Edward Lowery III

Special Agent in Charge
Criminal Investigative Division,
U.S. Secret Service

Prepared Testimony

Before the
United States Senate Committee on
Homeland Security and Governmental Affairs

November 18, 2013

Good afternoon Chairman Carper, Ranking Member Coburn, and distinguished Members of the Committee. Thank you for the opportunity to testify on behalf of the U.S. Department of Homeland Security (DHS) regarding the risks and challenges posed by digital currencies[1] and the role of the U.S. Secret Service (Secret Service) in investigating crimes associated with online payment systems. Fraudulent schemes and money laundering are the Secret Service's chief concerns with respect to digital currencies and the facilitation of other serious crimes. The Secret Service is committed to adapting to evolving cyber threats by conducting robust investigations of offenses involving digital currencies within its jurisdiction in order to effectively suppress criminal activity.

As the original guardian of the nation's financial payment systems, since 1865 the Secret Service has conducted investigations to protect American consumers, industries, financial institutions, and critical infrastructure from criminal exploit. Accordingly, the Secret Service has extensive authority and responsibility to investigate financial crimes and dismantle the infrastructure that supports these criminal activities, including when these crimes are conducted through cyberspace. In executing our mission, the Secret Service closely partners with Federal, state, local, and international law enforcement agencies and other interagency partners. Notably, the Secret Service and U.S. Immigration and Customs Enforcement's Homeland Security Investigations (ICE/HSI)[2] partner through the Secret Service's Electronic Crimes Task Forces (ECTFs),[3] which leverage the private sector, academia, and state and local law enforcement to support cyber crime investigations. As former Department of Treasury law enforcement agencies, the Secret Service and ICE/HSI partner closely with the Financial Crimes Enforcement Network (FinCEN) and the Department of Treasury in conducting financial crime investigations. In addition, the Secret Service and ICE/HSI participate in the Virtual Currency Threats Working Group and other collaborative efforts with regulators and the national security staff to address the challenges posed by digital currencies and new payment systems.

Over the past decade, in addition to their many legitimate uses, digital currencies—by which I mean digital representations of both real national currencies, or fiat currency, and virtual currencies, which do not constitute the legal tender of any jurisdiction—have attracted malicious actors seeking to hide illicit money transactions. Accordingly, the Secret Service has developed

[1] Digital currencies are a form of electronic money used as alternate currencies. Currently no digital currency serves as legal tender or administered by a national government or central bank; as such digital currencies are a subset of virtual currencies.

[2] ICE/HSI is an investigatory arm of DHS with the jurisdiction and authority to investigate violations involving the illicit importation and exportation of merchandise, bulk cash smuggling, and financial crimes involving a nexus to the border.

[3] Section 105 of the USA PATRIOT Act of 2001 directed the Secret Service to establish a "a national network of electronic crimes task forces, … for the purpose of preventing, detecting, and investigating various forms of electronic crimes, including potential terrorist attacks against critical infrastructure and financial payment systems." The first Secret Service ECTF was established in New York in 1995; today the Secret Service operates 33 ECTFs, as part of an expanding international network that partners Federal, state, and local law enforcement with the private sector and academia to effectively investigate cyber and cyber-related crimes.

extensive experience in conducting investigations that involve digital currencies. The Secret Service and its interagency partners have investigated and shutdown two major illicit providers of digital currencies that supported extensive criminal activity: e-Gold Ltd. in 2007 and Liberty Reserve earlier this year. Additionally, the Secret Service investigated and shutdown illicit digital currency exchangers, such as Western Express. This successful investigation and prosecution recently concluded with 15 convictions, thanks to the dedicated eight-year effort of the Manhattan District Attorney's Office and the Secret Service's New York/New Jersey ECTF. These and other criminal investigations have provided the Secret Service with a better understanding of the risks and challenges posed by digital currencies.

Criminal Use of Digital Currencies

In recent years, digital currencies have become a preferred form of money for criminals to conduct their illicit activities. Digital currencies provide an efficient means of moving large sums of money globally for both legitimate and criminal purposes. However, as a form of virtual currency,[4] many digital currencies attempt to operate outside the legal and regulatory systems many countries have established to govern legal tender. Additionally, digital currencies often provide a greater anonymity than the traditional banking system. These attributes make digital currencies a preferred tool of transnational criminal organizations for conducting their criminal activities, transmitting their illicit revenue internationally, and laundering their profits.

Based on Secret Service investigations into the criminal use of digital currencies, criminals prefer those they assess to offer:

1) The greatest degree of anonymity for both users and transactions.
2) The ability to quickly and confidently move illicit proceeds from one country to another.
3) Low volatility, which results in lower exchange risk, increasing the digital currency's ability to be an efficient means to transmit and store wealth.
4) Widespread adoption in the criminal underground.
5) Trustworthiness.

Consequently, as part of its mission to suppress criminal activity, the Secret Service's investigations into digital currency exchangers and administrators have focused on those currencies with the above attributes that play an instrumental role in enabling large-scale criminal activity in violation of laws under Secret Service jurisdiction.[5]

[4] FinCEN defines "virtual currency" as those currencies that operates like currency in some environments, but does not have legal tender status in any jurisdiction. Department of Treasury Financial Crimes Enforcement Network, Guidance FIN-2013-G0001 "Application of FinCEN's Regulations to Persons Administrating, Exchanging, or using Virtual Currencies" (March 18, 2013).

[5] Most notably 18 U.S.C. §§ 1028, 1029, 1030, 1343, 1956, 1960, et al.

Digital currencies differ as to their principal criminal uses. Some digital currencies are primarily used to purchase illicit goods and services (e.g., drugs, credit card information, personally identifiable information (PII), and other contraband or criminal services). Other digital currencies are primarily used for money laundering: concealing transactions involving large amounts of money—particularly transnational transfers. The greatest risks are posed by digital currencies that have widespread use for both of these criminal purposes: e-Gold and Liberty Reserve are prime examples of these high-risk digital currencies.

e-Gold

e-Gold was founded in 1996 and offered a pseudonymous digital currency that was originally backed with gold coins stored in a safe deposit box in Florida. A valid email address was the only information that was required to open an e-Gold account. Although other contact information was requested, it was not verified. Thousands of e-Gold users opened their accounts with blatantly false information, such as using the names "Mickey Mouse" or "Donald Duck," among others. Once people opened e-Gold accounts, they could fund them by using exchangers who converted U.S. currency into e-Gold. When these accounts were established and funded, the account holders could gain access through the Internet and conduct anonymous transactions with other e-Gold account holders anywhere in the world.

e-Gold quickly became the preferred financial transaction method of transnational cyber criminals—particularly those involved in the trafficking of stolen financial information and PII of U.S. citizens—and a tool for money laundering by cyber criminals. Criminals' reliance on e-Gold to facilitate certain crimes, including the purchase of child pornography and money laundering, made it the focus of a successful joint investigation by the Secret Service, IRS Criminal Investigations (IRS-CI), the Federal Bureau of Investigation, and the Florida-based St. Cloud Internal Revenue Service-Secret Service Financial Crimes and Money Laundering Task Force. The case was prosecuted by the U.S. Attorney's Office for the District of Columbia, the Department of Justice's Computer Crime and Intellectual Property Section and Asset Forfeiture and Money Laundering Section (AFMLS), with assistance from the Criminal Division's Child Exploitation and Obscenity Section. e-Gold and its corporate affiliate pled guilty to money laundering and operating an unlicensed money transmitting business. The principal director of e-Gold and its corporate affiliate, as well as senior leaders, pled guilty to conspiracy to engage in money laundering and operating an unlicensed money transmitting business. e-Gold's gold reserve was liquidated for $90 million to allow legitimate account holders to claim their assets. As of December 18, 2012, over $10.8 million contained in 12,869 accounts has been forfeited to the Federal Government as part of an on-going asset forfeiture process.

Liberty Reserve[6]

Liberty Reserve was a Costa Rica-based digital currency service that provided what it described as "instant, real-time currency for international commerce" that can be used to "send and receive payments from anyone, anywhere on the globe." Additionally, Liberty Reserve described itself as the Internet's "largest payment processor and money transfer system," serving "millions" of people around the world, including the United States. The alleged principal founder of Liberty Reserve moved to Costa Rica to operate Liberty Reserve after being convicted in the United States in December 2006 for operating "Gold Age, Inc." as an unlicensed money transmitting business.

Liberty Reserve was allegedly designed to make anonymous and untraceable financial transactions to support criminal activity and elude law enforcement. Liberty Reserve quickly became the predominant digital currency used for money laundering by transnational organized cyber crime and other criminals. Before the Secret Service-led investigation shutdown Liberty Reserve, it was estimated to have had more than one million users worldwide, with more than 200,000 users in the United States, and to have processed more than 12 million financial transactions, with a combined value of more than $1.4 billion annually. Overall, from 2006 to May of 2013, Liberty Reserve allegedly processed at least 55 million separate financial transactions and is believed to have laundered more than $6 billion in criminal proceeds.[7]

On May 24, 2013, five individuals were arrested in Costa Rica, Spain, and New York for operating Liberty Reserve under charges for conspiracy to commit money laundering and conspiracy and operation of an unlicensed money transmitting business. At the same time, in close coordination with this law enforcement 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.

Liberty Reserve's alleged role in supporting criminal activity made its shut down a high priority of numerous law enforcement agencies. The Secret Service worked closely with IRS-CI and ICE/HSI as part of the Global Illicit Financial Team (GIFT) to conduct this investigation, and the Secret Service New York/New Jersey ECTF provided vital assistance. In addition, the cooperation and assistance of international law enforcement partners, including the Judicial Investigation Organization in Costa Rica, the National High Tech Crime Unit in the Netherlands, the Spanish National Police, Financial and Economic Crime Unit, the Cyber Crime Unit at the Swedish National Bureau of Investigation, and the Swiss Federal Prosecutor's Office, was paramount to the apprehension of the defendants.

[6] Liberty Reserve is currently under prosecution, the information in this section is based on the documents released by Department of Justice at: http://www.justice.gov/usao/nys/pressreleases/May13/LibertyReserveetalDocuments.php.

[7] Other estimates of the total volume of transactions and money laundered are substantially higher.

This case is being jointly prosecuted by the U.S. Attorney's Office for the Southern District of New York and AFMLS. The investigation and prosecution of Liberty Reserve is also supported by the Department of Justice's Office of International Affairs and Computer Crime and Intellectual Property Section. Over $40 million in assets, located in numerous countries, have been identified and placed under restraint pending forfeiture, and over 30 Liberty Reserve exchanger domain names have been seized.

Western Express

Western Express International, Inc. was a Manhattan corporation that serviced Eastern European criminals and supported global cybercrime by, among other crimes, acting as a digital currency exchanger, illegal money transmitter, and money launderer. Western Express exchanged conventional currency to e-Gold and WebMoney. It was one of the largest digital currency exchangers to operate within the United States. In total, Western Express exchanged $15 million in WebMoney and $20 million in e-Gold, which supported the global trafficking of stolen account data. To date, sixteen individuals have been found guilty through this case, including three citizens of Eastern European countries who were arrested and extradited with the assistance of the Czech Republic and Greece, with the assistance of the Department of Justice's Office of International Affairs.

This investigation was conducted jointly by the Secret Service and the Manhattan (New York County) District Attorney's Office and was successfully prosecuted by the Manhattan District Attorney's Office. The corporation and its officers ultimately pleaded guilty to laundering about $2 million dollars in connection with the scheme. Nine of Western Express' customers were convicted by guilty plea in the conspiracy, which trafficked nearly 100,000 stolen credit card numbers and was responsible for identity theft resulting in losses of more than $5 million. After a two-and-a-half month jury trial, completed this past June, the remaining three defendants were convicted of every count. This case demonstrates how digital currency has allowed criminals around the globe to do their criminal business together while cloaked in anonymity, and despite never meeting each other in person.

Challenges Posed by Digital Currencies

The growing criminal use of digital 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 Secret Service investigations involving the illicit administration or exchange of digital 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, and associated Federal regulations. The ability of the Secret Service and

other 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.

Digital currencies are particularly well-suited for supporting 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 digital 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 the Secret Service, but is challenging in the present fiscal environment. Additionally, while digital currencies may support the activities of transnational criminals who prey upon Americans, the administrators and exchangers of digital currencies are often based in other countries in an effort to minimize their exposure to U.S. regulation and law enforcement.

Conclusion

Digital currencies have the potential to support more efficient and transparent global commerce. However, because digital currencies continue to be used to facilitate illicit activity as well, law enforcement must continually adapt their investigative tools and techniques to dismantle criminal groups that use digital currencies for fraudulent activity or money laundering. Chairman Carper and Ranking Member Coburn, thank you for this opportunity to testify regarding the investigations conducted by the Secret Service and the lessons learned from these investigations on the evolving use of digital currencies by criminal organizations.