Congressional Research Service
Informing the legislative debate since 1914

IN FOCUS

August 26, 2025

Financial Fraud and Scams: The Roles of Federal Law Enforcement and Financial Regulators

Reported losses associated with financial fraud and scams have been increasing, garnering attention from law enforcement, private industry, policymakers, and the general public. In 2024, the Federal Trade Commission (FTC) received 2.6 million reports of fraud and scams, including $12.5 billion in reported losses. Similarly, the Federal Bureau of Investigation's (FBI's) Internet Crime Complaint Center (IC3) received 859,532 complaints in 2024, including $16.6 billion in reported losses (of which $13.7 billion were attributed to cyber-enabled fraud). These frauds and scams can deprive victims of their savings, deteriorate their overall financial health, and undermine public confidence in the financial system. A range of federal entities have roles in countering scams; this In Focus highlights the roles of federal law enforcement, financial regulators, and the FTC.

Overview of Fraud and Scams

Fraud is a broad term that includes activities such as false representations, dishonesty, and deceit. While the terms *fraud* and *scam* are often used interchangeably, a *scam* is often described as a type of fraud that involves tricking people into willingly providing money—or their personal information that can in turn be used to gain access to funds. Scams come in many forms, including romance scams, phishing/spoofing, non-payment/non-delivery crimes, and investment and tech support scams. Certain types of fraud are not scams. For instance, selling counterfeit goods as authentic and making financial transactions using someone's stolen personal information are fraudulent activities but not scams.

Due to the nature of communications and financial transactions in today's world, most fraud has a cyber or technology component; the FBI reports that almost 83% of financial losses reported to the IC3 in 2024 were cyber-enabled and often initiated through technological means, such as through social media or email. Similarly, an April 2025 Pew Research Center survey found that "73% of U.S. adults have experienced some kind of online scam or attack, and ... most get scam calls, texts and emails at least weekly." After initial contact, scammers will often continue the conversation on direct messaging sites and eventually complete the scams through a host of payment methods, including bank transfers, peer-to-peer payments, or cryptocurrency (crypto).

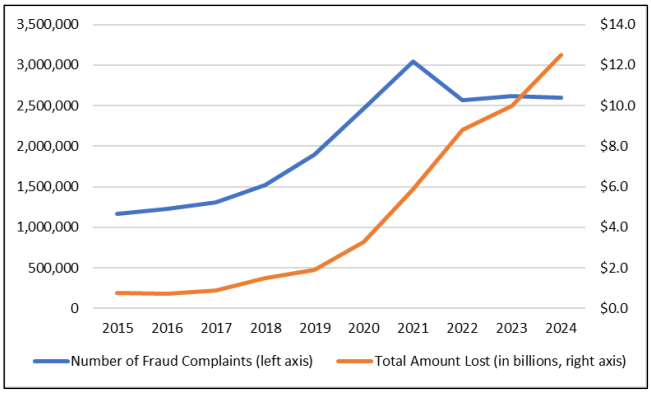
Investment Scams

According to the FBI, investment scams—while not the most common type of scam reported to the IC3—were the most lucrative for fraudsters. Across the nearly 48,000 investment scams reported to the IC3 in 2024, consumers reported almost $6.6 billion in losses. Most of these (41,557 complaints, involving $5.8 billion in reported losses) were *cryptocurrency* investment scams. In these scams, fraudsters establish trust with victims and then suggest they invest in crypto. Scammers may first advise victims to use a well-known crypto trading platform to prove their legitimacy before directing them to send crypto to another trading platform, which is the scam platform. Victims are encouraged to continue investing in this platform, and at some point, the scammer steals the crypto investments, leaving the victims with financial losses.

Trends and Financial Implications

Fraud complaints reported to the FTC rose from 1.2 million in 2015 to 2.6 million in 2024, with associated reported financial losses climbing from $765 million to $12.5 billion (See **Figure 1**). This includes a 25% increase in losses from 2023 to 2024, alone. Reported complaints are likely an underestimate of total *actual* fraud and scams. Similar recent increases in reported fraud are present in data from the FBI and in Suspicious Activity Reports (SARs) from the Financial Crimes Enforcement Network (FinCEN).

Figure 1. FTC Trends in Frauds and Scams 2015-2024



Source: FTC Consumer Sentinel Network annual reports.

According to the Pew Research Center, 30% of U.S. adults who have lost money to an online scam say it hurt their finances "a good deal" or "significant amount." The FTC reports a median loss of roughly $500 for each fraud report with associated losses in 2024. However, in 18% of fraud cases with an associated financial loss (175,000 cases), these costs were greater than $5,000. FTC data also indicate that older age groups report larger median losses, suggesting the financial consequences of scams to older consumers may be greater than those to younger consumers.

Financial Liability

Fraudulent electronic transactions that are not initiated by the consumer but involve financial institutions often limit

consumer liability to $50, with financial institutions liable for the remainder. For transactions authorized by a consumer but induced by a third party under fraudulent circumstances, the liability would generally rest with the consumer and not the financial institution. The losses from these scams can often cause negative financial consequences for consumers.

Federal Activities Countering Scams

This section highlights activities of federal law enforcement, financial regulators, and the FTC in countering financial fraud and scams.

Select Federal Law Enforcement

A host of federal law enforcement agencies are involved in countering fraud and scams. Within the U.S. Department of Justice (DOJ), the FBI is the lead investigative agency countering scams. In addition to investigating fraudsters and any associated criminal networks, the FBI provides consumer awareness and victim resources. As part of these activities, the FBI runs the IC3, which operates a hotline to collect reports of fraud from the public. The IC3 established the Recovery Asset Team (RAT), which streamlines communications between the IC3 and financial institutions. RAT assists FBI field offices in freezing funds for victims who have made transfers to domestic accounts under fraudulent pretenses.

The Office of the United States Attorneys (USAO) prosecutes violations of federal criminal law (including those related to scams), represents the federal government in civil actions, and initiates proceedings for the collection of fines, penalties, and forfeitures owed to the United States. The USAO works with other DOJ components, including the Criminal Division and its experts in the Fraud Section, to investigate and prosecute scams targeting consumers. The Criminal Division's Violent Crime and Racketeering Section also helps investigate and prosecute transnational organized crime, including their involvement in scams.

The U.S. Secret Service is charged with safeguarding the country's financial and payment systems. Their agents—including those assigned to Cyber Fraud Task Forces—investigate individuals and criminal networks targeting these systems in a variety of crimes, including financially motivated scams. The Secret Service also engages in public awareness activities aimed at preventing victimization.

U.S. Immigration and Customs Enforcement, Homeland Security Investigations (HSI) investigates a wide range of crimes including "financial fraud and scams and other crimes against vulnerable populations." HSI relies on Transnational Criminal Investigative Units to pursue cases against transnational criminal organizations with a financial nexus. It also utilizes Document and Benefit Fraud Task Forces to investigate fraud, including scams targeting vulnerable individuals.

Select Federal Financial Regulators

Within the U.S. Department of the Treasury, FinCEN enforces an anti-money laundering framework. FinCEN collects and maintains a central repository of financial intelligence including SARs, which select financial institutions are mandated to file if they suspect certain fraud, scams, or other potential illicit activity. It refers certain SARs to law enforcement and has a Rapid Response Program to help victims recover stolen funds. Like other financial regulators, and sometimes in conjunction with them, FinCEN produces awareness materials and advisories. These include a recent advisory on risks of Cryptocurrency ATMs and a 2024 interagency statement on Elder Financial Exploitation.

Prudential banking regulators supervise certain financial institutions to ensure they are filing relevant SARs and complying with underlying provisions in the Bank Secrecy Act. The Federal Reserve (Fed) offers a few additional services to decrease the prevalence of payment fraud, such as the ScamClassifier model and services to respond to check fraud. Recently, the Office of Comptroller of the Currency, the Federal Deposit Insurance Corporation, and the Fed issued a joint request for information on what these agencies could further do to reduce the prevalence of fraud.

The Consumer Financial Protection Bureau enforces certain consumer protection statutes related to scams and fraud in consumer finance and has previously brought civil enforcement actions against companies and individuals for alleged violations of those statutes, such as the Truth in Lending Act.

FTC

The FTC has enforcement authority over certain cases related to a prohibition on "unfair or deceptive acts or practices" in most industries. Related civil investigations have implicated investment scams and tech support scams, or have targeted companies that facilitate scams. The FTC maintains the Consumer Sentinel Network, which consolidates fraud-related complaints and shares them with law enforcement.

Congressional Considerations

Policymakers may examine a number of issues regarding federal efforts to prevent and counter scams. For instance, Congress may consider whether there should be a more coordinated federal effort, including a government-wide strategy, aimed at countering scams. The Government Accountability Office has offered that the FBI may be well positioned for this role; such efforts might include defining scams, consolidating complaint reporting, and aggregating data. Another option policymakers may consider is whether there are sufficient federal resources within each department or agency allocated to preventing and countering scams (e.g., are there adequate personnel at DOJ dedicated to investigating scams). Relatedly, Congress may debate whether these resources should be targeted broadly or more toward protecting certain populations who may be seen as vulnerable, such as some older adults.

Karl E. Schneider, Analyst in Financial Economics
Kristin Finklea, Specialist in Domestic Security

IF13094

Disclaimer