Department of Justice

STATEMENT OF

MYTHILI RAMAN
ACTING ASSISTANT ATTORNEY GENERAL
CRIMINAL DIVISION
U.S. DEPARTMENT OF JUSTICE

BEFORE THE

COMMITTEE ON HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS
UNITED STATES SENATE

FOR A HEARING ENTITLED

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

PRESENTED ON

NOVEMBER 18, 2013

Statement of Mythili Raman
Acting Assistant Attorney General, Criminal Division
Before the United States Senate
Committee on Homeland Security and Governmental Affairs
"Beyond the Silk Road: Potential Risks, Threats and Promises of Virtual Currencies"
November 18, 2013

Chairman Carper, Ranking Member Coburn, and distinguished Members of the Committee: Thank you for the opportunity to appear before the Committee today to discuss the Department of Justice's work regarding virtual currencies. I am honored to represent the Department at this hearing and to describe for you our approach to virtual currencies, our recent successes in prosecuting criminals who use virtual currencies for illicit purposes, and some of the challenges we face as virtual currency systems continue to evolve.

Introduction

The Department of Justice recognizes that many virtual currency systems offer legitimate financial services and have the potential to promote more efficient global commerce. We have also seen, however, that certain aspects of virtual currencies appeal to criminals and present a host of new challenges to law enforcement.

The concept of virtual currencies is not new to the Department and, indeed, the Department has investigated and prosecuted the illicit use of virtual currencies since the late 1990s, when criminals first began using systems such as WebMoney and e-Gold to conduct their business. Over the last 15 years, however, virtual currencies have evolved and diversified significantly, challenging the Department to adapt our capabilities to deal with new systems and threats.

As with all emerging technologies, the Department has aggressively used our existing tools and capabilities to combat illegal activities involving virtual currencies. The Department has two primary law enforcement interests in virtual currency: (1) deterring and prosecuting criminals using virtual currency systems to move or hide money that is used to facilitate, or is derived from, criminal or terrorist acts, *i.e.*, money laundering; and (2) investigating and prosecuting those virtual currency services that themselves violate laws aimed at illegal money transmission and money laundering. As I will describe in my testimony, the Department is committed to using all the tools at our disposal to ensure that those law enforcement interests are met, even as virtual currency systems evolve.

Illicit Use

"Virtual currency" is a medium of exchange circulated over a network, typically the Internet, which is not backed by a government. These systems can be both centralized and decentralized.

Early centralized models, where the currency is controlled by a single private entity, have expanded and now encompass a wide range of business concepts. Some centralized virtual currencies take the form of digital precious metals, such as e-Gold and Pecunix, where users exchange digital currency units ostensibly backed by gold bullion or other precious metals. Others exist within popular online games or virtual worlds, such as Farmville, Second Life, or World of Warcraft. Still others are online payment systems such as WebMoney and Liberty Reserve, which are available generally outside of specific online communities and denominate users' accounts in virtual currency rather than U.S. Dollars, Euros, or some other national currency. Decentralized systems such as Bitcoin, which have no centralized administrating authority and instead operate as peer-to-peer transaction networks, entered the scene relatively recently but are growing rapidly. A network of sites and services, including exchangers who buy and sell virtual currencies in exchange for national currencies or other mediums of value, have developed around virtual currency systems, as well.

Criminals are nearly always early adopters of new technologies and financial systems, and virtual currency is no exception. As virtual currency has grown, it has attracted illicit users along with legitimate ones. Our experience has shown that some criminals have exploited virtual currency systems because of the ability of those systems to conduct transfers quickly, securely, and often with a perceived higher level of anonymity than that afforded by traditional financial services. The irreversibility of many virtual currency transactions additionally appeals to a variety of individuals seeking to engage in illicit activity, as does their ability to send funds cross-border.

Cyber criminals were among the first illicit groups to take widespread advantage of virtual currency. We have seen that many players in the cyber underground rely on virtual currency to conduct financial transactions. Early users of virtual currency also included criminals involved in the trafficking of child pornography, credit card fraud, identity theft, and high-yield investment schemes. As virtual currency became more widespread and criminals became increasingly computer savvy, other criminal groups moved to capitalize on virtual currency, as well. There are now public examples of virtual currency being used by nearly every type of criminal imaginable.

It is not surprising that criminals are drawn to services that allow users to conduct financial transactions while remaining largely anonymous. And, indeed, some of the criminal activity occurs through online black markets, many of which operate as Tor hidden services. Tor hidden services are sites accessible only through Tor, an anonymizing network that masks users' Internet traffic by routing it through a series of volunteer servers, called "nodes," across the globe. Online black markets capitalize on Tor's anonymizing features to offer a wide selection of illicit goods and services, ranging from pornographic images of children to dangerous narcotics to stolen credit card information.

At the same time, we have seen that though virtual currency systems are growing rapidly, few systems currently exist that could easily accommodate the hundreds of millions of dollars often moved in a single large-scale money laundering scheme. Transaction size is limited by the carrying capacity of the virtual currency systems and the exchangers. When taken in the aggregate, however, the relatively small dollar values associated with most illicit virtual currency

transactions quickly add up. At their prime, e-Gold and Liberty Reserve, two virtual currency systems prosecuted by the Department, each moved the equivalent of over $1 billion in illegal proceeds annually. As virtual currencies grow, the capacity for larger single transactions grows, as well.

The Department has prosecuted several of these systems, such as e-Gold, based on evidence that they can be, and often are, intentionally designed to facilitate illegal activity. These services typically do not conduct any meaningful customer due diligence and do not screen for transactions related to money laundering or terrorist financing. At the same time, these complicit and illicit businesses allow users to conceal their identities and maintain high levels of anonymity during transactions.

To be clear, virtual currency is not necessarily synonymous with anonymity. A convertible virtual currency with appropriate anti-money laundering and know-your-customer controls, as required by U.S. law, can safeguard its system from exploitation by criminals and terrorists in the same way any other money services business could. As virtual currency systems develop, it is imperative to law enforcement interests that those systems comply with applicable anti-money laundering and know-your-customer controls.

Department Actions

Exploitation by malicious actors is a problem faced by all types of financial services and is not unique to virtual currency systems. Although malicious actors have utilized emerging technologies to further their criminal schemes, the Department has thus far been able to apply existing tools to ensure vigorous prosecution of these schemes.

The Department relies on money services business, money transmission, and anti-money laundering statutes to curtail this sort of unlawful activity. Many virtual currency systems, exchangers, and related services operate as money transmitters, which are part of a larger class of institutions called money services businesses. Money transmitters are required under 31 U.S.C. § 5330 to register with the Financial Crimes Enforcement Network (FinCEN). Most states also require money transmitters to obtain a state license in order to conduct business in the state. Any money transmitter that fails to register with FinCEN or to obtain the requisite state licensing may be subject to criminal prosecution under 18 U.S.C. § 1960. Additionally, the general money laundering and spending statutes, 18 U.S.C. §§ 1956 and 1957, cover financial transactions involving virtual currencies. Finally, where virtual currencies are used in furtherance of underlying criminal activity, the Department can rely on traditional criminal statutes proscribing that activity, such as narcotics, cybercrime, child exploitation, and firearms laws.

Some of the major prosecutions in recent years involving virtual currency services are as follows.

E-Gold

The Department first took major action against an illicit virtual currency service in 2007, when it indicted e-Gold and its three principal owners on charges related to money laundering

and operating an unlicensed money transmitting business. E-Gold offered digital accounts purportedly backed by physical gold bullion. A valid e-mail address was the only information required to set up an account, allowing users to conduct highly anonymous international transactions over the Internet. As a result, e-Gold became a popular payment method for sellers of child pornography, operators of investment scams, and perpetrators of credit card and identity fraud. At its peak, e-Gold reportedly moved over $6 million each day for more than 2.5 million accounts. In 2008, e-Gold and the three individuals pleaded guilty.

Liberty Reserve

Following the e-Gold indictment, several similar but smaller systems and exchangers were indicted or closed themselves down to evade law enforcement detection. According to publicly filed charging documents, an executive of one of those businesses, Arthur Budovsky, then set out to create Liberty Reserve, an improved centralized virtual currency variation allegedly designed to evade U.S. law enforcement. Among other things, Liberty Reserve operated offshore – it was based in Costa Rica – and purportedly recommended that its customers use money exchangers located in countries without significant governmental money-laundering oversight or regulation. Moreover, Budovsky, the principal founder of Liberty Reserve, was so committed to avoiding the reach of U.S. law that, according to the indictment, in 2011, he formally renounced his U.S. citizenship and became a Costa Rican citizen in order to avoid facing justice in the United States.

Despite Budovsky's alleged efforts, earlier this year, the Department indicted Liberty Reserve and its executives, including Budovsky, for running a $6 billion money laundering operation. In a coordinated action, the Department of the Treasury identified Liberty Reserve as a financial institution of primary money laundering concern under Section 311 of the USA PATRIOT Act, effectively cutting it off from the U.S. financial system.

According to the indictment, Liberty Reserve allowed users to send and receive funds with a high level of anonymity by not requiring users to validate their identities and allowing users to make untraceable fund transfers in exchange for a privacy fee. Many of the transactions were sent to or from users in the United States, but Liberty Reserve never registered with the appropriate U.S. authorities. As revealed in the Department's filings, Liberty Reserve became a system of choice for cyber criminals and was used in a wide array of illegal activity, including credit card fraud, identity theft, investment fraud, computer hacking, and child pornography. As a result of the Department's action, the site was shuttered and effectively put out of business, and seven defendants were charged. One is in custody in the United States, one has entered a guilty plea, three others, including the lead defendant Budovsky, are pending extradition, and two others are at large. The case exemplifies the Department's resolve to pursue purported major money laundering facilitators, even those who hide offshore.

Silk Road

Just last month, the Department took action against one of the most popular online black markets, Silk Road. Allegedly operated by a U.S. citizen living in California at the time of his arrest, Silk Road accepted bitcoins exclusively as a payment mechanism on its site. The

Department's complaint alleges that, in less than three years, Silk Road served as a venue for over 100,000 buyers to purchase hundreds of kilograms of illegal drugs and other illicit goods from several thousand drug dealers and other criminal vendors. The site also purportedly laundered the proceeds of these transactions, amounting to hundreds of millions of dollars in bitcoins. In addition to arresting the site's operator and shutting down the service, the Department to date has seized over 170 thousand bitcoins, valued as of this past Friday, November 15, 2013, at over $70 million.

A separate indictment charges Silk Road's operator with drug distribution conspiracy, attempted witness murder, and using interstate commerce facilities in the commission of murder-for-hire. With regard to the murder-related charges, the indictment alleges that the Silk Road operator paid an undercover federal agent to murder one of the operator's employees.

Unique Challenges

The cases I just described illustrate not only Department successes in combating illicit use of virtual currency, but also many of the challenges investigators face when they encounter these systems, some of which may ultimately require additional legal or regulatory tools.

Virtual currency allows users to send money across the globe without dealing with a traditional financial institution. While this feature provides several benefits for legitimate customers, it can significantly complicate law enforcement efforts to follow the money.

Virtual currency systems have a global reach and clientele. Virtual currency businesses can cater to U.S. clientele while operating on the other side of the world. Investigations into illicit virtual currency businesses therefore often require considerable cooperation from international partners. The Liberty Reserve investigation and takedown, for example, involved coordinated law enforcement action in 17 countries.

The international nature of the transactions poses an additional challenge where the overseas regulatory regime treats virtual currency differently or, as is true in some cases, fails to cover it at all. While this challenge may diminish with the Financial Action Task Force's recent guidance addressing the need for all countries to develop a risk-based approach to new payment products and services, incongruent regulatory regimes will likely remain a challenge when dealing with virtual currency services overseas.

Among the most significant challenges the Department faces in dealing with virtual currency is the difficulty in obtaining customer records. Because decentralized systems lack any sort of administering authority to collect user information or receive legal process, investigators must rely on information collected by other sources, such as exchangers. Even if the target used a centralized system or exchanger, however, accurate customer records may still be difficult to obtain, or may not exist at all. Illicit users are typically attracted to systems with lax anti-money laundering and know-your-customer controls. These services often attempt to evade U.S. action by operating out of countries that have poor regulatory oversight and are less willing to cooperate with U.S. law enforcement. Even if the system at issue operates in a country with effective regulation and a cooperative relationship with the United States, the legal process for

obtaining foreign records is relatively slow when compared to the near-instantaneous speed at which the virtual currency user can send the funds to another jurisdiction.

A final challenge arises from the link between virtual currency and encryption. Decentralized virtual currencies typically rely on an encryption algorithm, rather than a central authority, to administer the currency. These encryption-based currencies, also known as cryptocurrencies, lack a central administering authority that might otherwise possess valuable evidence. In addition, users of these currencies often encrypt their digital wallets, complicating our efforts to seize and forfeit criminal proceeds.

Collaborative Efforts

The Department recognizes that virtual currency's ability to facilitate the global movement of funds by a wide array of illicit actors necessitates a comprehensive and collaborative approach with our domestic and international partners. To promote such coordination, the Department is an active participant in the Virtual Currency Emerging Threats Working Group (VCET). VCET was founded by the Federal Bureau of Investigation (FBI) in early 2012 to mitigate the cross-programmatic threats arising from illicit actors' use of virtual currency systems. The group leverages the collective subject matter expertise of its members to address issues arising from illicit actors' use of virtual currency, and deconflicts and shares information and concerns. VCET members represent an array of U.S. Government agencies, including, within the Department, the FBI, the Drug Enforcement Administration, multiple U.S. Attorney's Offices, and the Criminal Division's Asset Forfeiture and Money Laundering Section and Computer Crime and Intellectual Property Section.

The Department contributes to several additional interagency groups concerning virtual 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. The FBI specifically has issued numerous intelligence products related to virtual currency, many of which were coauthored with other members of the U.S. Intelligence Community.

The Department is committed to working with our regulatory partners to ensure appropriate coordination on regulatory issues related to virtual currency. The Department participated in meetings and discussions with FinCEN regarding the July 2011 Final Rule on Money Services Businesses and its applicability to virtual currencies, as well as the related March 18, 2013, FinCEN guidance. The Department regards FinCEN's regulation of many virtual currency services as money transmitters, as well as the resulting applicability of anti-money laundering and know-your-customer requirements under the Bank Secrecy Act, as crucial tools in preventing malicious actors from exploiting virtual currency systems in furtherance of illicit activity.

The Department works closely with FinCEN and the Department of Treasury to coordinate enforcement actions when appropriate. This relationship allowed the Department to unseal the Liberty Reserve indictment in coordination with Treasury's announcement naming the company as a financial institution of primary money laundering concern under Section 311 of the

USA PATRIOT Act. Such coordinated actions are integral tools in combating illicit finance.

Future Trends

The Department anticipates that virtual currency will continue to evolve and grow in popularity. That growth inevitably will be accompanied by an increase in illicit transactions, which makes it critical that virtual currency services understand their legal obligations and requirements. The Department is encouraged by the increasing prominence of legitimate virtual currency services that are attempting to comply with U.S. law. While a number of services have registered at the federal level, many are still struggling with implementing appropriate anti-money laundering, know-your-customer, and customer due diligence programs, as well as complying with state-level regulations and licensing requirements. As members of the U.S. financial community, virtual currency services can and must safeguard themselves from exploitation by criminals and terrorists by implementing legally required anti-money laundering and know-your-customer controls.

As the Administration's Strategy to Combat Transnational Organized Crime recognizes, transnational organized crime networks are increasingly involved in cybercrime, and can imperil consumers' faith in emerging digital systems. We must also pay close attention to the critical role of facilitators who cross both the licit and illicit worlds and provide services to legitimate customers and criminals alike.

The Department recognizes that malicious actors are often resourceful, and even legitimate virtual currency services can become unwitting conduits for illicit transactions when these actors are able to defeat or circumvent anti-money laundering controls. Outreach to these systems, much as the Department conducts with the formal financial sector, is an important tool in combating the exploitation of the systems for criminal and terrorist purposes. Because centralized payment systems and exchangers often interact with the traditional financial sector and hold bank accounts at major financial institutions, the range of such Department outreach extends to the financial services community at large, complementing the outreach and training efforts of FinCEN, the primary BSA regulator, and the Department of the Treasury. Department of Justice personnel routinely provide trainings to the private sector, as well as to domestic and international law enforcement and intelligence personnel, and specifically address virtual currency.

Law enforcement, Congress, and regulators must remain vigilant to ensure that the U.S. legal and regulatory structure is sufficiently robust to cover decentralized virtual currencies. The Department looks forward to working with Congress to ensure that law enforcement continues to have the tools necessary to combat the use of virtual currency for illicit purposes.

Conclusion

Chairman Carper and Ranking Member Coburn, I thank you for this opportunity to discuss the Department's work on virtual currency.

I look forward to any questions that you may have.