STATEMENT

OF

U.S. IMMIGRATION AND CUSTOMS ENFORCEMENT

REGARDING A HEARING ON

"BEYOND SILK ROAD: POTENTIAL RISKS, THREATS, AND PROMISES OF VIRTUAL CURRENCIES"

BEFORE THE

UNITED STATES SENATE
COMMITTEE ON HOMELAND SECURITY
AND GOVERNMENTAL AFFAIRS

Monday, November 18, 2013 -- 2:30 p.m.
106 Dirksen Senate Office Building

Introduction

Chairman Carper, Ranking Member Coburn, and distinguished members of the Committee, thank you for the opportunity to highlight the efforts of U.S. Immigration and Customs Enforcement (ICE) to combat the exploitation of virtual currency[1] platforms by transnational organized criminals (TOCs). Although virtual currencies may support important innovation and serve legitimate purposes, like traditional currencies or other methods of transferring value, virtual currencies may also be exploited for the purposes of money laundering, the facilitation and financing of terrorism, and to enable other crimes such as child pornography, drug trafficking, and cybercrimes.

ICE has expansive investigative authority and is the largest force of criminal investigators in the U.S. Department of Homeland Security (DHS). With more than 20,000 employees nationwide and in 48 countries, ICE promotes homeland security and public safety through the criminal and civil enforcement of federal laws governing border control, customs, trade, and immigration. ICE's primary priorities are to prevent terrorism and enhance security; protect the borders against illicit trade, travel and finance; and protect the borders through smart and effective immigration enforcement.

The ICE Homeland Security Investigations (HSI) Directorate, a critical asset in the ICE mission, is responsible for investigating a wide range of domestic and international activities arising from the illegal movement of people and goods into, within, and out of the United States.

[1] There is no single commonly accepted definition of virtual or digital currency. For purposes of this statement, **virtual currency** is a digital representation of value that can be traded on the Internet and functions as (1) a medium of exchange; (2) a unit of account; and/or (3) a store of value, but does not have legal tender status in any jurisdiction. Virtual currency is distinguished from fiat currency (a.k.a. "real currency," "real money," or "national currency"), which is the coin and paper money of a country that is designated as its legal tender; circulates; and is customarily used and accepted as a medium of exchange in the issuing country. Virtual currency is also distinct from e-money, which is a digital representation of fiat currency used to electronically transfer value denominated in fiat currency. E-money is a digital transfer mechanism for fiat currency—i.e., it electronically transfers value that has legal tender status. **Digital currency** is a digital representation of either virtual currency or e-money.

HSI investigates immigration fraud, human rights violations, human smuggling and human trafficking, the smuggling of narcotics, weapons and all other types of contraband, intellectual property rights violations, and financial crimes—including those involving virtual currencies, cybercrimes, and export enforcement issues, among other offenses.

In addition, HSI oversees the agency's international affairs operations and intelligence functions. HSI consists of more than 10,000 employees, with over 6,700 special agents assigned to more than 200 cities throughout the United States and 48 countries around the world.

Illicit Finance

One of the most effective methods for dismantling TCOs is to attack the criminal proceeds that are the lifeblood of their operations. Through the work of HSI, ICE takes a holistic approach toward investigating money laundering, illicit finance, and other financial crimes by examining the ways that individuals and criminal organizations earn, move, store, and launder their illicit proceeds.

The combination of successful financial investigations, reporting requirements under the Bank Secrecy Act (BSA) of 1970, as amended, and anti-money laundering compliance efforts by financial institutions has no doubt strengthened payment systems and forced criminal organizations to continuously seek other means to diversify the movement of illicit funds.

Virtual Currency

In contrast to traditional currency, monetary instruments, or other methods of transferring value, virtual currencies serve as mediums of exchange, but are not accepted as legal tender in any recognized government jurisdiction. However, virtual currencies can be used to conduct

transactions entirely within a virtual economy, transferred between individuals, or used in lieu of a government-issued currency to purchase goods and services.

The appeal of virtual currencies, especially "open" or "convertible" currencies that can be exchanged for traditional currency, and vice versa, is that they may allow value to be transferred much more rapidly and cheaply (especially internationally) than through traditional banking payment systems, and often with greater anonymity and reduced oversight. Existing criminal statutes are available for law enforcement to target the illicit use of virtual currency systems by purchasers, administrators, and exchangers. Specifically, the transfer of virtual currency arguably does constitute a transfer of "funds" within the meaning of Sections 1956 and 1960 of Title 18 of the United States Code (U.S.C.). As a result, if criminals are using a virtual currency system to promote criminal activities, to disguise or conceal the source of their illicitly derived proceeds, or to evade federal or state reporting requirements, they may be prosecuted for money laundering.

Similarly, the failure of a virtual currency exchanger or administrator to register with the Treasury Department's Financial Crimes Enforcement Network (FinCEN) or the act of engaging in the transfer of criminally derived proceeds on behalf of the public, constitutes a violation of 18 U.S.C. §§ 1960 and 1956, respectively.

While electronic payment systems are certainly nothing new, ICE has recognized the potential for criminal exploitation and the money laundering threat posed by virtual currency. ICE has, therefore, strategically deployed a multi-prong investigative strategy designed to target illicit virtual currency platforms, currency exchangers, and underground black markets such as "carding," illegal drugs, illegal firearms, and child pornography forums.

Silk Road

On October 2, 2013, the collaborative efforts of ICE, the Federal Bureau of Investigation (FBI), Drug Enforcement Administration (DEA), the U.S. Postal Inspection Service (USPIS), and the Internal Revenue Service (IRS) resulted in the seizure of the website "Silk Road," which served as an online international marketplace for users to buy and sell controlled substances, false identifications and other contraband anonymously over the Internet. Silk Road utilized "bitcoins"[2] as the only accepted payment mechanism on the site.

The suspect was charged with a three-count indictment with conspiracy to distribute a controlled substance, attempted witness murder and using interstate commerce facilities in the commission of murder for hire. Between December 2012 and January 2013, the suspect is alleged to have knowingly conspired and agreed with others to distribute and possess with intent to distribute controlled substances including cocaine. The suspect is alleged to have profited from the operation of Silk Road by collecting a fee for each transaction.

During the course of the investigation, ICE special agents identified bitcoins used by buyers and sellers to complete their transactions on the Silk Road site. The bitcoins, worth an estimated $3.6 million, were located in Silk Road's operating account and ultimately seized by the FBI. Estimates indicate that Silk Road processed over $1.2 billion worth of business and earned commissions totaling 600,000 bitcoins, or about $80 million using bitcoin rates at the time of the seizure. ICE has subsequently provided additional leads to several international law enforcement partners resulting in the arrest of four additional co-conspirators.

[2] Bitcoin is a complex peer-to-peer virtual currency system that generates a virtual currency consisting of mathematical tokens (unique strings of numbers and letters) created entirely outside the world's regulated financial system by a network of computers' solving an algorithm. Because using bitcoins requires no personal identification and allows for transactions on networks in nearly complete isolation from the mainstream financial system, they have become an attractive option for money launderers and other illicit online activity.

Mt.Gox

In May 2013, through an interagency taskforce led by ICE in Baltimore, Maryland, three U.S. bank accounts associated with what was then the world's largest bitcoin exchanger, Japan-based Mt.Gox, which was moving approximately $60 million per month into a number of Internet-based hidden black markets operating on the Tor network, including Silk Road, were seized for violations of 18 U.S.C. § 1960, operating a money service business in the United States without a license. The bulk of the funds were associated with the illicit purchase of drugs, firearms, and child pornography. As a result of the forfeiture action, Mt.Gox, which allows users to trade bitcoins for U.S. dollars and several other currencies, has implemented varying degrees of user verification for its customers. These and many other ongoing criminal investigations have provided ICE with a better understanding of the risks and challenges posed by virtual currencies.

Illicit Pathways Attack Strategy (IPAS)

Transnational organized crime (TOC) poses a significant and growing threat to national and international security, with implications for public safety, public health, democratic institutions, and economic stability across the globe.

In July 2011, the Administration took an important step in fighting transnational crime when it issued its *Strategy to Combat Transnational Organized Crime* (TOC Strategy). This strategy complements the current *National Security Strategy* and other national initiatives related to human trafficking, money laundering, and transnational crime affecting the United States, by focusing on the growing threat of international criminal networks. The TOC Strategy's single unifying principle is to build, balance, and integrate the tools of American strength to combat

transnational organized crime, and related threats to national security—and to urge our international partners to do the same.

Consistent with the TOC Strategy, ICE developed the Financial Crimes Illicit Pathways Attack Strategy (IPAS) to enhance ICE's ability to disrupt the financial networks that support transnational criminal activity. By targeting the profits generated and used by criminal organizations, and not just targeting the contraband being smuggled, the IPAS will protect financial systems and strategic markets by addressing how criminal organizations earn, move and store illicit proceeds.

Partners and Cooperation

ICE recognizes that our approach to combating the illicit use of virtual currency systems must include collaboration and coordination with our domestic and international partners. ICE works closely with our federal, state, local, international law enforcement and other members of the interagency. Notably, ICE is an active participant in the Virtual Currency Emerging Threats Working Group, which was founded by the FBI in early 2012 to mitigate the cross-programmatic threats arising from illicit actors' use of virtual currency systems.

ICE also contributes to several other interagency groups dealing with digital currencies and emerging payment systems, including the New Payment Methods Ad Hoc Working Group, a subgroup of the Terrorist Finance Working Group led by the State Department; and the Financial Action Task Force, which is an inter-governmental body established in 1989 to set global standards and promote effective implementation of legal, regulatory, and operational measures for combating money laundering, terrorist financing and other related threats to the integrity of the international financial system.

ICE is also an active partner in the Secret Service-led Electronic Crimes Task Forces which leverage the private sector, academia, and state and local law enforcement to support cyber-crime investigations. Additionally, ICE is proudly supporting the Digital Economy Task Force spearheaded by the International Center for Missing and Exploited Children. The mission of the Digital Economy Task Force is to foster a balanced solution to the digital economy where people can enjoy the convenience of the digital currencies while there are controls in place to combat illegal activity, as the Federal Government does with any other form of money. The Digital Economy Task Force strives to achieve the goal of producing and releasing an official report in February 2014 to inform individuals and lawmakers globally about the current state of the digital economy. In addition, the task force intends to explore the inherent opportunities and risks associated with an increasingly digital economy and its impact on human rights, regulation, crime, and law enforcement.

Virtual currency systems have a global reach and clientele. Investigations into illicit virtual currency activities often require considerable cooperation from international partners.

ICE attachés work with international organizations and foreign law enforcement counterparts to build capacity, strengthen relationships, and conduct joint enforcement activities to ultimately disrupt and dismantle TOCs. As part of these efforts, ICE maintains nine vetted units worldwide that are composed of highly-trained host country counterparts that have the authority to investigate and enforce violations of law in their respective country. Since ICE officials who work overseas do not possess law enforcement or investigative authority in host countries, the use of vetted units enables ICE to dismantle, disrupt, and prosecute TOCs while respecting the sovereignty of the host country.

Challenges

The criminal use of virtual currencies challenges the effectiveness of U.S. laws and regulations intended to limit the ability of criminals to profit from their illicit activities and move their criminal proceeds. The key U.S. laws that typically pertain to investigations involving the illicit administration or exchange of virtual currencies include the Bank Secrecy Act of 1970, the Money Laundering Suppression Act of 1994, and Title III of the USA PATRIOT Act of 2001; which are further supported by various associated Federal regulations. The ability of agencies to enforce current laws and regulations to suppress the use of financial systems by criminal enterprises is complicated by the increasingly transnational nature of the criminal organizations and their continued efforts to circumvent these legal controls.

Virtual currencies often support crime that is transnational in nature, thus requiring close international partnership to conduct investigations, make arrests, and seize criminal assets. Fostering these partnerships and conducting these transnational investigations requires continual investment to maintain effective international law enforcement collaborations, and constant efforts to harmonize anti-money laundering laws and regulations. Investigating crimes involving virtual currencies and the transnational organized cyber criminals that use them also requires highly skilled criminal investigators. Hiring, developing, and retaining these special agents is a high priority for DHS, but is challenging in the present fiscal environment. Additionally, while virtual currencies may support the activities of transnational criminals who prey upon Americans, some administrators and exchangers of virtual currencies are based in other countries in an effort to minimize the exposure of individuals to potential arrest and prosecution by U.S. law enforcement officials.

Conclusion

Thank you again for the opportunity to highlight ICE's leading role in combating TOCs and their ability to launder illicit proceeds. ICE recognizes and fully supports the growth of the virtual currency payments as a legitimate financial platform via the Internet. However, as these and other new technologies continue to evolve, ICE will remain vigilant and adapt its investigative tools and techniques to effectively dismantle those criminal organizations that use virtual currencies to hide and launder their illicit proceeds.