the world.

Our own data shows over 75% of cybercrime originates from scams and social engineering, where cybercriminals manipulate people into giving money or personal information. 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 by criminal schemes. Fraud has become a tax on trust, undermining both financial security and personal confidence in the digital economy.

High-Impact Scams and the Price Americans Pay

Americans are facing a surge in increasingly sophisticated fraud schemes, many backed by organized international crime rings. Some of the most common and costly scams include:

- **Identity theft –** criminals obtaining personal information about an individual from a combination of breaches, the public internet or even the individual him or herself and using it to steal money through tactics such as applying for loans or credit cards, seeking employment or stealing tax returns cost Americans $23B in 2023.
- **Investment scams** – fraudulent investment opportunities, often exploiting cryptocurrency and digital platforms, cost Americans **$5.7 billion in 2024**.
- **Imposter scams** – criminals posing as government agencies, banks, employers, or even family members drained nearly **$2.95 billion in 2024**.
- **Job and business opportunity scams** – scams exploiting those seeking income or stability cost Americans **$751 million in 2024**.
- **Online shopping scams** – fake websites and ads targeting consumers with undelivered goods cost Americans **$432 million in 2024.**
- **Romance scams** – cost Americans **$1.14 billion in 2023**, preying on trust and emotional vulnerability.
- **Pig butchering scams** – one of the most devastating trends, blending romance, investment fraud, and emotional manipulation; losses often reach tens or hundreds of thousands per victim.

Together, these scams paint a stark picture: from fake investments and romance swindles to everyday identity theft and online shopping fraud, Americans are losing billions each year to schemes designed to exploit trust, urgency, and financial vulnerability. Behind every dollar from the $16.6 billion in fraud losses reported by the FBI in 2024 alone is a disrupted household, a stolen dream, or a family left picking up the pieces, underscoring the profound human and economic toll of modern fraud.

How Scams Work: Technology Meets Psychology

Fraud today is not just a technological problem; it is a psychological one. Criminals have learned to combine the precision of stolen data with the power of emotional manipulation. These scams are often triggered or amplified by emotionally charged events, a natural disaster like the recent floods in Texas or fires in California, a major political moment, or a sudden financial disruption. In those high-stress situations, people are more vulnerable to manipulation, and scammers exploit that urgency. Fraud tactics now rely just as much on emotional pressure as on technology, targeting individuals at their most vulnerable.

At the same time, the raw materials for fraud are everywhere. Billions of personal records circulate on the dark web, and an estimated 75% of Social Security numbers are already compromised**.** Much of this data is obtained through breaches and data brokers, while social media adds another layer. Every post, picture, or life update can give criminals the details they need to stitch together scams that feel authentic and personal.

Scammers then use this information in two ways. First, they can commit identity theft, posing as the victim to open credit cards, take out loans, or even apply for jobs in their name. Second, they can use the same personal data to target the victim directly, sending scam messages or calls that appear to come from a bank, a lender, a government agency, or even a trusted family member.

Artificial intelligence has made both approaches easier and more convincing. AI tools can generate polished phishing emails in seconds, automate scam operations at scale, and even create realistic audio or video "proof" that what the victim is seeing or hearing is legitimate. Deepfakes take this one step further: a cloned voice that sounds like a panicked child asking for money, or a manipulated video of a familiar face, can trick even the most cautious person into sending personal information or transferring funds.

This combination of breached data, emotional pressure, and AI-driven deception has made fraud harder to detect and far more dangerous. It is no longer just about spotting a misspelled word or a suspicious email. Today's scams are designed to bypass both technical safeguards and human instincts, leaving people exposed in ways that feel deeply personal.

Who's Being Targeted

Fraud does not discriminate, but its impact varies by age group. Gen's internal research shows that in 2025, 35% of Americans have already been targeted by a scam, well above the global average of 24%. Among those targeted, nearly three-quarters suffered financial harm, losing an average of $3,858, with some individual losses reaching as high as $149,000.

Younger adults are reporting scams at higher rates than older generations, according to FTC Sentinel data, often because they spend more time online and are more likely to trust digital platforms. But older adults, once victimized, lose far more. FBI Internet Crime Complaint Center (IC3) data shows the average reported loss for seniors is over $35,000, a devastating blow for those relying on retirement savings. In fact, seniors reported nearly 150,000 complaints in 2024, with total losses reaching almost $4.9 billion. Families across the country recognize the danger: according to Gen data, 59% say an older loved one has already been scammed, and another 71% are worried they will.

These numbers tell a clear story. Scammers adapt their tactics to exploit people's unique vulnerabilities, whether it's the digital exposure of the young, or the financial stability and trust of the old. Emotional manipulation is proving to be just as powerful a weapon as technical exploitation.

Areas of Fastest Growth

What is most concerning is not only the scale of fraud, but the rate at which it is accelerating and the way criminals are organizing themselves to industrialize these crimes.

Recent research confirms this trend. A study published by Cornell University on pig-butchering scams found that these scams follow a structured lifecycle: building trust, luring victims into fake platforms, and coercing ever-larger investments. Far from casual or opportunistic, these schemes are coordinated enterprises with specialized actors managing different stages of fraud.

Meanwhile, in the second quarter of 2025, the Gen Threat Report showed a 340% quarterly increase in the risk of being impacted by a financial scam. The increase in scams affected both desktop and mobile devices, the latter largely fueled by ads on social media where scammers lure their victims into fake messages and even false ads for sites that promote helping people fight scams.

The Identity Theft Resource Center's (ITRC) 2023 report documented a 118% increase in job scams and a surge in misuse of compromised credentials, including systematic abuse of tools like Google Voice. This illustrates how criminals scale identity theft across thousands of victims using repeatable methods.

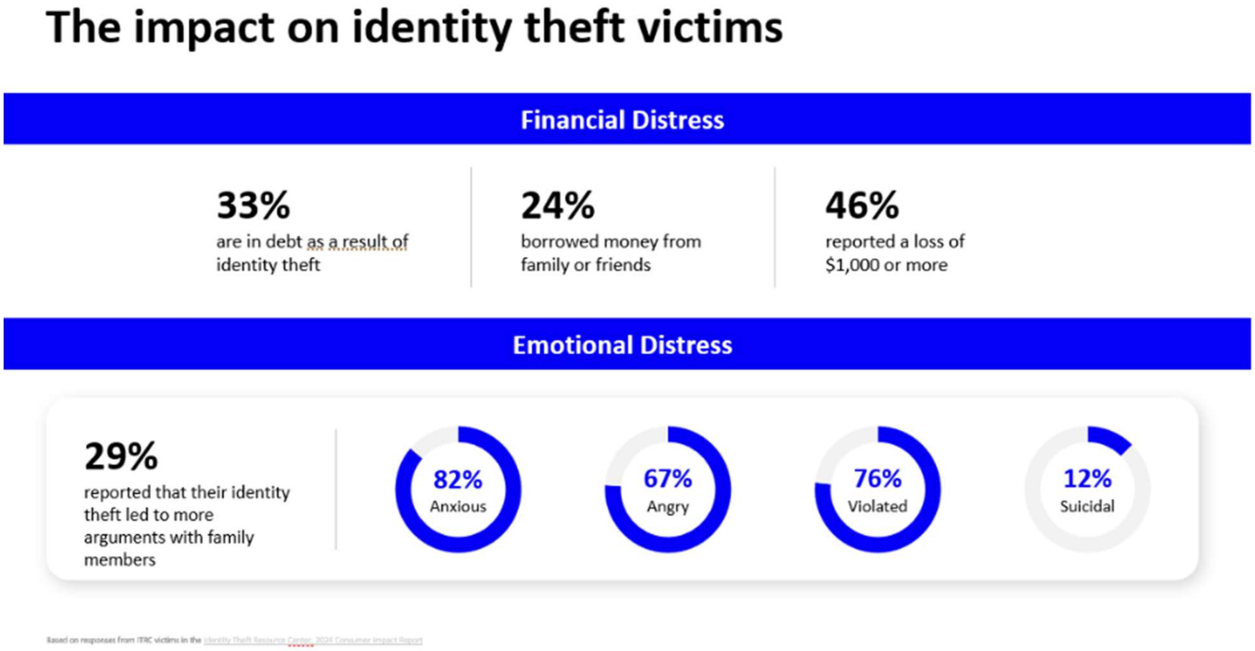
Industry studies also link fraud to organized criminal rings. The Onfido 2022 Identity Fraud Report found a 57% rise in document fraud, connecting forged IDs and synthetic identities to organized groups that create fraudulent accounts for money laundering and other downstream scams.

Taken together, these findings demonstrate why scams are accelerating so quickly. They are no longer isolated incidents but repeatable, scalable, and global operations, built on specialization, technology, and coordination. Three forces are fueling this growth: the flood of breached data, the use of AI to supercharge fraud, and the emotional manipulation that makes scams so effective. Together, they create a fraud economy that grows faster each year: more pervasive, more sophisticated, and harder for people to recognize and prevent.

The Human Impact

For every statistic, there is a family living through the fallout. Fraud victims lose retirement savings, homes, and financial stability. Many carry the weight of shame, isolation, and fear, which too often prevents them from reporting what happened. Families are forced to step in, not only to help recover stolen funds, but also to repair the emotional toll.

Identity theft victims often describe it as a lingering violation – a loss of control that doesn't end once the money is gone. Fraud is not just about money; it undermines people's confidence in technology, institutions, and the bonds of trust that hold families and communities together. The data bears this out: according to the 2024 Identity Theft Resource Center Consumer and Business Impact Report, 33% of victims end up in debt, 24% borrow money from family or friends, and nearly half (46%) lose $1,000 or more. Beyond finances, 29% say identity theft caused more family conflict, while 82% report feeling anxious, 67% angry, and 76% violated. Most alarmingly, 12% said the experience left them feeling suicidal.



The impact on identity theft victims

Financial Distress

33% are in debt as a result of identity theft

24% borrowed money from family or friends

46% reported a loss of $1,000 or more

Emotional Distress

29% reported that their identity theft led to more arguments with family members

82% Anxious

67% Angry

76% Violated

12% Suicidal

Based on responses from ITRC victims in the Identity Theft Resource Center, 2024 Consumer Impact Report

These numbers make clear that fraud and identity theft are not abstract crimes but deeply personal crises that ripple outward. The human toll of fraud underscores why stronger protections and coordinated responses are urgently needed. Data alone cannot capture the full cost when victims are left in debt, families are fractured, and trust is eroded.

AI: A Dual-Edged Sword

Artificial intelligence is now at the heart of this battle, both as a weapon for criminals and as a shield for protection.

On one side, fraudsters are using AI to supercharge their operations. Phishing emails that used to be riddled with spelling errors are now flawless, tailored, and persuasive. Criminals can clone voices to sound like a distressed family member or manipulate video to impersonate a trusted official. These deepfakes make scams far more believable, stripping away the warning signs people once relied on to spot fraud. AI has lowered the barrier to entry, making it faster, cheaper, and easier for criminals to target more victims at scale.

But on the other hand, AI is also our greatest defense. At Gen, we have invested in building AI-powered protections that keep people safe in real time. Our Genie AI Assistant technology scans millions of messages and images, flagging scams before harm occurs. We've started integrating Deepfake Protection into our products, so people can identify manipulated content that might otherwise fool even the most cautious among us. Every day, our machine learning systems analyze billions of data points, detecting unusual patterns that signal fraud and shutting down threats before they spread.

The truth is simple: AI is a double-edged sword. If left unchecked, it will allow fraud to grow at an unprecedented scale. But when deployed responsibly, it becomes a shield that protects people from the very dangers criminals are trying to exploit.

Gen’s Role and Response

At Gen, protecting people is not just our business, it is our mission. Across our family of trusted brands, including LifeLock, Norton, Avast, Avira, and AVG, we safeguard more than 500 million people worldwide. And we know that technology alone is not enough. Our approach combines protection, intelligence, and education.

- **Protection**: Through LifeLock, we provide identity monitoring, dark web alerts, and restoration services so people can recover quickly if their information is compromised.
- **Intelligence**: Our threat network processes billions of data points from hundreds of millions of devices, creating one of the most robust consumer-focused cyber intelligence systems in the world. That intelligence allows us to spot stolen credentials, fraud rings, and malware long before most people are even aware of the risk.
- **Education**: We invest heavily in awareness, from partnerships with the PTA to new training modules that teach families about AI safety. By equipping parents, teachers, and children with the knowledge to recognize scams, we break the cycle of silence and shame that so often leaves victims isolated.
- **Collaboration**: We share our threat and scams intelligence with law enforcement and policymakers, helping to disrupt criminal networks and inform strategies that strengthen consumer protections.

And behind each of these efforts are real stories. I think of the elderly man who was tricked into believing $9,000 had been mistakenly deposited into his account and was pressured to return it through a Bitcoin ATM. Because he was a customer with one of our scam protection products, Genie Pro, he was able to file a police report and was reimbursed for his loss. Or the woman who avoided losing thousands on a fake shopping site because she followed her family’s simple rule: before making an unusual purchase, check with a second trusted person first. That five-minute pause stopped her from entering her credit card details into a fraudulent site designed to steal them.

These stories remind us that while advanced technology is critical, sometimes the simplest protections, such as safe words, second checks, open conversations, can be just as powerful. That’s why we call our model an **All of the Above+ approach**. It means using every available best practice but also going further: embedding protections directly into the products and services people use every day, and ensuring that when fraud or breaches occur, there are trusted solutions ready to restore confidence and minimize **damage.**

Policy Considerations: A Unified Response to a National Challenge

Protecting American consumers from digital fraud requires more than good intentions. It demands coordination between government, industry, and civil society. Based on Gen's threat intelligence and experience with millions of consumers, we believe there are three essential priorities for Congress to consider:

Prevent Fraud Before It Happens

Launch national public education campaigns that cut across age groups, platforms, and communities. These campaigns should provide plain-language guidance on identifying scams, especially for seniors and younger digital natives. Formalize public-private partnerships with schools, nonprofits, and consumer platforms to deliver digital literacy training, especially focused on AI scams and identity fraud. Modernize breach notification standards so that alerts are timely, understandable, and come up with clear next steps for affected consumers.

Disrupt the Scam Supply Chain

Enact stronger oversight of data brokers and digital intermediaries that traffic in the personal information used to build scam campaigns. These entities should be subject to clear accountability for how data is collected, sold, and secured. Equip federal agencies with targeted enforcement tools, including sanctions against known international scam networks and the ability to take down infrastructure tied to repeat offenders. Increase scrutiny of digital advertising platforms and telecom providers that allow fraudulent content to spread. These companies must do more to detect and disrupt scam campaigns before they reach consumers.

Support Law Enforcement and Empower Victims

Provide funding and training for state and local law enforcement to investigate digital fraud and identity theft. Many scams are international in origin, but the harm is local. Police departments need better tools and coordination to pursue these cases.

Establish a centralized clearinghouse for breach information and consumer remedies. Victims should not have to hunt for answers across dozens of sources when their data has been compromised.
Set clear standards for consumer protection services, including identity monitoring, fraud remediation, and credit restoration tools. These services must be trustworthy, effective, and easy to access after a breach or scam.

Conclusion

The federal government has unmatched scale and policy reach. The private sector brings technical expertise and real-time threat data. Consumers face the consequences when those efforts do not align. We believe the time has come to treat fraud not as a series of isolated crimes, but as a systemic threat to national financial confidence and to act accordingly.