Statement by

Dara Daniels

Associate Director, Research and Analysis Division

Financial Crimes Enforcement Network

U.S. Department of the Treasury

before the

Committee on Financial Services

Subcommittee on National Security, Illicit Finance, and International Financial Institutions

U.S. House of Representatives

September 18, 2024

Introduction

Good afternoon, Chairman McHenry, Ranking Member Waters, Chairman Luetkemeyer, Ranking Member Beatty, and members of the Subcommittee. My name is Dara Daniels, and I serve as Associate Director for the Research and Analysis Division, informally referred to as "RAD," at the Treasury Department's Financial Crimes Enforcement Network, or FinCEN. I am career staff and have been with Treasury since 2016, and specifically at FinCEN since 2018.

I have carried out the duties of my current position in an Acting Capacity starting in January of 2023. At that time, RAD was referred to as FinCEN's Intelligence Division, and was subsequently renamed to better reflect the important work of the division. Prior to taking on the role of Associate Director of RAD, I served in other roles at Treasury, including within FinCEN and at the Office of Foreign Assets Control (OFAC), and I also worked in the private sector, where I was a consultant analyzing cyber threats for financial institutions and the U.S. Government.

Thank you for the opportunity to appear and to discuss this important topic. FinCEN, along with its partners at Treasury and throughout the U.S. government, is very focused on the threats posed by virtual asset investment scams—including scams commonly referred to as "cryptocurrency confidence scams" and referred to by perpetrators as "pig butchering"—and other types of fraud. Before discussing this heinous activity and how FinCEN is addressing it, I want to place it within the context of the broader threat environment. FinCEN has long dedicated resources towards targeting transnational organized crime groups, human traffickers, cybercriminals, and fraudsters. Virtual asset investment scams are merely one of the ways that criminals are targeting the public and exploiting the financial system for their own personal gain. FinCEN is committed to doing everything it can to detect and deter these bad actors and to help law enforcement hold them accountable. I will address in closing some of FinCEN's ongoing efforts to combat fraud in all its forms, including our Rapid Response Program that repatriates stolen funds to victims.

FinCEN's Mission

As this Committee knows, FinCEN is the nation's primary regulator responsible for implementing the Bank Secrecy Act (BSA) as well as the Financial Intelligence Unit (FIU) of the United States. FinCEN's mission is to safeguard the financial system from illicit use; to combat money laundering and related crimes, including terrorism, narcotics trafficking, and fraud; and to promote national security through the strategic use of financial authorities and the collection, analysis, and dissemination of financial intelligence. FinCEN's mission is "broad" in the sense that almost every form of crime and every threat to national security has some financial nexus—a fact that necessitates a careful allocation of FinCEN's resources to focus on work most likely to protect the lives and livelihoods of the American people.

FinCEN's Research and Analysis Division

RAD carries out FinCEN's statutory responsibility to analyze financial data and produce financial intelligence products for its stakeholders, including law enforcement and national security agencies, as well as regulatory agencies. RAD's work encompasses the following responsibilities:

- Collaborating with and supporting FinCEN internal and external partners;
- Producing cutting edge, multi-source financial intelligence products providing strategic and tactical perspectives about priority threats to the domestic and international financial systems;
- Developing financial analysis and FinCEN advisory products alongside other FinCEN divisions, including financial trend analyses, advisories, notices, and alerts; and
- Serving as global experts on money laundering, terrorism financing, and other forms of illicit finance, and on the application of innovative technologies for enhancing financial crime analysis.

RAD is comprised of three offices: the FinCEN Analytical Hub, the Office of Transnational Issues, and the Office of Cyber and Emerging Technologies.

FinCEN recently established the Analytical Hub as part of FinCEN's implementation of Section 6304 of the Anti-Money Laundering (AML) Act of 2020. The Analytical Hub organizes many of FinCEN's previously existing resources and expertise into a single office. This organizational shift has enhanced our communication with and support to partners at the federal, state, and local levels.

The Offices of Cyber and Emerging Technologies and Transnational Issues develop financial analytic products and provide support to law enforcement and other partners, each focusing on particular types of priority financial threats. The Office of Cyber and Emerging Technologies focuses on cyber-enabled financial crimes, including ransomware, misuse of identity, cryptocurrency scams such as virtual asset investment scams, the use of darknet marketplaces, and other cybercrime. The Transnational Issues Office focuses on a variety of illicit activity, including corruption, domestic and international terrorist financing, fraud, transnational criminal organizations, drug trafficking organizations, human trafficking and human smuggling, and proliferation financing.

FinCEN Publications & Analytic Products

As part of fulfilling its mission to protect the integrity of the U.S. financial system and safeguard the national security of the United States, FinCEN issues a variety of analytic products and publications. FinCEN works extensively with law enforcement and other partners on these products, which cover a variety of topics—including money laundering, terrorist financing, and other illicit financial activity. FinCEN publishes products that discuss trends, typologies, red flags, and case studies, available to financial institutions, law enforcement, and the public. These publications serve multiple objectives: (1) raising public awareness about criminal activity, thereby helping would-be victims avoid scams; (2) educating financial institutions so that they can better detect, prevent, and report on illicit financial activity; and (3) supporting law enforcement in the detection, investigation, and prosecution of illegal activity.

FinCEN's Financial Institution Advisory Program issues advisories to financial institutions that contain trends, typologies, red flags, and case studies to support effective anti-money laundering programs and suspicious activity reporting to FinCEN on activity of concern to law enforcement. RAD's analysis both informs these advisory products and is derived from the financial intelligence these products generate, namely the filing of suspicious activity reports, or "SARs," by financial institutions. For example, in September 2023, FinCEN published an Alert on a prevalent virtual asset investment scheme typology: the FinCEN Alert on Prevalent Virtual Currency Investment Scam Commonly Known as "Pig Butchering" (September 2023 Alert). These publications also typically provide financial institutions with a key term to include when filing a SAR to better assist FinCEN and law enforcement in identifying and reviewing reports that relate to a particular topic.

FinCEN also develops and publishes BSA-derived threat pattern and trend information, consistent with Section 6206 of the AML Act. To date, FinCEN has published 10 of these reports, known as Financial Trend Analyses, including four that address major fraud schemes such as business email compromise in the real estate sector, elder financial exploitation, identity-related suspicious activity, and, just this month, mail theft-related check fraud.

FinCEN Virtual Asset Investment Scam Alert and Related Work

Over the last several years, FinCEN has become increasingly aware of the threats posed by virtual asset investment scams. These criminal activities target the American public and have caused billions of dollars in losses, as well as other immeasurable, devastating consequences for

victims.[1] BSA data has played an important role in helping law enforcement detect, investigate, and prosecute virtual asset investment scams. FinCEN has and will continue to produce products that increase and enhance BSA reporting, as well as support law enforcement on a variety of matters including efforts to recoup victim funds. FinCEN—through its public-private partnership initiatives and information sharing authorities—has encouraged collaboration between the public and private sectors to increase awareness and help detect, investigate, and deter these schemes.

Virtual Asset Investment Scheme Typologies

FinCEN, based on analysis of BSA reporting and extensive engagement with federal regulatory and law enforcement partners, has identified typologies for an unfortunately all-too-common type of virtual asset investment scheme, sometimes referred to by perpetrators as "pig butchering."

First, a scammer typically makes initial contact with a potential victim through text messages, direct messages on social media, or other communication tools and platforms. Once the scammer elicits a response from a victim, the scammer will communicate with them over time to establish trust and build a relationship.

Once trust or a relationship has been established, the scammer will introduce the victim to a supposedly lucrative investment opportunity in virtual currency and direct them to use virtual currency investment websites or applications. These sites are designed to appear legitimate but are fraudulent and ultimately controlled or manipulated by the scammer.

Once the victim invests with the scammer, the scammer will show the victim what appears to be extraordinary returns on the investment. These returns are fabricated in an effort to further deceive the victim and encourage them to invest more. When a victim's pace of investment slows or stops, the scammer will use even more aggressive tactics to extract any final payments, such as by demanding that any attempted withdrawal of funds follow an additional payment by the victim for purported taxes or early withdrawal fees. Once the victim stops paying into the scam, the scammer will abruptly cease communication with the victim, taking all the victim's funds with them.[2]

[1] Federal Bureau of Investigation Public Service Announcement, "The FBI Warns of a Spike in Cryptocurrency Investment Schemes," (March 2023 FBI PSA) (Mar. 14, 2023). Fraud involving cryptocurrency, including virtual asset investment scams , totaled more than $5.6 billion in reported losses in 2023. FBI Internet Crime Complaint Center, "Cryptocurrency Fraud Report 2023," (Sept. 9, 2024), at pp. 3, 7.

[2] "FinCEN Alert on Prevalent Virtual Currency Investment Scam Commonly Known as 'Pig Butchering'," FinCEN Alert #FIN-2023-Alert005, (Sept. 8, 2023)https://www.fincen.gov/sites/default/files/shared/FinCEN_Alert_Pig_Butchering_FINAL_508c.pdf

As this description makes clear, these scams involve very personal and private communications and transactions. Scammers often target victims and engage them by text or phone using personal messages. Victims frequently do not realize they have been targeted until it is too late.

FinCEN comes into the picture when our regulated financial institutions may have involvement with any of the transactions involved in these schemes. There are often a number of financial "touchpoints" that FinCEN may see through BSA reporting, the primary one being when a victim sends money to the scammer to fund the purported "investment." This is where a FinCEN alert or advisory comes into play—an alert can help a financial institution identify red flag typologies, including looking for a seeming change in behavior or transactional pattern of their client, which may indicate that the client is a victim of a scam.

Virtual asset investment scams often rely on victims first converting large sums of their money into cryptocurrency-denominated "investments." As a result, a substantial number of reports filed with FinCEN about these schemes involve clients of traditional financial services like depository institutions making suspicious large-dollar transfers to U.S.-based cryptocurrency exchanges as part of the first steps of a virtual asset investment scheme. Not all investment scams involve cryptocurrency. FinCEN also observes victims being defrauded using traditional payment mechanisms.

September 2023 Alert and Other Publications

FinCEN's September 2023 Alert focused on BSA reporting relating to the virtual asset investment scheme typology described above. The September 2023 Alert explained common methodologies associated with these scams, including tactics used by scammers to extract payments from victims and provided red flag indicators to assist financial institutions with identifying and reporting related suspicious activity potentially linked to virtual asset investment scams.

FinCEN developed the September 2023 Alert following sustained engagement with law enforcement and other partners, all of whom were witnessing an increase in these complex virtual asset investment scams, often involving international networks and substantial losses by victims, many of whom are U.S. citizens. As of September 2023, U.S. law enforcement estimated victims in the United States had lost billions of dollars to virtual currency investment frauds. The September 2023 Alert highlighted that these virtual asset investment scams often involve transnational criminal organizations (TCOs), and, in particular, TCOs based in Southeast Asia that use victims of labor trafficking to conduct outreach to millions of unsuspecting individuals around the world.

In addition to identifying typologies and red flags to enhance effective BSA reporting and promote public awareness, the September 2023 Alert also strongly encouraged financial institutions to share between themselves, consistent with Section 314(b) of the USA PATRIOT Act and FinCEN's implementing regulations. Consistent with these authorities, financial institutions may share information with each other regarding individuals, entities, and organizations for purposes of identifying and, where appropriate, reporting activities that may involve possible money laundering. Information sharing among financial institutions is critical to identifying, reporting, and preventing crime. As FinCEN explained in 2020 guidance regarding Section 314(b), financial institutions need not identify specific proceeds of a fraud scheme to share information about that scheme under Section 314(b); rather, it is sufficient that a financial institution possess only a reasonable basis for believing the information to be shared relates to potential fraud.

This September 2023 Alert is one of the most recent in a series of FinCEN products alerting the public and financial institutions to fraud and other scams. In June 2022, FinCEN published an Advisory on Elder Financial Exploitation (EFE), which built on a 2011 advisory on the same topic. The 2022 Advisory highlighted trends, typologies, red flags, and case studies on both elder theft schemes and elder scams targeting older adults.

In April 2024, FinCEN published a financial trend analysis (FTA) on EFE. This FTA presented FinCEN's analysis of BSA reporting filed largely in response to the 2022 Advisory and provided a statistical overview of trends in elder scam and theft methodologies. This type of analytic product demonstrates the value of providing financial institutions with actionable information through alerts and advisories and the importance of feedback loops between FinCEN, law enforcement, and financial institutions in enhancing the usefulness of BSA reporting. By focusing on BSA reporting filed in response to the September 2023 Alert, FinCEN can better focus its analytic products which, in turn, help support law enforcement in investigating virtual asset investment crimes and financial institutions in detecting and reporting them.

BSA Reporting on Virtual Asset Investment Fraud Following the September 2023 Alert

Since FinCEN issued the September 2023 Alert, we have received over 8,600 filings that reference the Alert. FinCEN continues to receive new filings every day. Based on a preliminary review of the filings since September 2023, 98 percent detail newly identified suspicious activity, and the remaining two percent of filings amend information that was previously reported in some form. As of early September 2024, FinCEN received an average of 164 filings per week referencing the September 2023 Alert, and we have seen a steady increase in reporting on these schemes each month since the Alert's publication. For example, in December 2023, FinCEN received 437 reports that referenced the Alert; in August 2024, FinCEN received over 1,560 reports.

As of August 2024, FinCEN analysis indicates that filings referencing the September 2023 Alert are predominantly submitted by depository institutions and cryptocurrency exchanges. More than six-hundred different depository institutions filed 45 percent of all the alert filings. Twenty-seven different money services businesses (MSBs) filed 44 percent of all the alert filings (ninety-five percent of these MSB filings were submitted to FinCEN from cryptocurrency exchanges). The remaining eleven percent of filings referencing the Alert were submitted by securities or futures trading entities, insurance providers, housing government-sponsored enterprises, lenders, and check cashers.

Preliminary FinCEN's analysis of BSA reporting further indicates that the perpetrators of virtual asset investment scams may reside in a variety of jurisdictions, including Hong Kong, China, and Vietnam. While the relevant BSA reporting does not always indicate where a perpetrator may be located, those filings that listed a location often noted that perpetrators had successfully convinced a victim to make a payment to a fraudulent actor abroad.

FinCEN's preliminary analysis of reporting referencing the Alert has revealed dozens of variations on the typologies described in the Alert, including schemes that involve multiple victims. FinCEN has identified tens of thousands of victims in BSA reporting and the number continues to grow. BSA reporting indicates that victims are typically contacted through websites, social media applications, phone calls, text messages, dating applications, or other mobile applications. Victims were reported in at least 41 states across the United States, with a much smaller number of victims in a handful of other countries, including Canada, China, and Hong Kong. The top states where victims were located included California, Texas, Florida, Washington, Colorado, Michigan, Minnesota, and Oregon. Perpetrators of these schemes spend a significant amount of time developing a relationship with their victims. On average, perpetrators were in contact with victims for more than 100 days during the duration of the scam, according to the reports filed with FinCEN.

Ongoing Work to Combat Virtual Asset Investment Scams and Other Fraud

FinCEN has observed an increase in fraud and cybercrime in our data every year since at least 2013. Earlier this year, FinCEN published a Financial Trend Analysis that quantified 10 typologies that were associated with fraud or cybercrime in 2021.[3] General Fraud was the largest typology in both volume and value. We received 1.2 million records totaling at least $149 billion in 2021 related to General Fraud—about a third of all 3.8 million SARs we received that year. Preliminary analysis indicates that General Fraud reported in SARs continued to increase

[3] FinCEN Financial Trend Analysis "Identity-Related Suspicious Activity: 2021 Threats and Trends", 9 January 2024, https://www.fincen.gov/sites/default/files/shared/FTA_Identity_Final508.pdf.

approximately seven percent in value each year through 2023. Due to the scope of this threat, FinCEN has placed significant resources into addressing it.

The Value of BSA Reporting

FinCEN is continuing to use the leads and insights provided through BSA reporting to develop analytic products and to inform our collaboration with a variety of stakeholders targeting this issue including regulators, law enforcement, and other government partners. FinCEN actively provides leads to our partners and analytic support to further their existing investigations.

FinCEN also provides extensive training to federal, state, and local law enforcement entities with access to BSA information to ensure they understand how to use it appropriately and effectively in their investigations. In Fiscal Year 2023, FinCEN provided more than 515 separate training sessions to more than 20,000 registered users of the BSA database. FinCEN consistently sees powerful indicators of the success of these outreach and training efforts.

FinCEN's Law Enforcement Awards Program is an important mechanism through which FinCEN communicates with financial institutions and with the public about the tremendous value of BSA reporting. Over the past 10 years, FinCEN has recognized agencies that used BSA data to successfully pursue and prosecute criminal investigations. Last year, we recognized important cases investigated by a wide variety of federal law enforcement agencies across different categories, including fraud, cybercrime, human trafficking, and smuggling.

Use of Additional FinCEN Authorities

In addition to FinCEN's public facing products, FinCEN has a variety of authorities and programs that we leverage to combat fraud, cybercrime, and virtual asset investment scams including the Rapid Response Program, FinCEN Exchanges, and Sections 314(a) and 314(b) of the USA PATRIOT Act (and FinCEN's implementing regulations).

Through the Rapid Response Program, FinCEN helps victims and their financial institutions recover funds stolen as the result of certain cyber-enabled financial fraud schemes. The Rapid Response Program is a partnership among FinCEN, U.S. law enforcement, and foreign partner agencies that, like FinCEN, are the financial intelligence units (FIUs) of their respective jurisdictions. When appropriate, FinCEN shares financial intelligence rapidly with counterpart FIUs and encourages foreign authorities to interdict the fraudulent transactions, freeze funds, and stop and recall payments using their authorities under their own respective legal and regulatory frameworks. In Fiscal Year 2023, FinCEN's Rapid Response Program received 686 requests involving 88 foreign jurisdictions and as a result of the Rapid Response Program, foreign jurisdictions froze $100 million, about one-third of the stolen funds reported to the Rapid

Response Program. Since 2014, the Rapid Response Program has assisted in freezing more than $1.5 billion.

FinCEN also continues to leverage and expand the FinCEN Exchange program to bring together U.S. law enforcement and private sector audiences to discuss fraud schemes. FinCEN Exchange provides a forum for voluntary and confidential sharing of trends and typologies among participating entities. FinCEN Exchange events have focused on cryptocurrency confidence schemes and build on the success of FinCEN's ongoing series of nationwide FinCEN Exchange events on Promoting Regional Outreach to Educate Communities on the Threat of Fentanyl ("PROTECT").

FinCEN also encourages financial institutions and law enforcement to utilize information sharing authorities under Sections 314(a) and 314(b) of the USA PATRIOT Act. These authorities allow for information sharing in targeted ways to help law enforcement identify and investigate criminal activity, and both can be powerful tools for combatting money laundering associated with virtual asset investment scams and other fraud.

Section 314(a) and FinCEN's regulations permit authorized law enforcement agencies to submit requests through FinCEN to financial institutions to locate accounts and transactions of persons that may be involved in terrorism or significant money laundering. Law enforcement often reports that the 314(a) program is a critical source of information that helps them build their investigations.

Under Section 314(b) and FinCEN's regulations, financial institutions, upon providing notice to FinCEN, are permitted to share information with one another under a safe harbor to identify and report activities that may involve money laundering or terrorist activity. As of Fiscal Year 2023, 7,790 financial institutions were registered to participate in 314(b) information sharing, most of which were banks, credit unions, or securities and futures firms. Financial institutions that participate in 314(b) can file joint SARs that reflect their shared understanding of activity of concern. At FinCEN, we often call the SARs that result from 314(b) information sharing "super SARs" because of the insights they provide to us and to law enforcement and national security organizations. As with 314(a), we often receive feedback from law enforcement about the tremendous value of this program.

Closing

I want to conclude by thanking the Committee for the opportunity to testify today on this important topic.

My colleagues and I at FinCEN appreciate the continued, bipartisan support from Congress in our efforts to safeguard the financial system from illicit use. We take this responsibility seriously and we will continue to use our resources and authorities effectively to keep the American financial system and the American public safe.

I look forward to your questions.