Office of Legislative Affairs
U.S. Department of Homeland Security
Washington, DC 20528

November 12, 2013

The Honorable Thomas R. Carper
Chairman
Committee on Homeland Security
and Governmental Affairs
United States Senate
Washington, DC 20510

Dear Chairman Carper:

Thank you for your recent letter requesting information related to virtual currencies. I appreciate this opportunity to comment on the Department of Homeland Security's (DHS) expertise in this area. The most critical capability for transnational organized crime is to quickly and quietly move large quantities of money across borders. The anonymity of cyberspace affords a unique opportunity for criminal organizations to launder huge sums of money undetected. With the advent of virtual currencies and the ease with which financial transactions can be exploited by criminal organizations, DHS has recognized the need for an aggressive posture toward this evolving trend.

DHS, through its law enforcement components such as U.S. Immigration and Customs Enforcement and the U.S. Secret Service, has been actively investigating the emerging threat and criminal exploitation of virtual currency systems that further transnational criminal operations. This effort includes targeting the underground black markets on the Internet that are operated by transnational criminal networks. The multi-prong strategy employed by DHS also targets the virtual currency platforms and the network of virtual currency exchange makers. The strategic plan to combat this criminal activity relies heavily on building upon new and existing interagency partnerships as well as educating financial institutions, specifically their Anti-Money Laundering Departments, on this criminal methodology.

DHS is committed to safeguarding the Nation's financial payment systems by investigating and dismantling criminal organizations involved in cybercrime. Responding to the growth in these types of crimes and the level of sophistication these criminals employ requires significant resources and greater collaboration among law enforcement and its public and private sector partners. DHS will continue to be innovative in its approach and has enclosed relevant information, as well as significant case summaries.

The Department is pleased that the Committee recognizes the magnitude of these issues and the evolving nature of these crimes. I look forward to continuing to work closely with you on this and other homeland security matters. Senator Coburn will receive a separate, identical response. Should you need additional assistance, please do not hesitate to contact me at
(202) 447-5890.

Respectfully,

Brian de Vallance
Acting Assistant Secretary for Legislative Affairs

Enclosures

Department of Homeland Security's (DHS) Responses to Chairman Carper and Senator Coburn's August 12, 2013 Letter Regarding Virtual Currencies

1. Please provide any policies, procedures, guidance, or advisories related to the treatment or regulation of virtual currencies and any minutes of interagency working groups involved in the development of any such policies, procedures, guidance, or advisories.

On March 18, 2013, the Department of the Treasury (Treasury) Financial Crimes Enforcement Network (FinCEN) provided guidance (FIN-2013-G001) related to the definition of virtual currency and the registration requirements of participants involved in the purchase, exchange, and sale of virtual currency. FinCEN defines the participants as a user, exchanger, and administrator.[1] DHS law enforcement components work closely with several U.S. Government representatives such as the Department of Justice's (DOJ) Asset Forfeiture and Money Laundering Section (AFMLS) and Treasury's Office of Terrorist Financing and Financial Crimes. These partnerships leverage the collective subject-matter expertise to address the threats arising from the illicit use of the virtual currency system through various working groups. For example, DHS participates in the Virtual Currency Emerging Threats Working Group where topics include the Liberty Reserve prosecution; Bitcoin Seizure/Forfeiture; Perfect Money; and Treasury enforcement tools that could be brought to bear as a response to this growing phenomenon.

DHS law enforcement executes its enforcement actions consistent with 18 USC § 982, 1956, 1960, and other relevant laws, policies, procedures, guidance, and advisories pertaining to criminal investigations and asset forfeiture as they relate to virtual currencies.

2. Please provide information related to any ongoing coordination of your agency with any other federal agencies or state and local governments related to the treatment of virtual currencies.

Successful response to dynamic cyber threats requires leveraging homeland security, law enforcement, and military authorities and capabilities, which respectively promote domestic preparedness, criminal deterrence and investigation, and national defense. The cybercrime investigations conducted by DHS's law enforcement components depend heavily on developing and maintaining effective law enforcement partnerships including those with international stakeholders. The Department of State and DOJ have a critical role in developing these international relationships and in the execution of international law enforcement action through Multilateral Assistance Treaties.

DHS works closely with the FinCEN to address the virtual currency vulnerabilities and exploitation. The majority of the cooperative efforts with FinCEN focus on coordinating

[1] A user is a person that obtains virtual currency to purchase goods or services. An exchanger is a business in the exchange of virtual currency for genuine currency, funds, or other virtual currency. An administrator is a business, which issues (putting into circulation) a virtual currency, and who has the authority to redeem (to withdraw from circulation) such virtual currency. FinCEN Money Service Business (MSB) registration requirements state an exchanger and administrator must obtain a license to process genuine currency into virtual currency and therefore must be registered with FinCEN as an MSB and comply with all *Bank Secrecy Act* requirements. A user is exempt from any registration, per FinCEN guidance.

regulatory and law enforcement actions in regards to virtual currency platforms and associated money transmitters. This collaboration improves the effectiveness of efforts countering money laundering through virtual currency systems.

Immigration and Customs Enforcement's Homeland Security Investigations (ICE-HSI) and the Secret Service also coordinate with DOJ's AFMLS to address the fact that virtual currency transactions may not meet the definition of a financial transaction as prescribed by 18 USC 1956 money laundering statute. In considering a money laundering prosecution, certain legislative remedies may be needed to define and encompass elements of those transactions conducted through virtual currency networks to fit within the meaning of the statute.

3. Please provide any plans or strategies regarding virtual currencies and information regarding any ongoing initiatives you have engaged in regarding virtual currencies and the name of the person most knowledgeable about any such plans, strategies, or initiatives.

DHS law enforcement focuses their criminal investigations on those virtual currencies that enable wide-spread criminal activity. These criminal investigations are conducted across numerous offices and are coordinated with various interagency partners. DHS also works closely with interagency partners to develop specific plans, strategies, or initiatives to address particular challenges posed by virtual currencies. Significant among these is the efforts of the Global Illicit Financial Team which includes the Secret Service, ICE-HSI, and IRS-CI.

Ed Lowery, the Special Agent in Charge of the Secret Service Criminal Investigative Division oversees the numerous Secret Service efforts regarding virtual currencies.

U.S. Department of Homeland Security

Current Secret Service Investigations and Seizures:

Baltimore Field Office

The U.S. Secret Service (USSS) has partnered with Immigration and Customs Enforcement's (ICE) Homeland Security Investigations (HSI), Drug Enforcement Agency, U.S. Postal Inspection Service, and Internal Revenue Service (IRS) on an investigation into the Silk Road, a black market criminal marketplace located on The Onion Router network. Silk Road acts as a criminal eBay, allowing the purchase of counterfeit and genuine identification, counterfeit currency, narcotics, weapons, biological agents, and criminal services. The sole currency accepted and transacted on Silk Road is Bitcoins. The site has an annual revenue stream of over $250 million and a user base in excess of 300,000. The purpose of this investigation has been to focus on the identification of the site's main administrator, referred to as Dread Pirate Roberts (DPR).

Of recent noteworthy interest was the determination that the suspect who had sent Ricin to President Obama earlier this year was a vendor on the Silk Road site. A critical component in this investigation has been the ongoing undercover operation between an undercover agent (agency undisclosed per AUSA) and the site administrator, which has resulted in the site administrator soliciting the agent to commit a murder for hire, for which the government received a total payment of $80,000.

On May 1, 2013, an arrest warrant was issued pursuant to a sealed indictment in U.S. District Court of Maryland, charging DPR with violations of Title 21 USC 846 (Conspiracy to Distribute a Controlled Substance), Title 18 USC 1512(a)(1)(c) (Attempted Witness Murder), Title 18 USC 1958(a) (Use of Interstate Commerce Facilities in Commission of Murder-for-Hire), and Title 18 USC 2 (Aiding and Abetting). The investigation has utilized numerous buy-thru operations for weapons, identification, narcotics, and explosives to identify high value targets on the site.

The USSS is responsible for the forensics and cyber analysis in this ongoing criminal investigation and, along with our interagency partners, will attempt to identify the site's origin and the identity of the site administrator. As a result of this ongoing investigation, approximately $5.5 million has been seized by the USSS and ICE-HSI.

Newark Field Office

In March of 2013, the USSS discovered that an anonymous online payment processor, known as Tcash Ads Inc., was operating an unlicensed money services business through bank accounts held at Bank of America and Banner Bank. Bank records indicated that Tcash Ads Inc. authorized millions of dollars in wire transfers on behalf of the public into the bank accounts for BitInstant, a Virtual Exchange Broker dealing in Bitcoins.

On April 29, 2013, pursuant to Federal Seizure Warrants, agents seized the bank accounts of Tcash Ads Inc, totaling $219,370.76, for violations of 18 USC 1960, operating an Unlicensed

Money Transmitting Business. Additional seizures are expected as this criminal investigation continues.

Washington Field Office

Liberty Reserve, regarded as the oldest virtual currency network on the Internet, was recently shut down by the Global Illicit Finance Team, a task force consisting of investigators from the U.S. Attorney's Office, Southern District of New York, USSS, ICE-HSI, IRS, and the Department of Justice's Asset Forfeiture and Money Laundering Section. It is estimated that in excess of $6 billion in criminal proceeds have been laundered through Liberty Reserve. To date, this investigation has produced $29 million in seizures and has resulted in the arrests of five individuals.

U.S. Department of Justice

Office of Legislative Affairs

Office of the Assistant Attorney General

Washington, D.C. 20530

October 23, 2013

The Honorable Thomas R. Carper
Chairman
Committee on Homeland Security
and Governmental Affairs
United States Senate
Washington, DC 20510

The Honorable Tom A. Coburn
Ranking Minority Member
Committee on Homeland Security
and Governmental Affairs
United States Senate
Washington, DC 20510

Dear Mr. Chairman and Senator Coburn:

This responds to your joint letter to Attorney General Holder dated August 12, 2013, asking the Department of Justice (the Department) to provide information on its efforts pertaining to virtual currency. As you know, the Federal Bureau of Investigations (FBI) briefed your Committee staff on the topic and welcomes the opportunity to further elaborate on our work.

The FBI's approach to virtual currencies is guided by a recognition that online payment systems, both centralized and decentralized, offer legitimate financial services. Virtual currency – which the FBI defines as a medium of exchange that is circulated over a network, typically the Internet, and that is not backed by a government – may be utilized in both decentralized online payment systems, such as Bitcoin, and centralized online payment systems, such as Liberty Reserve. Like any financial service, virtual currency systems of either type can be exploited by malicious actors, but centralized and decentralized online payment systems can vary significantly in the types and degrees of illicit financial risk they pose.

Illicit users are typically attracted to systems with lax anti-money laundering and know-your-customer controls. Some online payment firms allow themselves to be exploited by illicit actors by failing to implement an appropriate compliance program, and some systems are intentionally designed to attract and facilitate illicit payments, a vital service for criminal business ventures. These systems pose a considerable money laundering threat, and the FBI will continue to identify and investigate these illicit services and their users engaging in illegal activity.

Additionally, legitimate virtual currency services can become unwitting conduits for illicit transactions when malicious actors are able to defeat or circumvent the company's anti-money laundering controls. Outreach to these systems, much as the FBI conducts with the formal financial sector, is an important tool in combating the exploitation of the systems for criminal and terrorist purposes. Since centralized payment systems and exchangers often interact with the traditional financial sector and hold bank accounts at major financial institutions, the range of such FBI outreach extends to the financial services community at large. FBI Special Agents and analysts routinely provide trainings and presentations to the private sector, as well as to domestic and international law enforcement and intelligence personnel, specifically addressing virtual currency and online payment systems.

The FBI recognizes that virtual currency's ability to facilitate the global movement of funds by a wide array of illicit actors necessitates a comprehensive approach coordinated with our domestic and international partners. To facilitate such coordination, the FBI founded and chairs the Virtual Currency Emerging Threats Working Group (VCET), an interagency working group formed in early 2012 to mitigate the cross-programmatic threats arising from illicit actors' use of virtual currency systems. The working group seeks to leverage the collective subject matter expertise of its members, who represent an array of U.S. Government agencies, to address new virtual currency trends and potential law enforcement and U.S. Intelligence Community implications.

The FBI 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 has created numerous intelligence products related to virtual currency, many of which were coauthored with other members of the U.S. Intelligence Community. Within the Department, the FBI coordinates closely with counterparts at the Criminal Division's Asset Forfeiture and Money Laundering Section and the Computer Crime and Intellectual Property Section regarding virtual currency matters.

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

The Committee can be assured that the FBI and the Department as a whole are actively engaged in addressing any threat posed by virtual currency, and we welcome the opportunity to continue to work with the Committee on the matter.

We hope this information is helpful. Please do not hesitate to contact this office if we may provide additional assistance regarding this or any other matter.

Sincerely,

Peter J. Kadzik
Principal Deputy Assistant Attorney General

BOARD OF GOVERNORS OF THE FEDERAL RESERVE SYSTEM
WASHINGTON, D. C. 20551

BEN S. BERNANKE
CHAIRMAN

September 6, 2013

The Honorable Thomas R. Carper
Chairman
Committee on Homeland Security
and Governmental Affairs
United States Senate
Washington, D.C. 20510

The Honorable Tom Coburn
Ranking Member
Committee on Homeland Security
and Governmental Affairs
United States Senate
Washington, D.C. 20510

Dear Senators:

Thank you for your recent inquiry regarding virtual currencies. As you noted, virtual currencies have been receiving increased attention from U.S. authorities over the past several months.

Historically, virtual currencies have been viewed as a form of "electronic money" or "stored-value"--an area of payment system technology that has been evolving over the past 20 years. Over time, these types of innovations have received attention from Congress as well as U.S. regulators. For example, in 1995, the U.S. House of Representatives held hearings on "the future of money" at which early versions of virtual currencies and other innovations were discussed.[1] Vice Chairman Alan Blinder's testimony at that time made the key point that while these types of innovations may pose risks related to law enforcement and supervisory matters, there are also areas in which they may hold long-term promise, particularly if the innovations promote a faster, more secure and more efficient payment system.

[1] U.S. House Subcommittee on Domestic and International Monetary Policy. *The Future of Money – Part 2* Hearing, October 11, 1995, Washington: Government Printing Office, 1996. (Y4.B 22/1:104-27/PT.2).

Although the Federal Reserve generally monitors developments in virtual currencies and other payments system innovations, it does not necessarily have authority to directly supervise or regulate these innovations or the entities that provide them to the market. In general, the Federal Reserve would only have authority to regulate a virtual currency product if it is issued by, or cleared or settled through, a banking organization that we supervise. Given the Federal Reserve's authority and the manner in which virtual currencies have developed, the Federal Reserve has focused primarily on a supervised banking organization's role in the products' sale and distribution, as well as the applicable regulations, such as Bank Secrecy Act (BSA) /anti-money laundering (AML) requirements.

Policies, Procedures, Guidance or Advisories

In March 2013, the Financial Crimes Enforcement Network (FinCEN) issued guidance to clarify that an *administrator or exchanger* of virtual currency is generally considered a *money transmitter* under FinCEN definitions and therefore subject to BSA requirements.[2] The Federal Reserve's supervisory expectations and guidance related to BSA/AML compliance for bank transactions using virtual currencies have been incorporated into the Electronic Cash section of the Federal Financial Institutions Examination Council (FFIEC) BSA/AML Examination Manual.[3] The overall objective of the guidance and examination procedures provided in this section is to assess the adequacy of a bank's systems to manage the risks associated with electronic cash and management's ability to implement effective monitoring and reporting systems. The section further lists applicable risk factors and risk mitigation steps for banks to consider. The Federal Reserve supervision staff has on-going initiatives with the FFIEC member agencies to identify additional areas of BSA/AML concern that require heightened attention by the banking organizations we supervise.

Ongoing Coordination

In May 2013, the U.S. Department of the Treasury (Treasury) named Liberty Reserve S.A. as a financial institution of primary money laundering concern under Section 311 of the USA PATRIOT Act (Section 311).[4] According to the announcement, Liberty Reserve, a web-based money transfer system or "virtual currency," was specifically designed and frequently used to facilitate money laundering in cyber space. This action also marked the first use of Section 311 authorities against a virtual currency provider.

---

[2] See http://www.fincen.gov/news_room/nr/pdf/20130318.pdf.
[3] See http://www.ffiec.gov/bsa_aml_infobase/documents/BSA_AML_Man_2010.pdf.
[4] See http://www.treasury.gov/press-center/press-releases/Pages/jl1956.aspx.

The statutory language of Section 311 requires Treasury to consult with the Federal Reserve Board when these special measures are being developed and proposed. Therefore, Federal Reserve Board staff participated in coordination and consultation efforts leading up to the designation of the virtual currency provider, Liberty Reserve, under Section 311.

Specific Plans or Strategies

As noted above, the Federal Reserve plans to work with other FFIEC member agencies on electronic cash and related issues such as virtual currencies, as needed, for banking organizations. The Federal Reserve will continue to monitor developments as part of its broad interest in the safety and efficiency of the payment system. We also stand ready to cooperate with other agencies in fulfilling their mandates, as appropriate.

I hope you find this information helpful.

Sincerely,

UNITED STATES
SECURITIES AND EXCHANGE COMMISSION
WASHINGTON, D.C. 20549

THE CHAIR

August 30, 2013

The Honorable Thomas R. Carper
Chairman
Committee on Homeland Security and Governmental Affairs
United States Senate
340 Dirksen Senate Office Building
Washington, D.C. 20510

Dear Chairman Carper:

Thank you for your August 12, 2013 letter in which you seek information in connection with the Committee on Homeland Security and Governmental Affairs' inquiry into virtual currencies. In the letter, you made three specific requests. Below please find responses to your requests.

1) **[P]rovide any policies, procedures, guidance or advisories related to the treatment or regulation of virtual currencies and any minutes of interagency working groups involved in the development of any such policies, procedures, guidance or advisories.**

As noted in your letter, last month the Commission charged Trendon T. Shavers and his company, Bitcoin Savings and Trust, with defrauding investors in a Ponzi scheme involving Bitcoin.[1] In conjunction with the filing of that action, the SEC's Office of Investor Education and Advocacy released an Investor Alert warning investors about fraudulent schemes that may involve Bitcoin and other virtual currencies. A copy of that alert can be found at http://www.sec.gov/investor/alerts/ia_virtualcurrencies.pdf. The alert recommends that investors be wary of purported investment opportunities that promise high rates of return with little or no risk, including investments that claim to have ties to new and emerging technologies.

Whether a virtual currency is a security under the federal securities laws, and therefore subject to our regulation, is dependent on the particular facts and circumstances at issue. Regardless of whether an underlying virtual currency is itself a security, interests issued by entities owning virtual currencies or providing returns based on assets such as virtual currencies likely would be securities and therefore subject to our regulation.

This is the situation with the exchange-traded virtual currency trust referenced in your letter. The trust filed a registration statement under the Securities Act of 1933 with the

[1] *See* http://www.sec.gov/News/PressRelease/Detail/PressRelease/1370539730583.

Commission in July of this year covering the offering of interests in the trust to the public.[2] Consistent with our standard practice for initial public offerings, staff of the Division of Corporation Finance is reviewing the registration statement. In general, Division of Corporation Finance staff, through its reviews, seeks to ensure that investors are provided with information they need about the issuer, security and offering in order to make informed investment decisions. When the staff identifies instances where it believes an issuer can improve its disclosure or enhance its compliance with the applicable disclosure requirements, it provides the issuer with comments. The range of possible comments depends on the issues that arise in a particular filing review. When an issuer has resolved all of the comments, the Division of Corporation Finance, through authority delegated from the Commission, declares the registration statement effective and the issuer may offer and sell the securities described in the registration statement.

Prior to listing and trading shares on a national securities exchange of either a trust such as the trust noted above or other products linked to virtual currencies, an exchange must file a proposed rule change with the Commission that, if approved, would permit the listing and trading of the product on the exchange. Such proposed rule change would be subject to public notice and comment. The Commission, or the Division of Trading and Markets through authority delegated from the Commission, would approve the proposed rule change only if it is consistent with the requirements of the Securities Exchange Act of 1934, which requires, among other things, that an exchange's rules be designed to prevent fraudulent and manipulative acts and practices, promote just and equitable principles of trade, remove impediments to and perfect the mechanism of a free and open market and a national market system, and in general protect investors and the public interest. In making a determination regarding whether a proposed rule change relating to a trust or other product linked to virtual currencies is consistent with the requirements of the Exchange Act, the Commission will consider all comments received from the public.

2) [P]rovide information related to any ongoing coordination of the agency with any other federal agencies or state and local governments related to the treatment of virtual currencies.

With regard to virtual currencies, staff from the Commission's Division of Enforcement has been and continues to be in communication with representatives from several federal and state agencies concerning potential fraudulent activity, including, for example, the Department of Justice, the Department of Treasury, the New York State Office of the Attorney General, and the New York State Department of Financial Services. As a general matter, Division of Enforcement staff coordinates and cooperates with other law enforcement agencies and regulators, both domestic and foreign, including referring matters more appropriately pursued by other agencies and self-regulatory organizations. Also, pursuant to Commission rules, Division of Enforcement staff routinely provides certain non-public information from investigative files to other agencies and certain third parties (e.g. state or foreign authorities or self-regulatory organizations) who provide appropriate representations of confidentiality.

---

[2] *See* http://www.sec.gov/Archives/edgar/data/1579346/000119312513279830/0001193125-13-279830-index.htm.

Additionally, in connection with the recently-filed registration statement from the above-referenced exchange-traded virtual currency trust, staff from the Commission's Division of Corporation Finance, consistent with staff practice, advised staff from the Commodity Futures Trading Commission ("CFTC") of the filing of the registration statement and noted that the assets of the trust were stated to be Bitcoins. In connection with its review of registration statements, Commission staff customarily provides information to CFTC staff if the registrant appears to hold assets that are or may be subject to CFTC jurisdiction.

Furthermore, staff from the Division of Trading and Markets recently attended an informational meeting with Bitcoin Foundation organized by Department of the Treasury's Financial Crimes Enforcement Network. The meeting was educational in format and Bitcoin Foundation representatives covered legal, policy, technology, and law enforcement issues from their perspective.

3) [P]rovide any plans or strategies regarding virtual currencies and information regarding any ongoing initiatives the Commission has engaged in regarding virtual currencies and the name of the person most knowledgeable about any such plans, strategies or initiatives.

In addition to the activities described above, consistent with the Commission's mission, we are closely monitoring the marketplace for potential violations of the securities laws and other developments relating to the interplay of virtual currencies or other emerging technologies and the federal securities laws. As these issues and activities involve multiple divisions and offices of the agency, requests for further information or assistance can be coordinated through Julie Davis in the Commission's Office of Legislative and Intergovernmental Affairs at (202) 551-2010.

I hope that this information is helpful to you. Please do not hesitate to contact me at (202) 551-2100, or have a member of your staff contact Ms. Davis, if you have any additional concerns or comments.

Sincerely,

Mary Jo White

Mary Jo White
Chair

DEPARTMENT OF THE TREASURY
WASHINGTON, D.C. 20220

ASSISTANT SECRETARY

September 18, 2013

The Honorable Thomas R. Carper
Chairman
Committee on Homeland Security and
Governmental Affairs
United States Senate
Washington, DC 20510

Dear Chairman Carper:

Thank you for your letter regarding virtual currencies and the relevant authorities of the Department of the Treasury to safeguard the U.S. financial system from financial crimes and national security threats. The Treasury Department is following the emergence of virtual currencies and their potential for licit and illicit use very closely. Virtual currencies, like other payment systems, provide legitimate financial services, but also may be exploited by criminal actors, including money launderers as well as terrorist financiers. However, practical constraints such as scope, liquidity and volatility have prevented virtual currencies from becoming the predominant mode of large-scale illicit transactions to date.

Treasury authorities relevant to responding to the illicit use of virtual currencies include: issuing advisories to financial institutions; taking action under Section 311 of the USA PATRIOT Act; imposing targeted financial sanctions and taking civil enforcement actions. The following are examples of how Treasury authorities have been or could be deployed:

- **Guidance on Virtual Currencies:** In March 2013, the Financial Crimes Enforcement Network (FinCEN) issued guidance clarifying that administrators and exchangers of virtual currencies are treated as money transmitters under its money service business regulations. As such, these entities are required to register with FinCEN, implement an anti-money laundering program, maintain certain transaction records, and file reports with FinCEN regarding large cash and/or suspicious transactions.

- **Section 311 of the USA PATRIOT Act**: In May 2013, FinCEN identified Liberty Reserve, a Costa-Rica-based virtual currency provider, as a primary money laundering concern and issued a proposed regulation that would prohibit U.S. financial institutions from maintaining correspondent accounts with foreign institutions that process transactions on behalf of the virtual currency provider through the U.S. correspondent account. This action was taken in coordination with the unsealing of an indictment by the Department of Justice charging Liberty Reserve and seven of its principals for their alleged roles in operating as an unlicensed money transmitter in the U.S. and facilitating the movement of $6 billion in illicit proceeds.

- **Designations Actions:** The Office of Foreign Assets Control (OFAC) has the authority to potentially target malicious cyber actors, including virtual currency providers, who fit the designation criteria of various existing sanctions authorities, including, for example, where they provide support to terrorists (Executive Order 13224) or engage in criminal activity on behalf of transnational criminal organizations (Executive Order 13581).

- **Civil Enforcement:** Both FinCEN and OFAC have authority to identify and impose civil penalties for violations of U.S. law. Virtual currency providers and exchangers that fail to comply with federal obligations can be subject to civil monetary penalties by FinCEN under the Bank Secrecy Act and penalties related to sanctions violations by OFAC.

- **Multilateral Engagement:** Promoting a transparent financial system is an essential component of Treasury's efforts to combat money laundering and terrorist financing and implement effective targeted financial measures. The success of our efforts domestically depends in large part on the willingness of other countries to also establish effective anti-money laundering (AML) and combating the financing of terrorism (CFT) safeguards. Treasury works with the Financial Action Task Force (FATF), the global AML-CFT standard-setting body to maintain an effective global AML-CFT framework.

In addition, Treasury closely coordinates with its state regulatory counterparts to encourage appropriate application of FinCEN guidance as part of the states' separate AML compliance oversight of financial institutions. Most recently, on August 26th, FinCEN included state and federal agencies in a discussion with the Bitcoin Foundation, at which government and Bitcoin Foundation representatives had an opportunity to describe to Treasury and others how Bitcoin works and how, as a decentralized virtual currency, it differs from centralized virtual currencies, such as Liberty Reserve.

Treasury also continues to participate in interagency efforts that focus on virtual currencies or discuss virtual currencies as part of a larger mission, including the Virtual Currency Emerging Threats Working Group led by the FBI, the National Cyber Investigative Joint Task Force (NCIJTF), and the Federal Financial Institutions Examination Council BSA Working Group.

We appreciate your interest in this matter and look forward to working with you on matters of mutual interest in the future. If you have additional questions on this topic, please contact Kathleen Mellody, Office of Legislative Affairs, at (202) 622-1900.

Sincerely,

Alastair Fitzpayne

Alastair M. Fitzpayne
Assistant Secretary for Legislative Affairs

Identical letter sent to:
The Honorable Tom A. Coburn