Congressional Research Service
Informing the legislative debate since 1914

IN FOCUS

May 21, 2025

Cryptocurrency Investment Scams

Law enforcement, policymakers, victims, and the general public have expressed concern over technology-enabled scams affecting individuals' finances. These scams come in many forms, ranging from phishing, personal data breach, and non-payment/non-delivery crimes to extortion, tech support, and investment scams. In 2024, the Federal Bureau of Investigation's (FBI's) Internet Crime Complaint Center (IC3) received 859,532 complaints of scams, resulting in $16.6 billion in losses. There has been particular interest in cryptocurrency investment scams—which some have referred to as *pig butchering* scams (this controversial term comes from fraudsters referring to victims who are "fattened" by gaining their trust before "butchering" them and taking their money). This In Focus provides an overview of these scams and outlines federal law enforcement initiatives to counter them, relevant federal statutes and prosecutions, and considerations for policymakers. It focuses on the federal *criminal* enforcement response to cryptocurrency investment scams (rather than civil enforcement actions).

Cryptocurrency Investment Scams

The FBI has noted increases in cryptocurrency investment scams in recent years. In 2024, the IC3 received 41,557 complaints of cryptocurrency investment scams, a 29% increase from the 32,094 received in 2023. The complaints in 2024 were associated with $5.7 billion in reported losses, a 47% increase over losses in 2023.

These scams are often socially engineered and trust-enabled schemes that may evolve out of a confidence or romance scam. In these types of scams, fraudsters may connect with potential victims through social media platforms or dating applications (apps). After establishing trust with victims, the scammer suggests they invest in cryptocurrency, and may first advise victims to set up an account on a well-known cryptocurrency trading platform before directing them to send crypto to another trading platform, which is the scam platform. This scam platform allows victims to make investment gains, and the scammer may even try to prove the platform's legitimacy by encouraging victims to withdraw some funds along the way. Victims are then encouraged to continue investing. At some point, the scammer steals the cryptocurrency investments, leaving the victims with substantial financial losses.

Cryptocurrency as a Tool, Not Just as an Investment Scam

Cryptocurrency *investment* scams, such as romance baiting, are distinct from other scams that involve cryptocurrency as a *tool* or a convenient means of payment rather than as the centerpiece of the scheme. To facilitate payment in scams such as tech support, government impersonation, investment, and extortion, for example, a fraudster may direct an individual to use a cryptocurrency ATM to deposit money (which the victim may have pulled from an investment, retirement, or other account) and then direct the deposit of those funds to the scammer's cryptocurrency wallet—often using account information on a QR code provided by the scammer. Other fraudsters may demand cryptocurrency directly in extortion or sextortion schemes. For instance, fraudsters may request cryptocurrency to prevent the release of sensitive or personal information.

Select Federal Law Enforcement Initiatives

A number of federal law enforcement agencies—including the FBI and U.S. Secret Service—are involved in investigating frauds, scams, and the illicit payment involved, including fraudulent cryptocurrency investment platforms and companies. In 2022, the FBI established the Virtual Assets Unit, with the mission of investigating cryptocurrency-related crimes. In an April 2025 media interview, the chief of that unit said that its work includes combatting cryptocurrency investment scams. In January 2024, the FBI and U.S. Secret Service launched Operation Level Up to identify and notify victims of cryptocurrency investment scams. The FBI announced that as of April 2025, Operation Level Up had notified 5,831 victims of cryptocurrency investment fraud (77% of whom were unaware they were being scammed), helped save victims over $359 million, and referred 59 victims to FBI victim specialists for suicide intervention. In February 2025, the FBI issued a press release encouraging potential victims to report to the IC3 and contact their banks. Federal law enforcement also coordinates with international law enforcement partners to share information and investigate cryptocurrency investment scams.

Select Federal Criminal Statutes

There is no single federal statute expressly criminalizing cryptocurrency investment scams, but depending on the circumstances fraudsters may run afoul of a number of federal criminal laws prohibiting fraud, money laundering, and related conduct. This section describes select statutory provisions used by the U.S. Department of Justice (DOJ) in the cryptocurrency investment scam context.

Practical Note: Conspiracy

Given that cryptocurrency investment scams can involve more than one offender, federal conspiracy statutes, such as 18 U.S.C. §371, may be relevant That statute authorizes fines and up to five years of imprisonment for certain agreements between at least two people to carry out an unlawful objective. Some statutes, such as 18 U.S.C. §1956 (discussed below), contain their own provisions specifying that conspiracies are subject to the same penalties that would apply to the underlying violations. In the cryptocurrency investment scam context, federal prosecutors have sometimes

obtained guilty pleas for conspiracy charges even where the defendants did not plead guilty to the underlying substantive offenses (e.g., money laundering) listed in the charging document. For more information about federal conspiracy law, see CRS Report R41223, *Federal Conspiracy Law: A Brief Overview*, by Charles Doyle (2020).

Wire Fraud: In at least one case, federal prosecutors charged a defendant with wire fraud conspiracy in connection with a cryptocurrency investment scam. The federal wire fraud statute (18 U.S.C. §1343) prohibits knowing or willing participation in a scheme to defraud using interstate wire transmissions, among other things. Courts have interpreted "scheme to defraud" to include the "common understanding" of depriving someone of money or property by "dishonest methods" such as deceit. Phone calls (cellular or landline), faxes, emails, instant messages, texts, and wire transfers may all qualify as wire transmissions for Section 1343 purposes, assuming they are interstate. In general, the interstate requirement may be satisfied when the transmissions cross state lines, as in the case of a telephone call originating in one state and received in another, or a communication sent and received in a single state but routed through equipment in another state. Some federal courts disagree on whether internet use by itself can establish an interstate transmission; an issue that has divided federal appellate courts in related contexts. In practice, internet use may still involve the requisite interstate transmission if, for example, there is evidence that "computers in multiple states access the same website," or that an email is transmitted between computers in different states. To violate the wire fraud statute, it need only be reasonably foreseeable that the interstate wires would be used in furtherance of the scheme to defraud, which generally requires that the wires be "'incident[al]' to an essential part of the scheme." Violations of Section 1343 may ordinarily be punished by a maximum fine of $250,000 or up to 20 years imprisonment, or both, but higher penalties are available in certain contexts.

Money Laundering: 18 U.S.C. §1956, a federal anti-money laundering statute, criminalizes certain transactions involving illicit proceeds, including when the transactions are designed to conceal the source of proceeds or to evade taxes. Violations of Section 1956 are punishable by fines and up to 20 years of imprisonment, or both (civil penalties are also available in some situations). In one cryptocurrency investment scam case, federal prosecutors charged a defendant with violating Section 1956(a)(1)(B)(i), which prohibits, among other things, conducting a financial transaction involving "proceeds of illegal activity" with knowledge that "the property represented proceeds of some form of unlawful activity" and that the transaction "was designed in whole or in part to conceal or disguise the nature, the location, the source, the ownership or the control of the proceeds of specified unlawful activity." Prosecutors alleged that the defendants engaged in numerous wire transfers with knowledge that the funds were proceeds of an illegal cryptocurrency investment scam under Section 1343 and that the transactions were designed to conceal their unlawful source. Prosecutors also alleged that the defendants transferred tens of thousands of dollars from a domestic bank to accounts in Hong Kong in violation of Section 1956(a)(2)(B)(i). That provision bars conduct including the international transmission of funds with knowledge that they are unlawful proceeds and that the transaction is intended to conceal their source. Three defendants in the case ultimately pled guilty to conspiring to violate Section 1956.

Practical Note: Offenses Originating Abroad

The applicability of statutes like Sections 1343 and 1956 to cryptocurrency investment scams may be restricted by external, practical considerations. In large part, this is because cryptocurrency investment scams, according to the FBI, often originate overseas. As CRS Report 94-166 explains in detail, investigating and prosecuting criminal conduct in other countries raises questions of national sovereignty and may involve significant legal, practical, and diplomatic obstacles. For example, the United States lacks extradition treaties with some countries, which may make domestic prosecution of cybercriminals residing in those countries challenging, though not impossible. DOJ may also be able to use civil asset forfeiture—a statutory regime enabling DOJ to file lawsuits against certain property when involved in various crimes—to recover property used in or obtained through cryptocurrency investment scams originating abroad. For example, in July 2024 DOJ issued a press release stating that it had "filed a civil forfeiture action ... to recover cryptocurrency seized by the FBI from perpetrators abroad," which it valued at over $2,500,000. DOJ described the cryptocurrency at issue as proceeds from a cryptocurrency investment scam. Forfeiture authorities have also been used by DOJ to seize domain names that facilitated alleged cryptocurrency investment scams.

Congressional Considerations

Policymakers may have interest in supporting or enhancing activities that raise awareness of cryptocurrency investment scams. They may examine existing awareness efforts by federal law enforcement and other entities to educate the public about preventing and reporting these scams. Policymakers have been concerned about scammers defrauding certain populations, including seniors. Of the 859,532 complaints the IC3 received in 2024, 147,127 involved scams of individuals age 60 and over, totaling more than $4.8 billion in scam-related losses. Congress may consider whether additional efforts—authorities or funding—may be warranted to continue or enhance investigations and prosecutions of scams, as well as efforts to support victims. The online nature of cryptocurrency investment scams may provide a jurisdictional basis for Congress to work from should it wish to create or amend applicable criminal laws. Law enforcement notes that many of these scams are facilitated by transnational criminal organizations based overseas; policymakers may also consider whether there are sufficient authorities and forms of mutual legal assistance to support federal law enforcement in these transnational investigations. Lawmakers may, alternatively, prefer to rely on existing statutes and law enforcement discretion.

Peter G. Berris, Legislative Attorney
Kristin Finklea, Specialist in Domestic Security

IF13008

Disclaimer