U.S. Immigration and Customs Enforcement

STATEMENT

OF

GREGORY C. NEVANO
DEPUTY ASSISTANT DIRECTOR
ILLICIT TRADE, TRAVEL, AND FINANCE DIVISION
HOMELAND SECURITY INVESTIGATIONS

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

REGARDING A HEARING ON

"Illicit Use of Virtual Currency and the Law Enforcement Response"

BEFORE THE

U.S. HOUSE OF REPRESENTATIVES
COMMITTEE ON FINANCIAL SERVICES
SUBCOMMITTEE ON TERRORISM AND ILLICIT FINANCE

Wednesday, June 20, 2018
2128 Rayburn House Office Building

Chairman Pearce, Ranking Member Perlmutter, and distinguished members:

Thank you for the opportunity to appear before you today to discuss the illicit use of virtual currency and the efforts of U.S. Immigration and Customs Enforcement (ICE) to target and investigate those who exploit virtual currency to carry out nefarious activity.

ICE's Homeland Security Investigations (HSI) has long stood at the forefront of combating transnational criminal activity that seeks to exploit our trade, travel, and financial systems for illicit purposes. HSI is the largest investigative agency within the U.S. Department of Homeland Security (DHS) with more than 6,000 special agents assigned to more than 200 domestic offices, and 67 international offices in 50 countries. HSI has authority to enforce more than 400 U.S. federal statutes, and some of our major investigative programs include financial crimes, counter proliferation, child exploitation, human smuggling and trafficking, narcotics smuggling, and intellectual property rights.

As a Deputy Assistant Director, I oversee the HSI Illicit Trade, Travel and Finance Division. The component of the Division overseeing our financial investigations is the Illicit Finance and Proceeds of Crime Unit (IFPCU). The IFPCU is one of many units within HSI which maintain equities addressing aspects of crime touching the virtual world. The primary focus of this Unit is to develop investigative techniques and typologies that help identify and eliminate vulnerabilities in the U.S. financial systems as well as provide HSI field offices the training and tools to pursue perpetrators of financial crimes. The IFPCU enhances cooperation and forges partnerships with domestic and foreign law enforcement, regulatory agencies, and non-governmental bodies to combat all types of financial crimes, to include the illicit use of virtual currencies to launder criminal proceeds. We also work alongside the U.S. Department of the Treasury and other government entities to provide anti-money laundering (AML) assessments, training, best practices, and lessons learned in the fight against global money laundering.

Positioned within the IFPCU is the Illicit Digital Economy Program (IDEP), forming the vanguard of HSI's investigative portfolio to counter the illicit use of virtual currency. Formed in 2013, the program was established to combat the money laundering and criminal exploitation of the rapidly emerging digital economy by Transnational Criminal Organizations (TCOs).

Rapid Growth of Virtual Currency

In 2009, bitcoin was introduced as the first decentralized convertible virtual currency. Bitcoin, like many convertible virtual currencies, is a "cryptocurrency." With its introduction, an entirely new world was created in relation to money laundering and financial investigations. Today, cryptocurrency has become more accepted for legitimate use in both commerce and investment. Bitcoin, for example, is accepted as a method of payment by hundreds of traditional brick and mortar stores as well as online merchants. There are currently more than 1,550 different cryptocurrencies in existence. Bitcoin is, by far, the largest and most widely accepted cryptocurrency.

Following its introduction, bitcoin quickly became the currency of choice on the Darknet as buyers and sellers enjoyed the pseudo-anonymity it provided. HSI continues to be a lead agency involved in the investigation and subsequent dismantling of several Darknet market places, including Silk Road and AlphaBay. The illicit use of cryptocurrency is not limited to use as a method of payment on Darknet market places. The pseudo-anonymity and ease of transfer cryptocurrency provides have led to expanded use by traditional criminal organizations with ample opportunity for expansion as it becomes more mainstream. The illicit use of cryptocurrency is found in many programmatic areas and case categories. Any crime committed for financial gain has the potential to involve cryptocurrency. Therefore, HSI does not treat the use of cryptocurrency for illicit purposes as a cybercrime, but rather as an online-enabled financial crime.

HSI's Lines of Effort

Financial Investigations:

Despite the pseudo-anonymity exploited by the users of bitcoin and other cryptocurrencies, as well as their ease of transfer, 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 by law enforcement means and methods. Utilizing traditional investigative methods such as surveillance, undercover operations, and confidential informants, coupled with financial and blockchain analysis, HSI is able to disrupt and dismantle the criminals and TCOs utilizing cryptocurrencies.

Most lawful users of cryptocurrencies are more than willing to conduct business with a cryptocurrency exchange that complies with Federal legal requirements. Many exchanges are registered with the U.S. Department of the Treasury's Financial Crimes Enforcement Network which issued guidance in 2013 clarifying that persons or companies involved in the exchange of cryptocurrency are money services businesses (MSBs) and making clear that exchanges must follow the same regulatory and reporting protocols as traditional MSBs. The protocols include developing and implementing an AML compliance program, filing suspicious activity reports, and registration protocols. These procedures are implemented to record personal identifying information from customers. Most lawful users are more than willing to provide personal identifying information and traditional financial institution account numbers in exchange for security, the lowest fees, and the ease of processing transactions.

Those who use cryptocurrency for illegal purposes, however, stay away from registered exchanges in an attempt to conceal their own identities. Instead, these criminals look to 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 on websites like Craiglist and others. Although some P2P exchangers do register and follow compliance laws, most do not. Rather, these illicit P2P exchangers position themselves as the money launderers of the cryptocurrency world. One type of P2P exchanger illegally generates 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 helps to open the door and pull back the veil of pseudo-anonymity provided by cryptocurrencies. Through interviews and suspect cooperation, along with forensic analysis of computers, mobile phones, and other seized electronics, as well as the use of advanced blockchain tracing tools, HSI can identify other criminals using cryptocurrency to fund and further their illicit activities.

Collaboration:

HSI Special Agents have always made it a practice to work cooperatively with federal, state, local, and international partners to investigate criminal networks operating around the globe. We use both established investigative techniques and models that have gradually evolved to keep pace with changing methodologies of TCOs. More so, HSI investigators are always on the lookout for innovative investigative approaches and the next developing threat over-the-horizon. Due to the rapidly increasing transformative nature of technology, it is more essential than ever that law enforcement agencies enhance their adaptability and fluidity when combating transnational crime. Nowhere is this more apparent than in the rapidly expanding world of cybercrime and online-enabled financial crime.

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.

HSI is combating the threat posed by the illicit manipulation of the cryptocurrencies through a multi-layered approach. By utilizing our broad authorities, HSI has dedicated units that are responsible for responding to this growing threat. Our IFPCU is responsible for investigating the movement and laundering of cryptocurrencies, our Cyber Crimes (C3) and Intellectual Property Rights Centers are responsible for monitoring bad actors located on the Darknet; our HSI agents assigned to EUROPOL coordinate multi-lateral foreign investigations of the Darknet, cryptocurrencies, and illicit travel connected to terrorism.

Training:

Like most law enforcement agencies, HSI has been engaged in a multiyear effort to increase its "cyber-enabled" workforce by training special agents, intelligence research specialists, and computer forensic analysts to conduct online investigations. The HSI IFPCU and the HSI Cyber Crimes Unit have partnered to conduct cryptocurrency and Darknet training for HSI agents and federal, state, local, tribal, and international partners. Special agents from HSI headquarters and field office subject matter experts conduct this specialized training. The training course "Cryptocurrencies and the Dark Web" is coordinated under the IDEP, has been well received, and to date in Fiscal Year (FY) 2018, HSI has conducted more than 50 outreach and training sessions, both nationally and internationally, reaching over 4,000 law enforcement, prosecutorial, judicial and other government personnel. Most recently, HSI has provided training in North Dakota where we had attendees from 18 different investigative agencies and

police departments; to Ohio with 400 attendees; and to Buffalo with 175 federal, state, and Canadian law enforcement partners.

This training enables U.S. law enforcement agencies to initiate prolonged and combined campaigns of coordinated investigations targeting the criminal organizations that are utilizing cryptocurrencies to launder illicit proceeds derived from various criminal schemes, to include fentanyl and opioid smuggling. HSI will continue this training and intends to follow up this course with intermediate and advanced-level training.

Outreach:

HSI abides by the belief and instills in its investigators that the "cornerstone" of virtually every investigation is financial. In 2003, HSI initiated the Cornerstone Outreach Initiative. Cornerstone is HSI's comprehensive initiative focused on financial investigations and with a primary outreach goal of detecting and closing vulnerabilities within the U.S. financial, trade, and transportation sectors. 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 outreaches 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 a directed effort to conduct outreaches and training with private industry involved in the cryptocurrency space. The private sector represents America's first line of defense against money laundering and the illicit use of cryptocurrency, which is why HSI partners with the business community, along with state and federal agencies, to combat financial crimes through a 21st century approach to law enforcement.

Investigative Successes and Statistics

Since the creation of cryptocurrency, HSI has steadily increased our knowledge, commitment, and capacity to combat money laundering regardless of the currency platform being used. HSI investigations into cryptocurrency have increased from one investigation initiated in FY 2011, to 203 investigations initiated in FY 2017. As of May 2018, HSI offices have initiated 144 cryptocurrency investigations, in addition to those already open and ongoing investigations. With the increase in our investigations, HSI has also seen a large increase in our seizures of cryptocurrency. For example, in FY 2014, HSI seized $151,459 in cryptocurrency. By the end of FY 2017, HSI seized $6,953,642 in cryptocurrency. Through the end of April 2018, HSI has already seized $25,442,611 in cryptocurrency.

I would like to take a moment to discuss some great HSI investigations involving the use of cryptocurrency and illicit Darknet sites. Like traditional robbery schemes aimed at pilfering a drug trafficker's profits, illicit Darknet sites and their virtual wallets can be compromised by various electronic methods aimed at stealing and diverting cryptocurrency. In 2013, in a multi-jurisdictional effort, HSI offices obtained indictments and arrest warrants for two online criminals who were electronically stealing cryptocurrency from an illicit Darknet site and then laundering the stolen currency through a series of virtual transfers. This HSI investigation

resulted in the seizure of a total of $4.5 million in virtual and hard currency that was stolen from the illicit site.

In another example, in July 2016, HSI Salt Lake City, Utah initiated a criminal investigation involving a TCO responsible for filling drug orders for regulated items such as Xanax through the Darknet. The investigative lead was forwarded to HSI by a cryptocurrency exchanger as a result of our Cornerstone initiative. The TCO dispensed approximately 1.8 million pills, half of which were laced with fentanyl. The TCO was responsible for thousands of drug laden postal shipments which were sent to almost every state in the nation. In November 2016, HSI agents received indictments and arrests warrants for seven members of the TCO and seized a total of $7,000,000 in virtual and hard currency as well as thousands of fentanyl laced pills and pill presses.

In March 2017, HSI Special Agents in Philadelphia, working in conjunction with their state and federal partners, intercepted a parcel sent from China to a U.S. address. Execution of a search warrant on the parcel revealed that it contained a synthetic opioid derivative. Further investigation discovered that the Philadelphia suspect had previously received two dozen similar shipments, and was acting as a trans-shipper under the direction of the Chinese organization. The developing investigation revealed that the Chinese source of supply was responsible for sending opioid laden parcels to approximately 19 other countries. The Chinese supplier operated as an illicit vendor on the Darknet and the payments were being remitted through cryptocurrency.

Investigations such as these are regularly highlighted in our trainings and outreach. When we identify trends, typologies are formulated to give our investigators potential models to apply. Equally, investigators in the field provide feedback to our trainers on the latest investigative exploits. While every investigation is unique, the crossroads joining virtual and fiat currency have been cited as one of the important investigative junctures that law enforcement can exploit to disrupt and dismantle these criminal and smuggling organizations.

Challenges

Many new cryptocurrencies have been and will continue to be developed. Some newer cryptocurrencies have features that make the tracing of them quite complicated. These new anonymity-enhanced cryptocurrencies are clearly ripe for illicit use in an effort to subvert legitimate law enforcement inquires. Although it is more difficult to trace the movement of illicit proceeds using these newer anonymity-enhanced cryptocurrencies, it is not impossible. Regardless of the cryptocurrency used, by targeting the chokepoints and nodes where convertible cryptocurrency activities intersect with the regulated fiat currency financial system, HSI is confident that we will still be able to conduct successful investigations and identify those criminals and TCOs utilizing cryptocurrency for illicit purposes.

Technology will inevitably continue to evolve, and law enforcement agencies everywhere must continue to adapt and evolve as well. HSI will continue to partner with all law enforcement agencies, along with cutting-edge private technology partners, to stay ahead of the curve and

keep technologically savvy criminals on their heels. These vital partnerships are the foundation that allows law enforcement to continue its effort in combating TCOs on all fronts, including the emerging threat of online-enabled financial crimes.

Conclusion

Thank you again for the opportunity to appear before you today and for your continued support of U.S. Immigration and Customs Enforcement, Homeland Security Investigations, and our law enforcement mission. We will continue to use our unique and powerful combination of law enforcement authorities and access to information to close vulnerabilities that can be exploited to harm our homeland in the real and virtual worlds. ICE HSI is committed to protecting America from the cross-border criminal organizations seeking to exploit and undermine our financial systems, preventing terrorism and combating the illegal movement of people and goods.

I appreciate your interest in the burgeoning field of cryptocurrency and its impact on illicit endeavors, and look forward to any questions.