Protecting Americans' Savings: Examining the Economics of the Multi-Billion Dollar Romance Confidence Scam Industry
House Financial Services Committee
Subcommittee on National Security, Illicit Finance, and International Financial Institutions
September 18, 2024
Deputy Assistant Secretary Scott Rembrandt
U.S. Department of the Treasury
Written Testimony

Good morning, Chairman McHenry, Chairman Luetkemeyer, Ranking Member Waters, and Ranking Member Beatty, as well as Distinguished Members of the subcommittee. Thank you for the invitation to speak today about virtual asset investment scams.

My name is Scott Rembrandt, and I am the Deputy Assistant Secretary for Strategic Policy in the U.S. Department of Treasury's Office of Terrorist Financing and Financial Crimes. I am a career staffer and have been with the Department for over fifteen years. Our office leads policy coordination, development, and outreach for Treasury's anti-money laundering/countering the financing of terrorism (AML/CFT) and sanctions functions. I also lead the U.S. delegation to the Financial Action Task Force (FATF), the international standard-setter for combating money laundering and the financing of terrorism and the proliferation of weapons of mass destruction.

Today, I plan to discuss (1) Treasury's assessments on the money laundering threats and vulnerabilities associated with virtual asset investment scams, (2) how Treasury employs its tools and resources to mitigate the risks associated with these schemes and misuse of virtual assets more broadly, and (3) Treasury actions to disrupt the criminal networks that underpin these scams.

Scope of the problem

Today's topic is a critical subject with a devastating impact. Virtual asset investment scams, in particular schemes commonly referred to by perpetrators "pig butchering" defraud victims of their savings and in one instance resulted in the failure of a bank. In this case, the Chief Executive Officer (CEO) of Heartland Tri-State Bank, a depository institution focused on agriculture lending in Kansas serving approximately 2,000 accountholders, initiated a series of wire transfers totaling about $47.1 million of Heartland's funds as part of a virtual asset investment scam. The wire transfers impaired the bank's capital and liquidity, causing the bank to become insolvent. In another instance, an Illinois woman lost over $1 million to a virtual asset investment scam after withdrawing cash from her bank account, investment accounts, and a home equity loan. She was forced to sell her home and possessions as a result. Importantly, these are only two of the tens of thousands of tragic stories demonstrating the consequences of these scams.

Over the last several years, investment schemes involving virtual assets eclipsed other types of investment scams, according to victim reporting to the Federal Bureau of Investigation (FBI). In 2023, reported losses from investment scams involving virtual assets reached nearly $4 billion, an increase of over 53 percent from the previous year. Reported losses from investment schemes involving virtual assets accounted for over 85 percent of all reported losses for investment scams in 2023.

Use of Technology to Profit off the Most Vulnerable

In seeking to tackle this issue, we need to ask how and why these frauds occur before we can effectively combat them. Of course, at bottom these investment scams are driven by the perpetrators seeking to steal money from victims. But t these crimes also involve human vulnerability, human desire for quick profit, growing reliance and comfort with utilizing technology for financial services, an ability to move funds cross-border nearly instantaneously, weak foreign AML/CFT regimes for virtual assets, and the use of tools and methods to obfuscate the identity of criminals and their criminal proceeds.

Virtual asset investment scams involve a variety of traditional fraud fact patterns based on misrepresentations concerning potential investment opportunities in virtual assets. The most potent of these schemes are cryptocurrency confidence schemes. Typically, in these kinds of schemes, the scammer develops an online relationship with the victim, entices the victim to transfer currency or virtual assets into purported investment platforms or wallet addresses controlled by others involved in the scheme, and the victim loses all access to those funds.

Once the conspirators receive funds from victims, they often need to launder their illicit proceeds before they are able to use them. As part of this laundering process, scammers often send funds to foreign-located VASPs, including VASPs in jurisdictions with weak or non-existent AML/CFT controls, for VASPs to exchange the virtual assets for fiat currency.

For example, scammers may move funds through several unhosted wallet addresses or exchange these funds between virtual assets on different blockchains, a process referred to as chain hopping. Criminals constantly evolve their techniques to obfuscate illicit proceeds and know how to use these techniques effectively. As part of this laundering process, scammers often send funds to foreign-located VASPs in jurisdictions with weak or non-existent AML/CFT controls for VASPs to exchange the virtual assets for fiat currency.

Defrauded investors, however, are not the only victims of these scams. Many individuals involved in the scams are themselves victims of human trafficking, who are forced to contact victims and manipulate them. Virtual asset investment scams are often run by criminal networks that place fake job advertisements on social media and online employment sites to attract young English-speakers from Asian, African, and other countries. The schemes cover a wide range of opportunities, to include tech support, call center customer service, and beauty salon technicians. Job seekers are offered competitive salaries, lucrative benefits and paid travel expenses, as well as room and board. Often throughout the process, the location for the position is shifted from the advertised location.

Upon job seekers' arrival in a foreign country, criminal actors confiscate passports and travel documents, threaten or use violence to coerce victims to commit virtual asset investment scams, and may transport these human trafficking victims to third countries. Forced labor victims are required to meet quotas for targeting fraud victims, using scripts provided by the criminal actors running the operations. Moreover, forced labor victims are often required to live in poor conditions and criminals assign debts to victims under the guise of travel fees and room and board, using victims' mounting debt and fear of local law enforcement as additional means to control victims. Trafficked victims are sometimes sold and transferred between compounds, further adding to their debt. While this generally occurs in Southeast Asia, we have seen this model replicated in other parts of the world, including Latin America and Africa.

Money Laundering Threats and Vulnerabilities

At the Treasury Department, we employ our arsenal of tools to identify and disrupt all forms of illicit finance, including virtual asset investment scams. To do so, we require a strong understanding of key threats, risks, and vulnerabilities facing our financial system. This includes identifying the key criminal networks misusing our financial system and the methods they use to do so and developing and implementing strategies to deter, detect, and disrupt their ability to profit from their crimes.

Every two years, the Treasury Department, led by my office, publishes national risk assessments on money laundering, terrorist financing, and proliferation financing, as well as a national illicit finance strategy that highlight how the United States combats these threats. The most recent iteration of our National Risk Assessments published in February of this year found that the United States faces a variety of illicit finance threats. The most concerning threats involve fraudsters, drug trafficking organizations, cybercriminals, corruption, human trafficking and human smuggling organizations, and those seeking to finance terrorism and proliferation. Virtual asset use by illicit actors is increasing across all typologies, even while traditional money laundering, terrorist financing, and proliferation financing methods remain most common. And for certain illicit finance typologies, the use of virtual assets has grown rapidly or become predominant.

Illicit actors capitalize on a range of key vulnerabilities in our AML/CFT regime to conduct their activities, including: (1) abusing legal entities to conceal the ultimate owner of assets; (2) exploiting uneven obligations on certain financial intermediaries; (3) utilizing touchpoints of the U.S. financial system to foreign jurisdictions with weaknesses in their AML/CFT regimes; (4) exploiting occasional AML/CFT compliance deficiencies at U.S. financial institutions; and (5) taking advantage of challenges in detecting illicit cash and complicit merchants and professionals.

In the virtual asset context, the 2024 National Money Laundering Risk Assessment (NMLRA) identified several threat actors using virtual assets and VASPs to generate revenue or launder their proceeds, including scammers, ransomware cybercriminals, Democratic People's Republic of Korea (DPRK) actors, and drug traffickers.

Ransomware criminals continue to pose a critical threat to U.S. national security and our infrastructure and mainly demand payments in virtual assets. For example, the ransomware attack on the company Change Healthcare earlier this year disrupted payment processing, prescription writing, and insurance claims for patients and health care providers nationwide. Ransomware actors have increased the potency of their attacks and exerted greater pressure on victims to pay, including by sharing resources or forming partnerships with other cybercriminals to enhance the effectiveness of their attacks. These criminals use many of the same money laundering methods as do scammers and other bad actors before exchanging them for fiat currency at foreign-based VASPs.

Additionally, DPRK continues to advance its illicit exploitation of new financial technologies, including using virtual assets to raise and move money. According to the UN Panel of Experts, the DPRK attempted to steal as much as $2 billion between 2015 and 2019 through cyber means. DPRK uses similar methods to launder funds as scammers and ransomware actors, although DPRK cyber actors tend to be more sophisticated and typically leverage over-the-counter traders to convert laundered virtual assets into fiat currency.

The NMLRA also identifies vulnerabilities related to misuse of virtual assets, including jurisdictional arbitrage, non-compliance by VASPs with applicable U.S. AML/CFT and sanctions obligations, and the use of anonymity-enhancing technologies.

While there has been notable progress worldwide in improving the regulation and supervision of virtual assets and VASPs, the fact of the matter is that virtual assets and VASPs continue to be poorly regulated and supervised across much of the globe, making our own financial system less safe The FATF clarified how its global standards apply to virtual assets and VASPs a half decade ago. But a voluntary survey of jurisdictions conducted by the FATF and released this year found that a large number of jurisdictions continue to struggle to implement AML/CFT regulations for virtual assets or fail to effectively regulate the sector. According to the FATF survey, nearly 40 countries had not even determined how they planned to approach virtual assets and VASPs for AML/CFT purposes, including five countries that had determined virtual assets to pose high illicit finance risks. Critically, nearly 100 jurisdictions had not conducted an adequate risk assessment as of mid-2024.

Woefully inadequate or non-existent regulation and supervision across many jurisdictions means that VASPs in countries without effective AML/CFT frameworks have little incentive to implement sufficient AML/CFT controls or other processes to identify customers. Failure to collect appropriate identifying information for virtual asset customers can allow placement, layering, and integration of illicit proceeds to occur instantaneously and pseudonymously.

The NMLRA also recognized that human trafficking is one of the most significant money laundering threats in the United States. Beyond its enormous human costs, human trafficking is one of the most profitable crimes and predicate offenses for money laundering. Financial activity from human trafficking can intersect with the regulated financial system at any point during the recruitment, transportation, and exploitation stages.

Transactions related to human trafficking can include payments associated with the transport and housing of victims; the collection of proceeds generated by the exploitation of trafficking victims; and the movement of proceeds. Illicit proceeds from human trafficking can be paid or transferred in cash, electronic funds transfers and remittance systems, credit card transactions, payment apps, or virtual assets. Money laundering schemes related to human trafficking use purchases of real estate, shell companies, wire transfers, credit cards, bulk cash transfers, and virtual assets to launder funds.

Combating Virtual Asset Investment Scams and Human Trafficking

The Department of the Treasury is hard at work to stop criminals from moving funds generated from virtual asset investment scams and human trafficking.

Our efforts to combat virtual asset investment scams involve: (1) working with domestic financial institutions to ensure that they have the latest information on fraud, including related to virtual assets and human trafficking; (2) supporting law enforcement investigations involving these crimes; (3) monitoring financial institution compliance with Bank Secrecy Act (BSA) obligations and taking action for non-compliance; (4) using Treasury sanctions authorities to identify and cut off from the international financial system criminal actors profiting from these activities; (5) engaging with international partners to level the playing field so that criminals cannot continue to take advantage of jurisdictions with weak or no AML/CFT controls for virtual assets and VASPs; (6) reforming our domestic AML/CFT framework; and (7) working with Congress to clarify and strengthen our authorities related to virtual assets and to ensure they are in line with emerging risks and vulnerabilities.

Working with domestic financial institutions

Treasury and others in the U.S. government are sharing information with financial institutions to support the identification and reporting of information that may be related to virtual asset investment scams. As my colleague Dara Daniels at FinCEN will elaborate, in September 2023 FinCEN issued an alert that outlines the scam methodologies and red flag indicators for this purpose and has published other products over the years outlining risks associated with other types of scams and fraud. Law enforcement and other regulators, such as the Federal Deposit Insurance Corporation and Consumer Financial Protection Bureau, have also issued several public notices as early as 2022 alerting potential victims to red flags that could be indicative of virtual asset investment scams. In fact, just last week, FBI published a comprehensive report specifically focused on virtual asset scams, including investment scams. This information can assist financial institutions, including compliant virtual asset services providers, working to detect these schemes. Financial institutions play a critical role in identifying, reporting, and preventing investment scams and related activity, and such reporting enhances important feedback loops that help the government better detect such activity.

Supporting law enforcement investigations

The effective use of financial information and intelligence aids law enforcement in investigating and prosecuting unlawful activities; seizing, restraining, and forfeiting assets; and taking other disruptive actions. My colleague from FinCEN will share more details on how FinCEN works with law enforcement to effectively leverage financial information and share their expertise on a daily basis. Part of combating virtual asset investment scams is disrupting the illegitimate websites and applications fraudsters use to steal victims' funds and recovering assets that can be returned to victims. We have seen several cases of successful recovery of virtual assets paid to scammers due to the hard work of our law enforcement partners. For example, in April 2023, the Department of Justice seized virtual assets worth an estimated $112 million linked to accounts that were allegedly used to launder the proceeds of various virtual asset investment scams.

Monitoring for BSA compliance and enforcement actions

As noted above, both victims and scammers use VASPs. Victims use VASPs to exchange fiat currency to fund transfers to virtual asset investment scam platforms; scammers use VASPs, including non-compliant VASPs, to receive, move, launder, and cash out criminal proceeds generated from these scams Critically, there have been several instances in which VASPs operating in the United States have failed to comply with applicable AML/CFT and sanctions obligations. These instances provide opportunities for criminals, like scammers, to exploit these services to receive virtual assets from victims, launder their illicit proceeds, and exchange them for fiat currency. In some cases of non-compliance, VASPs claim not to be subject to U.S.

jurisdiction despite doing business wholly or in substantial part in the United States. In other cases, VASPs subject to BSA obligations scaled up quickly without adequately assessing and mitigating potential regulatory risks associated with providing new or additional services.

When necessary, Treasury has used our tools and authorities to impose consequences on firms choosing to operate without regard for these risks or taking appropriate steps to mitigate them. For instance, last November, Treasury took the largest enforcement action in our history against Binance, the world's largest VASP, for willful violations of the BSA and apparent violations of sanctions laws. Binance had critical gaps in its AML program and practices, from a lack of risk-based procedures for various offerings to instructing staff to withhold information from law enforcement. As a result of its failure to institute proper AML controls, criminals used Binance to process transactions related to scams, child sexual abuse, illegal narcotics, and terrorism. Binance willfully failed to report well over 100,000 suspicious transactions.

FinCEN's settlement agreement with Binance assessed a penalty of $3.4 billion. Treasury's Office of Foreign Assets Control's (OFAC) settlement agreement assessed a penalty of nearly $1 billion. Among other requirements, the settlement agreements subject Binance to increased scrutiny for five years through a third-party monitor, overseen by FinCEN, who will ensure Binance's complete exit from the United States. Failure to live up to the agreements could expose Binance to substantial additional penalties.

Using OFAC sanctions authorities

Additionally, Treasury is using sanctions authorities to cut off actors that profit from investment scams, human trafficking, and other illicit activity. On September 12, OFAC took an important action to hold accountable one criminal network behind these schemes, which is detailed below. This action follows years of sanctions designations to expose and cut off actors misusing virtual assets, including VASPs, from the U.S. financial system. For example, OFAC has designated three mixers involved in laundering virtual assets, including for the DPRK; darknet markets, including Hydra, the world's largest and most prominent darknet market; and several VASPs transacting with illicit actors, including darknet markets and ransomware criminals. By targeting these nodes, we are shrinking the space in the virtual asset ecosystem available to profit from crime, including fraud and scams.

Treasury is also using sanctions to target individuals who create or maintain the infrastructure that criminals use to execute certain scams and fraud. For example, in May of this year, OFAC designated three individuals for their activities associated with a malicious botnet. The malicious botnet technology could be used by cybercriminals to disguise their digital tracks and defeat some fraud detection systems. The action was taken in partnership with the FBI, Defense Criminal Investigative Service, U.S. Department of Commerce's Office of Export Enforcement, as well as partners in Singapore and Thailand, maximizing the impact of any one effort.

Engaging international partners

As noted above, many countries lack effective AML/CFT frameworks for virtual assets and VASPs, which provides opportunities for illicit actors like fraudsters and scammers to use VASPs without providing identifying information or facing any risk of detection. The United States is co-leading critical work to address this vulnerability through the FATF, focusing on two key priorities: (1) closing gaps in implementation of the FATF standards, in particular in countries with substantial virtual asset activity, and (2) assessing potential impacts associated with emerging risks.

To close these global, regulatory gaps, the FATF in March released a public table to identify countries that have substantial virtual asset activity and highlight whether they have AML/CFT frameworks for virtual assets in place. In addition to publicly highlighting deficiencies, the FATF is also working to provide these countries with opportunities for formal technical assistance. Treasury also engages bilaterally with countries to provide training, briefings, and to share our experience in regulating and supervising the VASP sector in the United States.

Reforming domestic AML/CFT frameworks

While we work with other countries to address their AML/CFT gaps and vulnerabilities, strengthening our response to illicit finance here in the United States is also critical. Over the past few years—and especially over the past nine months—Treasury has advanced a series of historic reforms and upgrades to our AML/CFT regime to address our biggest vulnerabilities. While these reforms are not be specific to virtual assets, they will have a resounding effect on the broader U.S. financial system. In January, pursuant to the bipartisan Corporate Transparency Act (CTA), enacted as part of the William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021, FinCEN operationalized its new beneficial ownership information filing system, under which many companies operating in the United States are required to report to FinCEN information about their beneficial owners—the real people who own or control them. This new framework will help unmask the anonymous companies that illicit actors exploit to move and launder funds in the United States, while helping law enforcement pursue accountability for the people behind illicit schemes.

Last month, FinCEN finalized two rulemakings that will help prevent illicit activity through two other sectors that are frequently misused by illicit actors to launder funds: the residential real estate sector and the investment adviser industry. The residential real estate rule will require certain industry professionals to report information to FinCEN about non-financed transfers of residential real estate to a legal entity or trust, which present a high illicit finance risk. The rule will increase transparency, limit the ability of illicit actors to anonymously launder illicit proceeds through the American housing market, and bolster law enforcement investigative efforts. The investment adviser rule will apply AML/CFT requirements, including Suspicious Activity Report filing obligations, to certain investment advisers that are registered with the U.S. Securities and Exchange Commission (SEC), as well as those that report to the SEC as exempt reporting advisers. These advisers manage upwards of $100 trillion in assets, but until last month were not subject to comprehensive or consistent AML/CFT obligations. This uneven regulatory landscape across the financial services industry allowed illicit actors to "shop around" for an adviser that did not need to inquire into their source of wealth or funds.

Proposals for Congress

Deputy Secretary Adeyemo has testified about the growing illicit finance risks associated with virtual assets and VASPs. Last fall, he sent a term sheet of proposed legislative solutions to help Treasury better address emerging risks and ensure that our tools are fit for purpose. We have been working with Congress to provide technical assistance with regards to these proposals. While we have had some success in rooting out illicit finance in the digital asset ecosystem, we need to continue to build a more robust regime to help effectively address this kind of activity as scammers and other illicit actors increasingly use virtual assets.

This work has focused on strengthening our ability to meet the challenges presented by VASPs operating in or with touchpoints to jurisdictions with weak or non-existent AML/CFT and sanctions frameworks for virtual assets and VASPs. For example, the proposals sent in

November 2023 included requests for clarification about the application of both OFAC and FinCEN authorities to offshore VASPs and an extension of OFAC jurisdiction to issuers of stablecoins pegged to U.S. dollars.

Moreover, we have also proposed statutory changes that would update our AML/CFT and sanctions frameworks to clarify how they apply in the digital asset ecosystem, to drive compliance and enhance enforcement efforts. This includes provisions related to creating a new virtual asset-related category of financial institution under the BSA that would explicitly provide OFAC the authority to deploy secondary sanctions, an impactful and flexible tool, against virtual asset firms doing business with sanctioned entities.

In addition to this work, Treasury has long advocated for legislation to address the risks of stablecoins in a comprehensive and consistent manner. This includes strong AML/CFT standards.

Importantly, while Treasury appreciates the support from Congress since passage of the Anti-Money Laundering Act of 2020 (AMLA), enacted as part of the William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021, the President's budget request continues to more accurately reflect Treasury's mission requirements.

Human trafficking

Another crime that we see associated with virtual asset investment scams and other forms of illicit finance is human trafficking. Perpetrators of this abhorrent crime prey on vulnerable populations, infiltrate critical supply chains and industries, and launder proceeds through U.S. and international financial systems. By pursuing the profits associated with human trafficking, we can disrupt the illicit networks behind this crime. In looking at the ways in which human traffickers launder, move, or stash their illicit proceeds, we can see how our historic reforms can further protect the U.S. financial system from abuse by these criminals.

As noted above, human traffickers often use shell companies to obscure their criminal activities. That is one reason why Treasury has prioritized efforts to prevent human traffickers and other criminals from laundering illicit funds through anonymous shell companies in the United States. The creation of the new beneficial ownership information filing system mentioned above will equip law enforcement with beneficial ownership information to disrupt the financial anonymity that enables human trafficking. Additionally, human trafficking networks also mask profits through real estate transactions. Treasury's finalized rule on residential real estate will help prevent human traffickers from achieving impunity through financial anonymity. Furthermore, our work in closing gaps in AML/CFT frameworks for virtual assets and VASPs around the world can mitigate against human traffickers misusing virtual assets to perpetuate or profit from their crimes.

Human trafficking remains a focus of Treasury's sanctions authorities. I would like to highlight Treasury's most recent action, which demonstrates our commitment to disrupting the criminal networks that both defraud investors and perpetrate human rights abuses.

Just last week, OFAC designated Cambodian Senator and tycoon Ly Yong Phat, his conglomerate the L.Y.P. Group Co., LTD, and O-Smach Resort under the Global Magnitsky sanctions authority for their role in serious human rights abuse related to treatment of trafficked workers forced to engage in virtual asset investment scams. OFAC also designated Garden City Hotel, Koh Kong Resort, and Phnom Penh Hotel for being owned or controlled by Ly.

This action illustrates the scale and atrocities involved in these schemes. For more than two years, from 2022 to 2024, O-Smach Resort has been investigated by police and publicly reported on for extensive and systematic serious human rights abuses. Victims reported being lured to O-Smach Resort with false employment opportunities, having their phones and passports confiscated upon arrival, and being instructed to work scam operations. People who called for help reported being beaten, tortured with electric shocks, made to pay a hefty ransom, or threatened with being sold to other online scam gangs. There have been two reports of victims jumping to their death from buildings within O-Smach Resort.

This action builds upon previous designations to expose and hold accountable criminal networks that use forced labor to perpetrate further crimes. Treasury will continue to investigate cases like this one, use our tools to disrupt this activity, and call on host governments to secure the safe release and return of all people held in such conditions.

Closing

I appreciate the opportunity to highlight this critical issue and share Treasury's work to protect the U.S. financial system from misuse related to virtual asset investment scams and human trafficking. I want to close by thanking the subcommittee for its support and its collaborative work with Treasury. I look forward to taking your questions.