U.S. Immigration and Customs Enforcement

STATEMENT

OF

JOHN EISERT
ASSISTANT DIRECTOR FOR
INVESTIGATIVE PROGRAMS
HOMELAND SECURITY INVESTIGATIONS

U.S. IMMIGRATION AND CUSTOMS ENFORCEMENT
DEPARTMENT OF HOMELAND SECURITY

REGARDING A HEARING ON

"Terrorism and Digital Financing: How Technology is Changing the Threat."

BEFORE THE

U.S. HOUSE OF REPRESENTATIVES COMMITTEE ON HOMELAND SECURITY
SUBCOMMITTEE ON INTELLIGENCE AND COUNTERTERRORISM

Thursday, July 22, 2021
310 Cannon House Office Building

Chairwoman Slotkin, Ranking Member Pfluger, and distinguished members:

Introduction

Thank you for the opportunity to appear before you to discuss the critical investigative role U.S. Immigration and Customs Enforcement (ICE) Homeland Security Investigations (HSI) plays in the fight to protect the homeland from transnational crime and other threats. My testimony today will focus on HSI's efforts to identify, investigate, and ultimately bring to justice criminal and terrorist organizations whose illicit use of cryptocurrency jeopardizes the national security and public safety of the United States.

The HSI Mission

As the largest investigative component of the Department of Homeland Security, HSI is the premier law enforcement organization responsible for conducting federal criminal investigations into the illegal cross-border movement of goods, money, technology, people, and other contraband into, out of, and throughout the United States. HSI strives to protect the homeland's digital borders and pursue malicious cyber actors with the same dedication it safeguards our land and sea borders from traditional organized transnational crime.

HSI's operational priorities serve as the foundation of HSI's investigative and enforcement focus. HSI applies its unique authorities and capabilities to conduct complex and significant transnational investigations aligned with these priorities, which include combating financial crime, investigating cybercrime, and protecting national security. The illicit use of cryptocurrency by nefarious actors relates to each of these priorities and represents a key area of focus for HSI's investigations and operations.

HSI participates in and has representation on dozens of collaborative cyber-related efforts, including the HSI Cyber Crimes Center, the Federal Bureau of Investigation's National Cyber Investigative Joint Task Force, the U.S. Secret Service Electronic Crimes Task Force, and the DHS Science and Technology Internet Anonymity Project Working Group.

Cryptocurrency and the Threat it Poses to the Homeland

A cryptocurrency is a digital asset that works as a medium of exchange, a unit of account, or a store of value. Cryptocurrency uses strong cryptography to secure financial transactions, control the creation of additional units, and verify the transfer of assets. In 2009, Bitcoin was introduced as the first decentralized convertible virtual currency and offered a high level of pseudo-anonymity for people to send and receive money over the internet. While Bitcoin is by far the most popular and well-known cryptocurrency, thousands of cryptocurrencies have been created and new ones are created every day. There is open source or proprietary software that anyone can use to create a cryptocurrency.

Since 2009 cryptocurrencies have increasingly been used as the currency of choice to facilitate crime. From individual actors to large scale transnational criminal organizations

(TCOs), cryptocurrency can be exploited by any criminal organization engaged in almost any type of illicit activity. Cryptocurrencies are attractive to criminal and terrorist organizations because they offer a relatively fast, inexpensive, and pseudonymous system of transactions as compared to more traditional financial transactions.

HSI has seen that nefarious actors are inclined to use cryptocurrency based on the perception that there is anonymity associated with their transactions or that because cryptocurrency used during an illicit scheme can be moved immediately offshore to a foreign exchange or over the counter trader (OTC), that U.S. law enforcement entities will be unable to trace or to seize and recover the assets. In addition, cryptocurrency offers the ability to engage in money laundering with minimal effort. By using OTCs or offshore exchanges, cryptocurrency can be laundered and reintroduced into the U.S. financial system relatively easily by utilizing typical laundering techniques of placement and layering. When used to fund terrorist operations and activities, terrorist organizations often have the opposite requirement. They seek to conceal the origin of funds from donors, businesses, and other legitimate sources to avoid law enforcement scrutiny.

HSI has seen nefarious actors expend cryptocurrency in furtherance of a wide array of crimes HSI investigates. Both at home and abroad, cryptocurrency can be used to purchase illicit items such as drugs or guns on darknet marketplaces; to launder criminally derived proceeds; or to provide material support to or funding for terrorist actors or organizations to carry out operations. Cryptocurrency can also be used to pay fraudsters, ransomware actors, or individuals involved in other illicit schemes such as intellectual property theft and illegal technology procurement. In addition, current trends indicate cryptocurrency is becoming prevalent within criminal organizations involved in child exploitation and human trafficking. Whether expended by TCOs, or terrorist organizations, or facilitators of such organizations, the use of cryptocurrency by bad actors continues to expand and evolve and presents a potential threat to the national security and public safety of the United States.

HSI's Lines of Effort

Given that cryptocurrency is used across the spectrum of crimes that HSI has the authority to investigate, HSI plays a critical role in the U.S. government's efforts to detect, investigate, and prevent its illicit use by criminal and terrorist actors. Using its authorities and subject matter expertise in financial, cyber, and national security cases; its strong strategic partnerships; and its robust international footprint, HSI employs a multi-faceted approach to combat crimes enabled by the use of cryptocurrency. This approach is rooted in HSI's investigative expertise, and supplemented by robust collaboration, training, and outreach programs. These efforts are described below.

Investigations:

Bitcoin and other cryptocurrencies are attractive to bad actors because of their pseudo-anonymity and ease of transfer, but at some point, criminals need to convert their cash into cryptocurrency or their cryptocurrency into cash. Whenever monetary exchanges are made, a chokepoint is created. This is the time when criminals are most vulnerable and can be identified

through law enforcement means and methods. Using traditional investigative methods such as surveillance, undercover operations, and confidential informants, coupled with sophisticated financial and blockchain analysis, HSI can take advantage of these chokepoints and use them to identify, disrupt and dismantle the terrorist organizations and TCOs.

In 2013, the U.S. Department of the Treasury's Financial Crimes Enforcement Network issued guidance clarifying that certain persons or companies that exchange convertible virtual currency, such as cryptocurrency, are considered money services businesses (MSBs), and therefore must follow the same regulatory and reporting protocols as traditional MSBs. The protocols include developing and implementing an anti-money laundering compliance program, filing suspicious activity reports, and registration requirements, among others. These procedures include "Know Your Customer" measures to record personal identifying information from customers to mitigate fraud. Lawful users of cryptocurrencies tend to use registered, compliant cryptocurrency exchanges that adhere to regulatory and operational measures in exchange for security, low fees, and the ease of processing transactions.

Those who use cryptocurrency for illegal purposes generally avoid registered exchanges and seek illicit or unregistered exchanges that do not require or ask for personal identifying information. These illicit exchanges often take the form of a direct Peer-to-Peer (P2P) exchanger. P2P exchangers post advertisements stating the price for which they are willing to either buy or sell cryptocurrency online. Although some P2P exchangers do register with FinCEN and state authorities and follow compliance laws, most do not. Rather, these illicit P2P exchangers position themselves as the money launderers in the cryptocurrency world. P2P exchangers illegally generate revenue by charging a premium for allowing their customers to remain anonymous. They will sell cryptocurrency above market value and buy below market value to or from those customers who want to remain anonymous.

Targeting these illicit P2P exchangers enables HSI to open the door and pull back the veil of pseudo-anonymity provided by cryptocurrencies. HSI can identify other criminals using cryptocurrency to fund and further their illicit activities through interviews and suspect cooperation; forensic analysis of computers, mobile phones, and other seized electronics; and the use of advanced blockchain tracing tools.

Since 2018, HSI's Cryptocurrency Intelligence Program (CIP), housed at the National Bulk Cash Smuggling Center, has targeted unlicensed cryptocurrency MSBs and other gatekeepers in the cryptocurrency space. CIP provides blockchain forensics and analytics support to HSI investigators, as well as state, local, and international partners investigating cryptocurrency-enabled crimes. CIP uses technical and subject matter expertise to exploit blockchain evidence, guide agency policy, monitor market intelligence, and regularly engages with private sector partners such as exchanges, other virtual asset service providers and the blockchain industry groups.

Collaboration:

With the rapid development of new technologies, TCOs and terrorist organizations often adapt new methodologies to facilitate their illicit activities. It is now more essential than ever that

law enforcement agencies work together to enhance our abilities to address this threat. Currently, HSI uses established investigative techniques that have gradually evolved to keep pace with this change but, HSI often engages its federal, state, local, and international partners to learn and exchange new and innovative approaches in the cryptocurrency space. HSI leads and participates in numerous task forces and working groups such as, the HSI Cyber Crimes Center, the FBI's National Cyber Investigative Joint Task Force, the U.S. Secret Service's Cyber Fraud Task Force, and the DHS Science and Technology Internet Anonymity Project Working Group.

HSI's extensive international footprint, comprised of more than 80 offices in over 50 countries, equips HSI with a global ability to connect and engage with international partners in this space. HSI special agents assigned to EUROPOL coordinate multi-lateral foreign investigations of darknet markets, cryptocurrencies, and illicit travel connected to terrorism. HSI also sits on multiple committees and engages with international partners to exchange ideas, guide regulatory developments, and exchange investigative information. Given the transnational nature of the crimes HSI investigates, these international partnerships are essential to investigations into cryptocurrency use in illicit and terrorist activities.

Training:

HSI has been engaged in a multiyear effort to increase its "cyber-enabled" workforce by training special agents, criminal analysts, and computer forensic analysts to conduct more effective and comprehensive online investigations. The HSI headquarters-based financial crimes unit and the HSI Cyber Crimes Center have partnered to provide cryptocurrency and darknet training for HSI special agents, as well as federal, state, local, and international partners. Since 2017, HSI's subject matter experts in cryptocurrency have conducted beginner and advanced cryptocurrency training to over 1000 international law enforcement partners and government officials worldwide. The training enables U.S. law enforcement agencies to initiate prolonged and combined campaigns of coordinated investigations targeting the criminal organizations that are using cryptocurrencies to launder illicit proceeds derived from various criminal schemes.

Outreach:

In 2003, HSI initiated the Cornerstone outreach initiative, a nationwide program designed to promote cooperation and collaboration with private sector partners in order to detect and close vulnerabilities within the financial industry. This mission is accomplished through proactive outreach and collaboration with businesses and industries that manage the very systems terrorists and other criminal organizations seek to exploit. Within the financial sector, HSI's efforts focus on conducting outreach with traditional financial institutions as well as MSBs. With the rapid growth of cryptocurrency, and with it the expansion of private companies involved in cryptocurrency, HSI has expanded Cornerstone to include outreach and training to private industry involved in the cryptocurrency space, who often represent the first line of defense against money laundering and the illicit use of cryptocurrency.

Statistics and Investigative Successes

While HSI's investigative portfolio is extensive and diverse, financial investigations are at the core of every investigative program area that we investigate. TCOs, terrorist organizations and the myriad of criminal networks have grown increasingly more technical in their approach to obfuscating their criminal acts, while also morphing operations to the perceived anonymity of the darknet. Traditional money laundering methods remain, yet cryptocurrency can now be used with relative ease to facilitate any type of illicit activity. As such, HSI investigations related to cryptocurrency have risen from one criminal investigation in 2011, to over 604 active criminal investigations in 2021. To date in 2021, HSI has already seized $79,825,606.65 in cryptocurrency. This marked increase signifies growing confidence in cryptocurrency use by bad actors and requires that law enforcement remains technically proficient in performing these complex investigations.

These metrics also reflect an ability of HSI and our partners to engage in a concerted effort to identify and disrupt illicit economies, but to also use that intelligence to disrupt and dismantle the command-and-control structure of TCOs and those that proliferate or support terrorist acts.

To illustrate the above point, HSI led a global cyber operation, along with the Internal Revenue Service (IRS) and Federal Bureau of Investigation (FBI), which resulted in the dismantlement of an online infrastructure of Hamas's militant wing, Al Qassam Brigades. Beginning in October 2019, HSI established several undercover personas who executed undercover donation payments, using Bitcoin and undercover electronic communications, with the subjects operating the Hamas cryptocurrency fundraising campaign. The undercover payments were executed in a method that enabled investigators to identify those supporters based in the United States and allowed investigators to further identify money flows. Through additional communications exploitation, HSI was able to identify 64 unique communication channels, which led to the execution of a seizure warrant on a Hamas donor's Bitcoin wallet.

Through additional court-ordered search warrants, HSI identified 64 terrorist affiliated email addresses, which illuminated the organizational blueprint, as well as covert access of Hamas's online recruitment, financing, domain, and network infrastructure, which was spread across the U.S., Canada, Russia, Germany, and Saudi Arabia. In July 2020, HSI and IRS special agents executed a total of twenty-four (24) federal search and seizure warrants at numerous cryptocurrency exchanges, domain registration providers, VPN service providers, online payment providers, DDOS protection providers, and email providers, resulting in numerous account take-overs, server seizures, email account seizures, and domain redirections. Additionally, this cyber operation was executed in cooperation with foreign partners and ultimately resulted in the seizure of terabytes of terrorist-controlled data, the seizure of several million dollars from hundreds of Bitcoin wallets, and the account takeover of a terrorist-administered website that solicits terrorist donations via Bitcoin. This account takeover of website, www.alqassam.net, enabled HSI to seize terrorist donations for a thirty (30) day period.

To highlight another investigative example, in 2020, HSI, IRS and FBI initiated an investigation related to twenty-four (24) cryptocurrency accounts, all of which were identified as foreign assets or sources of influence for Al-Qaeda. This investigation was initiated to investigate the unlawful use of cryptocurrency to support and finance terrorism. As a result of

this investigation, HSI subsequently seized sixty (60) virtual currency wallets used in this terrorism financing scheme. The results of this case and others illustrate how law enforcement can effectively disrupt terrorist groups, though the use of HSI's financial and global investigative authorities, technical aptitude, undercover and asset forfeiture authorities and ability to use law enforcement and the private sector as force multipliers in this fight.

Gaps and Solutions

While HSI has had success in countering the use of cryptocurrency to facilitate crime, investigative and regulatory challenges still remain. On the investigative front, the pseudo-anonymity offered by cryptocurrencies, combined with enhanced encryption being implemented by some platforms, restricts law enforcement's ability to trace financial transactions between illicit actors in support of a broad range of criminal activities. Cryptocurrency protocols are continuously being refined, and new cryptocurrencies are regularly developed and deployed with ever growing technological complexity. As a result, law enforcement organizations such as HSI are confronted with the need to continuously update and expand their training and expertise to enable effective investigations. This presents a resource and training challenge, particularly in light of competing priorities within an agency such as HSI with a broad mission set.

Additionally, significant challenges in international regulation remain, including the classification of cryptocurrency, which varies from country to country, and the lack of a common understanding and definition for cryptocurrency and what it is under the law. From HSI's perspective, the implementation of consistent global regulatory oversight would be an important step towards mitigating the illicit use of cryptocurrencies by terrorist and criminal actors. HSI has and will continue to engage with stakeholders across the branches of the U.S. government to address questions, provide insight, and respond to requests related to cryptocurrency and the digital economy.

Conclusion

Thank you again for the opportunity to appear before you today to discuss this important topic and for your continued support of HSI and our investigative mission. HSI remains committed to protecting the physical and digital borders of the United States from TCOs and terrorist networks seeking to exploit and undermine our financial and cyber systems and will continue our efforts at home and abroad to uphold the national security and public safety of the United States.