California State Senate

BANKING AND FINANCIAL INSTITUTIONS

TIMOTHY GRAYSON
CHAIR

Informational Hearing
Senate Committee on Banking and Financial Institutions

The Golden Age of Scams:
How Technology and Transnational Fraud Rings Threaten California Consumers
Wednesday, March 5, 2025
1:30 PM, 1021 O Street, Room 2100

Background

Purpose of the hearing:

The Senate Committee on Banking and Financial Institutions will convene an informational hearing on March 5, 2025, to examine the problem of consumer scams, particularly scams perpetrated by foreign organized crime networks. As detailed further in this background paper, American consumers lose billions annually to scams and fraud, up to $158 billion in 2023 according to the Federal Trade Commission. These crimes affect people of all ages, though the effects on senior Americans are especially pernicious. The purpose of the hearing is to explore how these crimes are committed and how society can better protect consumers through preventative and remedial measures.

During the hearing, the Committee will hear from the following witnesses across three panels:

Panel 1: The Nature of the Scam Industrial Complex and the Limits of Existing Consumer Protection Laws

- Lynn Knox, Resident of Oxnard
- Shawn Bradstreet, Special Agent in Charge, U.S. Secret Service
- Carla Sanchez-Adams, Senior Attorney, National Consumer Law Center

Panel 2: The Tools of the Trade: How Criminals Weaponize Consumer Services and the Need for Stronger Defenses

- Josh Bercu, Senior Vice President, USTelecom

- Sean Farrell, Assistant General Counsel, Microsoft
- Dylan Hoffman, on behalf of TechNet
- Darius Kingsley, Head of Consumer Business Practices, JPMorgan Chase & Co.

Panel 3: Seeking Progress: A Call for Societal Action to Combat a Growing Threat

- Scott Pirrello, Deputy District Attorney, Head of Elder Abuse Prosecutions, San Diego District Attorney's Office
- Ken Westbrook, Founder and CEO, Stop Scams Alliance
- Ken Palla, Retired Director, MUFG Union Bank

Consumer fraud and scams: "As old as falsehood and as versatile as human ingenuity."

The focus of the hearing is on a particular subset of fraud perpetuated against consumers, wherein the fraudster tricks a consumer into giving the fraudster money or other assets under false pretenses. The term "scam" is often used when describing such a crime, and one will often see "fraud" and "scam" used interchangeably. Rather than seek a precise definition of either term, it may be better to accept the expansive and ever evolving range of activities that may be deemed frauds and/or scams. As articulated by a Fifth Circuit judge reviewing a mail fraud case in 1941, "[fraud] needs no definition; it is as old as falsehood and as versatile as human ingenuity."[1]

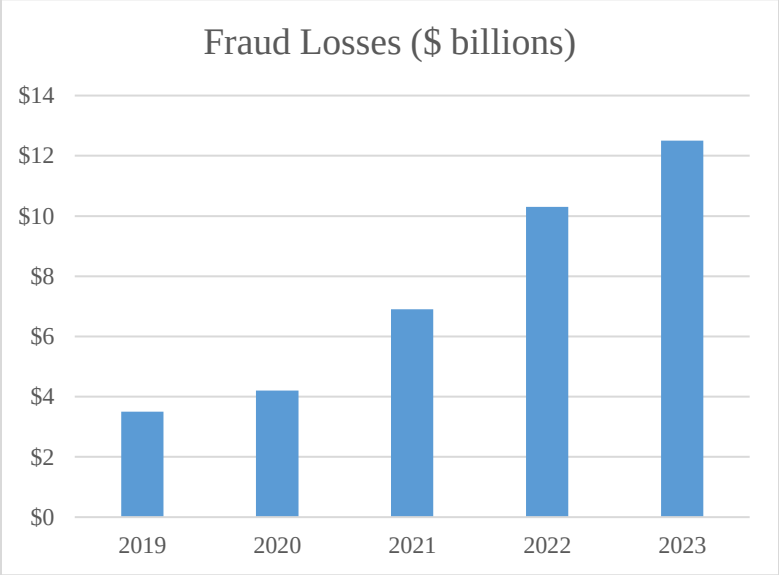
Criminals use innumerable schemes, tactics, and modalities in their efforts to target, persuade, and deceive potential victims. Although scams can still be perpetrated face-to-face, the days of con men and snake oil salesmen going town to town with their relatively small scale swindles have been replaced with highly sophisticated schemes conducted by criminal networks that reach millions of potential targets every year through telephonic and cyber channels. These criminals target people of all ages and backgrounds. Some schemes seek to extract relatively small, one-time amounts from consumers, while others aim for longer-term engagements with victims with the goal of methodically and ruthlessly stealing a consumer's entire net worth. These longer-term and more involved schemes often target older adults who have considerable retirement savings and other assets.

How much is lost to fraud and scams?

Americans lose large amounts of money to scams each year, and losses are growing at a staggering rate. Data related to the prevalence of scams reveal an incomplete picture, marred by underreporting of incidents and varying reporting and collection methodologies. But based on the best data sources available, it is abundantly clear that Americans face an enormous threat and that significant financial flows are moving from Americans' financial accounts into the hands of nefarious criminal organizations.

[1] U.S. Court of Appeals for the Fifth Circuit - 122 F.2d 675 (5th Cir. 1941)

The Federal Trade Commission (FTC) conservatively estimates at least $23.7 billion of fraud losses in 2023, based on reports to Consumer Sentinel, an investigative cyber tool and complaint database for law enforcement officials.[2] After adjusting for assumed underreporting of cases, the FTC posited a potential loss of up to $158 billion. Focusing solely on internet-related crimes, the Federal Bureau of Investigation (FBI) received 880,418 complaints in 2023 resulting in financial losses of $12.5 billion, compared to 467,361 complaints in 2019 with associated losses of $3.5 billion – an increase of 250% in four years, as shown in the chart below.[3]



One way to counter the problem of underreporting is to take the questions to the people, rather than waiting for victims to come forward to law enforcement. Gallup conducted a poll in October 2023 that found 8% of adults reported being tricked by a scammer into sending money or providing access to a financial account, translating to about 21 million Americans.[4] This figure dwarfs the 717,000 reports to the FTC related to financial losses from fraud over the same time period, revealing the scale of underreporting.

Most frauds reported to Sentinel are related to a financial loss of $500 or less, with nearly one-quarter of losses being less than $100. Large losses, however, are prevalent as indicated by more than 100,000 complaints related to a loss of $10,000 or more in 2023, representing nearly 15% of all fraud losses reported that year.

In addition to the financial burden, scams can levy an even higher psychological toll. Some scam victims suffer from embarrassment, alienation from friends and family, depression, and even suicide. A recent USA Today story finds at least 30 teen boys have committed suicide since 2021 related to sextortion, where a criminal threatens to distribute private material or harm a victim if

[2] Protecting Older Americans 2023-2024: A Report of the Federal Trade Commission; October 18, 2024. https://www.ftc.gov/system/files/ftc_gov/pdf/federal-trade-commission-protecting-older-adults-report_102024.pdf. (All links in footnotes were accessed on 2/28/2025.)
[3] Federal Bureau of Investigation Internet Crime Report 2023, Internet Crime Complaint Center. https://www.ic3.gov/AnnualReport/Reports/2023_IC3Report.pdf.
[4] https://news.gallup.com/poll/544643/scams-relatively-common-anxiety-inducing-americans.aspx.

the person does not comply with financial demands.[5] There are also numerous stories of elder adults committing suicide after losing large sums to scams.[6]

Who are the scammers

Transnational criminal networks are behind the industrial-scale scam operations that have driven the large increase in scam losses in recent years. The focus of this section on such criminal networks does not mean that all scammers are foreign nationals or that all scammers are part of highly organized schemes. When considering policy options to address the explosive growth of scams, however, policymakers must understand the methods employed by the perpetrators and their geographic locations, less one incorrectly believe that the problem can be addressed solely through local law enforcement.

The scale and sophistication of certain scam networks are comparable to those of a large, multinational corporation. These scams networks bring in billions of dollars of annual "revenue," rely on a wide variety of technological tools, and are operated by tens of thousands of people. While far from a comprehensive review of these networks, consider the following:

- The United Nations reported in 2023 that at least 120,000 people across Myanmar and 100,000 people in Cambodia may be held in situations where they are forced to carry out online scams.[7]
- Black Axe, the Nigerian organized crime group, has an estimated 30,000 members across dozens of countries involved in drug and human trafficking, kidnapping, and extortion. Cybercrime is the organization's most profitable activity, thought to have netted the gang tens of billions of dollars over the years.[8]

The ways that scammers contact and manipulate victims

In order to carry out their crimes, scammers must initiate contact with a target and then manipulate that person into sending them money or other assets. Scammers operating overseas rely on an array of communication technologies and platforms to make their initial contact. Contact is usually made through some form of "spoofing," where a person uses false information to assume a deceptive identity. Online identities are typically easy to spoof – the open nature of the internet has always made it difficult to know the nature of the person behind an email address, an online dating profile, a social media account, a website, or an online advertisement. With the aid of internet-enabled telephony, phone numbers are also easy to spoof, meaning scammers can make calls or send text messages from overseas that appear to originate from a target's financial institution, a law enforcement agency, a trusted contact, or a local caller.

Complex scams often utilize multiple communications channels once the scammer has initiated contact with a target. Conversations often move to channels with lower risk of creating evidence

[5] https://www.usatoday.com/story/life/health-wellness/2025/02/25/teenage-boys-mental-health-suicide-sextortion-scams/78258882007/
[6] See, e.g., https://www.cnn.com/2024/06/17/asia/pig-butchering-scam-southeast-asia-dst-intl-hnk/index.html.
[7] https://bangkok.ohchr.org/sites/default/files/wp_files/2023/08/ONLINE-SCAM-OPERATIONS-2582023.pdf
[8] https://africacenter.org/spotlight/black-axe-nigeria-transnational-organized-crime/

for law enforcement, such as encrypted messaging platforms like Telegram or WhatsApp. The methodology of a particular scheme may also influence the preferred communications channel. For example, a scheme that hinges on establishing a strong sense of urgency in a victim and preventing the victim from soliciting advice from friends or family may rely primarily on telephone calls.

As mentioned in the introductory section of this paper, the array of scams is limited only by human ingenuity, making a full taxonomy of scam types difficult to summarize. The following examples cover several of the more prominent schemes. Commonly, these schemes rely on psychological warfare; the criminal networks behind these schemes are constantly refining, updating, and changing their tactics based on their effectiveness; and the schemes are being incessantly deployed upon millions of targets every year.

- *Investment scams*: This category of scams targets victims with promises of lucrative returns on their investments. Investment scams represent the largest category of losses reported to the FBI Internet Crime Complaint Center (IC3), with over $4.5 billion of losses in 2023. Nearly 80% of these losses are associated with crypto-related investments. Some of these schemes are known as "pig butchering," a long-term scam where a victim is gradually manipulated into making larger and larger contributions into a fraudulent crypto investment until the scammer decides it is time to "slaughter" the victim by stealing all their assets and ceasing communication.

- *Tech support scams*: Perpetrators of this scam type impersonate a tech or customer support representative, convincing victims that their computer has been taken over by malware. The scammer often convinces the victim to allow the scammer to remotely access and control the victim's computer, allowing the scammer to commandeer the victim's financial accounts or to otherwise convince the victim to hand over money under false pretenses. This type of scam often originates with a telephone call initiated in a scam call center in India. It is particularly effective in victimizing older adults.

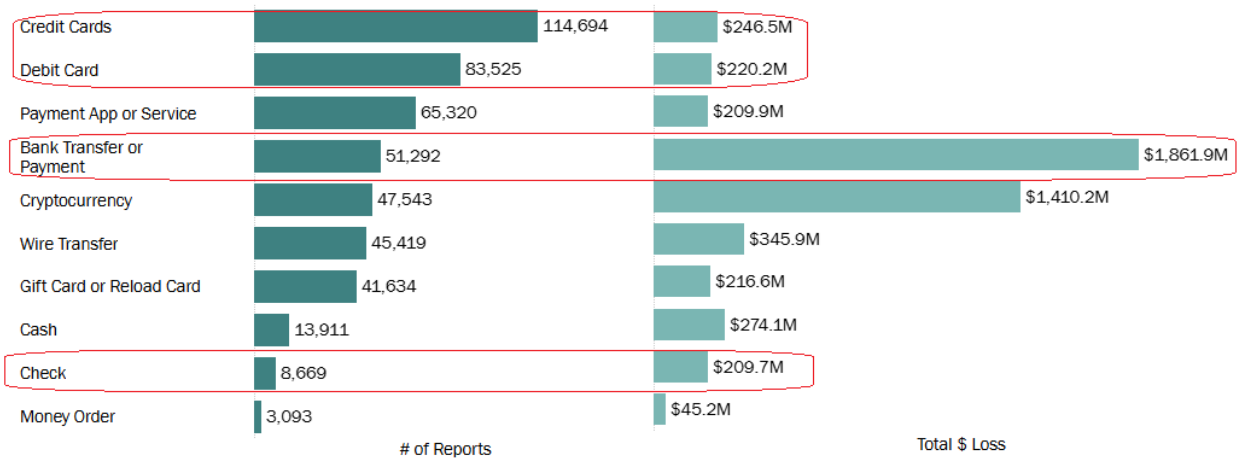
- *Other imposter scams*: Imposter scams describe schemes where a criminal pretends to be a trusted person and convinces a victim to send money or hand over personal information. In addition to the tech support scam mentioned above, imposter scams include schemes where the scammer impersonates a romantic interest, a family member in an emergency, a government agency, or a charity or company.

In conducting some of these scams, criminals may use fairly sophisticated technological tools to manipulate or deceive targets. The commercial availability of AI-related technologies likely makes imposter scams significantly more effective, fueled by persuasive scripts drafted by large language models and deepfake videos and audio. Some scammers can exploit vulnerabilities in mobile or desktop environments that allow the scammer to control the victim's device, deny all incoming calls, or manipulate the interface. Other tools of the trade include phone spoofing technology, voice modulation, and fraudulent mobile apps.

How scammers get paid

Scam victims transfer value to criminals in a variety of ways. This section discusses how victims initiate payments to scammers. Scammers may subsequently move funds through a multitude of means to get money out of the reach of U.S. law enforcement and into a form that the scammers can use wherever they are located. These types of funds transfers and money laundering are beyond the scope of the hearing and of this background paper.

Given the central role that banks play in many consumers' financial lives, a majority of scam payments are tied to banking products or services. As reflected in the FTC Sentinel data visualized below, a large majority of reported scams and associated losses are tied to banking products (see circled categories).[9]



The category "Bank Transfer or Payment" includes wire transfers between banks, which can accommodate large transaction sizes, provide immediate settlement, and are often impossible to reverse, making them a preferred method for criminals. Though not always tied to a bank transaction, the category "Cash" often has a nexus to banking as some scam victims withdraw large sums of cash from their bank and send the cash via mail, courier, or money mule to scammers. Payments via credit card or debit card may provide fraud protection for consumers in some cases; however, wire transfers, check payments, and cash withdrawals from a bank branch often provide no legal protections for consumers to seek reimbursements or refunds from the bank.

Crypto is another payment method favored by scammers. For a variety of reasons that are beyond the scope of this paper, crypto assets often have characteristics related to ownership and transfer that makes it more difficult for law enforcement agencies to track, trace, and freeze funds. Additionally, consumers generally have less knowledge about how crypto works or what to expect when engaging in transactions, providing criminals with an even stronger upper hand when seeking to deceive a target. Furthermore, the amount of crypto activity conducted outside

[9] Fraud reports by payment method, 2023, FTC Consumer Sentinel Network. Accessed here: https://public.tableau.com/app/profile/federal.trade.commission/viz/FraudReports/PaymentContactMethods.

the oversight of typical market regulators creates a kind of Wild West that makes crypto-native scams far easier to pull off.

Bank transfers and crypto transactions account for many high-dollar losses, but losses from other channels should not be dismissed. Lower-income consumers are more likely than wealthy consumers to use certain payment mechanisms – like a wire transfer at Western Union or a fintech payment service like CashApp. For a low-income household, a loss of $2,000 or $3,000 can have a more disruptive effect than a five-figure loss by a higher-income one.

Societal response

A serious effort to address the problem of scams will require collaboration and coordination across society. The scam ecosystem cuts across businesses and industries. The most effective upstream solutions to prevent scams before they occur will likely come from actions in the areas of telecom, social media, online advertising, and mobile and desktop operating environments. The financial sector can also do more in serving as a last line of defense by prioritizing scam prevention efforts. Banks and crypto exchanges have the most important roles to play, but other payment apps and platforms also need improvement.

Governments have a role to play in driving towards a comprehensive approach to significantly reduce the incidence and severity of scams. Governments can serve an important coordinating role in aligning activities among and between disparate private sector actors. Public policy can be shaped to ensure appropriate incentives are in place to motivate private actors. Importantly, the law must allow for the sharing of information between parties so that criminals do not simply slip into the shadows once they find themselves temporarily in the sights of corporate or governmental surveillance.

An ideal society-wide approach would likely be spearheaded by the federal government, but the prospects of leadership in Washington on this issue are uncertain. Voluntary efforts by the private sector, even if coupled with policy support at the state level, will likely encounter frictions and barriers posed by federal data privacy laws. State-level mandates could also be hampered by federal preemption related to national banks or communications. In spite of those constraints, the persistent and growing threat of scams demands action.

A nascent effort being led by the Aspen Institute provides some glimmer of hope. The National Task Force on Fraud and Scam Prevention consists of leaders across the public sector, industry, and civil society who are working together to better understand the scam ecosystem and work towards preventative interventions.[10] At this early stage, the fruits of this effort are not yet knowable, but the parties involved in the task force represent the leaders in government, tech, telecom, and finance who are in positions to make a difference.

[10] https://fraudtaskforce.aspeninstitute.org/membership