AUTHENTICATED
U.S. GOVERNMENT
INFORMATION
GPO

S. HRG. 113–210

# THE PRESENT AND FUTURE IMPACT OF VIRTUAL CURRENCY

## JOINT HEARING

BEFORE THE

SUBCOMMITTEE ON NATIONAL SECURITY AND INTERNATIONAL TRADE AND FINANCE

AND THE

SUBCOMMITTEE ON ECONOMIC POLICY

OF THE

COMMITTEE ON
BANKING, HOUSING, AND URBAN AFFAIRS
UNITED STATES SENATE

ONE HUNDRED THIRTEENTH CONGRESS

FIRST SESSION

ON

EXPLORING THE DEVELOPMENT OF VIRTUAL CURRENCIES, THEIR CURRENT AND POTENTIAL FUTURE USE, AND THE REGULATORY, MONETARY, NATIONAL SECURITY, AND OTHER IMPACTS AND ISSUES ASSOCIATED WITH THEM

NOVEMBER 19, 2013

Printed for the use of the Committee on Banking, Housing, and Urban Affairs

Available at: http://www.fdsys.gov/

U.S. GOVERNMENT PRINTING OFFICE

87–095 PDF WASHINGTON : 2014

For sale by the Superintendent of Documents, U.S. Government Printing Office
Internet: bookstore.gpo.gov Phone: toll free (866) 512–1800; DC area (202) 512–1800
Fax: (202) 512–2104 Mail: Stop IDCC, Washington, DC 20402–0001

## COMMITTEE ON BANKING, HOUSING, AND URBAN AFFAIRS

TIM JOHNSON, South Dakota, *Chairman*

JACK REED, Rhode Island
CHARLES E. SCHUMER, New York
ROBERT MENENDEZ, New Jersey
SHERROD BROWN, Ohio
JON TESTER, Montana
MARK R. WARNER, Virginia
JEFF MERKLEY, Oregon
KAY HAGAN, North Carolina
JOE MANCHIN III, West Virginia
ELIZABETH WARREN, Massachusetts
HEIDI HEITKAMP, North Dakota

MIKE CRAPO, Idaho
RICHARD C. SHELBY, Alabama
BOB CORKER, Tennessee
DAVID VITTER, Louisiana
MIKE JOHANNS, Nebraska
PATRICK J. TOOMEY, Pennsylvania
MARK KIRK, Illinois
JERRY MORAN, Kansas
TOM COBURN, Oklahoma
DEAN HELLER, Nevada

CHARLES YI, *Staff Director*
GREGG RICHARD, *Republican Staff Director*

DAWN RATLIFF, *Chief Clerk*
KELLY WISMER, *Hearing Clerk*
SHELVIN SIMMONS, *IT Director*
JIM CROWELL, *Editor*

---

## SUBCOMMITTEE ON NATIONAL SECURITY AND INTERNATIONAL TRADE AND FINANCE

MARK R. WARNER, Virginia, *Chairman*
MARK KIRK, Illinois, *Ranking Republican Member*

SHERROD BROWN, Ohio
JOE MANCHIN III, West Virginia

JERRY MORAN, Kansas

MILAN DILAL, *Subcommittee Staff Director*
LINDSEY JOHNSON, *Republican Subcommittee Staff Director*

---

## SUBCOMMITTEE ON ECONOMIC POLICY

JEFF MERKLEY, Oregon, *Chairman*
DEAN HELLER, Nevada, *Ranking Republican Member*

JOHN TESTER, Montana
MARK R. WARNER, Virginia
KAY HAGAN, North Carolina
JOE MANCHIN III, West Virginia
HEIDI HEITKAMP, North Dakota

TOM COBURN, Oklahoma
DAVID VITTER, Louisiana
MIKE JOHANNS, Nebraska
MIKE CRAPO, Idaho

ANDREW GREEN, *Subcommittee Staff Director*
SCOTT RIPLINGER, *Republican Subcommittee Staff Director*

# C O N T E N T S

## TUESDAY, NOVEMBER 19, 2013


| | Page |
|---|---|
| Opening statement of Chairman Warner | 1 |
| Opening statement of Chairman Merkley | 3 |
| Opening statements, comments, or prepared statements of: | |
| Senator Heller | 2 |
| Senator Kirk | 4 |
| Prepared statement | 31 |


## WITNESSES


| | |
|---|---|
| Jennifer Shasky Calvery, Director, Financial Crimes Enforcement Network, Department of the Treasury | 4 |
| Prepared statement | 32 |
| Response to written questions of: | |
| Senator Kirk | 71 |
| David J. Cotney, Commissioner of Banks, Massachusetts Division of Banks, on behalf of the Conference of State Bank Supervisors | 6 |
| Prepared statement | 38 |
| Paul Smocer, BITS President, on behalf of the Financial Services Roundtable | 16 |
| Prepared statement | 46 |
| Response to written questions of: | |
| Senator Kirk | 73 |
| Sarah Jane Hughes, University Scholar and Fellow in Commercial Law, Indiana University Maurer School of Law, | 18 |
| Prepared statement | 51 |
| Response to written questions of: | |
| Senator Kirk | 74 |
| Mercedes Kelley Tunstall, Partner and Practice Leader, Privacy and Data Security Group, Ballard Spahr LLP | 19 |
| Prepared statement | 58 |
| Anthony Gallippi, Cofounder and CEO, Bitpay | 21 |
| Prepared statement | 60 |
| Response to written questions of: | |
| Senator Kirk | 77 |


## ADDITIONAL MATERIAL SUPPLIED FOR THE RECORD


| | |
|---|---|
| Prepared statement of Aaron J. Greenspan | 81 |

# THE PRESENT AND FUTURE IMPACT OF VIRTUAL CURRENCY

**TUESDAY, NOVEMBER 19, 2013**

U.S. SENATE, SUBCOMMITTEE ON NATIONAL SECURITY AND INTERNATIONAL TRADE AND FINANCE, SUBCOMMITTEE ON ECONOMIC POLICY, COMMITTEE ON BANKING, HOUSING, AND URBAN AFFAIRS,
*Washington, DC.*

The Subcommittees met at 3:34 p.m., in room SD–538, Dirksen Senate Office Building, Hon. Mark R. Warner and Hon. Jeff Merkley, Chairmen of the Subcommittees, presiding.

## OPENING STATEMENT OF SENATOR MARK R. WARNER

Senator WARNER. I am pleased to co-chair this joint Subcommittee hearing on "The Present and Future Impact of Virtual Currency." My friend Senator Merkley and I also appreciate the work that Senator Heller has done, and I know Senator Kirk is going to be joining us as well.

We are going to do this a little different. Because this is a joint Subcommittee hearing, I will chair the first panel, and Senator Merkley will chair the second panel.

The uses of virtual currencies have proliferated in recent years. My hope for this hearing is to educate the Senate Members and others and start the education of the public about virtual currencies, including the potential and drawbacks. I also hope to explore how regulators are keeping up with this technological innovation to protect consumers.

I have got a full statement here, but I actually have to acknowledge that, you know, I have been following this development of bitcoins for the last few months, and I think I am only starting to wrap my head around the potential upside, downside, regulatory issues, monetary policy issues, taxation issues, consumer protection issues that this innovation represents. And rather than going through my whole statement, I just will point out to the witnesses that back in 1982 I had the opportunity to get engaged in a new industry at that point that was on the cutting edge of innovation called cellular telephones. And all of the experts at that point thought it would take the world 30 years to develop out a wireless network and at the end of that 30 years about 5 percent of Americans would use them. Luckily for me, the experts were wrong, and now these devices transform our lives.

Getting it right from all of the regulatory, financial, consumer points around virtual currencies, and Bitcoin in particular, could pose as great, if not greater challenge and opportunity. And what

my hope is is that this will be the beginnings of an effort to come in with open minds, to hear about the potential, but to also hear about the important ramifications around monetary policy, around taxation. Think about the notion with this 21 million bitcoins that could be created, and as we see acceptance—I understand already the FEC has allowed political contributions to be made in bitcoins, so this is a development that is already in process. But if this becomes a standard currency or tool, it could radically and dramatically transform the role of central banks, monetary policy. It could transform—it has enormous security concerns.

So I am very, very interested about this hearing as a member of the Intelligence Committee. I am concerned as well about the potential abuse of this development. But I think as we see now about somewhere between 10 to 12 million bitcoins that have been mined and just the reactions yesterday from Senator Carper's hearing where I believe bitcoins spiked at over $700 per unit, we are talking about a currency that has already been monetized, and we as policymakers in ways will have to catch up.

So I am very much looking forward to this and really appreciate my colleagues and, in particular, Senator Merkley's interest in this, and with that I will turn to Senator Heller, and we will go back and forth with just a couple quick opening statements, and then I want to get to introducing the witnesses.

**STATEMENT OF SENATOR DEAN HELLER**

Senator HELLER. Very good. Thank you, Mr. Chairman. I want to thank you and Chairman Merkley for holding this Subcommittee. I want to thank Ranking Member Kirk, and I am happy that we are having this joint Committee. I think we need to have more of these, and with that, I will keep my statement relatively brief.

Today we are here to learn about virtual currencies and cryptocurrencies, the most popular, of course, which is Bitcoin. While generations in Nevada have mined for gold and silver and copper, today Nevadans can now mine for new virtual currencies on their computer.

While these virtual currencies are not yet widely accepted, the number of users continue to grow, and we must recognize that these innovations decentralize digital payment systems.

Today I look forward to learning about the long-term viability and practicality of virtual currencies. I also want to learn how various Government regulators interact with virtual currencies and which by their design are meant to be independent, of course, of any government.

I will end with this note: The Internet is a new frontier of innovation. With every new Internet-based technology, I believe that Members of Congress should recognize that we often do not know what these new advancements will development into. While we must ensure proper safeguards, it is my hope that through hearings like this we can help maintain an environment that continues to promote new financial technologies and innovative growth.

So thank you again to my colleagues. I look forward to hearing all the testimonies from our witnesses. Thank you.

Senator WARNER. Thank you, Senator.

Senator Merkley.

**OPENING STATEMENT OF SENATOR JEFF MERKLEY**

Senator MERKLEY. Thank you, and it is a pleasure to co-chair this gathering. I can see by the full room the level of interest and enthusiasm in this topic. Certainly this is a new technological strategy that has a tremendous number of implications. The wave of innovation is reaching into the world of currency payments and money transmission. We have all heard about exciting developments such as mobile payments and companies like Square, which rely on classic banking system payments.

This latest generation of technology which we are talking about today takes things to a whole new level. With the creation of virtual currencies like Bitcoin and more recently Ripple, we are actually seeing payments transacted entirely with peer-to-peer trust driving the stores of value. Combined with open-source code and a public transaction ledger listing every transaction, virtual currencies are truly a completely different animal.

Similar to the ways that the last decade's innovations out of the Silicon Valley and Silicon Forest have improved people's lives—I had to throw "Silicon Forest" in there because that is in Oregon. [Laughter.]

Senator MERKLEY. Developments in virtual currency have real potential to provide value to American consumers and businesses. More transaction costs, more secure money transmission—these are significant qualities. At the same time, leaving this space unwatched and unregulated will all but ensure it is full of pitfalls for users and law enforcement alike. We have had recent news about illicit activities, narcotics money laundering; we have had rapid fluctuations in the value of the market for the bitcoins. We have questions about consumer protections, and there is certainly, therefore, a lot of issues about whether virtual currencies are ready for prime time.

Today's hearing will explore the current and future state of virtual currency, especially how it affects core financial services that families and businesses rely on to move money and make payments, where is the potential for innovation and opportunity, and where are the gaps and weaknesses along the way.

I wanted to note I have a recent article here called "Portland Businesses Enter the World of Digital Currency." Back in 2009, Gregg Abbott, the owner of Whiffies Fried Pies, was hanging out with a bunch of tech enthusiasts along his food cart, and he was discussing the potential of the then-new online currency known as Bitcoin. And one of the folks hanging out, an early investor, offered Abbott 1,000 bitcoins for one of his ham pies. He says, "I did not say no. I just got distracted, and the individual wandered off." And then he says, "That was a $250,000 mistake. Silly me." Well, based on yesterday's value, that is a $700,000 mistake. That certainly would have been the most expensive pie in the history of humankind.

This is absolutely fascinating. By the way, he did proceed to start accepting bitcoins, as a number of Portland facilities have done, using a mobile app that converts from dollar, bitcoin to dollar, and

back and forth based on the most recent exchange rate. So this is actually a functional, viable technology at this very moment.

So, with that, Senator Kirk.

Senator WARNER. Senator Kirk.

**STATEMENT OF SENATOR MARK KIRK**

Senator KIRK. Thank you, Mr. Chairman. I just thank you for gathering us together on this Bitcoin effort. I would say that I have been worried about Bitcoin, that because it is so complicated it could facilitate illegal activities or terrorist activities.

Senator WARNER. Thank you, Senator Kirk, and I think that is obviously one of the focuses we will have on this first panel.

Let us get to the witnesses. Let us get to the real experts. The first panel, as I mentioned, will focus from the governmental side; the second panel will focus more from some of the advocates, and I think it will be an interesting afternoon.

We have Ms. Jennifer Shasky Calvery, the Director of Financial Crimes Enforcement Network, FinCEN, a bureau of the Treasury Department. Prior to joining Treasury, she was Chief of the Asset Forfeiture and Money Laundering Section at the U.S. Department of Justice. As Chief, Ms. Shasky Calvery managed a Justice Department program responsible for the annual forfeiture of more than 1.5 billion in criminal assets and related programs to ensure that those assets were returned to victims and reinvested in law enforcement. She has also testified before Congress on a wide range of issues, including transnational organized crime, financial crime, State business incorporation practices, and this one will probably break some new boundaries as well. Welcome, Ms. Shasky Calvery.

Mr. David Cotney is Commissioner of Banks for the Commonwealth of Massachusetts. He has served in that position since November 2010 overseeing the supervision of over 200 banks and credit unions without assets in excess of $325 billion. Mr. Cotney is an active contributor to consumer protection efforts, both in Massachusetts and nationally. In 2013, he was elected as Vice Chairman of the Board of Directors of the Conference of State Bank Supervisors, on whose behalf he testifies here today. Welcome, Mr. Cotney.

Ms. Shasky Calvery, if you could start.

**STATEMENT OF JENNIFER SHASKY CALVERY, DIRECTOR, FINANCIAL CRIMES ENFORCEMENT NETWORK, DEPARTMENT OF THE TREASURY**

Ms. SHASKY CALVERY. Chairmen Warner and Merkley, Ranking Members Kirk and Heller, and Members of the Subcommittees, I am Jennifer Shasky Calvery, the Director of Treasury's Financial Crimes Enforcement Network, or FinCEN. I am pleased to be here today to discuss the important regulatory, enforcement, and analytical work we are doing at FinCEN to prevent illicit actors from exploiting the U.S. financial system as technological advances, such as virtual currency, create new ways to move money.

Recognizing the potential for abuse of emerging new payment methods and understanding that anti-money-laundering protections must keep pace with these advancements, FinCEN began

working with our partners several years ago to study the issue. Here is what we learned.

Illicit actors might decide to use virtual currency for many of the same reasons as legitimate users, but also for some more nefarious ones. Specifically an illicit actor may choose to use a virtual currency because it provides anonymity, is easy to navigate, may have low fees, is accessible globally with a simple Internet connection, does not typically have transaction limits, is generally secure, and provides a loophole from the AML/CFT regulatory safeguards in most countries around the world.

Indeed, the idea that illicit actors might exploit the vulnerabilities of virtual currency to launder money is not theoretical. Liberty Reserve engaged in a $6 billion major money-laundering operation, and just recently, the Department of Justice alleged that customers of Silk Road, the largest contraband marketplace on the Internet, were required to pay in bitcoins to evade detection and facilitate laundering hundreds of millions of dollars.

That being said, it is also important to put virtual currency in perspective. It has been publicly reported that Bitcoin processed transactions worth approximately $8 billion over the last year. But by way of comparison, in 2012 Bank of America alone made $245 trillion in wire transfers. Thus, while of growing concern, to date virtual currencies have yet to overtake more traditional methods to move funds, whether for legitimate or criminal purposes.

Nonetheless, to address growing concerns, in July 2011, after a public comment period, FinCEN released two regulations which update several definitions and provide flexibility to accommodate payment systems innovation, including virtual currencies, under our pre-existing regulatory framework. Then last March, FinCEN issued additional guidance to further clarify the compliance obligations for virtual currency actors covered by our regulations. In short, they are required to register with FinCEN, put AML controls in place, and provide certain reports to FinCEN.

It is in the best interests of virtual currency providers to comply with these regulations. Any financial institution could be exploited for money-laundering purposes. What is important is for institutions to put controls in place to deal with those money-laundering threats.

At the same time, being a good corporation citizen and complying with regulatory responsibilities is good for a company's bottom line. Every financial institution needs to be concerned about its reputation and show that it is operating with transparency and integrity within the bounds of the law. Legitimate customers will be drawn to a virtual currency or administrator or exchanger where they know their money is safe and where they know the company has a reputation for integrity. And banks will want to provide services to administrators or exchangers that show not only great innovation but also great integrity and transparency.

The decision to bring virtual currency within the scope of our regulatory framework should be viewed as a positive development for the sector. It recognizes the innovation virtual currencies provide and the benefits they might offer society. Several new payment methods in the financial sector have proven their capacity to empower customers and expand access to financial services. We

want such advances to continue. However, those institutions that choose to act outside of the law will be held accountable. FinCEN will do everything in its regulatory power to stop abuses of the U.S. financial system.

We have proven our willingness to do just that by using our targeted financial measures under Section 311 of the PATRIOT Act to name Liberty Reserve as a primary money—laundering concern and take steps to terminate its access to the U.S. financial system. We stand ready to take additional regulatory actions as necessary to stop other abuses.

As the financial intelligence unit for the United States, FinCEN must stay current on how money is being laundered in the United States so that we can share this expertise with our domestic and foreign partners and serve as the cornerstone of this country's AML/CFT regime. We are meeting this obligation in the virtual currency space as we continue to deliver cutting-edge analytical products to inform the actions of our many partners. The Administration has made appropriate oversight of the virtual currency industry a priority, and FinCEN is very encouraged by the progress we have made thus far.

Thank you for inviting me to testify before you today. I would be happy to answer any questions you may have.

Senator WARNER. Thank you so much.

Mr. Cotney.

**STATEMENT OF DAVID J. COTNEY, COMMISSIONER OF BANKS, MASSACHUSETTS DIVISION OF BANKS, ON BEHALF OF THE CONFERENCE OF STATE BANK SUPERVISORS**

Mr. COTNEY. Thank you. Good afternoon, Chairmen Warner and Merkley, Ranking Members Kirk and Heller, and Members of the Subcommittees. My name is David Cotney, and I serve as the Commissioner of Banks for the Commonwealth of Massachusetts.

It is my pleasure to testify before you today on behalf of the Conference of State Bank Supervisors. I thank you for holding this hearing today to address the risks and benefits of virtual currency.

The risks of virtual currency include consumer protection, payment systems, national security, money laundering, and other illicit activities. The potential benefits are also diverse: speed and efficiency, lower transaction costs, and providing an outlet for the unbanked and underbanked.

With these evolving payment technologies, States are exploring the connection between existing money transmitter regulation and virtual currencies. State regulators have long supervised money transmitters to protect consumers and preserve national security and law enforcement interests.

State regulators are talking with industry and other regulators about evolving methods of moving funds. This includes virtual currencies, prepaid cards, mobile services, and peer-to-peer transactions. State regulators believe that an open dialogue among regulatory, industry, and other stakeholders is key to accomplishing the goal of determining the appropriate level of oversight and supervision.

Emerging payment technologies and alternative currencies are, at their core, about the electronic movement of other people's

money. This is not unlike the activities of money transmitters for which the States have an established structure for regulation and oversight.

Licensing is the foundation of supervision, ensuring that businesses in a position of trust are legitimate and accountable. And entities seeking a State license must submit information to verify their credentials, typically including criminal background and credit checks, business plans, financial statements, and surety bonds.

State regulators examine money transmitters on an ongoing basis, ensuring that a company does not lose its customer's money and complies with consumer protection laws. Further, States actively examine for Bank Secrecy Act and anti-money-laundering requirements, coordinating with FinCEN and the IRS.

In addition to licensing and examinations, enforcement is a key part of State supervision. After working with the Brazilian Central Bank and two private banks in Brazil, my division earlier this year found evidence of forgery and ongoing illegal conduct by a licensed money transmitter. Relying on existing State-to-State coordination processes, 37 States were able to ensure that all customers were made whole after we shut down the company.

Cooperation has been a hallmark of State supervision, manifested in a uniform licensing system for all States. Originally developed by the States as a mortgage licensing platform and codified into Federal law by the SAFE Act of 2008, the Nationwide Multi-State Licensing System has become an integral part of State supervision for a variety of nonbank financial services providers. Massachusetts and 14 other States currently use NMLS as the licensing platform for money transmitters, and 14 more will start using the system in the next year.

To improve the States' ability to use the NMLS for other licenses like money transmitters, I want to note CSBS' support for S. 947, which enhances the SAFE Act's protections for confidential or privileged information.

To address the rapidly changing technology and payments landscape, CSBS continues to explore policy options for digital issues facing regulators. We look forward to working with Congress and policymakers to continue a collaborative approach to all innovative financial products and services, ensuring individuals and economies are well served.

Thank you, and I look forward to answering any questions you may have.

Senator WARNER. Thank you both for your testimony.

We will put 5 minutes on the clock and go back and forth.

I want to pick up on something Senator Heller said in his opening statement as I try to, again, wrap my head around this. We have to strike the right balance since we are talking about here no governmental entity, and we are talking about here the anonymity that is allowed to take place, the ability to set up these exchanges with very little oversight. If we lay too much a regulatory burden, we could simply chase these exchanges offshore and still leave Americans unprotected.

So I guess my first question for both of the witnesses is: We are talking about this as a currency, but have we really determined even that? I mean, there are some who said this may simply be an

Internet protocol. Or is this a security? Have we thought through—or is it a currency? And from FinCEN, and also, David, if you want to make a comment as well, you know, has FinCEN consulted at all with the SEC or the CFTC as you have started to develop your guidance? And then, Mr. Cotney, if you would answer the question as well, you know, is there any kind of beginnings of an international regime, as you talked about with the Brazilians, how they are categorizing this development?

Ms. SHASKY CALVERY. Thank you, Senator. I will attempt to take those questions in turn.

So first on the issue of is it a currency, FinCEN is the regulator for anti-money-laundering and counterterrorist finance purposes, and so we have never opined and still are not opining as to whether virtual currency is a real currency, or a commodity, as those questions are really outside our purview.

What we do recognize is that it exists and that it is operating and value is being transferred through the U.S. financial system, and as such, we need to protect that financial system from illicit actors.

And so we were able to cover it under our pre-existing definitions and regulations, which include the concept of other value that substitutes for currency. So we did not need to take a position. But in terms of have we consulted with other regulatory bodies here, at least federally, the answer is we have. Again, as a part of our rulemaking and our guidance on our narrow lane and issue, we spoke with the FBI, the Secret Service, DEA, ICE, FDIC, OCC, IRS, the Federal Reserve, NCUA——

Senator WARNER. And they all have sophisticated opinions on Bitcoin?

[Laughter.]

Ms. SHASKY CALVERY. Yes. Now that I will let them answer. But we did consult with—including CFPB from the consumer fraud perspective. But, you know, we have consulted with all of them as we can. This is a developing and innovative arena. We were lucky to be able to cover it under pre-existing regulations. As we talked to our counterparts abroad, which I think was kind of the last portion of your question, there is great interest by fellow regulators abroad, as they are trying to get their heads around what is this and what does it mean. Our German counterparts, like us, had fairly flexible regulations in place that they could fit this within pre-existing regulations, and so they have done so. And other countries thus far have been asking us to see what we are doing and why.

And, finally, I understand the Financial Action Task Force, which is the AML standard-setting body for the international community, plans to take up this topic.

Senator WARNER. Mr. Cotney?

Mr. COTNEY. In answer to your first question about the level of regulation, that is exactly what the States are trying to do by working with our colleagues, both State and Federal regulators, law enforcement, working with industry, to make sure that we have the appropriate level of oversight and supervision, and that we have the tools to detect and prevent illegal activity.

In terms of your second question on international regimes, I think it is important to note that many of these evolving alter-

native payment systems are in response to consumer demand. And as we have seen in Europe and as we have seen in Canada and elsewhere, there is a big demand for more real-time payments at lower transaction costs, including the transmission of money from one country to the next.

There are many members of Europe and Canada that have embarked on efforts to speed the payment systems. Ours has not really evolved substantially in the last 40 years. So I think now is the time to be talking about this subject.

Senator WARNER. Well, I am going to turn to Senator Kirk, who I know will press on some of the potential for abuse, but, you know, I may want to get back some of the folks from Treasury at some point, because I do think there could at least be the potential of serious implications about monetary policy. We have taken—even though with Congress' recent actions sometimes we seem to be jeopardizing America's status as the reserve currency, with some of our, I think, mistakes we have made, but, you know, if you think a little broadly, this could, again, have huge, huge implications. So I am looking forward to further pursuing this.

Senator Kirk?

Senator KIRK. Thank you, Mr. Chairman. I would just ask Jennifer one quick question. Have we seen any recognized terrorist group ever express interest or actually use Bitcoin for its operations?

Ms. SHASKY CALVERY. So we have certainly recognized the possibility and the vulnerability there. There is nothing in terms of information in the public domain about a terrorist organization expressing such interest or using it, but we would always be more than happy to have any outside briefings to discuss that topic further.

Senator KIRK. Thank you.

Thank you, Mr. Chairman.

Senator WARNER. Senator Merkley.

Senator MERKLEY. Thank you very much.

I wanted to ask a couple things related to different forms of crimes that have occurred with bitcoins. The first thing I want to ask is: There is a centralized public ledger that is encrypted, and so the anonymity is only in terms of—you are not truly anonymous. There is an encrypted version of who owns what. And so one concern about, if you will, the reliability of a currency is whether that encryption can actually be broken. So I want to ask that question. There are some very powerful code breakers in the world, and we certainly have discussions about our own U.S. capability to break codes quite often up here.

But the second is we have had this series of reported crimes. One was a Bitcoin savings and trust which ran a pyramid scheme in bitcoins. We also had the hacking of a Bitcoin exchange called BitFloor, and as it was reported, 24,000 bitcoins were stolen. And we had Instawallet, a wallet provider that was hacked, and they lost 35,000 bitcoins. These are not small-dollar items given the value of the individual coins. But maybe to paint a little bit of a picture for us, how does this all work? If there is a public ledger that is keeping track of who owns what, then how does one actually steal a bitcoin?

Ms. SHASKY CALVERY. All right. So in terms of breaking the code and the really powerful cryptologists that are out there, I just do not know the answer to that. I do not know if there is anyone out there that can break the code. It has certainly been represented to us at FinCEN that it is as strong an encryption as exists out there, and so it seems quite safe from that standpoint.

Senator MERKLEY. This is prime number trapdoor cryptology?

Ms. SHASKY CALVERY. To tell you the truth, I do not know the type of cryptology that is used, but I would be happy to take that back and get you an answer.

In terms of some of the types of schemes you mentioned, whether it is a pyramid scheme or hacking, probably the most relevant concept that comes up there is the irrevocability of the transactions of bitcoins. So the idea that when I take a bitcoin and pay you with that bitcoin, there is no way for me to get that money, so to speak, or that bitcoin back unless you choose to give it to me and choose to tell me who you are. And so that can be a great tool for fraudsters in the pyramid scheme sense or hackers who hack into your computer and are able to get your code that is your half of the bitcoin, so to speak.

So as I understand it, there is a public key and a private key to Bitcoin. I think of the public key myself almost like the routing number on my bank account, and I do give that to others who might want to send me money, and I am happy to give that public information. What I am not going to give you is the PIN that I use to access the ATM in my account, and the private key is like that PIN. And so typically the person holds onto the PIN, as it is—or the private key. It is only when you put the public and private key together that you now have some bitcoin that you can actually do something with. And so if a hacker gets your private key, they are able to take your bitcoin, and you cannot get it back.

Senator MERKLEY. They can modify essentially the public ledger, and the public ledger becomes *de facto* record of ownership.

Ms. SHASKY CALVERY. That is exactly right.

Senator MERKLEY. OK. So in these—well, OK. Let me see if Mr. Cotney has any comments on this.

Mr. COTNEY. Well, you bring up an interesting case regarding consumer protections, because as the Director noted, these transactions are irreversible. And as a regulator charged with consumer protection, that is what we are interested in every day: the interests of consumers to make sure that their money gets from Point A to Point B and that there is someone reliable standing behind that transaction. And that is what we are interested in.

Senator MERKLEY. Well, in the few seconds I have left, I will just say it is fascinating that this system, which is not, if you will, continuously tended but is in this public space, has been robust enough to hold up for this long without a major flaw that brought the entire thing down, it certainly has attracted the attention of innumerable other programmers around the world asking, well, can we create a similar system, and so thus we are here today.

Thank you.

Senator WARNER. And I would just echo, based upon other commodities where there is a physical presence, you can somehow

trace it back. The fact that we are talking about something in the virtual world really has, again, remarkable ramifications.

Senator Heller?

Senator HELLER. Thank you, Chairman. I want to thank our witnesses for being here today. We are trying to grapple with this, trying to figure this out, and we have more questions than answers, and hopefully you can answer some of these questions.

Ms. Calvery, I just want to know when the first time—when did FinCEN first start to take notice of these bitcoins and other virtual currencies?

Ms. SHASKY CALVERY. Back in probably 2007 with the e-gold case. It was back then that we put out, I believe it was, an administrative ruling talking about e-gold, which was a commodity-backed virtual currency, and even back then put out our view that it fell under the money-transmitting regulations issued by FinCEN. And so we have been keeping up with it since that time.

Senator HELLER. Do you have any idea what percentage of the current virtual currency users and perhaps businesses are participating in illegal activities?

Ms. SHASKY CALVERY. We would have no way to know that. What we do know is if you take a currency, a virtual currency like Liberty Reserve, that was an instance where we believe it was set up for the purpose of laundering money, and the vast majority of transactions using Liberty Reserve were to facilitate criminal activity of all types. It is what the Department of Justice alleged; that is what we alleged in our 311 action.

With regard to Bitcoin, I think we may have a bit of a different situation. It seems that there is a lot of legitimate users out there, and like any type of payment system, it can be exploited by illicit actors, and we have seen it exploited by illicit actors, at least with regard to the allegations made by the Department of Justice in the Silk Road matter alleging that it was used—Bitcoin was used to facilitate hundreds of millions of dollars of money laundering.

Senator HELLER. On that Silk Road issue, the FBI seized about 144,000 bitcoins. What does the Federal Government do with those?

[Laughter.]

Ms. SHASKY CALVERY. So luckily that is not an issue that we will have to deal with at FinCEN, but I can tell you from my past job as the head of the forfeiture program that they will be thinking about whether they can sell those assets.

Senator HELLER. Do they still have them?

Ms. SHASKY CALVERY. I would have to defer to my colleagues at the Department of Justice.

Senator HELLER. I want to talk, Mr. Cotney, a little bit about volatility. As we know, last week it was trading somewhere around $400. It went up to as high as, I think, $900 yesterday, and it finally settled at $600. Why the volatility?

Mr. COTNEY. Well, I think that there is a great interest in this particular space. There is, as I mentioned, a demand for real-time payments and lower transaction costs. And one of the means today now that we are looking at is through virtual currency.

Certainly at the State level, we have a regulatory regime in place. As I mentioned, we are consumer protection regulator. We

are not an investor protection regulator like the SEC, like the States. So we want to make sure that those consumers are protected, and just like any investment, someone who is looking at making an investment, whether it is in virtual currency or in a stock or a bond investment, they need to do their due diligence.

Senator HELLER. Do you follow anything that goes on in China and Europe? It is my understanding that they are increasing in volume in other countries. Is there any reason for this? Would you have any knowledge?

Mr. COTNEY. I do not have any direct knowledge, sir, no.

Senator HELLER. Jennifer?

Ms. SHASKY CALVERY. My understanding is in some countries there may be an interest in Bitcoin because it can—where you have a home currency that might be considered extremely volatile itself, Bitcoin might be considered a better place in which to store value. And in other places, it is also considered a good medium for transacting—or transferring value. And so if there is not a good internal system for transferring value efficiently, it might be used for that purpose as well.

Senator HELLER. Thank you.

Thank you, Mr. Chairman.

Senator WARNER. Senator Heitkamp.

Senator HEITKAMP. In the category of shameless plugs, congratulations on holding a hearing on something that could be a problem later on and is not a crisis right now. It is such a rare moment.

[Laughter.]

Senator HEITKAMP. Seriously the Homeland Security Committee is starting to weigh in on this, and I am going to take this conversation away from the illegal to the practical realities of what we are dealing with here. As this becomes, as Senator Merkley suggested, a common method of transmitting goods and services, payment of goods and services, replacing a dollar bill or replacing a credit card, which we know are longstanding methods, there are a tremendous number of challenges by not categorizing this.

Now, I noticed both of you, especially you, Jennifer, have deferred that, saying thank goodness we did not have to achieve, you know, that result because we had enough broad authority that allowed us to pursue this.

But let us take, for example, a bitcoin being used to buy a pie. How do you ring that up on the cash register? What is the sales tax on that? How do you record it for income tax purposes? How do you transmit it for purposes of payroll taxes? How do you deal with this when it becomes a more commonly accepted method of transmission?

And so what I am saying is that it is not just nefarious groups, you know, terrorists and illegal operations that have a potential of really skirting on the edges. It is, in fact—the more commonly accepted it is and the more available it becomes, the more difficult it is for regular kind of regulatory activities to be carried out, especially tax activities.

I would like maybe your thinking on whether categorizing a bitcoin achieves a result so that we then can think about the regulatory regime or whether we need to create a whole new category

and think about this differently. Either one of you can answer that question.

Ms. SHASKY CALVERY. Sure. From an anti-money-laundering/counterterrorist financing perspective—and I will go broader in a moment, but from that limited perspective, it is not as important. We have similar regulations across different parts of the industry, the idea that they are going to have anti-money-laundering controls in place, that they are going to provide certain reports on suspicious activity to FinCEN, regardless of whether it is a commodity or a currency or a security, those basic protections will follow however we define it. So from our perspective it is not as important.

But I take your point. Look, this country and all countries are going to have an interest in protecting consumers and protecting investors and thinking about monetary policy and thinking about taxing. All those things and reasons why we have regulatory and statutory schemes in every country around the world covering these issues, if Bitcoin truly takes off and becomes a serious part of the financial system, then those issues will need to be brought to the forefront.

I think there is still a question and that we cannot assume that Bitcoin is going to become the major player that many enthusiasts think it will. It very well might, and far be it for me to know which way this is going to go. I did hear some venture capitalists speak recently, though, and say that they saw this as a binary investment. This is either going to take off and be the next great thing. It is going to be the cell phone of 20 years ago. Or it is going to be a nice experiment that completely fails. And so I think we are waiting to see, and in the meantime, at least at FinCEN, we are trying to make sure that we protect our U.S. financial system from illicit actors.

Mr. COTNEY. Senator, I think you rightly pointed out the differences between legal activity and illegal activity. Illegal activity—and we cannot be distracted by this—is illegal no matter what the means, whether it is paid for by cash, paid for by ACH, or——

Ms. SHASKY CALVERY. Guns.

Mr. COTNEY. Exactly, or through now virtual currency.

On the legal side, those actors who want to play by the rules will work through, you know, agencies like mine, will play by the rules set by FinCEN, and that is really the importance of a comprehensive set of regulations, both on the State and the Federal level.

Senator HEITKAMP. Just to follow up on a comprehensive set of regulations, you tell me—I am now the State tax commissioner, and someone paid in a bitcoin, and I call you up because I find out you have expertise, and I say, OK, I just heard that this thing is trading for $700, is that what the pie is worth? Do you think you could come down and be my expert witness when I collect sales tax on $700?

Mr. COTNEY. Well, fortunately I am not the tax commissioner.

[Laughter.]

Senator HEITKAMP. I used to be. And so, I mean, this is going to be a big challenge. And my point is that we can focus on the illegal part of this, but to the extent that it becomes recognized as a valid method in the perfectly legitimate commercial world of transferring goods and services, this is going to become an increasing

problem. And the more the opportunity presents itself to evade, not illegally but to avoid taxation, to say that actually was speculation, you know, so are you going to pay capital gains on it—I mean, it is a really interesting challenge. And I think we need to be thinking about these issues if, in fact, we see this becoming a way to transmit goods and services that is more generally and regularly accepted.

Senator WARNER. I think you raised a great point, and since many—you know, we point here to today's focus on nefarious schemes, but since it seems from, as I learn about this, a lot of folks who are interested lack trust in central banks, you know, want to be, in fact, kind of off the grid, a huge, huge number of questions.

Senator Moran?

Senator MORAN. Mr. Chairman, thank you. Thank you both for being here.

Earlier this afternoon I posted on Reddit this hearing topic and asked Kansans in particular to comment on what I should know, what would be some suggestions for questions that they might have. And, interesting, in just the last few hours 125 responses, most of them very long and thoughtful.

Let me explore one of the topics that was raised, and in a sense it is regulatory arbitrage. Is there an effort to make certain that the regulations are uniform globally? And in the absence of that, is there not a risk that the activity is simply taken offshore if we are the country that is the regulator? And is there an economic consequence to that happening? What is the downside to our country and its economy and the opportunities for innovation if the United States is the heavy regulator and other countries are not?

Ms. SHASKY CALVERY. Sure. Maybe I can take that from both the domestic perspective and then the international, because here, of course, in the United States we have the States and we have the Federal regulation.

We do, I think, a fairly good job, as Mr. Cotney mentioned in his testimony, of the States working together to try to find common approaches whenever possible, and then with FinCEN to work with the States on the Federal approach and try to get as much common ground there as we can so that we have as much consistency as we can at least within the United States. Then we go externally.

Externally, at least from the money-laundering and counterterrorist finance perspective, the Financial Action Task Force is the international standard-setting body that attempts to keep a consistency in standards across the globe, and it is a body that has both carrots and sticks, and it has been fairly effective in getting countries to put regulations in place.

But all that being said, I think if businesses are going to leave the United States based on perceived or real regulatory burden, I think they are going to find the gain short-lived because, as mentioned, countries are going to have an interest in figuring out the tax implications and monetary policy. It is not just the United States that has an interest in these things and in protecting consumers and investors and so forth. So the regulation is going to catch up, and I think there are plenty of good reasons to bring in-

novative business and keep innovative business in the United States.

Mr. COTNEY. I think it is very important to leverage the strengths of each of us, the State regulators and the Federal agencies. At the local level, as a State regulator, I know, for example, that there is a large Cambodian population in Lowell. I know Lowell, Massachusetts. I know that there is a large Brazilian population in Framingham. I send examiners out every day to conduct examinations, to do transaction testing, testing actual transactions of money going abroad. So we have the boots on the ground and a local understanding of these companies.

And then we pair that with the national perspective and knowledge of Federal agencies who also interact on an international level. By leveraging these strengths, I think we do a much better job at detecting and preventing this illegal activity.

Senator MORAN. I appreciate both those answers. Do you have a sense about the importance of this activity being centered in the United States? What is it that—this is a broader question than a regulatory one, but what benefits does our economy and our innovative environment gain by encouraging or at least not discouraging the bitcoin from being centered here?

Ms. SHASKY CALVERY. So I think what we gain is our continued reputation and economic advantages as being a country where innovators come to start new businesses, and that gives us great economic value, and it is something we would want to continue. So I think the great challenge for the regulators is to encourage innovation wherever we can and put smart regulation in place that tries to deal with risks, very real risks about which we need to be concerned, but minimizes burden on innovation.

Mr. COTNEY. Clearly the United States, the mother of invention, we want to take advantage of innovation, and to the extent that we see innovation in this space, that could have spillover effects into other payments or other financial industries or even beyond the financial services industry. So we want to be able to encourage innovation and have it developed here locally.

Senator MORAN. I appreciate that.

Mr. Chairman, thank you.

Senator WARNER. I think we have all got a lot more questions for you, but we understand a vote will be held around 5, so we want to make sure we get to the second panel. I want to thank you both for your testimony, and I look forward to continuing the dialogue.

Ms. SHASKY CALVERY. Thank you for the opportunity.

Mr. COTNEY. Thank you.

Senator WARNER. Now I will turn the chair over to Senator Merkley at this point, and he can go ahead and maybe start introducing the next panel.

Senator MERKLEY. [Presiding.] Because of the time, I am going to start introducing you as you come up, so feel free to take your seats quickly.

I will start with Paul Smocer, the President of BITS. BITS in this case I do not believe has any relation to the term "bitcoin." BITS is the technology policy division of the Financial Services Roundtable. Mr. Smocer joined the Roundtable in February 2008 as

Vice President of Security. In this role, he led BITS work in promoting the safety and soundness of financial institutions through best practices and successful strategies for developing secure infrastructures, products, and services.

Second, we have Professor Sarah Jane Hughes. She is a University Scholar and Fellow in Commercial Law at Indiana University's Maurer School of Law. For the past 25 years, Professor Hughes has regularly taught payments law, commercial law, and banking regulation at the Maurer School of Law. She is a nationally recognized expert on payment systems, public and private methods to detect, deter, and prosecute domestic and international money laundering, and consumer protection and financial privacy.

Next we have Mercedes Kelley Tunstall. She is a partner at Ballard Spahr and the practice leader of their Privacy and Data Security Group. She has substantial experience working with clients to develop new financial products and services, including virtual currencies. She also works with clients from a spectrum of industries on mobile and other e-commerce initiatives, privacy and cybersecurity issues, and the use of social networking sites for marketing, consumer service, and crowdsourcing purposes.

And we have Anthony Gallippi. Anthony is the cofounder and CEO of BitPay, an electronic payment processing system for Bitcoin. Mr. Gallippi founded BitPay in 2011. He has 15 years of experience in sales and marketing working in the robotics industry. Before founding BitPay, Mr. Gallippi was district sales manager at Aerotek and regional sales manager at Industrial Devices Corporation.

So, Paul, we will start with you. Thank you to all of you for bringing your expertise to bear on this topic.

**STATEMENT OF PAUL SMOCER, BITS PRESIDENT, FINANCIAL SERVICES ROUNDTABLE**

Mr. SMOCER. Thank you, Chairman Merkley and Chairman Warner, Ranking Members Kirk and Heller, and Members of the Subcommittees for the opportunity to testify today. My name is Paul Smocer, and I am the President of BITS, the technology policy division of the Financial Services Roundtable.

Attempts to develop digital currencies have existed for decades. As consumers have become more comfortable with Internet financial activity and computer systems have become more powerful and less expensive, we are witnessing the viability of digital currencies increase. However, we need to recognize that digital currency usage exists outside of traditional currency, financial accounting, and payment systems. In my testimony today, I will address both opportunities and risks in the environment.

One measure of a currency's success is its acceptability. We are beginning to see select retailers accepting digital currencies for goods and services. For example, the Web publishing service WordPress accepts bitcoin as a form of payment. Just last week, the Federal Election Commission indicated it is considering allowing Bitcoin's use as in-kind contributions. Merchant and Government agency acceptance will establish these currencies' legitimacy and increase the trust parties have in them and their stability.

Digital currencies also allow merchants access to new consumers in countries where traditional payment systems do not permit access. The lack of interchange fees and chargebacks also appeal to merchants.

Digital currencies may also have the ability to provide access to the underbanked and unbanked. For example, a mobile phone-based money transfer and microfinancing service in Kenya called M Pesa recently added a bitcoin payment option for its customers.

Digital currencies can also help individuals in countries with repressive regimes to support causes they might otherwise not be able to support through their country's traditional payment providers. They can also serve as a potentially stable currency in countries whose own currencies are in distress. For example, during the recent Cyprus financial crisis, citizens transferred funds to digital currencies.

Another interesting aspect related to certain digital currencies is cryptographic protections, which some providers claim prevent counterfeiting and duplication.

Digital currencies and the supporting infrastructures do present opportunities to watch, including facilitating real-time payments, particularly those involving international parties and those involving micro payments; possibly deeper cryptographic options for Internet-based transactions; and opportunities to serve the underbanked and politically repressed more effectively.

While there are opportunities, we also have to recognize the potential risks. First, as noted, digital currencies pose significant market risk. Without Government funding or support, digital currencies are often subject to significant market volatility, creating risks to both holders of the currency and to merchants and others who accept the currency as payment.

Beyond the March 2013 guidance issued by FinCEN, the digital currency environment incorporates virtually no existing regulatory protections, particularly consumer protections. For example, and also as noted, within the last 2 months there have been multiple reports of currency disappearances from various bitcoin trading platforms. In none of these cases is it likely that the owners will recover anything.

The lack of consumer protections extends to other areas, such as liability limits for fraudulent or unauthorized payments. Currently none of the digital currency operators or infrastructure providers is subject to regulatory oversight applied to regulated financial providers, such as the Gramm-Leach-Bliley Act's cybersecurity and data breach notification requirements, the Federal Financial Institutions Examination Council's regulatory guidance, or often to independent regulatory examinations.

Given the anonymity of the digital currency world and the lack of Know Your Customer requirements that apply to traditional financial institutions, using digital currencies individuals may also be able to donate to illegal organizations that would otherwise be legitimately banned, such as those engaged in terrorist financing.

Some recent studies, as we have been discussing, suggests the anonymous nature of digital currencies has made them a haven for illegal activity. We talked about Silk Road, and we talked about Liberty Reserve, but those I think are probably just the prime ex-

amples of the point that criminals are using digital currencies to assist in a broad array of criminal activities.

So as we look at the lack of regulatory oversight, the risks to consumers, and the market risks associated with digital currency, there is a continuing challenge to their overall legitimacy, usage, and endorsement.

In conclusion, clearly the use of digital currencies will continue to evolve, and there are opportunities to explore, but we will need to address both the concerns to consumers, to society, the need for appropriate regulation, and the effectiveness of risk mitigations.

Thank you for your invitation to testify to the Subcommittees, and we look forward to continuing to work with you.

Senator MERKLEY. Thank you.

Professor Hughes.

**STATEMENT OF SARAH JANE HUGHES, UNIVERSITY SCHOLAR AND FELLOW IN COMMERCIAL LAW, INDIANA UNIVERSITY MAURER SCHOOL OF LAW**

Ms. HUGHES. Thank you, Mr. Chairman, Chairman Warner, Ranking Members Heller and Kirk, and honorable Members of both Subcommittees, I am honored to be here with you today.

Monitoring the developments in digital currencies and taking a responsible approach to their regulation reflects their growing presence in domestic and international transactions. Recent negative publicity associated with law enforcement actions against Silk Road and reports of the disappearance of bitcoin exchange values in China and the Czech Republic raises important policy concerns.

I have, as the Chairman said, worked in areas that are like this for a long time, not as a provider but as a watcher. And I also wish that my late father could be here today because he served in World War II as a cryptographer for the United States and was early involved in the computing industry in the United States. I remember being a teenager when he brought home two big briefcases, and he said, "It is a computer." And it was.

So one of the things is that we are seeing in a relatively short period of time important, path-breaking changes in technology of the character that Senator Warner suggested earlier, and we need to be very cautious not to chill those innovations, but we still need to have appropriate legal regimes around them. And I think it is important that we take some time and craft those legal regimes with great care and in as flexible a way as possible, particularly with regard to the remarks of Director Calvery and Commissioner Cotney.

So I had a number of recommendations that responded to the questions that the invitation to appear put forward, and taking them slightly out of order from my prepared testimony, obviously there has already been some support for the idea of retaining the current division between the States and the Federal Government for portions of the role that each do very well. And I share those views.

Second, I think it is incredibly important that we enforce our anti-money-laundering, anti-terrorism, and economic sanctions laws. And as a corollary, I also believe that customers of programs such as Bitcoin and other virtual currencies that may develop

should get the same Federal protections that people get under Gramm-Leach-Bliley, under the Right to Financial Privacy Act of 1978, *et cetera.*

I think FinCEN has taken important steps toward clarifying the application of their existing authority, and I think we need to continue to clarify particularly so that banks and investors do not get cold feet, because we have no way of knowing today what second-stage innovations that may have completely different roles in our economy these new technologies may offer us, and we want to be certain we do not do anything to take them offline.

I would encourage on an interim basis payment systems operators, assuming that we all agree that this is a payment system and not something else like commodities or securities, to adopt and publicize their own transparent standards of how they will behave. As you suggested, legal liability limits, dispute resolution possibilities, guarantees for redemption opportunities, and clear rules about when redemption can happen are all important user protections. Notice I said "user" and not "consumer," because businesses who use have many of the same needs as consumers, and we tend to be focused on regulating for consumers. I spent lots of my life looking at consumer issues, but I am equally interested in businesses being protected.

I think we need to leave room for depository and nondepository providers to innovate in the virtual currency space. And so we want a regulatory climate—we do not want a regulatory climate, rather, in which early entrants can freeze out later ones. We would like to have a lot of innovation in all of this space.

I worked at the Federal Trade Commission many years ago, and one of the projects I worked on was the rescission of a number of 1940s and 1950s trade regulation rules that had essentially been written by industries for themselves. We would like not to see that again because they can be very anti-competitive, and if they are anti-competitive, they are very anti-consumer. So we need an open set of rules.

I am going to run out of time, but I would say that the other thing is do not buy the Wild West argument. Just because something is new does not mean it should not be regulated on the same basis as the types of activity with which it competes.

Thank you so much for this invitation. I would be delighted to answer your questions.

Senator MERKLEY. Thank you very much, Professor.

And now Ms. Tunstall.

## STATEMENT OF MERCEDES KELLEY TUNSTALL, PARTNER AND PRACTICE LEADER, PRIVACY AND DATA SECURITY GROUP, BALLARD SPAHR LLP

Ms. TUNSTALL. Chairman Merkley, Ranking Member Heller, and Members of the Subcommittee, I am Mercedes Kelley Tunstall, a partner at Ballard Spahr here in DC, and I am the head of our Privacy and Data Security Group. My testimony today reflects my personal experience with the virtual currency industry and represents my own opinion. It does not necessarily reflect the opinions of Ballard Spahr or our clients.

Thank you for this opportunity to testify about the present and future impact of virtual currency. I currently work directly with a number of clients in financial innovation issues, and one of the things, as I have been listening to the testimony today, that I feel like is worth saying is that one of the things that I often say with financial innovation is there is a tendency to say, "Well, it is completely new. It is so new, we have never seen anything like it before."

But the fact is that it is like a lot of things that have happened in the past, so I am going to go through some of the statements that I have in my testimony, but let us start with the discussion of currency generally in the United States.

The United States actually has a long history of having concerns around currency. It finally settled down in the 1870s when the Supreme Court had a series of opinions called the "legal tender cases," and basically what they said at that time is we are going to stop all this different stuff with the currencies, happening, we are going to say there is a U.S. currency, and the rule is everyone in the United States has to accept that currency. So there could be other currencies, you can accept other currencies, but you have to accept U.S. currency. It is the currency of the land, *et cetera.*

So that is the basis that we are working from, and we do actually have a long history, long legal precedent that talks about how to handle different types of currency in our financial ecosystem.

Having said that, when we take a look at Bitcoin and the lessons that we can learn from Bitcoin—and I want to point to you where we can talk about a bit of their failures.

The first point is that Bitcoin was really designed to not integrate with our existing financial ecosystem. It was designed to be its own thing and try to, you know, break apart the world without working within the practical realities that we have today. And as a result, financial institutions, especially in the United States, view Bitcoin and other types of virtual currencies as being unreliable, getting involved into them affects their safety and soundness concerns, and so it really is something that right now, not much interest in.

The next point that Bitcoin really focused on is that the transactions need to be anonymous. There is the sense that because it is virtual currency and we are trying to remake a cash transaction, it has to be anonymous. But if I am going to take a dollar bill and hand it to you, I have to see you and I know the personal information about you, at least some personal information, what you look like. So in the virtual currency world, there is no need for the currency transactions to be anonymous. It can be.

The other two elements that Bitcoin addressed besides anonymity is taking out the middleman, so the bank involvement, and not having a record that has personally identifiable information in it. So I would say that in order to address the excesses that we are seeing with virtual currencies, where it is being used by criminals and terrorists and money launderers today—we do know that that is occurring—that the anonymity part of it, let us let that go. The whole point should be keep that middleman out of it, if that is what the virtual currency—and there are lots of reasons—we have had lots of people talk about the value that a virtual currency could

have. Keep the middleman out of it, and we do have the technology today to make it possible that there is no a record with personally identifiable information for others to see, but it is something that is retained by the two parties involved in the transaction.

Finally, Bitcoin has caused some of its own problems because it has this commodity aspect to it, and you could design—and some of the other virtual currencies out there have specifically been designed to avoid the boom-and-bust cycle that we have heard about today.

So those are the three points really that we can learn from Bitcoin to allow virtual currency innovation to continue.

In terms of looking at what has to happen from a legal perspective, I am just going to mention we do need to come to what a definition of virtual currency is. Is it a commodity? Is it not—is it a commodity or a security or not? We do need stronger FinCEN guidance as virtual currency develops.

And then, finally, on the consumer protection side, we touched briefly on the unauthorized transactions issue. That issue also needs to be addressed and considered.

Thank you very much for the opportunity today, and I am happy to take any questions.

Senator MERKLEY. Thank you very much.

Now we are going to turn to Anthony Gallippi, cofounder and CEO of BitPay.

**STATEMENT OF ANTHONY GALLIPPI, COFOUNDER AND CEO, BITPAY, INCORPORATED**

Mr. GALLIPPI. Thank you, Chairmen Merkley and Warner, Ranking Members Heller and Kirk, and distinguished Members of the Committee, for the opportunity to speak today.

My name is Tony Gallippi, and I am the cofounder and CEO of BitPay. I appreciate the Members for their interest in the commercial and international trade aspects of digital currencies and, more importantly, the opportunities for digital currencies to create jobs in America and to increase America's exports.

Our company, BitPay, was started in May 2011. We have been operating for over 2 years now, which makes us pretty old in the Bitcoin space. During this time we have acquired over 12,000 merchants to accept bitcoin using our service. Our merchants include many small and medium-sized businesses in every State, who accept bitcoin side by side with credit cards and other forms of payment.

Most online payments today are made with credit cards, but credit cards were never designed for the Internet. Credit cards were designed in the 1950s, and last year, over 12 million people became victims of identity theft, mostly from shopping online. Businesses lose over $20 billion a year due to payment fraud. The banks do not take responsibility for the fraud. If you are a business, it is your fault that you took a stolen credit card, even if the bank approved it. And credit card fees are discriminatory. The highest fees are paid by the smallest Mom-and-Pop businesses and the lowest-income consumers. Bitcoin is a cheaper, faster, and more secure payment system with no discrimination against smaller businesses.

At BitPay, our role in the Bitcoin ecosystem is very close to that of the traditional merchant acquirers in the credit card space. Our software helps merchants clear and settle transactions over the Bitcoin network. BitPay has a strict Know Your Customer policy to verify all of our merchant applications. We need to know who our merchants are and what they are selling. We only want the good actors using our service.

BitPay also follows all Bank Secrecy Act guidelines to prevent, detect, and report suspicious activity. Our strict policies to comply with laws and protect our brand have earned BitPay the reputation as a leader and well-respected company in the payments space.

Bitcoin does have some limitations that will keep it a small player in the payments space for quite some time. Compared to credit cards, for example, Visa's payment network can handle 20,000 transactions per second worldwide. Bitcoin can handle seven—not 7,000, but seven transactions per second. So even though it is very small, Bitcoin has invented something pretty amazing. With Bitcoin, it is now possible to transfer an asset remotely and immediately settle the transaction, with no counterparty risk. That type of instrument has never existed before. And the possibilities of this instant worldwide settlement are very interesting. The Bitcoin block chain, which is the public accounting ledger of Bitcoin, is a large property rights database. It can handle quadrillions of individual asset accounts, with a full chain of custody every time an asset is transferred from one party to another.

If you want to energize the housing market, think of Bitcoin. The biggest up-front costs for consumers trying to buy a home today are the closing costs, high fees for deeds, titles, stamps, insurance, and other redundant tasks to record the sale in different record books. Bitcoin can replace thousands of dollars in closing costs with a single transaction that costs 5 cents.

Bitcoin does have risks. Criminals use cell phones, criminals use email, criminals use dollars, and criminals use banks. Many businesses like BitPay, offering innovative services on top of Bitcoin, share the Committee's goals to protect consumers from fraud and keep the criminals away from our businesses.

Guidance from the IRS, Treasury, Justice, and SEC have all established that bitcoins are legal and that those dealing with them must follow the existing tax laws and anti-money-laundering regulations.

In the early 1990s, when the Internet was in its infancy, Congress took a wait-and-see attitude to let the Internet develop. So where would social media and other free applications of the Internet be today if in the 1990s we required licenses for the Internet and we taxed Internet access as if it was a telecom?

In 1995, the National Science Foundation lifted its strict prohibition of e-commerce, and immediately companies like Amazon, eBay, and Dell were born. Americans will benefit from a similar openness and wait-and-see approach to Bitcoin.

Bitcoin is a technology with tremendous cost savings for businesses and consumers. Bitcoin is a more secure, faster, and more affordable option for transferring funds. If America is the leader in Bitcoin technology, America will create more jobs and more exports.

In conclusion, today Bitcoin is in its infancy. It is much like the Internet in the early 1990s. If we look 10 to 20 years in the future, we will see many companies built upon Bitcoin-related technology, and we want those companies to be based in America, creating jobs in America, and building a revenue base and a tax base in America.

I commend the Committee for recognizing the real, practical uses of virtual currencies, and thank you for the opportunity to speak today.

Senator MERKLEY. Thank you very much.

We are going to jump right into questions, and given we have 16 minutes and four of us, I am going to ask for 4 minutes to be on the clock. I am going to take my 4 minutes now, and I have three questions, so I am going to try to move them quickly and see if I can get through all of them.

First, Mr. Gallippi, what is your transaction fee?

Mr. GALLIPPI. So our transaction fee, when we first started, was 1 percent. So compared to credit cards that are around 3 percent, we are 1 percent. But we realized very quickly that our marginal cost to do a transaction is low, so we have actually switched over to a software as a service pricing model. Different features and different levels of service, merchants pay 1 monthly fee. Then they can transact all they want with no transaction fees.

Senator MERKLEY. So I have got Whiffies out in Oregon that says it likes to accept bitcoins because it has a one-tenth of 1 percent transaction fee. Do any of your transaction fees go that low?

Mr. GALLIPPI. Possibly. If you take our monthly service and divide it by the volume that you put through, you could get something that low. That is correct.

Senator MERKLEY. OK. That is fascinating. Thank you.

Professor Hughes, I recently read the book "The Wolf of Wall Street," and I think this is coming out as a movie soon, but this broker makes a lot of money, and at one point—this is a true story—he has his wife's aunt strapping money and taking it to Switzerland to put into Swiss bank accounts.

Are Bitcoin wallets, like Instawallet, going to replace Swiss bank accounts?

Ms. HUGHES. Mr. Chairman, I do not know the answer to that question, but I would be delighted to speculate about it for a second.

So there are two ways that you can currently—you could store anything you want, including bitcoins, right now on a private wallet. The trick is that it would be harder to transact business that way, so most people who do it use exchanges.

But there are so many ways in which one can store value, which could and have included in the past putting it on stored value cards and loading them and taking them to Switzerland and not even needing to do that.

So the answer is, yes, technically you can, and, yes, technically they could be. And I think that that is one of the reasons why rigorous and clear guidelines for how our anti-money-laundering, anti-terrorist, and economic sanction regimes are applied to virtual currencies, not just bitcoins but those that may come in the future, are very important to us. We really do not want to facilitate hiding

money, and we do want to be very careful that we protect people who are using currencies of this kind in war-torn areas or areas in which the governments are not reliable or the banking system is not like ours.

Senator MERKLEY. Thank you. And I will follow up with some questions about the Electronic Funds Transfer Act and issues that may arise there. But I want to use my last minute to get to this question.

Mr. Gallippi is talking about these very low transaction fees, which will make many of my merchants in Oregon, their eyes light up. And as we think about this, this actually—not Bitcoin by itself because we have a limited number of bitcoins under the structure it has created. It has security issues. But the concept in general poses some interesting models that could significantly change our credit card system, our bank deposit system, our debit card system. And, Mr. Smocer, in your role with the financial services world, can you give us a little insight on kind of the current thinking of those challenges?

Mr. SMOCER. Sure. And I actually like the way you characterized it because when I think about Bitcoin, we kind of tend to use it as a generic term, but in reality, at least for me, it really is three things: it is a currency, potentially, or a security; it is secondarily the way we use it a depository system, so the wallets and whatnot; and, third, it is a payment system. So we are talking about kind of three different realms that I think we need to think about individually.

I do think that, as I mentioned in the testimony, it has value in showing us that there are ways that we can make the payment system more rapid; we can perhaps make it less expensive. We can make it more available to the unbanked and in some cases to people who might not otherwise be able to use a payment system. But I think, having said that, I think without the consumer protections that we think about in traditional systems, there are a lot of risks to those users as well.

And, you know, if I could go back actually to answer your question that you posed to Ms. Hughes as well, I am not sure you even have to move money to Switzerland in this case because, to me, the anonymity that is associated with users and their wallets would suggest I really do not need to try and cover who owns the money.

Senator MERKLEY. Thank you. I am out of time, so we are going to pass this on to our Ranking Member.

Senator HELLER. Thank you.

Mr. Gallippi, I have a couple questions for you. I would love to be at your home as you are explaining to your wife how your virtual company gave you a virtual paycheck using virtual money.

[Laughter.]

Senator HELLER. But that being the case, I assume your business wants more consumers than investors.

Mr. GALLIPPI. Well, actually, our business model—and I have detailed it more in my written testimony—we are just a merchant acquirer, so we only facilitate the payments for merchants. We do not have a consumer wallet. We do not offer an exchange for consumers. So we are strictly focusing on State acceptance and business adoption of Bitcoin, and the rules and regulations around that

are fairly well defined, you know, in the credit card space, and our business model is very similar to them.

Senator HELLER. I am just wondering what would happen if someone like Senator Warner cornered the market of virtual coins. How would that impact the consumer marketplace?

Mr. GALLIPPI. Well, it is interesting. You know, we look at Bitcoin being traded in open markets today, and China is getting very aggressive in the open market. And if we want America to remain a leader in technology and in Bitcoin, you have to look at the exchanges, because that is where all the liquidity is. And right now the number one exchange in the world for Bitcoin is in China. The number two exchange is in Japan. Numbers three, four, and five are in Europe. Number six is in Canada. America is not a leader right now in the liquidity and the exchange of bitcoins.

Senator HELLER. You talked a little bit earlier in your testimony about vetting these businesses. What is that? What do you have to do?

Mr. GALLIPPI. Well, it is modeled really around the credit card system. You know, what does it take to get a merchant account with a credit card processor? We have modeled our system after that. So we need to know that, A, you are a legitimate business; we need to know who you are; and we need to know what you are selling. And then depending on the different levels of volume that you want to process, we will go even deeper into getting background checks and that kind of thing.

Senator HELLER. Ms. Tunstall, if virtual currencies become more and more popular, what keeps a bank from starting their own virtual currency?

Ms. TUNSTALL. Absolutely nothing, except that, like I said, they do have to maintain their safety and soundness concerns, and a U.S. bank needs to be very focused on U.S. money. But there is nothing to stop a financial institution from getting into virtual currency themselves.

Senator HELLER. Are you familiar with other virtual currencies?

Ms. TUNSTALL. I am sorry?

Senator HELLER. Are you familiar with other virtual currencies besides bitcoins?

Ms. TUNSTALL. I am, yes.

Senator HELLER. Can you share some knowledge?

Ms. TUNSTALL. Sure. So there are a number of virtual currencies that are designed for very kind of niche purposes that are designed for online video gaming-type situations, so you can play with your partners across in China and Japan and wherever, so there are a number of those types of virtual currencies.

There are also a number of virtual currencies that are based on Bitcoin and try to basically fix some of the issues that I detailed in my testimony here today.

And then there is also a virtual currency called Ripple that has started very differently from Bitcoin and started with the premise we are operating in an existing financial ecosystem, and we need to, you know, be able to comply with the criminal laws and anti-money-laundering laws that are in place.

Senator HELLER. Thank you.

Thank you, Mr. Chairman.

Senator WARNER. I am going to try to go through the lightning round as well. First of all, I do not want to overuse my telecom analogy, but just as we saw in developing countries in many ways as they developed telecom networks, to skip the wired system and immediately go to wireless, wouldn't those regimes that have either huge currency restrictions or are enormously underbanked, couldn't you actually see initially the development of these virtual currencies actually quicker and faster in the underdeveloped world than in the developed world? Could we get quick responses? Because I have got two or three more questions.

Ms. TUNSTALL. So my quick response on that is one of the reasons that virtual currencies in the United States have actually proliferated and succeeded is because of the strength of our financial system's security, and so for these other countries where there is not that kind of infrastructure, it is unlikely to be able to support the growth of a virtual currency as you are discussing.

Senator WARNER. Other views? Similar?

Ms. HUGHES. I agree.

Mr. GALLIPPI. Yes, I think the example of Kenya is a great one. Kenya is a country where more people have access to smartphones than to running water. And, you know, the telecom companies stepped up and saw that there was a need, that the existing banking infrastructure was not meeting the needs of the people, and so the telecoms built a mobile payment system in Kenya that today represents 30 percent of the GDP of Kenya. It is done by people sending text messages on their cell phone.

Senator WARNER. And I guess, Mr. Gallippi, I want to just make an editorial comment. I agree with you. We have got to get this balance right. We want to keep this innovation in America. But as a former Governor, the revenue leakage from Internet-based transactions for States that depend upon a sales tax is an enormous challenge. So we have got to get this balance right, and that is one of our challenges going forward.

I guess I would want to press as well Senator Heller's comments. We have thought about and, Ms. Tunstall, you have commented about some of these other competing virtual currencies. I think about a few years back when Second Life was going to be all the rage and everybody was going to have an avatar and we were going to trade.

You know, it seems, though, that the Bitcoin currency—that my understanding is—now has about 90 percent of the folks who are not users but actually investors rather than users, you know, at some point do you think one of these currencies will emerge and does Bitcoin seem to be going down that path? Or do you think there will always be that threat that other currencies—and, again, I think particularly your comments about one that tries to fit within the legal regime?

Ms. TUNSTALL. So I think it is more—unless Bitcoin makes some big changes that allow the Silk Road-type situation to stop from happening, I do not see how it will become commercially viable in the United States. And I would like to—you mentioned Second Life. I would like to mention that. Actually in Second Life, I looked at for a client—they wanted to brand the banks in Second Life and be the bank in Second Life. And as I looked at it, the way that the

law works, even if it is in a virtual world, if the bank is doing the transactions, the U.S. banking laws apply.

And so that was a very interesting result, and what is fascinating about virtual currency actually is that it has found a way to fall through what our infrastructure is right now for financial regulation, which is why we do need to have some kind of framework put around it.

Senator WARNER. My time is going to run out, but I would simply say, though, that because of some of the illicit activities and because of perhaps the interest of some of the folks who want to do this off the grid or not be controlled by a central banking system, you know, we have got to get this—you know, we have got to sort through this right.

I would also make mention, Mr. Chairman, that as a politician who had a Second Life avatar, that got me attention for a nanosecond.

[Laughter.]

Senator HEITKAMP. Mr. Chairman, thank you. Just take this a different direction and just use my little time to tell a little story about when I used to regulate truth in advertising, and I could not get my advertisers to tell the truth, and so I told them they could tell whatever they wanted in an ad, but I was going to take out a full-page ad right next to theirs saying I do not regulate them. I do not regulate them; buyer beware. And we are really at that point because the more we legitimize this in regulation, the more we commercialize it.

And so how do we strike that balance? And I am interested in the academic point of view and maybe the legal point of view. How do we strike that balance? Because to me, if we get involved in regulation, we legitimize it as a true opportunity.

Ms. HUGHES. Well, I think that there is a lot to what you say, Senator, that if we regulate, we do legitimize. And some of today's witnesses have talked about trust, and trust is a very important factor, particularly with financial products and services. So there is that risk.

There is a bone in my body that says I think that is a risk worth taking. And I think it is particularly worth taking as we think of these virtual currencies as having functions that are a lot like credit cards or debit cards in some respects.

Senator HEITKAMP. But wouldn't you agree that right now, without any form of intervention, without legitimizing it, every buyer out there has to be careful, and that has restricted or limited or tapped down the willingness of people to participate? And you really are—you know, it is kind of ironic because we want all the free enterprise system, but the regulatory scheme and saying I have adapted to the regulatory scheme buys you the opportunity to participate in the market in a way that other financial institutions participate.

Ms. HUGHES. I could not agree more. And I think that there is—in my prepared statement, I make the observation that right now it looks like all the risks fall on the users, and that——

Senator HEITKAMP. And what is wrong with that?

Ms. HUGHES. Well, that is why maybe we are not seeing the growth that we would see if there was a bigger structure around

it and greater clarity in that structure. But if people want to do their business that way, they——

Senator HEITKAMP. Well, we would just tell them, you go ahead, do your business that way, but——

Ms. HUGHES. Right, and we are not going to help you.

Senator HEITKAMP.——you are not responsible, and we will deal with the sales tax consequences, we will work through those issues in terms of value-for-value transfer, because you can deal barter to barter. I mean, people can barter, and you still can do an analysis. You can do an analysis on what, in fact, is the capital gains or the short-term or long-term capital gains and just let—try and adapt on a case-by-case basis the existing regulation without legitimizing. I am interested in your point of view, Ms. Tunstall.

Ms. TUNSTALL. So my perspective on that is it is an analogy to social media, where a number of companies have decided to kind of stick their head in the sand and say we are not going to engage in social media, and then, you know, thecompanysucks.com gets founded and then somebody sets up a fake Facebook page and pretends to be that company, and that company loses significant reputation when they choose to stick their head in the sand and not engage and not pay attention to what is happening.

And so my concern with not getting into regulating this area and being interested in what happens here is that it will be—it could eventually affect our financial system's reputation.

Senator HEITKAMP. And I understand that, but my point is frequently in these situations we think about how we are going to fix it or facilitate it when maybe we should just leave it alone, and maybe that is the approach that we need to think about and warn people, you are on your own.

Ms. TUNSTALL. And I think from a consumer perspective and from a user perspective, I think that was a very good comment, that that is where we are. And I think that that is a very fair point.

Senator MERKLEY. Well, we are all left with a lot of questions. We are going to turn to Senator Schumer, but first I just want to note that we will follow up on some of those questions, the separation of the payment system from the banking system, Professor Hughes, your thoughts about how you avoid the boom-and-bust cycle that is inherent in Bitcoin where it is both a speculatory instrument as well as a payment system. And, of course, we are all absolutely enthralled to find out exactly what Senator Warner's avatar looked like.

[Laughter.]

Senator MERKLEY. And with that, we are going to turn to Senator Schumer. Welcome.

Senator SCHUMER. I for one do not want to see what Senator Warner's avatar looked like.

Anyway, I want to thank Chairmen Merkley and Warner for letting us have this hearing and allowing me to participate. I have been very interested in this issue. I have a somewhat different approach than Senator Heitkamp.

A while back, as you know, I called on Federal authorities to shut down the Web site Silk Road, which they recently did. Many people interpreted my action at the time as directed at Bitcoin be-

cause Bitcoin was the sole method of payment on Silk Road, and assumed that I also wanted to shut down or stamp out Bitcoin. That is not the case. I do not want to shut down or stamp out Bitcoin.

New York sits in many ways at the nexus of all the issues being discussed today. As financial capital, the potential for creation of a new payment platform and the rise of alternative currencies could have profound and exciting implications for the way we conduct financial transactions. As a rapidly growing hub for technology and VC, venture capital, New York has every interest in building on the promise that technologies like Bitcoin have to revolutionize payment systems or even form the building blocks for whole new technology platforms.

But all of that promise is threatened by the association of virtual currencies with criminal activities, from purchasing illicit goods and services to money laundering. If Bitcoin continues to attract attention, mostly as a way to finance purchases on Web sites like Silk Road, it is going to find itself in the digital wasteland.

So in order for the legitimate uses of technology like Bitcoin to flourish, it is imperative that its susceptibility to illicit uses be addressed. There must be a way to separate the wheat from the chaff.

So bottom line is very simple. I would ask Mr. Gallippi, do you have any specific suggestions of how we would separate the wheat from the chaff? What would you suggest to the witnesses on panel one to ensure that we address legitimate law enforcement concerns without duly inhibiting the development of these promising new technologies?

Mr. GALLIPPI. Yes, thank you, Senator Schumer. So I think you have to first understand that there are multiple parts of Bitcoin. There is the low-level protocol, which are the bits and bytes that make it work, and then there is the application and service layer that businesses and consumers can engage in. And this is typically where you find businesses like mine operating.

So when you want to try to separate the legitimate uses from the illegitimate ones, clearly the point to do that are by the visible service providers like ourselves, like BitPay. We have over 12,000 businesses using our service to accept bitcoin, and we have a very strict Know Your Customer policy to make sure that we know every merchant, you know, who they are and what they are selling, because we only want the legitimate and good actors using our service.

The bad guys are going to try to figure out how to do it on their own, but it shows you with the recent arrest of the guy from Silk Road that just because you use Bitcoin does not mean that you can evade law enforcement, right? They caught the guy. He is in jail. So——

Senator SCHUMER. It took long enough.

Mr. GALLIPPI. Yeah. So I think there is a lot of effort, and services like ours and others are willing to work with regulators to make sure that what we do complies with the rules, because we all share in the same common goal: to protect consumers from fraud and to prevent the bad actors from using the system.

Senator SCHUMER. Right. And I am sure you have thought about this, because you realize the danger Silk Road-type actors have to this appropriate new way of payment.

Do you have any specific suggestions? And if you do not, if you would like to try to spend a little time thinking them up and sending them to us—I know the record probably, Mr. Chairman, will remain open for a week—that would be helpful.

Mr. GALLIPPI. Yes, I would be happy to do that.

Senator SCHUMER. OK.

Senator SCHUMER. Other witnesses in answer to my specific question? Anyone have any thoughts? Ms. Tunstall?

Ms. TUNSTALL. Yes, so I think that a very good point was made by Mr. Gallippi, and that is that the face to the user is the point to catch the transaction. So very similar to the Internet gambling restrictions that are in place, and I would actually be curious. Do you screen against merchant codes for Internet gambling as a credit card processor would do?

Mr. GALLIPPI. Yes, correct—we do not allow that.

Ms. TUNSTALL. OK. So that type of approach, you know, for tagging the transactions and knowing what the parties are, you can still be anonymous as long as it is a transaction between an individual and, you know, this company for a purchase. So we do have some existing controls and examples that can help on this side.

Senator SCHUMER. Good. Well, I would, again, be interested in your submitting the specifics in writing.

Senator SCHUMER. Any of the other witnesses? My time is up, so you do not——

Mr. SMOCER. I would just say that while I think Mr. Gallippi deserves a lot of credit for creating the company that he created with the kinds of controls he created, I would question if that is applicable across the industry and whether there are things we could do to make sure that the kinds of mitigations and controls that he has put in place are applicable to all in that business.

Senator SCHUMER. OK. Well, thank you all very much, and I hope you will submit some specific suggestions and, Mr. Gallippi, in detail about what you have been able to do so we might be able to parlay that to other companies, although as Mr. Smocer says, we may not be able to do it in certain places.

Thank you, Mr. Chairmen.

Senator MERKLEY. Thank you very much, Senator Schumer, and thank you to all of our witnesses, and thank you, Co-Chair Warner. We will, in fact, keep the record open for additional questions for 7 days, and this concludes the hearing of the Subcommittee on National Security and International Trade and Finance and the Subcommittee on Economic Policy.

[Whereupon, at 5:10 p.m., the hearing was adjourned.]

[Prepared statements, responses to written questions, and additional material supplied for the record follow:]

## PREPARED STATEMENT OF SENATOR MARK KIRK

I am very pleased to be having this hearing today. I think virtual currencies have for too long been something that we were content to let occur and develop without fully understanding. Yet the headlines covering virtual currencies are more and more each day—many related to the enormous challenges and threats that exist in this currency space. What is often overlooked however is the massive innovation in the virtual currency space that provides incredible opportunities—a technology space where the United State can and should be the global leader. As we seek to understand and hopefully curtail many of the nefarious practices that seem to be drawn to the virtual currency space, we must also make sure that we do not stifle innovation—especially innovation that could be used to help so many people around the world.

As eloquently stated in Jerry McGuire, "Show me the money". The directive within this statement has become both more significant and more challenging than ever before as financial transactions have evolved from simple people to people transactions to social networks and complex systems and software—using not only traditional State-backed currencies, but also purely digital ones.

The movement and transfer of currency in exchange for goods and services have been contemplated since the beginning of time. To a great extent, the value and legitimacy of a currency depend on individuals' confidence and willingness to accept it for any particular item.

One major rationale cited by promoters of virtual currencies is that there is no Central Bank and therefore, digital currency is far less susceptible to currency manipulation. This notion is largely correct—the U.S. dollar and other widely accepted government currencies are proof. The dollar, which was originally pegged to gold reserves, now essentially derives its value from the confidence that the people using it place in it. As we have witnessed during the latest financial crisis, Central Banks, including the U.S. Federal Reserve, the Central Bank of Japan and several European Central Banks' willingness to engage in monetary policies that often resemble currency manipulation—which have significant impacts on the value of currency. Therefore, I tend to agree that it is appropriate to question if a centralized institution that is susceptible to political and public pressure can be truly "independent" and free from currency depression or manipulation.

Another key justification given by some virtual currency promoters is that there is some anonymity to an individual or group's financial transactions. Parties of financial transactions can have reasons—some legitimate and some not—for desiring anonymity. While many of us understand the negative that can come from this anonymity, it is also critical to understand that this anonymity has helped finance revolutions against tyrannical governments and has helped NGO's and others get money to individuals and groups without having to pay a middleman or losing it to illegitimate forces.

Further, traditional currencies often fail in reaching the nearly 2.5 billion people who are unbanked across the globe—those "credit invisible" persons without bank accounts, credit lines, or credit histories. This is what makes the prospect of virtual currencies so amazing—that it can and already has helped revolutionize access to financial services for millions of individuals across the globe.

Virtual currencies, however, are not without significant problems and complex issues that not only users and investors, but also Central Banks and law enforcement agencies, must grapple with. Media headlines surrounding the use of virtual currencies for financing the Silk Road, drug and human trafficking and terrorist financing make us aware of the most notorious problems with these currencies that can make the user in the transactions and even the transactions themselves anonymous and obscure.

In addition to these headline stories, other problems exist for virtual currencies including massive fluctuations in value, the lack of security in the exchanges, and hackers stealing money from Bitcoin users. Other macro concerns include potential challenges these currencies create for the U.S. dollar, how governments will choose to recognize virtual currencies, and how law enforcement and financial regulators can effectively monitor, report, and control illicit activities conducted through the use of virtual currencies. Just over a week ago, there was a report of an Australian man that had 4,100 bitcoins, worth more than $1.1 million, stolen from him. This alleged theft is one of the largest since Bitcoin was created 4 years ago.[1] Bitcoin hit an all-time high yesterday closing over 600—a fluctuation of over 5000 percent over its 52-week low—which compares to a 7 percent 52-week change for the dollar.

---

[1] *http://www.dailymail.co.uk/news/article-2492813/Bitcoin-site-hacked-1million-virtual-currency-stolen.html.*

Further, there have been a number of hacks into Mt. Gox, the largest exchange for BitCoin, which in a hacking event in 2011 resulted in an estimated $8.75 million USD worth of bitcoins lost to individuals.

Many of the more significant problems arise from the anonymity that can be achieved through the use of virtual currencies. These headlines warn us that virtual currencies, like most other currencies in the developed world, need parameters and some visibility. While many developers and others in the virtual currency space suggest that anonymity is critical to the currencies' success, I question whether it is privacy, not anonymity that is most critical and if there is anonymity, whether complete anonymity is necessary. I don't think that there is anyone that would argue that governments should not be able to track activities such as terrorism, drug and human trafficking and other illicit activities conducted through the use of virtual currencies. Yet the many questions related to how, why and where governments can and should have access and the ability to track this type of data is debatable. Some virtual currencies and exchanges thrive on anonymity, while others try to be more transparent, stressing privacy and a lack of a central bank rather than anonymity as the selling point.

Bitcoin, for example, one of the most well known virtual currencies, stresses anonymity as a feature that *could* be achieved if the user wants it. However it really underscores the value of having a decentralized currency as the selling point. Bitcoin is a peer-to-peer network, math-based currency. The network is decentralized, which makes it more attractive because it is less susceptible to human judgment errors and manipulation. While Bitcoin touts this decentralization, this lack of centralization also makes Bitcoin more susceptible to use of illicit money transfers and manipulation including through the use of malware and botnets. Further, this decentralization makes Bitcoin incapable of conducting due diligence, monitoring, and reporting of suspicious activity and conducting anti-money laundering compliance programs.

While it appeared that many virtual currencies, such as Bitcoin, allowed financial transactions to become completely anonymous, we are learning through cases such as the Silk Road scandal that virtual transactions are not entirely anonymous, largely dependent on the actions of the user. We also know that not all virtual or algorithmic currencies seek or promote anonymity. Other virtual and math-based currencies, such as Ripple, seem to be less focused on anonymity and more focused on a decentralized currency that has little-to-no counterparty risk. Ripple and others appear to also be on the cusp of bringing virtual currencies into mainstream financial services.

The ability for law enforcement to understand and trace illicit activities being financed through virtual and digital currencies is critical to ensuring the national and financial security of the United States. However, it seems imperative that we don't rush to over-regulate this system, pushing it offshore and truly into the shadows.

Given the rate of change in the virtual and technology-based money transfer systems, it will be nearly impossible for a single government agency to codify a set of rules and regulations that will not quickly become obsolete. It appears that the only way for governments to address some of the formidable technical and organizational challenges associated with detecting and monitoring illicit activities done using digital currencies will come through a combination of self-regulation, government and industry collaboration, and large-scale government technological upgrades.

I look forward to hearing from our first panel to better understand how the U.S. Government, including our financial regulators and enforcement agencies are looking at, studying and preparing for the challenges and opportunities presented by virtual currencies.

I also look forward to hearing from our second panel to understand their views on possible regulations or standards that might improve the industry, the new innovations, technology developments, and what if any safeguards are being considered and developed to better protect the system. I would also like to understand ways that the private sector might be able to help self-regulate itself through best practices and standards to make the illicit actors even that much more obvious.

---

## PREPARED STATEMENT OF JENNIFER SHASKY CALVERY

DIRECTOR, FINANCIAL CRIMES ENFORCEMENT NETWORK
DEPARTMENT OF THE TREASURY

NOVEMBER 19, 2013

Chairmen Warner and Merkley, Ranking Members Kirk and Heller, and distinguished Members of the Subcommittees, I am Jennifer Shasky Calvery, Director of

the Financial Crimes Enforcement Network (FinCEN), and I appreciate the opportunity to appear before you today to discuss FinCEN's ongoing role in the Administration's efforts to establish a meaningful regulatory framework for virtual currencies that intersect with the U.S. financial system. We appreciate the Committee's interest in this important issue, and your continued support of our efforts to prevent illicit financial activity from exploiting potential gaps in our regulatory structure as technological advances create new and innovative ways to move money.

FinCEN's mission is to safeguard the financial system from illicit use, combat money laundering and promote national security through the collection, analysis, and dissemination of financial intelligence and strategic use of financial authorities. FinCEN works to achieve its mission through a broad range of interrelated strategies, including:

- Administering the Bank Secrecy Act (BSA)—the United States' primary anti-money laundering (AML)/counter-terrorist financing (CFT) regulatory regime;
- Sharing the rich financial intelligence we collect, as well as our analysis and expertise, with law enforcement, intelligence, and regulatory partners; and
- Building global cooperation and technical expertise among financial intelligence units throughout the world.

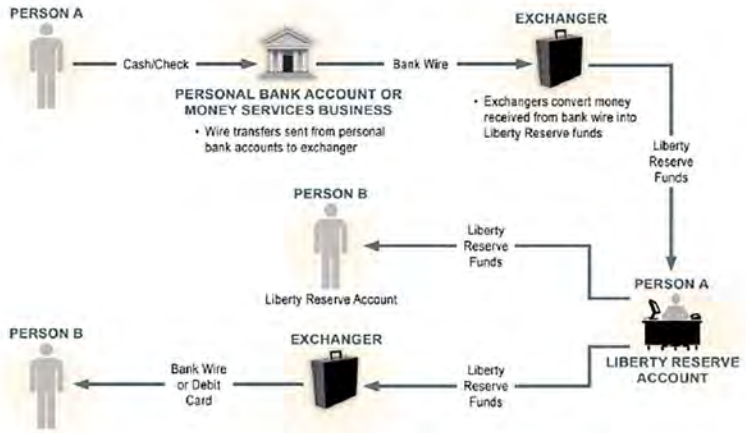
To accomplish these activities, FinCEN employs a team comprised of approximately 340 dedicated employees with a broad range of expertise in illicit finance, financial intelligence, the financial industry, the AML/CFT regulatory regime, technology, and enforcement. We also leverage our close relationships with regulatory, law enforcement, international, and industry partners to increase our collective insight and better protect the U.S. financial system.

**What is Virtual Currency?**

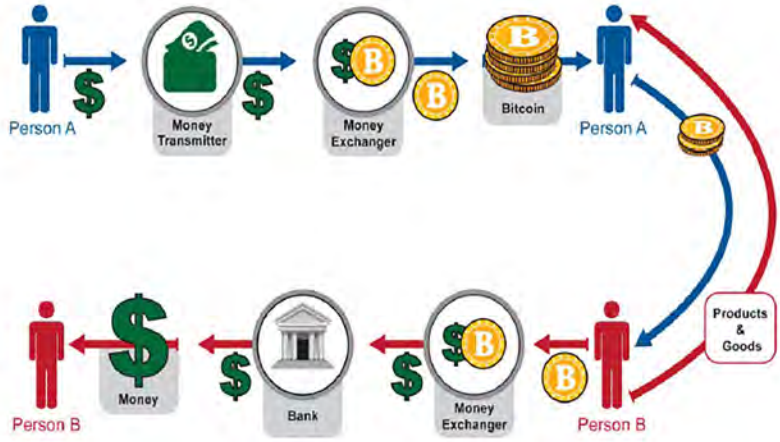
Before moving into a discussion of FinCEN's role in ensuring we have smart regulation for virtual currency that is not too burdensome but also protects the U.S. financial system from illicit use, let me set the stage with some of the definitions we are using at FinCEN to understand virtual currency and the various types present in the market today. Virtual currency is a medium of exchange that operates like a currency in some environments but does not have all the attributes of real currency. In particular, virtual currency does not have legal tender status in any jurisdiction. A convertible virtual currency either has an equivalent value in real currency, or acts as a substitute for real currency. In other words, it is a virtual currency that can be exchanged for real currency. At FinCEN, we have focused on two types of convertible virtual currencies: centralized and decentralized.

Centralized virtual currencies have a centralized repository and a single administrator. Liberty Reserve, which FinCEN identified earlier this year as being of primary money laundering concern pursuant to Section 311 of the USA PATRIOT Act, is an example of a centralized virtual currency. Decentralized virtual currencies, on the other hand, and as the name suggests, have no central repository and no single administrator. Instead, value is electronically transmitted between parties without an intermediary. Bitcoin is an example of a decentralized virtual currency. Bitcoin is also known as cryptocurrency, meaning that it relies on cryptographic software protocols to generate the currency and validate transactions

There are a variety of methods an individual user might employ to obtain, spend, and then "cash out" either a centralized or decentralized virtual currency. The following illustration shows a typical series of transactions in a centralized virtual currency, such as Liberty Reserve:




By way of comparison, the next illustration shows a very similar series of transactions in a decentralized virtual currency such as Bitcoin:




From a "follow the money" standpoint, the main difference between these two series of transactions is the absence of an "administrator" serving as intermediary in the case of Bitcoin. This difference does have significance in FinCEN's regulatory approach to virtual currency, and that approach will be addressed further during the course of my testimony today.

**Money Laundering Vulnerabilities in Virtual Currencies**

Any financial institution, payment system, or medium of exchange has the potential to be exploited for money laundering or terrorist financing. Virtual currency is not different in this regard. As with all parts of the financial system, though, FinCEN seeks to understand the specific attributes that make virtual currency vulnerable to illicit use, so that we can both employ a smart regulatory approach and encourage industry to develop mitigating features in its products.

Some of the following reasons an illicit actor might decide to use a virtual currency to store and transfer value are the same reasons that legitimate users have, while other reasons are more nefarious. Specifically, an illicit actor may choose to use virtually currency because it:

- Enables the user to remain relatively anonymous;
- Is relatively simple for the user to navigate;

- May have low fees;
- Is accessible across the globe with a simple Internet connection;
- Can be used both to store value and make international transfers of value;
- Does not typically have transaction limits;
- Is generally secure;
- Features irrevocable transactions;
- Depending on the system, may have been created with the intent (and added features) to facilitate money laundering;
- If it is decentralized, has no administrator to maintain information on users and report suspicious activity to governmental authorities;
- Can exploit weaknesses in the anti-money laundering/counter terrorist financing (AML/CFT) regimes of various jurisdictions, including international disparities in, and a general lack of, regulations needed to effectively support the prevention and detection of money laundering and terrorist financing.

Because any financial institution, payment system, or medium of exchange has the potential to be exploited for money laundering, fighting such illicit use requires consistent regulation across the financial system. Virtual currency is not different from other financial products and services in this regard. What is important is that financial institutions that deal in virtual currency put effective AML/CFT controls in place to harden themselves from becoming the targets of illicit actors that would exploit any identified vulnerabilities.

Indeed, the idea that illicit actors might exploit the vulnerabilities of virtual currency to launder money is not merely theoretical. We have seen both centralized and decentralized virtual currencies exploited by illicit actors. Liberty Reserve used its centralized virtual currency as part of an alleged $6 billion money laundering operation purportedly used by criminal organizations engaged in credit card fraud, identity theft, investment fraud, computer hacking, narcotics trafficking, and child pornography. One Liberty Reserve cofounder has already pleaded guilty to money laundering in the scheme. And just recently, the Department of Justice has alleged that customers of Silk Road, the largest narcotic and contraband marketplace on the Internet to date, were required to pay in bitcoins to enable both the operator of Silk Road and its sellers to evade detection and launder hundreds of millions of dollars. With money laundering activity already valued in the billions of dollars, virtual currency is certainly worthy of FinCEN's attention.

That being said, it is also important to put virtual currency in perspective as a payment system. The U.S. Government indictment and proposed special measures against Liberty Reserve allege it was involved in laundering more than $6 billion. Administrators of other major centralized virtual currencies report processing similar transaction volumes to what Liberty Reserve did. In the case of Bitcoin, it has been publicly reported that its users processed transactions worth approximately $8 billion over the twelve-month period preceding October 2013; however, this measure may be artificially high due to the extensive use of automated layering in many Bitcoin transactions. By way of comparison, according to information reported publicly, in 2012 Bank of America processed $244.4 trillion in wire transfers, PayPal processed approximately $145 billion in online payments, Western Union made remittances totaling approximately $81 billion, the Automated Clearing House (ACH) Network processed more than 21 billion transactions with a total dollar value of $36.9 trillion, and Fedwire, which handles large-scale wholesale transfers, processed 132 million transactions for a total of $599 trillion. This relative volume of transactions becomes important when you consider that, according to the United Nations Office on Drugs and Crime (UNODC), the best estimate for the amount of all global criminal proceeds available for laundering through the financial system in 2009 was $1.6 trillion. While of growing concern, to date, virtual currencies have yet to overtake more traditional methods to move funds internationally, whether for legitimate or criminal purposes.

**Mitigating Money Laundering Vulnerabilities in Virtual Currencies**

FinCEN's main goal in administering the BSA is to ensure the integrity and transparency of the U.S. financial system so that money laundering and terrorist financing can be prevented and, where it does occur, be detected for follow on action. One of our biggest challenges is striking the right balance between the costs and benefits of regulation. One strategy we use to address this challenge is to promote consistency, where possible, in our regulatory framework across different parts of the financial services industry. It ensures a level playing field for industry and minimizes gaps in our AML/CFT coverage.

Recognizing the emergence of new payment methods and the potential for abuse by illicit actors, FinCEN began working with our law enforcement and regulatory partners several years ago to study the issue. We understood that AML protections must keep pace with the emergence of new payment systems, such as virtual currency and prepaid cards, lest those innovations become a favored tool of illicit actors. In July 2011, after a public comment period designed to receive feedback from industry, FinCEN released two rules that update several definitions and provide the needed flexibility to accommodate innovation in the payment systems space under our preexisting regulatory framework. Those rules are: (1) Definitions and Other Regulations Relating to Money Services Businesses; and (2) Definitions and Other Regulations Relating to Prepaid Access.

The updated definitions reflect FinCEN's earlier guidance and rulings, as well as current business operations in the industry. As such, they have been able to accommodate the development of new payment systems, including virtual currency. Specifically, the new rule on money services businesses added the phrase "other value that substitutes for currency" to the definition of "money transmission services." And since a convertible virtual currency either has an equivalent value in real currency, or acts a substitute for real currency, it qualifies as "other value that substitutes for currency" under the definition of "money transmission services." A person that provides money transmission services is a "money transmitter," a type of money services business already covered by the AML/CFT protections in the BSA.

As a follow-up to the regulations and in an effort to provide additional clarity on the compliance expectations for those actors involved in virtual currency transactions subject to FinCEN oversight, on March 18, 2013, FinCEN supplemented its money services business regulations with interpretive guidance designed to clarify the applicability of the regulations implementing the BSA to persons creating, obtaining, distributing, exchanging, accepting, or transmitting virtual currencies. In the simplest of terms, FinCEN's guidance explains that administrators or exchangers of virtual currencies must register with FinCEN, and institute certain recordkeeping, reporting and AML program control measures, unless an exception to these requirements applies. The guidance also explains that those who use virtual currencies exclusively for common personal transactions like buying goods or services online are users, not subject to regulatory requirements under the BSA. In all cases, FinCEN employs an activity-based test to determine when someone dealing with virtual currency qualifies as a money transmitter. The guidance clarifies definitions and expectations to ensure that businesses engaged in such activities are aware of their regulatory responsibilities, including registering appropriately. Furthermore, FinCEN 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.

It is in the best interest of virtual currency providers to comply with these regulations for a number of reasons. First is the idea of corporate responsibility. Legitimate financial institutions, including virtual currency providers, do not go into business with the aim of laundering money on behalf of criminals. Virtual currencies are a financial service, and virtual currency administrators and exchangers are financial institutions. As I stated earlier, any financial institution could be exploited for money laundering purposes. What is important is for institutions to put controls in place to deal with those money laundering threats, and to meet their AML reporting obligations.

At the same time, being a good corporate citizen and complying with regulatory responsibilities is good for a company's bottom line. Every financial institution needs to be concerned about its reputation and show that it is operating with transparency and integrity within the bounds of the law. Legitimate customers will be drawn to a virtual currency or administrator or exchanger where they know their money is safe and where they know the company has a reputation for integrity. And banks will want to provide services to administrators or exchangers that show not only great innovation, but also great integrity and transparency.

The decision to bring virtual currency within the scope of our regulatory framework should be viewed by those who respect and obey the basic rule of law as a positive development for this sector. It recognizes the innovation virtual currencies provide, and the benefits they might offer society. Several new payment methods in the financial sector have proven their capacity to empower customers, encourage the development of innovative financial products, and expand access to financial services. We want these advances to continue. However, those institutions that choose to act outside of their AML obligations and outside of the law have and will continue to be held accountable. FinCEN will do everything in its regulatory power to stop such abuses of the U.S. financial system.

As previously mentioned, earlier this year, FinCEN identified Liberty Reserve as a financial institution of primary money laundering concern under Section 311 of the USA PATRIOT Act. Liberty Reserve operated as an online, virtual currency, money transfer system conceived and operated specifically to allow—and encourage—illicit use because of the anonymity it offered. It was deliberately designed to avoid regulatory scrutiny and tailored its services to illicit actors looking to launder their ill-gotten gains. According to the allegations contained in a related criminal action brought by the U.S. Department of Justice, those illicit actors included criminal organizations engaged in credit card fraud, identity theft, investment fraud, computer hacking, narcotics trafficking, and child pornography, just to name a few. The 311 action taken by FinCEN was designed to restrict the ability of Liberty Reserve to access the U.S. financial system, publicly notify the international financial community of the risks posed by Liberty Reserve, and to send a resounding message to other offshore money launderers that such abuse of the U.S. financial system will not be tolerated and their activity can be reached through our targeted financial measures.

**Sharing Our Knowledge and Expertise on Virtual Currency**

As the financial intelligence unit for the United States, FinCEN must stay current on how money is being laundered in the United States, including through new and emerging payment systems, so that we can share this expertise with our many law enforcement, regulatory, industry, and foreign financial intelligence unit partners, and effectively serve as the cornerstone of this country's AML/CFT regime. FinCEN has certainly sought to meet this responsibility with regard to virtual currency and its exploitation by illicit actors. In doing so, we have drawn and continue to draw from the knowledge we have gained through our regulatory efforts, use of targeted financial measures, analysis of the financial intelligence we collect, independent study of virtual currency, outreach to industry, and collaboration with our many partners in law enforcement.

In the same month we issued our guidance on virtual currency, March 2013, FinCEN also issued a Networking Bulletin on crypto-currencies to provide a more granular explanation of this highly complex industry to law enforcement and assist it in following the money as it funnels between virtual currency channels and the U.S. financial system. Among other things, the bulletin addresses the role of traditional banks, money transmitters, and exchangers that come into play as intermediaries by enabling users to fund the purchase of virtual currencies and exchange virtual currencies for other types of currency. It also highlights known records processes associated with virtual currencies and the potential value these records may offer to investigative officials. The bulletin has been in high demand since its publication and the feedback regarding its tremendous value has come from the entire spectrum of our law enforcement partners. In fact, demand for more detailed information on crypto-currencies has been so high that we have also shared it with several of our regulatory and foreign financial intelligence unit partners.

One feature of a FinCEN Networking Bulletin is that it asks the readers to provide ongoing feedback on what they are learning through their investigations so that we can create a forum to quickly learn of new developments, something particularly important with a new payment method. Based on what we are learning through this forum and other means, FinCEN has issued several analytical products of a tactical nature to inform law enforcement operations.

Equally important to our ongoing efforts to deliver expertise to our law enforcement partners is FinCEN's engagement with our regulatory counterparts to ensure they are kept apprised of the latest trends in virtual currencies and the potential vulnerabilities they pose to traditional financial institutions under their supervision. FinCEN uses its collaboration with the Federal Financial Institutions Examination Council (FFIEC) BSA Working Group as a platform to review and discuss FinCEN's regulations and guidance, and the most recent and relevant trends in virtual currencies. One such example occurred just recently, when several FinCEN virtual currency experts gave a comprehensive presentation on the topic to an audience of Federal and State bank examiners at an FFIEC Payment Systems Risk Conference. The presentation covered an overview of virtual currency operations, FinCEN's guidance on the application of FinCEN regulations to virtual currency, enforcement actions, and ongoing industry outreach efforts.

FinCEN also participates in the FBI-led Virtual Currency Emerging Threats Working Group, the FDIC-led Cyber Fraud Working Group, the Terrorist Financing & Financial Crimes-led Treasury Cyber Working Group, and with a community of other financial intelligence units. We host speakers, discuss current trends, and provide information on FinCEN resources and authorities as we work with our partners

in an effort to foster an open line of communication across the Government regarding bad actors involved in virtual currency and cyber-related crime.

Finally, FinCEN has shared its strategic analysis on money laundering through virtual currency with executives at many of our partner law enforcement and regulatory agencies, and foreign financial intelligence units, as well as with U.S. Government policymakers.

**Outreach to the Virtual Currency Industry**

Recognizing that the new, expanded definition of money transmission would bring new financial entities under the purview of FinCEN's regulatory framework, shortly after the publication of the interpretive guidance and as part of FinCEN's ongoing commitment to engage in dialogue with the financial industry and continually learn more about the industries that we regulate, FinCEN announced its interest in holding outreach meetings with representatives from the virtual currency industry. The meetings are designed to hear feedback on the implications of recent regulatory responsibilities imposed on this industry, and to receive industry's input on where additional guidance would be helpful to facilitate compliance.

We held the first such meeting with representatives of the Bitcoin Foundation on August 26, 2013 at FinCEN's Washington, DC, offices and included attendees from a cross-section of the law enforcement and regulatory communities. This outreach was part of FinCEN's overall efforts to increase knowledge and understanding of the regulated industry and how its members are impacted by regulations, and thereby help FinCEN most efficiently and effectively work with regulated entities to further the common goals of the detection and deterrence of financial crime. To further capitalize on this important dialogue and exchange of ideas, FinCEN has invited the Bitcoin Foundation to provide a similar presentation at the next plenary of the Bank Secrecy Act Advisory Group (BSAAG) scheduled for mid-December. The BSAAG is a Congressionally chartered forum that brings together representatives from the financial industry, law enforcement, and the regulatory community to advise FinCEN on the functioning of our AML/CFT regime.

**Conclusion**

The Administration has made appropriate oversight of the virtual currency industry a priority, and as a result, FinCEN's efforts in this regard have increased significantly over recent years through targeted regulatory measures, outreach to regulatory and law enforcement counterparts and our partners in the private sector, and the development of expertise. We are very encouraged by the progress we have made thus far. We are dedicated to continuing to build on these accomplishments by remaining focused on future trends in the virtual currency industry and how they may inform potential changes to our regulatory framework for the future. Thank you for inviting me to testify before you today. I would be happy to answer any questions you may have.

---

## PREPARED STATEMENT OF DAVID J. COTNEY

COMMISSIONER OF BANKS, MASSACHUSETTS DIVISION OF BANKS
ON BEHALF OF THE CONFERENCE OF STATE BANK SUPERVISORS

NOVEMBER 19, 2013

### INTRODUCTION

Good afternoon Chairmen Warner and Merkley, Ranking Members Kirk and Heller. My name is David Cotney and I serve as the Commissioner of Banks for the Commonwealth of Massachusetts. The Massachusetts Division of Banks is responsible for the overseeing all State-chartered banks and credit unions as well as regulating a range of nonbank financial service providers including money transmitters. I also serve as the Vice Chairman of the Board of Directors of the Conference of State Bank Supervisors (CSBS), and as the Chairman of the State Liaison Committee of the Federal Financial Institutions Examination Council (FFIEC).[1]

It is my pleasure to testify before you today on behalf of CSBS. CSBS is the nationwide organization of banking regulators from all 50 States, the District of Columbia, Guam, Puerto Rico, and the U.S. Virgin Islands. For more than a century,

[1] Since 2006, State depository regulators have had a voting seat on the FFIEC, an interagency body empowered to prescribe uniform principles, standards, and report forms for financial institution examinations. The State Liaison Committee is made up of representatives of State bank, credit union and savings bank regulators and serves as the formal means for State input and representation on the FFIEC.

CSBS has given State supervisors a national forum to coordinate supervision and to develop regulatory policy. CSBS also provides training to State banking and financial regulators and represents its members before Congress and the Federal financial regulatory agencies.

State banking regulators supervise over 5,200 State-chartered banks.[2] The majority of State banking departments also regulates a variety of nonbank financial services providers, including money services businesses (MSBs) as well as mortgage lenders, check cashers, and payday lenders. This broad supervisory portfolio provides State regulators with a unique perspective in the payments landscape. Unlike any single Federal prudential regulator, most States regulate all of the financial intermediaries in the payments system: banks, credit unions, and money transmitters.

I thank you for holding this hearing on virtual currency. The risks virtual currency presents impact consumer protection, payment systems stability, money laundering, national security, and tax evasion. The potential benefits are similarly multi-faceted: speed and efficiency, lower transaction costs, and providing an outlet for the unbanked and underbanked around the world. To address these areas, State regulators view our responsibility as supervising in a manner that mitigates risks while not impeding industry innovation and flexibility.

States and State regulation have served as a forum for market experimentation as well as an early warning system of troublesome consumer and market trends. As the laboratories of innovation, the States welcome technology developments in the payments system that can lead to greater choice, security, and lower costs for consumers. Whether it's the Cambodian community in Lowell, the Somali community in Minneapolis, or the unbanked in Portland, Oregon, the States have a responsibility to ensure their citizens have the best possible options for transmitting value in a manner that does not put people, businesses, the payments system, or national security at risk.

My testimony today discusses existing State regulatory regimes and processes that offer the ability to supervise payment systems participants in a manner that promotes trust, confidence, and regulatory collaboration. I will also set out State regulators' efforts to further define priorities and approaches moving forward.

**PAYMENT SYSTEMS AND STATE SUPERVISION**

Payments systems are increasingly dynamic, signaling a shift in the way consumers and businesses pay for goods and services as well as the manner in which funds are remitted domestically and globally. Whether point of sale technologies, payment system intermediaries, or virtual currencies, development is ongoing and the possibilities are promising. However, while the opportunity for economic and consumer benefit is significant, so is the opportunity for real time losses and other destabilizing effects.

Nowhere are opportunities and challenges more starkly visible than in the emerging field of virtual currencies. Virtual currencies are decentralized digital mediums of exchange that, depending on the structure, serve as a hybrid of types of value. Today's virtual currencies are mostly math based, finite, verifiable, and open source, factors that present an opportunity to enhance the basic manner in which we conceive the exchange of value. In addition to virtual currencies, the business of transmitting value continues to evolve through mobile and Web-based technologies that allow for instant and mobile payments on a secure basis.

To understand the opportunities and the risks presented in this sector, State agencies are actively monitoring new entrants into the digital market, including recent high-profile law enforcement actions related to virtual currency. State regulators are engaged in open discussions with a broad range of industry participants, joint State and Federal working groups, and State-to-State coordination and strategic planning. States are also using their regulatory and legislative tools to learn more about the industry and increase transparency. For example, the New York Department of Financial Services launched an inquiry in August[3] and recently announced it will hold public hearings on virtual currency with an eye toward identi-

---

[2] Federal Deposit Insurance Corporation Statistics on Depository Institutions, Report Date June 30, 2013.

[3] Notice of Inquiry on Virtual Currencies, NYDFS (12 August 2013) *available at http://www.dfs.ny.gov/about/press2013/memo1308121.pdf.* Superintendent Lawsky explains: "The emergence of Bitcoin and other virtual currencies has presented a number of unique opportunities and challenges. Building innovative platforms for conducted commerce can help improve the depth and breadth of our Nation's financial system. However, we have also seen instances where the cloak of anonymity provided by virtual currencies has helped support dangerous criminal activity, such as drug smuggling, money laundering, gun running, and child pornography."

fying possible licensing regimes.[4] New York's goal is one all States share, to determine appropriate regulatory guidelines that "allow new technologies and industries to flourish, while also working to ensure that consumers and our national security remain protected."[5] The California legislature has also worked to give regulators more tools to make the licensing process more transparent, authorizing the Department of Business Oversight to make written guidance public and offer guidance to prospective licensees.[6]

The States have a legal and regulatory structure that encompasses a broad range of financial services offered by a variety of bank and nonbank providers. For emerging payment technologies and alternative currencies, the threshold issue is the electronic movement of value owned by others—conduct over which the States have an existing structure for regulation and oversight. Money services businesses are entities that provide money transmission, currency exchange, prepaid access, monetary instruments as well as check cashing products and services. These companies provide a variety of financial products and services to a diverse customer base ranging from sophisticated financial customers to the underbanked and unbanked. One type of MSB, money transmitters, conducts remittance transfer services, domestically and internationally.

State MSB regulation recognizes the reality that money transmitters are local in touch, global in scale, and include a broad range of business models. A money transmitter's business platform may include telephone, online, authorized agent locations, or a combination thereof to reach its customer base. Additionally, a money transmitter may offer several different types of MSB activities simultaneously. For example, Moneygram Payment Systems—a company licensed in 48 States, the District of Columbia, and Puerto Rico—offers money transmission, bill payment, prepaid cards, and money orders through their online platform and authorized agents nationwide. As technology has evolved to include mobile payments and digital commerce, State money transmitter regulation has demonstrated the flexibility to supervise these products and services to consumers.

At the most basic level, many of the new products and services receive, hold, and send funds domestically or internationally. As such, these activities could fit into State money transmission definitions: the accepting or delivering of currency, funds, or other value, to another location or person by electronic means.[7]

## CREDENTIALING OF FINANCIAL SERVICES PROVIDERS

Given the position of trust and confidence held by money transmitters and their critical function within local economies,[8] State law generally requires the licensing of companies and individuals that transmit other people's funds. By credentialing those who take and send monetary value on behalf of others, the States limit potential consumer harm and add stability to financial markets. In turn, licensed companies increase consumer and commercial confidence, which encourages the economic stability needed to support successful innovation.

Licensing communicates to the public that a licensee is viable, secure, and able to protect funds. State regulatory agencies license and regulate money transmitters to ensure compliance with State and Federal regulatory requirements, to help prevent the use of money transmitters to finance illicit activities such as narcotics trafficking and terrorism, while also providing consumer protection for residents. Oversight includes ensuring the proper policies, procedures, and safeguards are in place to protect the company and its customers from operational, monetary, and fraud risk. Many States have utilized the Uniform Money Services Act, adopted by the

---

[4] Notice of Intent to Hold Hearing on Virtual Currencies, Including Potential NYDFS Issuance of a 'BitLicense,' NYDFS (14 November 2013) *available at http://www.dfs.ny.gov/about/press2013/virtual-currency-131114.pdf.*

[5] Notice of Inquiry on Virtual Currencies, *supra.*

[6] California Assembly Bill No. 786, Money Transmissions (2013–2014). Effective January 1, 2014. *Available at http://leginfo.legislature.ca.gov/faces/billNavClient.xhtml?bill_id=201320140AB786.*

[7] "'Money transmission' means . . . receiving money or monetary value for transmission . . ." Alaska Stat. § 06.55.990; Arkansas A.C.A. § 23–55–102 (12) (A); Hawaii HRS § 489D–4; Iowa Code § 533C.102; Kansas K.S.A. § 9–508; La. R.S. 6:1032; Michigan MCLS § 487.1003; Miss. Code Ann. § 75–15–3; N.C. Gen. Stat. § 53–208.2; N.D. Cent. Code, § 13–09–02; S.D. Codified Laws § 51A–17–1; New Hampshire RSA 399–G:1; Tex. Finance Code § 151.301; Vermont 8 V.S.A. § 2500; Va. Code Ann. § 6.2–1900.

[8] See, *e.g.,* The California Money Transmitter Act, Cal Fin Code § 2000 *et seq.* ("The [California] Legislature finds and declares all of the following: * * * (c) The failure of money transmission businesses to fulfill their obligations would cause loss to consumers, disrupt the payments mechanism in this State, undermine public confidence in financial institutions doing business in this State, and adversely affect the health, safety, and general welfare of persons in this State.").

National Commission on Uniform State Laws as the outline for their statutory provisions, which includes licensing standards, financial stability requirements, and regulatory principles.

Prospective licensees must file an application that typically includes the submission of credit reports, fingerprints, a business plan, financial statements, and a surety bond. The prospective licensee may provide evidence of policies, procedures, and internal controls that will facilitate the organization's compliance with State and Federal regulations, including required Financial Crimes Enforcement Network (FinCEN) registration and documentation of a Bank Secrecy Act (BSA) compliance program.[9] Once a license is granted, management is required to maintain requisite permissible investments,[10] surety bonds, and submit periodic reports that often include financial statements, permissible investments calculations, branch and agent reporting, and transmission volume activity.

One of the main purposes of licensing is credentialing the entities and individuals seeking to engage in money transmission. Prospective licensees may be required to undergo rigorous requirements with the State agencies that include dialogue with the applicant regarding their business plan. The application may also include a background check on all owners, a requirement common in the MSB, banking, mortgage, securities, and other financial industries to ensure persons in a position of trust meet established standards to protect consumers and businesses alike. While some have complained that the process is cumbersome, most licensees recognize the value of identifying and validating market participants.

Credentialing requirements are vital and elementary to consumer protection. Some comments to date suggest this process is invasive and/or unnecessary, a view that reflects inexperience with time-validated requirements and unfamiliarity with the public policy goals served by licensing and regulatory oversight. We have seen this type of initial reaction as the States have enhanced their regulatory responsibilities, such as with the licensing of mortgage brokers and payday lenders. State legislatures have been very deliberate in crafting a credentialing process designed around the core objectives of consumer protection and promoting safety and soundness. State agencies would be negligent in their responsibilities if they simply allowed the push of technological innovation to preempt the need to apply the law in a thorough and deliberate manner.

**SUPERVISION OF FINANCIAL SERVICES PROVIDERS**

State agencies examine licensed money transmitters on a 12-to-24 month cycle to ensure licensees operate in a safe, sound, and legal manner. Between exams, State regulators monitor their licensees on an ongoing basis by reviewing the information submitted pursuant to reporting requirements. Licensees have periodic reporting requirements covering financial statements, permissible investments adequacy, branch and agent listings, and transmission volume activity. Consumer complaints provide another input into the supervisory process.

During the course of an examination, State examiners review complaints, capital, asset quality, management, earnings, operations, and compliance with the Bank Secrecy Act and the institution's anti-money laundering program. All these areas of review provide State agencies with data and other information to assess if a licensee is complying with applicable laws and conducting business in a safe and sound manner. If a licensee is found operating in an unsafe manner or out of compliance with State and Federal requirements, the licensee may face State enforcement actions.

State enforcement actions vary depending on the entity, substantiated behavior, and violation. Importantly, enforcement is subject to appeal to an administrative hearing, ensuring licensees are afforded due process. For less serious findings warranting redress, the regulator and the regulated entity might agree to a letter of understanding or consent order, acknowledging the violation and setting forth a corrective plan. For more serious violations, temporary or permanent cease and desist orders will be issued, potentially limiting or even halting an entity's ability to operate. In more egregious circumstances, civil money penalties will be imposed in addition to any consumer restitution. Additionally, an entity's license could be revoked and the regulator's findings may necessitate referral to State and/or Federal law enforcement.

---

[9] BSA compliance programs include policies, procedures, and internal controls to detect and deter money laundering and other illegal activity.

[10] Permissible investments are low risk, liquid assets such as cash and high rated investments required to be maintained in case an institution is unable to meet its commitments or fails. Permissible investments must be equal to the outstanding transmissions, payment instruments, or prepaid access values in the State or in all States.

**STREAMLINED AND COORDINATED OVERSIGHT**

Many State MSB licensees hold licenses in more than one State. Consequently, State agencies have proactively built a foundation for multi-State coordination and examinations. The Money Transmitters Regulators Association (MTRA)[11] formed the foundation for multi-State MSB efforts by executing the Money Transmitter Regulators Cooperative Agreement (MTRA Agreement) in 2002[12] and the MTRA Examination Protocol (MTRA Protocol) in 2010. These documents established the initial framework for States to coordinate MSB examinations and share information.

The MTRA Agreement started the States on the path to coordinated regulatory oversight by promoting concurrent and joint examinations among States. The MTRA Protocol provided a process for examinations, including multi-State examination schedules, work programs, and reports designed to increase effectiveness and reduce regulatory burden. Since the MTRA Agreement and Protocol were implemented, State agencies have conducted over 300 multi-State MSB examinations. Through coordination, regulatory oversight is applied in a uniform manner, a benefit that has been publicly noted by industry.[13]

To foster consistency, coordination, and communication, the States have collaborated on the enhanced CSBS/MTRA Nationwide Cooperative Agreement for MSB Supervision[14] and the Protocol for Performing Multi-State Examinations. The CSBS/MTRA Agreement and Protocol will supplement an effective and efficient regulatory framework for licensees by establishing the Multi-State MSB Examination Taskforce (MMET) to oversee joint examinations. Representing all States, the MMET has 10 members, currently comprised of State regulators from California, Florida, New York, North Carolina, Ohio, Pennsylvania, Texas, Virginia, Washington, and Wyoming. The MMET is working on developing an enhanced supervisory program tailored to multi-State licensees that fosters a process of consistency and coordination among State agencies. In its first year, the MMET has improved the MSB examination work program and identified MSBs that meet the criteria for multi-State examinations.

As a result of established processes and lines of communication, State agencies promptly communicate to one another to reduce the possibility of consumer harm when enforcement is necessary across State lines. Over the last several years, the Massachusetts Division of Banks and our sister States have been active in ensuring that the monies that consumers transmit are received by the intended recipients. When companies fail to deliver, we are the only regulators out there to help consumers who may have lost their hard earned money. When we learn that someone has lost their funds, either through fraud or the financial instability of the company, the Division can act swiftly and in collaboration with our State regulatory counterparts. State collaboration and coordination was evident earlier this year when it became clear to the Division that a money transmitter was possibly misappropriating customer funds. The money transmitter in question primarily remitted funds to Brazil with transfers in excess of $122 million originating from Massachusetts in 2012 alone. During an examination that involved coordination with the Brazilian Central Bank and two private Brazilian banks, it was determined that transaction records were falsified, evidencing an even broader pattern of illegal activity.

As a result, we promptly issued a Cease and Desist order[15] to stop this company from accepting and transmitting money from Massachusetts consumers and initi-

---

[11] MTRA is a national nonprofit organization dedicated to the efficient and effective regulation of the money transmission industry in the United States of America. The MTRA membership consists of State regulatory authorities in charge of regulating money transmitters and sellers of traveler's checks, money orders, drafts, and other money instruments.

[12] The MTRA Cooperative Agreement can be found at *http://www.mtraweb.org/about/cooperative-agreement/*.

[13] "Recent developments in money transmitter regulation have been positive for regulated entities, as examinations by multi-State regulator teams have blossomed." Ezra C. Levine, Counsel, The Money Services Roundtable. Hearing before the Subcommittee on Financial Institutions and Consumer Credit of the Committee on Financial Services, U.S. House of Representatives, 112th Congress, Second Session, Serial No. 112–139, 9 (June 21, 2012). *See also,* Timothy P. Daly, Senior Vice President, Global Public Policy, The Western Union Company. *Id.* at 49. ("Recent developments in money transmitter regulation have been positive for both consumers and regulated entities, as examinations of multi-State organizations have grown more efficient, effective and consistent.").

[14] The Enhanced CSBS/MTRA Nationwide Cooperative Agreement for MSB Supervision, *available at http://www.csbs.org/regulatory/Cooperative-Agreements/Documents/MSB/MSB-CooperativeAgreement010512clean.pdf.*

[15] Braz Transfers Cease and Desist Order, *available at http://www.mass.gov/ocabr/business/banking-services/banking-legal-resources/enforcement-actions/2013-dob-enforcement-actions/braz04012013.html.*

ated a coordinated response across 37 States.[16] My agency communicated the enforcement action to our sister States, held multi-State calls, and worked with other State regulators to ensure remittance transfers were received and customers were assisted in a timely manner. All consumers who lost money have been made whole. This investigation is ongoing, but demonstrates that State regulators are prepared and capable of promptly acting on a national and international basis.

**STATE-FEDERAL COORDINATION**

Equally important as inter-State action is meaningful coordination with Federal regulatory agencies. States recognize the importance of a larger regulatory fabric and integrated oversight for consumer protection and national security. In many areas of bank and nonbank regulation and supervision, the States have found that a more coordinated approach better serves both consumers and regulated entities.

The FFIEC has proved a valuable venue for coordination on processes between State regulators and Federal financial regulators across a wide range of supervisory issues and processes. Through the State Liaison Committee to the FFIEC, the States collaborate with the FFIEC on the Bank Secrecy Act/Anti-Money Laundering Examination Manual, and participate as voting members of the FFIEC BSA/AML Working Group, an interagency effort to enhance coordination of BSA/AML training, guidance, and policy. The responsibilities of the working group include ensuring consistent agency approaches and collaborating on emerging issues.

The States have also entered into memorandums of understanding with FinCEN and the Internal Revenue Service (IRS) to coordinate BSA/AML supervision in the nonbank sector.[17] As such, State agencies provide information to FinCEN and the IRS on a quarterly and annual basis. This information may include the number of BSA examinations conducted, referrals of BSA violations, and State enforcement actions. Additionally, State agencies worked collaboratively with FinCEN and the IRS on the FinCEN/IRS Bank Secrecy Act/Anti-Money Laundering Examination Manual for MSBs that was issued in 2008. State agencies also have provided resources to develop and conduct training for State and IRS examiners nationwide on BSA compliance for MSBs.

The Dodd-Frank Wall Street Reform and Consumer Protection Act (Dodd-Frank) recognized the importance of a holistic approach to supervision. States bring a local point of view and a hands-on approach that complements the national priorities and perspective of Federal regulators. In addition to existing State/Federal cooperative frameworks, Dodd-Frank established new expectations for coordination, collaboration, and information sharing between the States and Federal regulators, including with the Consumer Financial Protection Bureau (CFPB).[18] In 2011, the States entered into an Information Sharing Memorandum of Understanding with the CFPB (Information-Sharing MOU).[19] This was the first such MOU that the CFPB signed. Sixty-one State agencies and the six State regulatory associations[20] have signed the Information-Sharing MOU, which lays the foundation for information-sharing and supervision and enforcement cooperation between the CFPB and State regulators. Additionally, the State system is coordinating with the CFPB through CSBS on examiner training, examination technology and procedures, and complaint sharing.

Building on the foundation of the Information-Sharing MOU, on May 20, 2013, CSBS on behalf of the State regulators entered into the 2013 CFPB–State Super-

---

[16] Braz Transfers was licensed in 7 of the 14 States currently using NMLS to license MSBs. According to NMLS Consumer Access, the company is no longer authorized to do business in any of these States. *See http://www.nmlsconsumeraccess.org/EntityDetails.aspx/COMPANY/907744.*

[17] Memorandum of Understanding between the Internal Revenue Service and the States concerning Money Services Businesses and Certain Other Nonbank Financial Institutions. *Available at http://www.csbs.org/regulatory/Cooperative-Agreements/Documents/IRS-States BSA_MOU_4-22-2005.pdf.*

[18] "The Bureau shall coordinate with . . . State regulators, as appropriate, to promote consistent regulatory treatment of consumer financial and investment products and services." Dodd-Frank Act § 1015, *codified* at 12 U.S.C. 5495.

[19] Memorandum of Understanding Between the Consumer Financial Protection Bureau, the Conference of State Bank Supervisors, and the Other Signatories Hereto On the Sharing of Information for Consumer Protection and Other Purposes. *Available at http://www.csbs.org/regulatory/Cooperative-Agreements/Documents/CFPB %20CSBS%20MOU.pdf.*

[20] The six State regulatory associations are the American Association of Residential Mortgage Regulators, Conference of State Bank Supervisors, Money Transmitter Regulators Association, National Association of Consumer Credit Administrators, North American Collection Agency Regulatory Association, and National Association of Credit Union Supervisors.

visory Coordination Framework (Framework)[21] for the purposes of implementing a State-Federal process for coordinated supervision. Under the Framework, the State Coordinating Committee (SCC)[22]—representing nearly 100 State regulatory agencies covering mortgage, MSBs, payday lending, consumer finance, student lending, debt collection, and others—is charged with coordinating examination and enforcement efforts directly with the CFPB. Through the SCC, the State system has the opportunity to influence and direct supervisory policy on a nationwide basis for nondepository industries including emerging and innovative players in the mobile, payments systems, and virtual currency markets.

**NATIONWIDE MULTI-STATE LICENSING SYSTEM**

State regulators have long understood that regulation needs to adapt alongside marketplace changes in order to capture the benefits and mitigate the risks of innovation. State regulators also understand that, in the modern economy, businesses and markets grow irrespective of geographic boundaries. Accordingly, the States recognized a need to be able to effectively and efficiently license mortgage companies and mortgage loan originators, to keep track of bad actors, and to provide responsible actors with greater efficiency and consistency in the licensing process. To achieve these goals, the States collectively developed and currently operate through CSBS the Nationwide Multi-State Licensing System and Registry (NMLS or System). After success in the mortgage licensing arena, States are currently using the System to license other regulated businesses, including all 12 license types issued by the Massachusetts Division of Banks.

Originally developed as a voluntary State system for mortgage licensing and then codified in the Secure and Fair Enforcement for Mortgage Licensing Act of 2008 (SAFE Act),[23] NMLS is a Web-based system that allows State-licensed nondepository companies, branches, and individuals in the mortgage, consumer lending, money services businesses, and debt collection industries to apply for, amend, update, or renew a license online for all participating State agencies using a single set of uniform applications.

Last year, NMLS expanded functionality to include MSBs. Massachusetts is among 15 States currently using NMLS for MSB licensing, and 14 more are scheduled to come onto the system in the next year. The System enables licensees to manage their licenses in one location for multiple States, while States are able to track the number of unique companies and individuals, as well as the number of licenses they hold in each State. As a system of record for State regulatory authorities and a central point of access for licensing, NMLS brings greater uniformity and transparency to these nondepository financial services industries while maintaining and strengthening the ability of State regulators to monitor these industries.

Both industry and regulators see great advantages to NMLS. During last year's House hearing on money services businesses, industry representatives testified that widespread adoption of the system "would eliminate duplication of effort and opportunities for error" and "urge[d] any changes at the Federal level to accommodate and encourage its further development."[24] To that end, I want to thank Senators Hagan and Toomey for taking the lead in sponsoring S. 947, which enhances the confidentiality and privilege already built into the NMLS. I also want to thank the other Members of the Committee—Senators Merkley, Manchin, Heitkamp, and Johanns—who have signed on as co-sponsors of S. 947. With the passage of S. 947, State regulators will have full confidence in the expanded use of NMLS, bringing greater efficiency to the regulatory process.

In addition to shared functionality between regulators and industry, NMLS provides transparency to consumers seeking information on regulated companies and individuals. NMLS Consumer Access (*www.nmlsconsumeraccess.org*) is a fully searchable public Web site that allows consumers to view information concerning companies, branches, and individuals holding State licenses in the NMLS. In 2012, the information available on the Web site was upgraded to include public State regulatory actions for State licensees. The Web site also enables consumers to connect directly to State agencies for the purpose of submitting a consumer complaint against a State licensed company.

---

[21] 2013 CFPB–State Supervisory Coordination Framework. *Available at http://www.csbs.org/regulatory/Cooperative-Agreements/Documents/2013-CFPB.pdf.*

[22] The SCC is comprised of representatives of the six State Regulatory Associations and is responsible for representing the State system as a single body to the CFPB.

[23] P.L. 110–289. *Codified at* 12 U.S.C. 5101 *et seq.*

[24] Timothy P. Daly, Senior Vice President, Global Public Policy, The Western Union Company. Hearing before the Subcommittee on Financial Institutions and Consumer Credit of the Committee on Financial Services, U.S. House of Representatives, 112th Congress, Second Session, Serial No. 112–139, 49–50 (June 21, 2012).

As we continue to expand NMLS into other license types, regulators and industry alike will have the benefit of streamlined licensing requirements at a single source, and NMLS will be an important tool to provide understanding and responsiveness to companies that are local in touch but global in scale. Considering this, we continue to recommend to our colleagues at FinCEN and the CFPB that they use NMLS for any Federal registration requirements.[25] State regulators and CSBS are ready to work with our Federal counterparts to bring registration and licensing requirements under one shared structure, and NMLS already has the proven capabilities and widespread support for such a streamlined process.[26]

**LOOKING FORWARD**

State regulators are keenly aware that constantly emerging technologies have brought exciting and innovative products to the financial marketplace that consumers are utilizing on a daily basis. I and my fellow State banking commissioners recognize the need to understand these innovations. We also understand that there is a desire by many in the payments and technology industries for greater clarity for both State and Federal regulatory requirements.

State regulators have structures, processes, and systems in place to bring clarity and consistency, while promoting consumer protection, safety and soundness, and national security goals. The States stand ready to work with our Federal counterparts, as well as with representatives from industry and consumer groups, to seek opportunities for greater clarity and consistency, allow for innovation in the payments systems, and both exploit the benefits and minimize the risks of such innovations.

To address this changing landscape, CSBS is currently exploring policy processes for framing and considering issues facing regulators. These threshold issues include establishing the right characterization of virtual currency,[27] the consumer protection needs raised by instantly settled payments,[28] the resolution of conflicts between commercial entities in an instantaneous transfer system, and whether—and in what manner—States should license entities involved with digital currency.[29] Our consideration of these and other issues will inform our efforts to preserve marketplace stability while supporting constructive innovation. The States will continue to work with this goal in mind, expanding on a framework that ensures safety and soundness, minimizes the use of digital currencies to fund illicit activities, and protects consumers and across a diverse landscape of companies and business models.

Local understanding, coordination between regulators, and collaboration with policymakers has provided the States a unique ability to actively regulate a broad range of financial products and services in an effective and timely manner. We look forward to working with Congress and our Federal regulatory partners toward an integrated and collaborative approach to all innovative financial products and services, ensuring individuals and economies are well served.

---

[25] Section 1022(c) of the Dodd-Frank Act directs the CFPB to "consult with State agencies regarding requirements or systems (including coordinated or combined systems for registration), where appropriate."

[26] NMLS complies with the moderate baseline security controls contained in National Institute of Standards and Technology (NIST) Special Publication 800–53, and is fully accredited (FISMA Certification and Accreditation) by the Consumer Financial Protection Bureau. Technical Details and Data Security Protocols for NMLS are available at *http://mortgage.nationwidelicensingsystem.org/about/Documents/NMLS%20Data%20Security%20Overview.pdf.*

[27] Whether virtual currency is "money" is a critical question. Congress has the sole power to "coin money" and "regulate the value thereof" under Article I, Section 8 of the Constitution. Conversely, Article I, Section 10 prohibits States from coining money and from "mak[ing] any Thing but gold and silver Coin a Tender in Payment of Debts." If virtual currency is not money, the States must determine whether it holds monetary value for the purposes of money transmission laws, or whether it is an instrument securing an interest in another currency.

[28] The Electronic Funds Transfer Act requires disclosure and other consumer protections for the transfer of funds. As technology accelerates payment clearing, disclosures and liability standards will be of the utmost importance. For example, if a virtual currency wallet is hacked, who is responsible for the lost funds?

[29] Article 4A of the Uniform Commercial Code currently governs commercial fund transfers. Though "funds transfer" is broadly defined under the law, the process is reliant on relationships through the banking system.

## PREPARED STATEMENT OF PRESIDENT PAUL SMOCER

PRESIDENT, BITS, ON BEHALF OF THE FINANCIAL SERVICES ROUNDTABLE

NOVEMBER 19, 2013

Thank you Chairmen Warner and Merkley, Ranking Members Kirk and Heller and Members of the Committee for the opportunity to testify before you today.

My name is Paul Smocer and I am the President of BITS, the technology policy division of The Financial Services Roundtable. BITS addresses issues at the intersection of financial services, technology and public policy, on behalf of its one hundred member institutions, their millions of customers, and all of the stakeholders in the U.S. financial system.

The financial services market constantly evolves and matures to reflect the explosive growth of technological capacity, entrepreneurial innovation and consumer needs and preferences. The topic of today's hearing, "Virtual Currency," has been and continues to be an area of focus for our member companies and within the industry. As virtual or digital currencies have evolved, our members discuss the potential benefits as well as potential drawbacks—particularly drawbacks related to security, fraud and consumer impact. My testimony today will cover the evolution of digital currency, as well as opportunities and risks.

### Digital Currency Evolution

Since the commercialization of the Internet, the concept of digital money has held intrigue. The terms "virtual currencies" and "digital currencies" are the generally accepted vernacular terminology used to identify forms of electronic currency that can be used to effect transactions involving true goods and services.

Attempts to develop digital currencies, and the methodologies used to exchange them for value, have existed for several decades. For example, in the 1990s, we saw attempts such as NatWest's Mondex card, which was an attempt at creating an electronic cash card that acted as alternative to coins and banknotes, and DigiCash Inc., which was an electronic money corporation founded by David Chaum. The regulatory community has also been thinking about this subject for some time. For example, in September 1996, the United States Department of the Treasury held a conference entitled "Toward Electronic Money and Banking: The Role of Government" that explored this issue. Until recently, however, attempts to launch digital currencies have been unsuccessful. What makes today's environment different and enhances the probability of success in launching digital currencies? The answers to that question include:

- Consumers are much more comfortable in transacting online through traditional financial systems as well as other vehicles such as online games that leads consumers to an increasing overall comfort with the online world.
- Computer systems are more powerful and less expensive thus facilitating some of the processing intensive techniques associated with emergent digital currencies.
- A growing interest in having an international currency free of some of the factors such as exchange rate considerations, inter-currency transactional fees, *etc.*
- The increasing desire for privacy.
- The general cache that some attach to the concept and to innovative developments on the Internet.
- And sadly, but realistically, a desire to facilitate illegal activities such as money laundering, fraud, and terrorism financing.

This has allowed a market for, though still on a limited basis, digital currency and the development of some infrastructures to support the exchange of digital currency.

Bitcoin is often the focus of digital currency discussions as it is the largest independent digital currency. Bitcoins are created through a digital process, "mining", which involves computer programs working on the same set of data to solve a puzzle. Across the Internet, a bitcoin is mined every 10 minutes through this process with allegedly a maximum of 21 million allowed in circulation. Once mined, the owner is able to use his or her bitcoins at any participating merchant and the transactions are tracked through a public ledger known as a block chain, which identifies users by a unique code. Bitcoin users review these ledgers to validate transactions and to ensure that users are spending existing bitcoins. These transactions operate outside of the traditional payments system. Thus, they would not intersect with credit card, ACH or other trusted financial services networks. The system is not run

by any one entity or company, but rather is supported by participants in the Bitcoin environment.

Unlike depository accounts held in traditional financial institutions, bitcoin ownership is not associated with any named individuals. Owners of individual accounts are recognized by unique codes intended to assure their anonymity. Even the creator of Bitcoin is considered anonymous. Its creation is often attributed to a Satoshi Nakamoto, though it is speculated that this is actually a pseudonym for an anonymous individual or group of anonymous Web developers. In general, Bitcoin provides a decentralized system, using peer-to-peer networking, digital signatures and cryptographic proofing to enable funds transfers between participants.

Other entities in the digital marketplace, such as Ripple, rely on the efficiencies of the Internet by developing an open source digital transaction protocol. Ripple uses existing currencies or valuable items (*e.g.,* airline miles), which are converted into its internal currency called XRP. Users can then quickly transact within XRP. Individuals can convert funds back to a monetary value by selling the XRP. Similar to Bitcoin, Ripple includes an open ledger to allow all participants to see the activity of the system and validate transactions, again with individual accounts recognized by a unique code. These transactions also would not cross the traditional payments, but could leverage the existing funds in a financial institution consumer's account as an individual could directly transfer dollars into their Ripple account. A unique feature of Ripple is to allow individuals to provide loans to others within the network. Individuals establish their own ability to trust different users and decide how much they would like to loan the individual. In addition, a trust score can be assessed to different users.

**Opportunities**

As we think about the opportunities associated with digital currencies, I believe we need to think of them in two distinct areas—the concept of the currency itself and the infrastructure mechanisms being created to exchange them.

We have witnessed the concepts of new, emerging currencies before. Some have noted that even within our country, the creation of new currencies was an early part of our history as the States, regions, and even merchant exchanges established currencies. What makes digital currencies different is that they allow the concept of cash or a cash equivalent to be used over the Internet. That fact, in turn, essentially makes them a global form of currency.

One measure of a currency's success is its acceptability. An emergent trend is that institutions such as international and large retailers are beginning to accept select digital currencies as payment for goods and services. For example, in November 2012, the Web publishing service WordPress announced they would accept Bitcoin as a form of payment for WordPress upgrades. Interestingly too, just last week, we all became aware that the Federal Election Commission is seriously considering letting candidates and committees accept bitcoins as in-kind contributions. Given digital currencies today rely neither on Government-Sponsored central banks nor have the backing of any national currency, merchant acceptance and certainly acceptance by government agencies tends to help these currencies establish their legitimacy and increase the trust parties have in them and their stability in the marketplace. At this point, however, the established financial services industry still does not generally recognize these currencies as broadly accepted.

One important aspect to recognize is that, as digital currencies become more internationally accepted, there is a growing recognition of their ability to increase international sales opportunities and their ability to facilitate simpler international funds transfers. Returning to the WordPress example of retailer acceptance, WordPress found the acceptance of digital currencies allowed it access to new consumers in countries where traditional payment systems do not permit access for financial, security or international sanction reasons.

Because of the ability to work internationally and outside of existing markets, some suggest digital currencies also have the ability to provide affordable access to the unbanked on a global scale. For example, a mobile phone based money transfer and microfinancing service in Kenya backed by Kenya's largest two mobile network operators called M–Pesa, recently added a bitcoin payment option for customers in Kenya.

In addition, digital currencies can assist individuals in countries with repressive regimes to support causes or efforts that they might otherwise not be able to support. For example, in certain countries where citizens fall under strict government control, individuals can often not donate to or purchase from sites that are banned by their country's traditional payments providers. These transactions are made easier using decentralized, unaffiliated, anonymous currencies with their own payment

infrastructures. Because of this, often times digital currencies are referred to as a "censorship-resistant" currency.

If digital currencies reach a state where their economic stability is more assured, they can also function as an outside currency that can provide additional economic security for individuals living in a country whose own currency is under financial distress. For example, during the recent Cyprus and Argentina financial crises, citizens transferred funds to digital currencies, mostly Bitcoin, to provide a more steady assurance for the security of their funds.

The infrastructure supporting digital currency payments has some appealing quality to merchants also due to the lack of interchange fees. For many, digital currencies can provide a lower transaction cost to the benefit of both merchants and consumers. Digital currencies may be more attractive to merchants as many do not allow the payments to be reversed, so there is no opportunity for chargebacks.

Another interesting aspect related to certain digital currencies is their cryptographic protections. Ostensibly, the cryptography is intended to provide a level of security that both helps limit the amount of a currency in circulation and to bolster their providers' claims that their currencies cannot be duplicated or counterfeited. The currency providers also claim that the financial information about any particular user's wallet (*e.g.,* their identity, their balance) is anonymous and, therefore, more secure than in other Internet-based financial transaction environments. If these claims hold true, which is questionable, this could be very significant for the future of monetary security.

In summary then, digital currencies and their supporting infrastructure do indeed present opportunities that we are closely watching. They could provide a model for how to facilitate real-time payments—particularly those involving international parties and those involving micropayments. They offer some opportunity to explore deeper cryptographic options for Internet-based transactions and they may offer opportunities to serve more effectively the under-banked and those who are truly politically repressed.

**Risks**

While the opportunities noted above have piqued the interest of the financial services industry in digital currencies, we also have to recognize a plethora of potential risks.

First, digital currencies pose significant market risk. Without government funding or support, digital currencies may be subject to extreme market volatility. The participants in the market itself have to decide the worth of each currency. Given the immaturity of the market, slight changes in the market can produce significant swings in value. In addition, the value of items purchased could change drastically and there would not be a single arbitrator to provide final decisions as to the value of the currency. Bitcoin is the best example of market volatility. Since its creation 4 years ago, the market has gone through several significant swings in value, including in 2011 when the value fell 90 percent from $30 to $3. Recently, its value took a steep dive again when the use of bitcoins was associated with the alleged operations of the drug ring known as "Silk Road." While its value has bounced back, broad swings in value create significant risk to both holders of the currency and to merchants and others who accept the currency as payment. With an established currency, merchants can generally be assured that the payment they receive will be of equal value to the service or merchandise purchased. With a currency that can fluctuate wildly, there is significantly more risk and little to no recourse for the merchant if the payment currency's value falls significantly. If the transaction happens to be international, the payment settlement methods used with established currencies do not apply. If, for example, one makes a purchase with a credit card issued in the United States from a UK-based merchant, the payment infrastructure will convert the purchase price from British pounds to U.S. dollars at a market rate and post that amount to the purchaser's account. The infrastructure to support this type of conversion is only in its infancy with the digital currency world. As well, we simply do not yet have enough experience to know if these currencies will even continue to exist. Many factors including broader acceptability will influence whether we see an increase or collapse in value of these currencies.

On the consumer side, the use of these currencies and the infrastructure exchange mechanisms they utilize are currently subject to few of the consumer protections we have come to expect in the traditional world of currency and payments. In addition, since these currencies do not carry clear and effective disclosures, even the most sophisticated consumers are unlikely to be aware of and understand the risks associated with them.

At this point, in the United States, the Financial Crimes Enforcement Network (FinCEN) has taken the regulatory lead by creating its formal statement on digital

currencies. This March 2013 guidance clarified the responsibilities of participants in the digital currency marketplace to register as money services businesses and money transmitters. Given the decentralized approach of the currencies, this requires registration by many individuals who previously did not consider themselves part of this network. Beyond this March guidance of FinCEN, digital currency providers have virtually no existing regulatory oversight. This is even more meaningful for currency providers and users operating outside regulated countries. Without regulations, these digital currencies are not providing appropriate consumer protections to ensure individuals understand the risks much less are protected in ways we now take for granted. As examples:

- If the value in an individual's digital currency account is fraudulently stolen, the victim has no recourse to recover the funds. In fact, within the last 2 months there have been multiple reports of Bitcoin currency disappearances from various Bitcoin trading platforms. Some allegedly involved hacks into Bitcoin repositories. At least one allegedly involved the creation of an "unlicensed" repository into which Bitcoin owners deposited their funds only to have the repository suddenly disappear. In none of these cases is it expected that the owners will recover a single bitcoin. Contrast that to the recourse available to a consumer who is a bank customer. If funds are fraudulently taken from the consumer's deposit account, the bank will make that customer whole. If an entire institution that is an FDIC-insured depository institution were to fail due to a major cyber-attack, consumers would generally be afforded protections that would allow them to recover a significant balance of their deposit accounts.
- If a consumer's digital currency account were used to make an unauthorized payment, laws that limit the amount of consumer financial responsibility and require investigation by the financial institution holding the consumer's transaction or credit card would not apply. The consumer would simply lose the value of the fraudulent payment.
- While there is an emerging trend in the regulatory community, led by FinCEN at the Federal level, to consider the classification of certain parties in the digital currency world as money transmitters, laws and regulations that apply to funds transfers occurring through traditional financial institutions currently have little relevance in the digital currency world. There is no method for attrition or preemptively stopping the transfer of digital currency funds.

These types of fraud protections provided by the financial services industry have developed into an essential part of overall consumer protection. Without some level of parity, today's digital currency consumers are essentially unprotected.

It is important to note however, that while the digital currency market seems ripe for further oversight and regulation, the act of regulating it, in and of itself, adds legitimacy to the market.

Another risk related to digital currencies involves the fact that most digital currencies are stored in digital wallets that are associated with personal computers or devices. Once these devices are compromised, there are no additional ways for the consumer to access their funds. In addition to the fraud risks noted above, there have been several recent cases of hacks on digital wallets that hold digital currencies. These hacks use similar techniques to traditional hacking efforts we have seen in the financial services industry. For example, phishing techniques are used to gain access to a user's information needed for authentication.

It is important to recognize too that while FinCEN has taken some action and others at the Federal and State levels are considering regulatory actions, currently none of the digital currency operators or infrastructure providers are subject to the intense level of regulatory oversight applied to regulated and chartered financial providers. They are not subject to any required regulatory standards regarding, for example, cyber security and data breach notification requirements that grew out of the Gramm-Leach-Bliley Act. They are not subject to the regulatory and best practices guidance issued by the Federal Financial Institutions Examination Council and its member agencies that they have developed over the last 20 years. Likewise, they are not subject to independent examination of their controls environments by any regulatory authority. Because digital currency transactions typically occur within privately operated, unregulated networks, financial and security risk determination and mitigation is left up to the currency or infrastructure provider.

In addition, while many digital currencies tout that they are anonymous, they rely on a unique identifier for each account. Through analysis of transactions or confirmation by an individual, these identifiers could be connected with an individual. Given that digital currencies rely on a public ledger, the individual's transaction could become knowledgeable to individuals who have been identified.

Earlier I noted in the "Opportunities" section the ability for individuals to provide funds to legitimate organizations that their native country might inappropriately ban. This can also work in the reverse. Using digital currencies, individuals may also be able to donate to illegal organizations that would otherwise be legitimately banned by one or more governments. The ability for governments to ban payments to sites, for example, is a useful technique in thwarting illegal activity and terrorist funding.

Allowing digital currencies, particularly ones that by design are intended to provide full anonymity to the currency holders, has also invited their use for illicit activities. In fact, some recent studies suggest that the anonymous nature of digital currencies has made them a haven for illegal activity. The most notable recent example is the FBI case that resulted in the take down of Silk Road—an operation that allegedly was used to anonymously buy or sell illegal drugs, offer guns and assassins for sale, and provide tutorials on hacking ATM machines. The operation was completely reliant on digital currency for transactions. When this site was taken down, law enforcement had numerous challenges in seizing the funds of the site and those of Silk Road's alleged operators and customers.

The digital currency environment is also being used as a new way to launder money. A recent major example would be the situation involving the May 2013 indictment of Liberty Reserve. Liberty Reserve was a global currency exchange that allegedly ran a $6 billion money-laundering operation online ostensibly serving as an exchange for criminals engaged in various illegal activities. According to the prosecutors who presented the charges, Liberty Reserve was responsible for laundering billions of dollars, conducting 55 million transactions that involved millions of customers around the world, including about 200,000 in the United States. It is also important to note that all a user need to do to use the system was to provide a name, address and date of birth. However, unlike the Know Your Customer requirements that apply to traditional financial institutions, Liberty Reserve, being unregulated and incorporated outside the United States, was not required to validate customers' identities. As the indictment stated, "Accounts could therefore be opened easily using fictitious or anonymous identities."

While the Silk Road and Liberty Reserve situations serve as examples, the point here is that digital currencies are being used to assist a broad array of criminal activities including illegal drug sales, stolen identities, child pornography, prostitution, human trafficking, and illegal weapons sales. It is also being used as a favorite of cyber criminals to pay for services such as developing and distributing malicious software to the movement of stolen funds resulting from account take overs.

One additional consideration is the level of clarity that currently exists regarding how virtual currencies will be treated within the tax code and whether virtual currencies offer an ability to evade taxes. In May 2013, the U.S. Government Accountability Office issued a report to the U.S. Senate's Committee on Finance entitled, "Virtual Economies and Currencies, Additional IRS Guidance Could Reduce Tax Compliance Risks." The report suggests that the IRS should determine and subsequently address the need for additional tax guidance and additional taxpayer education. The lack of regulatory oversight, the risks to consumers and the market risks associated with digital currency provide a continuing challenge to its overall legitimacy, usage and endorsement by the financial services industry.

**Conclusion**

In conclusion, there is no denying that the use of digital currencies will continue to evolve. Consequently, we will continue to discuss that growth and the associated opportunities and risks. As with the Internet and electronic commerce in general, we have seen innovations grow from early concepts where the risks outweighed the advantages to, over time, becoming an accepted norm. For now, I would opine we are not yet there with digital currencies. They do provide opportunities—or more accurately perhaps suggest areas of opportunity, but we will need to address the threats to consumers and society, the need for appropriate regulation and the effectiveness of risk mitigations. As the discussion continues, we would be happy to continue to participate, particularly where it would be advantaged by public-private collaborations such as through the Federal Reserve Banks study of the future of the payments system.

Thank you for your invitation to testify to the Subcommittees this afternoon. We look forward to continuing to work with you relative to this emerging technology.

## PREPARED STATEMENT OF SARAH JANE HUGHES

UNIVERSITY SCHOLAR AND FELLOW IN COMMERCIAL LAW
INDIANA UNIVERSITY MAURER SCHOOL OF LAW

NOVEMBER 19, 2013

Chairman Merkley and Chairman Warner, Ranking Members Heller and Kirk, and Honorable Members of the Subcommittees on Economic Policy and National Security and International Trade and Finance, I am honored to be here with you today to discuss virtual currencies.

Monitoring the developments in virtual currencies and taking a responsible approach to their regulation reflects their growing presence in domestic and international transactions. Recent negative publicity associated with law enforcement action against Silk Road and reports of the disappearance of bitcoin exchanges in China and the Czech Republic raises important public policy concerns.

Part I: Recommendations and a Roadmap to the Balance of This Testimony

The Committee has invited testimony on a variety of subjects that I have addressed in this prepared statement. I have a number of recommendations that pertain to the Committee's question.

My recommendations include:

1. Retain the current division of regulation between the States and Federal Government—with prudential regulation of the nondepository providers of new payments systems with the States and retaining the anti-money-laundering, anti-terrorism and economic sanctions regulations with the Federal Government.
2. Make providers of virtual currencies comply with the customer-identification program and AML compliance program requirements of Sections 326 and 352 of the USA PATRIOT Act, and with the economic sanctions regulations enforced by OFAC, just as other payments systems providers do. Virtual currency customers will have to reveal their identities to issuers of the currencies they use. As a corollary, customers should get the same Federal financial privacy rights that users of other payments products have under the Right to Financial Privacy Act of 1978 and Title V of the Gramm-Leach-Bliley Act.
3. Encourage FinCEN to clarify the manner in which customer-identification and AML compliance requirements apply to virtual currencies. This is needed to help banks ensure that they can do business with providers and users of virtual currencies and other payments innovators. Second-stage innovations from distributed computing and database technologies could offer benefits to payments and commerce far beyond those that virtual currencies now offer. If banks cannot determine how to comply with FinCEN regulations, for example, they may continue to terminate their relationships with payments innovators before the innovators can attract investors and users to make it to the second-stage technologies their current work may generate.
4. Encourage payments systems innovators to adopt and publicize transparent payment systems rules for their own systems and even to compete for customers on the basis of the system rules they adopt. It is too early to enact user protections for virtual currencies.
5. Ignore the claims that
   a. additional regulation of virtual currencies will halt innovations,
   b. innovators deserve freedom from regulations that apply to other payments systems and their providers, and
   c. virtual currencies deserve a single Federal licensure system that preempts State prudential regulation and licensure.
6. Monitor the development of virtual currency providers in case they transform their products into commodities or securities and, if this happens, then decide whether regulating their products under the applicable regulations makes more sense.
7. Leave room for nondepository and depository providers of payments products to innovate in the virtual currency space.
8. Authorize and fund a study of virtual currencies to be carried out by the Federal Reserve Board or pursuant to the Federal Advisory Committees Act by an inter-agency task force and industry participants.

The balance of this statement begins in Part II with a brief history of "legal tender" and the regulation of payments products in the United States. Part III dis-

cusses my recommendations in some greater detail. Part IV responds to questions posed in the Committee's invitation to testify.

Part II: A Short History of "Legal Tender" and Governments' Roles in Establishing it and its Value

The emergence of a large digital "currency" unconnected to a sovereign threatens a sovereign right recognized back to Renaissance times. In one of the earliest court decisions involving "legal tender"—the 1605 decision in Britain of *The Case of Mixed Money* [1] in which the House of Lords observed that the regulation of currency was a sovereign right and declaring the sovereign's right to declare "legal tender" by decree, the affixing of the sovereign's stamp, and to decision of the value of increments of currency—and later to change its mind about valuation. "The prince, the stamp, and the value" became from that point forward hallmarks of what could pass as "legal tender" that participants in trade transactions were required by the sovereign to take from others in satisfaction of obligations (trade or debt) they undertook. Proponents of virtual currencies often seek to end sovereign "monopolies" over legal tender, fiat currencies.

Contributing to the history of sovereign, stamps, and values was the rambunctious, highly problematic period in the United States in the pre-Civil War 19th Century in which "wild cat" banks operated. Banks issued paper notes—a form of what economists call *fiat currencies*— As opposed to coins or other "specie." Persons who took paper "bank notes" encountered significant problems with redeeming the value that the notes were supposed to represent.[2] They either encountered long waits while the notes moved for collection from banks near them to distant issuers of these notes, additional long periods while the issuing bank assembled enough funds to pay them off, or were forced to take huge discounts from local depositary banks against the prospect of these long waits or insolvency when the notes were eventually presented for payment to their issuing banks. "Wild cat banking" was cited as a cause of regional recessions and of decades of financial instability on the parts of businesses and individuals who had no other providers of financial intermediation services close enough to their homes.

The problems associated with wild cat banks and the pressures of sustaining the Federal effort during the Civil War led Congress to create a national paper currency and national banks in the 1860s.[3] Eventually, the need for financial stability, in-

---

[1] The Case of Mixed Money in Ireland, Trin. 2 James I. AD 1605 [Davies' Reports]. A key sentence from the opinion in that case proclaimed: "that it appertaineth only to the King of England, to make or coin money within his dominions. [2 Ro. ab. 166. 1 Co. 146, 5 Co. 114. 1 H.H.P.C. 188.]" The court also announced its conviction that there were three attributes of "money" and "legal tender" that distinguished them: the price, the stamp, and the value. *Id.*

[2] *See* Marine Bank v. Fulton Bank, 69 U.S. (2 Wall.) 252 (1864) (upholding the depositor's right to the sum owed on bank notes by its bank, rather than the lower value prevailing for Illinois notes of the time, which had decreased by 50 percent in value during the year that collection took). "Wildcat banks" did not have reserves sufficient to back their issues. Lissa L. Broome & Jerry W. Markham, Regulation of Bank Financial Service Activities 17 (Thomson Reuters, 2011).

[3] The Stamp Payments Act of 1862, 12 Stat. 592; Rev. Stat. 711, sect. 3583 (prohibiting circulation of bank notes worth less than one dollar); National Currency Act of 1863, ch. 58, 12 Stat. 665 (Feb. 25, 1863) (authorizing the chartering of national banks); and the National Bank Act of 1864, act June 3, 1864, ch. 106, 13 Stat. 99, as amended (superceding the National Currency Act). The goal of these collective National Banking Acts

> . . . was to create a uniform national currency. Rather than have several hundred, or several thousand, forms of currency circulating in the States, conducting transactions could be greatly simplified if there were a uniform currency. To achieve this all national banks were required to accept at par the banknotes of other national banks. This insured that national banknotes would not suffer from the same discounting problem with which State banknotes were afflicted. In addition, all national banknotes were printed by the Comptroller of the Currency on behalf of the national banks to guarantee standardization in appearance and quality. This reduced the possibility of counterfeiting, an understandable wartime concern.

American History from Revolution to Reconstruction and Beyond, *http://www.let.rug.nl/usa/essays/general/a-brief-history-of-central-banking/national-banking-acts-of-1863-and-1864.php* (last visited Nov. 17, 2013). Problems of counterfeit or altered notes caused the creation of John Thompson's Bank Note Detector, a precursor of the listing of counterfeit and altered notes issued routinely by the Office of the Comptroller of the Currency and Federal Deposit Insurance Corporation today. The national currency was *commodity currency* backed by specie (*e.g.,* gold certificates) in place of "greenbacks." Eventually, as the Members know, the United States replaced commodity currency with fiat currency in the form of Federal Reserve Notes. Proponents of virtual currencies and other followers of the Austrian School of Economics distrust fiat currencies for their roles in business cycles and consequences of monetary interventions reasons as explained well in the European Central Bank's 2012 report on Virtual Currency Schemes, *virtualcurrencyschemes201210en.pdf,* at 21. The Austrian School economists also prefer the "denationalization" of currency, effectively an end to governments' monopoly on the issuance of

cluding stable prices, and sound monetary policy was so great as to cause Congress to establish the Federal Reserve System. Federal authority in this arena has remained in place since that time—through various "gold standard" debates, the creation of the Bretton Woods' Agreement that established the current international monetary systems in the 1940s, and to the present. The Federal Government has the sole power to issue "legal tender."[4]

All of our principal trading partners also operate in national systems in which a single, State-specified currency constitutes "legal tender" for all transactions. There is little literature on the attitudes of our principal trading partners about "virtual currencies"—with the exception of coverage of Canada's development and plan to issue as "legal tender" forms of "digital currencies known as "MintChips,"[5] and the European Central Bank's 2012 report on *Virtual Currency Schemes.*[6] Canada's "Mint Chip" experiment reveals no intention of abandoning the principles set forth in *The Case of Mixed Money* in 1605: the prince, the stamp, and the value will continue to be the province of the sovereign. The ECB's report, as one would expect, also favors a continuing role for central banks and sovereign currencies.

But, just because "legal tender" exists as a fact in most developed nations, it does not follow that individuals or businesses cannot agree to take barter or nonlegal tender in exchange for goods and services. It just dramatically increases some, primarily legal risks in those transactions, much as we saw with "wild cat" banking in the pre-Civil War period here, and in the disappearance of bitcoin exchanges in China and also the Czech Republic. In these cases, the risk of engaging in virtual currency transactions currently falls entirely on users.

We must recognize that some individuals and, apparently, an increasing number of businesses, see value in using forms of "virtual currencies" to complete their own transactions.[7] Can we prevent them from doing so? Probably not. Should the United States step up their regulatory efforts in this arena? My answer is not yet, and not until such time as stronger evidence suggests problems exist with these currencies that contribute to financial instabilities, or otherwise enable issuers or intermediaries to commit fraud on users or complicate monetary or other important public policies.

Part III: Discussion of Recommendations

**Recommendation 1:** Retain the current division of regulation between the States and Federal Government—with prudential regulation of the nondepository providers of new payments systems with the States and retaining the anti-money-laundering, anti-terrorism and economic sanctions regulations with the Federal Government.

The current balance between State and Federal regulation affords more opportunities to follow developments in this area with lots of eyes on these innovations, ensure AML and economic sanctions goals are met, and allow room for innovation of these intriguing technologies that a comprehensive Federal licensure and supervision scheme might not allow as well. Furthermore, having prudential regulation should contribute to the confidence among users—whether consumers or businesses—that their stored value is safe and that their transactions will be executed as expected.

The split between prudential money transmission regulation by the States, and anti-money laundering and economic sanctions/ anti-terrorism regulations by the Department of the Treasury reflects a robust regulatory, supervision and examination scheme for virtual currency transactions with much room on the prudential side of State regulation to promote product innovation without sacrificing important protections for users or, on the Federal side, anti-money laundering (AML) or economic sanctions goals.

---

money. *Id.* These economists criticize fractional-reserve banking systems like ours, and urge the re-adoption of the gold standard. *Id.* Broome & Markham also note that as "electronic money" came into the market in the 1990s, commentators considered The Stamp Payments Act to bar its issuance in the Nation. *Supra,* note 1 at 19.

[4] Congress' authority was upheld in a series of decisions including United States v. Van Auken, 96 U.S. (6 Otto) 366 (1977); Legal Tender Cases, Know v. Lee & Parker v. Davis, 79 U.S. (12 Wall.) 457 (1870); Veazie Bank v. Fenno, 75 U.S. (8 Wall.) 533 (1869). The Federal Government's authority thus preempts the issuance by States such as Virginia of competing currencies, as the Virginia Legislature proposed to do in the past year.

[5] Canada's plans have revolved around a State-created digital "currency" that they call "Mint Chips." For more information on the status of this development, see John Greenwood, *Canadian Mint ready to test its own digital money project,* Fin. Post (Canada) (Sept. 19. 2013).

[6] Available at *virtualcurrencyschemes201210en.pdf* (last visited Nov. 17, 2013). (The ISBN for this report is 9778–92–899–0862–7 (online).)

[7] Media reports cite reasons such as avoiding the expense of exchange of currencies and other transaction costs associated with use of debit or credit cards, or even checks.

Some advocate for a single, Federal scheme of licensure and regulation of virtual currencies and their providers. The proponents of this view should be careful what they wish for: they could find themselves unable to qualify for a Federal license as the efforts of certain retailers to obtain approval from the Federal Deposit Insurance Corporation for their industrial loan operations (even after they had obtained a State ILC charter) or national bank or Federal savings and loan charters. These Federal approvals are also expensive and time-consuming processes with considerable discretion left to regulators to reject applicants. It is not clear to me that early applicants will enjoy the relief from 50-State regulation that they seem to expect.

Some individuals will not adopt payment methods they do not understand and whose rules of the road are not transparent. Thus, we should appreciate the longstanding role the States have played in *innovating regulations that have encouraged users to adopt new payments methods.* The work of the Uniform Law Commissioners and American Law Institute, begun more than 65 years ago, created the uniform and predictable provisions of the Uniform Commercial Code (UCC) that State Legislatures enacted. The UCC's predominance in payments regulation is now complemented by payments systems rules and bilateral agreements, including those that govern transactions that the UCC does not address, as well as limited Federal laws and regulations. Federal regulations also may prompt faster user adoptions of new technologies, as many believe the Fair Credit Billing Act (FCBA) and the Electronic Fund Transfers Act (EFTA) did in the late 1960s and 1970s, respectively, even though the EFTA has been criticized for chilling certain ATM developments.

**Recommendation 2:** Make providers of virtual currencies comply with the customer-identification program and AML compliance program requirements of Sections 326 and 352 of the USA PATRIOT Act, and with the economic sanctions regulations enforced by OFAC, just as other payments systems providers do. Virtual currency customers will have to reveal their identities to issuers or transaction intermediaries of the currencies they use. They should get the same Federal financial privacy rights that users of other payments products have under the Right to Financial Privacy Act of 1978 and Title V of the Gramm-Leach-Bliley Act.

My concern is that disintermediation of payments—the separation of payment flows from the comprehensive recordkeeping and retention requirements applicable to payments that eventually flow through the banking system—makes it more difficult to determine the identities of senders and recipients of payments. This may contribute to the efficacy of the "layering" stage of money laundering, the passage of the funds or credits through so many hands that the identities of payments participants is obscured. This is an important concern for anti-money-laundering, anti-terrorism, anti-proliferation, and anti-tax-avoidance purposes.

**Recommendation 3:** Encourage FinCEN to clarify the manner in which customer-identification and AML compliance requirements apply to virtual currencies to a greater degree if that is needed to stop banks from discontinuing their business relationships with virtual currency providers and other payments innovators. If banks cannot determine how to comply with FinCEN regulations, for example, they will cutoff payments innovators before the innovators can attract investors and users to make it to the second-stage distributed computing and database technologies their current work may generate.

Depository institutions deserve the clearest guidance on how customer-identification and AML compliance requirements apply to virtual currencies. This is one of the few ways in which we can stop the recent spate of terminations of banking relationships with providers of virtual currencies—colloquially called "bank discontinuance."

Without the clearest possible guidance available for banks and investors, we are likely to experience a domestic decline in innovations and the potential loss of development of future associated uses of the distributed computing and database technologies such as for tracking tangible goods transactions or even in tracking and trading intangibles such as electronic mortgages and other evidences of equity or debt. Moreover, if bitcoins or other virtual currencies prove to garner even more widespread international adoptions, the United States will want to have a share of the productive research and applications capacity in the United States and may regret actions that send it offshore.[8] This would be even more important if distributed

[8] For a valuable discussion of the regulation of virtual currencies from the perspective of the European Central Bank, see *Virtual Currency Schemes, supra* note 6. This study does not accurately reflect current state of regulation of virtual currencies in the United States in two respects. First, it ignores the presence of State prudential regulation of "money transmitters." Also, it fails to reflect the fact that widely used payments systems here have already moved away from reliance on "payments laws" and toward system rules and bilateral agreements for processing payments. These system rules and bilateral agreements often augment laws that oth-

technologies developing in the next 5 years that would not suffer the perceived disadvantages of bitcoins today were to emerge.

On the other hand, we should not condone the virtual currency systems that market the anonymity of their users or claim immunity from otherwise applicable compliance responsibilities in the name of "innovation." If proponents of virtual currencies want access to profits for transactions in the United States, they should be prepared to comply with applicable laws, and, in specific, they should obtain sufficient information from customers to enable them to respond to properly authorized requests for access from Federal or State regulators and law enforcement agencies.

A corollary of this recommendation involves providing financial privacy rights to users of virtual payments systems equal to those provided to users of more traditional payment systems. In the United States, two functionally different, Federal financial privacy statutes should govern virtual currency transactions—the Right to Financial Privacy Act of 1978, which governs access to account and transaction information of individuals and businesses by the Federal Government, and Title V (Privacy) of the Gramm-Leach-Bliley Financial Services Act of 1999, which governs how providers of consumer financial products and services may use and share the nonpublic, personally identifiable information they hold, including with their functional or prudential regulators and with Federal, State, and local law enforcement agencies. It is unclear that participants in virtual currency systems are enjoying these rights today. As banks increasingly buy providers of digital currencies to develop their own products, it is even clearer that customers should enjoy the same financial privacy protections, including due process rights, however limited they may be with border seizures and other Title 18 forfeiture provisions.

**Recommendation 4:** Encourage payments systems innovators to adopt and publicize payment systems rules for their own systems and even to compete for customers on the basis of the system rules they adopt.

Whenever a consumer or business prepares to make or receive a payment it will want to have certainty that:

- the payment is authorized by the person from whose funds or credits the payment will be made,
- the person has sufficient funds or credits for the payment processor to deliver those funds on time to the payee/ recipient so that the payee/ recipient will receive "goods funds" instantly or in a reasonable period of time,
- the payment is made to the proper payee and in the timeframe specified or expected by the person whose funds or credits are being used or consistently with any applicable contract between the obligor and payee,
- the payment, from the obligee's perspective, will become final at a specified time or after a specified interval and, from the obligor's perspective, that it will discharge the underlying obligation to pay for goods or services or to retire a debt, and
- the payment has integrity—that is, the named payee/ recipient has not been altered, the amount has not been lowered or raised, or the funds will not be held up unreasonably in transit.

These are "regulatory" or system rule qualities that will allow the provider to maintain users' trust.

Additionally, every person or business that stores funds or other value with a bank or broker—or in this case with the issuer, exchange or other provider/ participant in a virtual currency transaction—wants suitable assurances that they can redeem/ retrieve their funds or value when they want to do so. This issue surfaced with bitcoins when the Federal Government froze some bank accounts belonging to the Mt. Gox Exchange and the Exchange was unable to pay holders of bitcoins when they sought to redeem value stored in bitcoins. Other issues related to value storage include whether any form of insurance against the insolvency of the issuer or exchange is available to protect those who deposit value or otherwise hold accounts that they have reasonable expectations to redeem on little or no notice, or even on predictable terms.

---

erwise apply to the underlying form of payment being used, but in other cases they provide uniformity and certainty to forms of payments that neither Federal or State laws comprehensively govern (credit cards, electronic fund transfers, and certain aspects of payroll cards, for example).

The Bank's report mentions a case in which French "banks shut down the currency exchange facility for accounts handling [bitcoins], on the presumption that Bitcoin should conform to electronic money regulations. *Id.* at 43, citing Finextra: *http://www.finextra.comnews.fullstory.aspx?newscemid=22921.*

Some virtual currencies have attracted negative publicity, including recent publicity about the disappearance of a Bitcoin exchange based in China with $4.1 million of value that belonged to others. This type of negative publicity stands in the way of broader adoption of virtual currencies.

Prudential regulation and transparent system operating rules should help legitimate businesses offering virtual currencies attract more customers—assuming we have no reason today to fear competition for legal tender from current-day virtual currencies.

I encourage virtual currency issuers to create *payment systems rules* for their own systems and harbor some hope that issuers will compete to offer system rules that match the needs of the individuals and businesses who participate. Payment systems rules often precede full government regulations by long periods of time. Examples include traveler's cheques and bank wire transfers, and more recently automated clearing house transactions governed by the National Automated Clearing House Association and electronic checking processing systems that use ECCHO Operating Rules. New payments methodologies regulated too soon often do not receive the same levels of innovations. The primary example I can cite was based on a report by the Board of Governors of the Federal Reserve System following the enactment and implementation of the Electronic Fund Transfers Act in the late 1970s. The alternative to provider-created system rules may be more government regulation. This gives providers a choice between self-regulation for these specific customer protection purposes or more government regulation. I imagine they will give self-regulation careful consideration.

Payments systems that have not established transparent and uniform system rules normally suffer a worse fate: so few individuals or businesses will use them that they wither for lack of investors and of income. This happened to some extent in the United States to early offerors of "electronic money," including Mondex and Digicash, despite talented senior management and significant investments. Consumers did not adopt them so merchants did not adopt them—in part because neither group was certain of their rights if they adopted them.

**Recommendation 5:** Ignore the claims that any regulation of virtual currencies will halt innovations or that innovators deserve freedom from regulations that apply to other payments systems and their providers, and their wishes for a single Federal licensure system.

I urge Members to resist the "we're new so don't regulate us at all" arguments that you've heard since the advent of electronic commerce. Payments are payments and stored value is value storage. The "don't regulate us or you will stifle innovation" arguments did not persuade many as digital money, prepaid cards, payroll cards and other new products appeared in markets and they offer no reason to abandon existing prudential regulation now.

There also is no reason to reward "innovators" with freedom from regulations with which their "real world" competitors must comply. That would provide anti-competitive advantages to certain new entrants for which no justification appears.

**Recommendation 6:** Monitor the development of virtual currency providers in case they transform their products into commodities or securities and, if this happens, then decide whether regulating their products under the applicable regulations makes more sense.

Bitcoins' values have been highly volatile over the past year. This volatility looks like price volatility associated with commodities and securities; bitcoin prices seemingly move separately from the values of the world's major currencies. If other virtual currencies demonstrate this market freedom from legal tender currencies, this may be the signal that a reconsideration of type of regulation to be applied from regulation as payment systems to regulation as commodities or securities.

**Recommendation 7:** Leave room for nondepository and depository providers of payments products to innovate in the virtual currency space.

It is important not to rush new laws or regulations following negative publicity from a new technology when existing laws regulate issuers prudentially and clarity in enforcement of AML regulations can allow some space for innovators in the virtual currency space. I was delighted to read last week that the New York State Department of Financial Services was considering offering a BitLicense. Careful development of licensure standards will help develop stable payments products. As I have mentioned, virtual currency technologies can produce secondary, distributed computing and database applications that could yield enormous benefits to domestic and cross-border commerce.

**Recommendation 8:** Ask for a study of virtual currencies to be carried out by the Federal Reserve Board or the Department of the Treasury or fund a study pursuant to the Federal Advisory Committees Act by an inter-agency task force and industry participants.

The Subcommittees sponsoring today's hearing should ask for a study by the Board of Governors of the Federal Reserve System or the Department of the Treasury of virtual currencies, the potential for innovations and efficiencies they may offer more broadly, and the kinds of risks—to price stability, financial stability, payment system stability, reputational risks and for users—identified in an October 2012 report by the European Central Bank entitled "Virtual Currency Schemes."[9]

Another option is for Congress to authorize and separately fund an inter-agency working group to produce a study of how the various Federal agencies involved in payments, regulating of banking, commodities, securities and law enforcement.

Regardless of which agency leads the study, the work should be organized under the Federal Advisory Committees Act so that all industry segments can be included.

Part IV: Responses to Other Questions Posed by the Committee

*A. Issues implicated in cross-border payments and cross-border trade and finance*

Monetary policy is one of the concerns cited by the European Central Bank in its 2012 report on Virtual Currency Schemes. But that report did not discuss enforcement of collateralized debt obligations.

Virtual currency transactions could render finance transactions nontransparent so that current and potential providers of financing might not be able to ascertain their relative priorities to assets that underlie those trade transactions. The United States will want to follow closely developments that frustrate creditors' claims to inventory or other assets if the obligor fails to complete payments for goods that it has purchased here or abroad.

The trend away from bank-issued letters of credit to supply chain financing not involving banks—indeed including financing provided by logistics suppliers—has not yet degraded the ability of sellers, buyers or their financers to monitor cross-border trade transactions. This may be because logistics suppliers of supply chain finance enjoy hard-earned reputations as honest participants delivering the goods they carry and collecting payments if required on behalf of senders. But the potential for trade finance disruption still exists.

*B. Possible regulatory models for providers of payments products and systems*

In addition to the current State prudential regulation of virtual currency providers and to Treasury's comprehensive registration, AML and economic sanctions regulations applicable to money services businesses, we have a number of potential models for regulating, requiring registration or supervising and examining providers of virtual currencies. I mention these more for future purposes than for any need I perceive at this point, but the eventual use of alternative regulatory models depends in large measure on how the products offered as "virtual currencies" work in fact.

For example, State prudential regulation of money transmitters is framed to ensure that competent transaction execution. Those who take funds from one person with a promise to deliver them to a second person need to have the capacity to do just what they promise—to pay in the manner, in the time, and to the person that the first person instructed them to pay.

Prudential regulation by States establishes qualifications for providers—depository and nondepository providers they license to do business with their own residents, and establishes a system of reserves or bonds or both so that funds will be available to complete transactions on those persons' parts.[10] State licensing and bonding requirements are cited by many entrepreneurs as a reason why virtual currencies are not attracting the widespread uses and investor funding that entrepreneurs seek. However, without these State requirements, the prospect of value disappearing—as it apparently has with the disappearance of the bitcoin exchange in China—likely would rise and injure users of these products.

State prudential regulation began in the late 18th Century when Massachusetts and New Hampshire prohibited unincorporated banks from operating.[11] New York State followed them with its prohibition in 1804. Some States banned banking—period. These included Texas until 1904, and Iowa, Arkansas, Oregon and California before the Civil War. State laws also established "safety deposit" systems and have regulated them. Items in safety deposit boxes are not immune from asset freeze or-

[9] *Supra,* note 6. For more information about this report, see *supra,* note 8.

[10] This system has features of fractional reserves that our banking system depends on, as well as of bonding or comparable requirements to ensure completion of transactions in the event of provider failure. The Board of Governors of the Federal Reserve System also establishes reserve requirements for depository institutions on an annual basis, in Regulation D.

[11] For a brief discussion of this period in bank and payments regulation in the United States, see Broome & Markham, *supra,* note 2 at 1–28.

ders issued by courts, or seizure by the IRS. States have been regulating money transmitters since the advent of the telegraph.

The regulation of safe-storage systems is even more ancient, beginning with the Knights Templar and Vatican as lenders in the pre- and early-Renaissance periods, and with the Silver Vaults in London and lenders in Belgium, the Netherlands, and Florence whose services contributed to the early Renaissance flows of commerce and modern trade. I mention safety deposit systems because of the similarities they have, and that their predecessors had, to products such as e-Gold, and even bitcoins. Some of these contemporary products are more like commodities to be bartered than they are true "currencies."[12]

Alternative regulatory schemes for virtual currencies include commodities and securities regulation. The securities model offers advantages such as registration and requirements for disclosing material events that may affect the value of the security or the health of its issuer.

One reason to consider commodities or securities regulatory schemes for virtual currencies that do not track the movements of legal tender currencies is evidence that investors are speculating in these currencies. To the extent that virtual currencies seem to be used more for speculative purposes and less for transaction execution, the nonpayments models of regulations present feasible alternatives.

V. Conclusion

I applaud the Subcommittees for holding this important hearing and urge them to continue to watch developments in virtual currencies. Thank you again, Chairman Merkley and Chairman Warner, and Ranking Members Heller and Kirk, for this opportunity to share my views with your Subcommittees. I will be pleased to take questions.

---

## PREPARED STATEMENT OF MERCEDES KELLEY TUNSTALL

PARTNER, PRACTICE LEADER, PRIVACY AND DATA SECURITY GROUP
BALLARD SPAHR LLP

NOVEMBER 19, 2013

### INTRODUCTION

Chairman Merkley, Ranking Member Heller, and the Members of the Subcommittee, I am Mercedes Kelley Tunstall, a Partner at Ballard Spahr LLP and the Practice Leader of our firm's Privacy and Data Security Group. My testimony today reflects my personal experience with the virtual currency industry and represents my own opinion. My testimony does not necessarily reflect the opinions of Ballard Spahr LLP or our clients.

Thank you for this opportunity to testify about the present and future impact of virtual currency. I work directly with multiple clients that offer their own forms of virtual currency. I also advise large banking clients on how to interact with virtual currencies as well as how to structure their programs and services as to avoid being treated as virtual currency. I have spoken extensively on this topic during Webinars and other public forums, and I have been quoted frequently by the press. I will focus my remarks today on the important steps that the virtual currency industry and Federal regulators should take in order for virtual currency to have a commercially viable future.

### THE NEXT GENERATION OF VIRTUAL CURRENCY

In only a few short years, Bitcoin may have become the most well-known virtual currency today, but Bitcoin has also demonstrated a number of weaknesses that the next generation of virtual currency should be careful to address.

*I. Bitcoin ≠ Integration*

Bitcoin has built its reputation and structured its virtual currency around being both antigovernment and anti-establishment. Although this reputation may be attractive to a certain type of consumer, the structure has limited, and will continue to limit, Bitcoin's adoption by a wider population. Due to Bitcoin's reputation, large financial institutions view the currency as being unreliable and therefore not able to meet their safety and soundness requirements. If a virtual currency could be reliable, then financial institutions may very well incorporate the currency as a solution

---

[12] Francois R. Velde, *Bitcoin: A primer,* Chic. Fed Letter No. 317 (Dec. 2013) (copy on file with the witness) (describes the operations of bitcoins and, particularly, its unique methods for controlling two challenges of digital money—controlling the creation and avoiding duplication of units).

to certain problems faced. For example, virtual currency could be attractive to large financial institutions if the fees associated virtual currency transactions, including the exchange fees, are lower than the fees accompanying other payments methods (*e.g.,* interchange fees). The next generation of virtual currency should figure out a way to better align with existing payment methods, or virtual currency will never be able to move from a "niche" into the mainstream.

*II. Virtual Currency ≠ Anonymity*

One of the most frequently cited advantages of virtual currency is the increased privacy and anonymity associated with using bitcoins. However, even Bitcoin is not completely anonymous as a public record of each Bitcoin transaction is electronically recorded. In order for the industry to continue maturing, the next generation of virtual currencies should dispel the perception that an important element of using virtual currency is the ability for an individual to engage in online transactions with complete anonymity.

In a transaction involving hard currency, the two parties to the transaction may not know each other, but in order for the currency to be handed from one person to the next, the two people must see each other and be in each other's presence (or have a proxy to do the same for them).

This transaction is hardly anonymous, and yet many have compared Bitcoin transactions to cash exchanges between strangers and referred to such exchanges as being anonymous. Instead, the distinction is that such cash transactions can occur without being recorded by any financial system or government and without the involvement of middlemen such as banks. As such, bitcoins, like cash, have been used in transactions to perpetrate fraud, money laundering, and other illegal activities. Unlike hard currency, however, technological solutions could be developed to track the digital exchange of virtual currency so that the transaction is not conducted through a middleman. Bitcoin and other virtual currency providers have a responsibility to prevent criminal activity and to comply with anti-money laundering and other laws. The next generation of virtual currencies must address the ability of individuals to use virtual currency to engage in illegal activities anonymously or the Congress, the Federal agencies, or the courts may take action, which could result in harmful consequences to the industry's overall growth.

*III. Bitcoin = Commodity or Bitcoin ≠ Commodity*

Bitcoin displays some features that allow Bitcoin to function like a commodity, such as the self-imposed limit of 21 million bitcoins and the volatility of the value of bitcoins. However, Bitcoin does not presently comply with current securities or commodities laws and regulations. In order for banks to work with virtual currencies, those virtual currencies either need to comply with or protect against commoditization. Unless the next generation of virtual currencies can resolve the question as to whether virtual currency should be considered a commodity, the industry will remain characterized by volatility. Without further stabilization, mainstream adoption of virtual currency remains unlikely.

**REGULATORY CERTAINTY**

As the virtual currency industry matures, regulatory certainty will also be needed to ensure a future for this industry.

*I. Legal Definition of Virtual Currency*

The virtual currency industry would benefit greatly from guidance from the Federal Government as to the legal definition of virtual currency. Although it is clear from the Legal Tender Cases of the 1870s and 1880s that virtual currencies can legally operate in the United States of America, it is unclear as to what regulations could and should apply to virtual currency.

The Commodity Futures Trading Commission and the Securities Exchange Commission have both examined Bitcoin-related issues and determined that there are times when the currency operates as a commodity/security, but beyond that, there is no existing legal framework that addresses the unique features and functionality of virtual currency.

*II. Financial Crimes Enforcement Network*

Existing FinCEN guidance has offered much-appreciated guidance for the industry and related players, but as the industry continues to mature, additional guidance will be needed on how to integrate virtual currency into the existing financial ecosystem, especially with regard to compliance with anti-money laundering requirements.

*III. Electronic Fund Transfer Act / Federal Reserve Board Regulation E*

Currently, consumer protections contained in financial regulations such as the Electronic Funds Transfer Act and its implementing regulation, Regulation E, do not apply to virtual currencies. Therefore, unauthorized transactions involving virtual currency have no recourse—once the currency is gone, it is gone, just as surely as when someone swipes bills from a wallet. Due to the electronic nature of virtual currencies, consumers may not understand the reasons for the disparate protections conferred on the use of these disparate payment forms. If consumers are unable to embrace virtual currency as a safe, effective means to conduct online (and even offline) transactions, industry growth will be stalled.

**CONCLUSION**

Thank you again for the opportunity to testify on these important issues. I would also like to express my appreciation to your staff for all their assistance in preparing for this hearing.

I would be happy to address any specific questions that the Members of the Subcommittee may have for me.

**Mercedes Tunstall**

***Biography***

Mercedes Kelley Tunstall is the Practice Leader of Ballard Spahr's Privacy and Data Security Group. She is also a member of the software and business methods practice team in the firm's Patents Group.

Ms. Tunstall counsels clients on compliance with consumer financial services laws, including unfair, deceptive, and abusive acts or practices, as well as the investigations, rulemakings, and proceedings of the Consumer Financial Protection Bureau and the Federal Trade Commission.

Ms. Tunstall has substantial experience working with clients to develop new financial products and services, including mobile wallets, virtual currencies, and prepaid cards. These engagements typically include negotiating agreements with technology vendors, reviewing technical designs, drafting customer communications and agreements, and advising on potential regulatory and privacy and data security concerns.

She also works with clients from a spectrum of industries on mobile and other ecommerce initiatives, privacy and cybersecurity issues, and the use of social networking sites for marketing, customer service, and crowdsourcing purposes.

Before joining Ballard Spahr, Ms. Tunstall was lead counsel for Global Marketing and Deposits at Ally Financial. She also worked in-house for Bank of America, where she managed all legal aspects of e-commerce, and at HSBC, where she managed consumer financial services litigation.

Ms. Tunstall was a Staff Attorney at the Federal Trade Commission, where she investigated and litigated the Commission's first Internet hijacking case, among other Internet fraud matters.

---

## PREPARED STATEMENT OF ANTHONY GALLIPPI

COFOUNDER AND CEO, BITPAY

NOVEMBER 19, 2013

Thank you Chairmen Merkley and Warner, and Ranking Members Heller and Kirk, and Distinguished Members of the Committees for the opportunity to speak with you today.

My name is Tony Gallippi and I am the Cofounder and CEO of BitPay. I graduated magna cum laude from Georgia Tech with a degree in Mechanical Engineering. BitPay is a startup company with 16 fulltime employees, based in Atlanta.

I appreciate the Members for their interest in the commercial and international trade uses of digital currencies, and more importantly, the opportunities for digital currencies to create jobs in America and to increase America's exports. Since Bitcoin represents the dominant market share of virtual currencies, my testimony will focus on Bitcoin specifically and not on any of the alternative virtual currencies.

Our company, BitPay, was started in May 2011 and we have been operating for over 2 years now, which makes us pretty old in the Bitcoin space. During this time we have acquired over 12,000 merchants to accept bitcoin with our service. Our merchants include many small and medium-sized businesses in every State, who accept bitcoin side-by-side with credit cards and other forms of payment.

Most online payments today are made with credit cards, but credit cards were never designed for the Internet. Credit cards were designed in the 1950s, and they still function the pre-Internet age. Last year, over 12 million people became victims of identity theft, mostly from shopping online (source: *https://www.javelinstrategy.com/news/1387/92/1).* Businesses lose over $20 billion per year due to payment fraud (source: *http://www.lexisnexis.com/risk/downloads/assets/truecostfraud2013.pdf).* The banks don't take responsibility for the fraud. If you are a business owner, it is your fault that you took a stolen credit card, even if the bank approved it. Credit Card fees are discriminatory the highest fees are paid by the smallest mom-and-pop businesses and the lowest income consumers. Bitcoin is a cheaper, faster, and more secure payment system.

**Background on Merchant Acquiring**

Even though we deal with bitcoin, our business model of merchant acquiring is fairly traditional. Merchant Acquiring began in the 1950s with credit cards, and the big marketing push to get businesses to accept credit cards as payment. Over the years, companies such as First Data, TSYS, Fiserv, and others would emerge with new tools for merchants. These companies are typically not household names. They operate behind the scenes, facilitating merchant payment acceptance as a business-to-business service. Most consumers, even when making a payment through one of these service providers, don't even know that these companies exist.

Fast forward 40 years to the 1990s with the launch of the worldwide Web and the first Web browser. Businesses could build a Web site to reach customers, but how could they take a payment from a Web page? It was the mail-order companies who figured it out first. If they could accept a credit card over the phone, then perhaps they could also accept a credit card over the Internet. Companies like Cybersource and *Authorize.net* built payment gateways for processing credit cards over the Internet, and today, 20 years later, credit cards are still the most widely used form of payment over the Internet.

**Differences between Credit Cards and Bitcoin**

Credit cards are "pull" transactions. The shopper provides their account number, and secret credentials that the business can use to pull money from their account. The problem is that the same credentials to pull money one time can be used to pull money many more times by that same business, or by anyone who has these credentials. This is the fundamental design problem with credit cards, and it is the root cause of the identity theft and fraud that we see today.

Think about that for a minute. Why would you ever give someone full access to your $20,000 line of credit to pay them $20?

Because of this design flaw, security around credit cards is massively expensive. Apple has iTunes, with over 500 million credit card numbers stored on file. The cost and risk of securing this data is enormous. Visa alone spends $200 million a year on fraud prevention. They are throwing big money at the problem and it is not working, because every year fraud remains very high.

In 2009, Bitcoin was invented. Bitcoin takes everything we know about the Internet, Security, and Cryptography, and builds a payment system designed for the Internet.

Bitcoin is an open standard, an open protocol, and an open source payment network. Nobody owns the network, and nobody controls the network. All of the users collectively own the network, its rules, and its ledger.

Anyone can use bitcoin or build an application on top of bitcoin. Bitcoin is much like the Internet itself, where anyone can use the Internet and build an application on top of the Internet. And because Bitcoin is borderless, a business can receive a payment from China just as easily as they can receive it from someone in the same room.

Bitcoin payments are "push" transactions, which are very different than credit cards. If I want to pay someone, I push them the exact amount I want to give them. The recipient does not get my account number, they do not get my secret credentials, and they do not get any permission to ever pull money from my account. Only I can push out a payment. Bitcoin works similar to email, and text messages. Text messages are a push transaction. You cannot pull an email from me or a text message from me, only I can push the message to you. Bitcoin works the same way, for payments.

**BitPay is a Bitcoin Merchant Acquirer**

At BitPay, our role in the bitcoin ecosystem is very close to that of the traditional merchant acquirers in the credit card space. We act as an agent of the payee, to help merchants clear and settle transactions over the bitcoin network. Merchants could accept bitcoin directly, but automating this is very difficult, and most mer-

chants choose to use our software and service rather than try to figure it out themselves.

BitPay has a strict Know Your Customer (KYC) policy to verify all of our merchant applications. We need to know who our merchants are and what they are selling. We only want the good actors using our service. We routinely audit our merchants, and we suspend and terminate those who violate our Terms of Use. A copy of BitPay's Merchant Terms of Use is attached in Exhibit A.

BitPay also follows all Bank Secrecy Act (BSA) guidelines to prevent, detect, and report suspicious activity. Our strict policies to comply with laws and protect our brand have earned BitPay the reputation as a leader and well respected company in the payments space.

BitPay is not a bitcoin exchange, but we use nearly all of the bitcoin exchanges around the world to manage our own asset allocation. We do not act as a broker dealer to facilitate trades, and we also do not offer any bitcoin services for consumers. Consumers do not need to store funds with BitPay, they can simply pay the merchant invoice from whichever bitcoin wallet they choose to push the payment from. In the near future, our service will be more integrated into the merchants branding and checkout experience.

**Bitcoin protects Consumers from Identity Theft**

For consumers, Bitcoin is another choice of payment which is voluntary to use. One of the main reasons why a consumer would choose to pay with Bitcoin is that Bitcoin can reduce, if not completely eliminate, the risk of the consumer becoming a victim of identity theft. Identity theft happens when a criminal gets access to the victim's account number and credit card credentials, and uses those credentials to make unauthorized purchases. When using Bitcoin, the consumer never needs to provide their identity to make a payment, so there is no identity information to steal, and no risk of identity theft. Bitcoin is a massive win for consumers, saving 12 million people per year the expense and hassle of dealing with the fallout of identity theft.

Consumers will be educated of the different ways in which they store their bitcoin. It functions more like cash, where if you lose it, it's gone. The funds are locked in the private key, which defines the ownership of the asset. Consumers can create many wallets with varying levels of convenience and security. The technology is being developed, and consumers will be educated on data security and proper data backups to ensure proper use of the technology. If consumers understand how bitcoin works, they should be allowed to use it.

**Bitcoin protects Businesses from Payment Fraud**

For businesses, Bitcoin can also stop the $20 billion/year fraud problem. When your business receives a bitcoin payment, it's confirmed, and it's yours. It cannot be reversed or taken away from you. Businesses can now reach customers in emerging markets, where they could not collect payments from before. Credit cards for online businesses don't really work beyond 8 or 10 countries, so most businesses simply choose not to sell internationally not because their Web site can't reach, or their shipping company can't reach, but only because they can't take the payment.

It is the small mom-and-pop businesses that are most excited about Bitcoin, and represent most of the adoption today. The businesses who accept Bitcoin are now opening up new markets, and creating more exports, and more jobs in America. If the United States doesn't allow our businesses to accept bitcoin and create more jobs and exports, then countries like Germany and China certainly will.

**Bitcoin's limitations**

Bitcoin does have limitations that will keep it a small player in the payments space for quite some time. Compared to credit cards, Visa's payment network can handle 20,000 transactions per second, worldwide. Bitcoin can handle seven. Not seven thousand, but seven transactions per second. Today, the average rate on the bitcoin network is one transaction per second. So compared to the collective networks of credit cards, debit cards, payment cards, ACH, and wires, there are 50,000 times more transactions taking place on traditional networks than on the bitcoin network.

Bitcoin also has some limitations on its usability. The global money supply of Bitcoin is worth around $5 billion. Compare this with the global M2 money supply of around $70 trillion, there is 15,000 times more money in the world in traditional currencies than in bitcoin.

**Bitcoin's potential for nonmonetary use**

Even though it's small, Bitcoin has invented something previously thought to be impossible. Many times when parties transfer assets to each other, they are trading

a digital representation of an asset. The asset itself settles 13 days later. With Bitcoin, it is now possible to transfer an asset remotely, and immediately settle the transaction, with no counterparty risk. That type of instrument has never existed before.

The possibilities of this instant worldwide settlement are very interesting. And this is where the real potential for Bitcoin exists. The Bitcoin blockchain, which is the public accounting ledger of bitcoin, is a large property rights database. It can handle quadrillions of individual asset accounts, with a full chain of custody every time an asset is transferred from one party to another party.

If you want to energize the housing market, think of Bitcoin. The biggest upfront costs for consumers trying to buy a home are the closing costs, which include fees for deeds, titles, stamps, title insurance, and other redundant tasks to record the sale in different record books. Bitcoin can replace thousands of dollars in closing costs with a single transaction that costs 5 cents. By reporting deeds and titles on the blockchain, the information would be public record forever, for pennies, and eliminate the need for title insurance.

The property rights aspect of Bitcoin can go one step further, to create smart property. This can be used for purchases like cars, where if a loan is attached to the car, the ownership of the car can be transferred back to the lender in case of default, or if the loan is paid off the owner would have full ownership of the car, and then they can transfer it to whomever they want.

**Bitcoin Risks**

Bitcoin does have risks. Criminals use cell phones, criminals use email, and criminals use dollars and banks. Many businesses like BitPay, offering innovative services on top of bitcoin, share the Committee's goals to protect consumers from fraud, and keep the criminals away from our businesses.

The Board of Governors of the Federal Reserve System acknowledged that virtual currencies "may pose risks related to law enforcement and supervisory matters," but "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."

**Bitcoin Regulation**

Guidance from the IRS, Department of Treasury, Department of Justice, and SEC has all established that bitcoins are legal, and that those dealing with them must simply follow existing tax laws and antimoney-laundering regulations.

In the 1990s when the Internet was in its infancy, Congress took a wait-and-see attitude to let the Internet develop. Where would Social Media and other free apps be today if in the 1990s we required licenses for the Internet, and taxed Internet access as if it was a Telecom?

In 1995, the National Science Foundation lifted its strict prohibition of commercial enterprise on the Internet, and immediately companies like Amazon, Ebay, and Dell were born. Americans will benefit from a similar openness and wait-and-see approach to Bitcoin.

**Bitcoin Regulation outside the United States**

Bitcoin by design is borderless, like the Internet itself. Businesses using bitcoin are forming every day, at a pace not seen since the expansion of the worldwide Web in the 1990s. There is a tremendous amount of capital, resources and effort being spent to create innovation in finance.

We don't believe that new legislation or regulation around bitcoin is needed. The rules for consumer protection and antimoney laundering already exist today.

Germany has declared Bitcoin to be "private money" and other countries are working to categorize Bitcoin and Bitcoin-related services into regulatory frameworks that exist today. Bitcoin is a technology with tremendous cost savings for businesses and consumers. Bitcoin is a more secure, faster, and more affordable option for transferring funds. If America is the leader in Bitcoin technology, America will create more jobs and more exports.

**Bitcoin is Disruptive**

Bitcoin is a disruptive technology. Bitcoin will not replace the dollar, or the euro, or gold, but it will certainly disrupt existing financial services and their fee structures. Today banks charge many fees to consumers: overdraft fees, overlimit fees, interest fees, application fees, monthly fees, authorization fees, processing fees, ATM fees, maintenance fees, minimum balance fees, late fees, and even fees to send your paper statement in the mail. With bitcoin, users can handle many of their daily payments needs themselves and avoid the bank fees, so banks relying on fee revenue could be impacted the most by virtual currencies.

Most IT systems used by banks and financial services today were built in the 1970s. They were designed well before the Internet and they lack many of the technical innovations that other industries use today. Bitcoin could offer immediate cost reductions and technical advancements to our financial institutions, particularly in the areas of interbank settlement, international transfers, and foreign exchange. The current 13-day settlement times on many types of transactions can be reduced to 13 seconds.

Bitcoin is a technology with tremendous cost savings for businesses and consumers. Bitcoin is a more secure, faster, and more affordable option for transferring funds. If America is the leader in Bitcoin technology, America will create more jobs and more exports.

**Conclusion**

In conclusion, today Bitcoin is in its infancy. It is much like the Internet in the early 1990s. Thanks to Congress's protection, the Internet was allowed to evolve and develop, and today it has greatly improved our lives.

If we look 10–20 years in the future, we will see many companies built upon bitcoin-related technology. We want those companies to be based in America, creating jobs in America, and building a revenue base and tax base in America.

The original application of the Internet was commerce, with companies like Amazon and Ebay. Over time, the killer apps for the Internet emerged, and these apps were not the original application. Search, Social Media, and Big Data are all powerful industries built on the Internet, and where would all of the free applications like Social Media be today if the early Internet was pigeonholed, overly regulated and required expensive telecom licenses?

I commend the Committee for recognizing the real, practical uses of virtual currencies and the potential future applications of this technology. Thank you for the opportunity to speak today.

**Appendix A BitPay Merchant Terms of Use**

These Merchant Terms of Use (the Terms) govern your use of the products, services or any other features, technologies or functionalities (the Services) provided by BitPay, Inc. (BitPay, we, our, or us) through BitPay's Web site, API or through any other means. You and your mean the merchant to which we will be providing the Services and the person signing below or otherwise agreeing to the Terms on behalf of the merchant. Please read the Terms carefully; by using the Services, you agree to the Terms and confirm that you accept them.

**The Services.** We are a Bitcoin payment processor—we enable you to accept bitcoins as payment for goods or services, and process Bitcoin payments that you receive from your customers. We are not a Bitcoin exchange, Bitcoin wallet, or a place to purchase Bitcoin. By using the Services, you authorize us to receive, hold and disburse funds on your behalf and to take any and all actions that we think are necessary or desirable to provide the Services and to comply with applicable law.

**Registration**

**Generally.** In order to use the Services, you must open a BitPay account. When you open an account, we will ask you for contact information such as, for instance, your name, mailing address, phone number, email address, and Web site. The information that you provide at the time of account opening must be accurate and complete, and you must inform us in a timely fashion of any changes to such information. We may require additional information about you (including any person signing below or otherwise agreeing to the Terms on behalf of the merchant) such as, for instance, your date of birth, tax identification number or Government-issued identification, and we may also obtain information about you from third parties, such as credit bureaus and identity verification services. We have the right to reject your account registration, or to later close your BitPay account, if you do not provide us with accurate, complete and satisfactory information.

Merchant Tiers. BitPay imposes daily transaction processing limits on merchants. When you register for a BitPay account, you will be required to select the limit (the Tier) that will apply to your BitPay account, and to provide us with the documentation necessary to qualify for that Tier. A description of the Tiers, as well as a list of the documentation required to qualify for each, is available on our Web site. If your business is a High Risk category, as determined by BitPay, you will be required to qualify for the "Trusted" Tier in order to use the Services. We will not begin to process payments on your behalf until we have reviewed the documentation that you provide, in accordance with applicable law. If you wish to change to a

Tier with a higher limit, you must provide us with the additional required documentation. We will not approve your request to change Tiers and permit you a greater processing volume unless and until we have reviewed your documentation to our satisfaction. Please also refer to Section 3.1, "Daily Transaction Volume; Tiers."

**Guarding your Password.** You will choose a password when registering. You are responsible for maintaining the confidentiality of your password and account. You are fully responsible for all activities that occur using your password or account. Please notify us immediately of any unauthorized use of your password or account or any other breach of security. We will not be liable for any loss that you may incur as a result of someone else using your password or account, either with or without your knowledge. You may not use anyone else's password at any time.

**Prohibited Accounts.** Use of the Services is subject to the laws and regulations of the United States regarding the prevention of terrorist financing and antimoney laundering. You agree and acknowledge that your use of the Services would and will comport with such laws and regulations, including, without limitation, the sanctions programs administered by the Office of Foreign Assets Control of the United States Department of the Treasury.

**Your Sales.**

**Daily Transaction Volume; Tiers.** You agree to adhere to the transaction processing limits applicable to your Tier. You agree that, if you exceed that limit, BitPay has the right to hold the over-the-limit funds until you have provided us with the additional documentation required to qualify for the next Tier, and until we have had the opportunity to review such documents. We will take additional measures if you exceed your limit. If you are a "Trusted" merchant, you may create an unlimited value of invoices (see Section 8.1), although you will only receive payments from us up to the specified limit. If you are not a "Trusted" merchant, you may not create a value of invoices that exceeds your specified limit.

**Invoices and Records.** You must keep all records needed for fulfilling the merchandise to the purchaser and providing any post-sale support to the purchaser. If the sale of the item requires any government registration of the sale, you are responsible for such registration.

**Customer Verification.** You are solely responsible for obtaining any information required of those who purchase your goods or services. For instance, if applicable law prohibits a sale to persons under the age of 18 years, you must ensure that a purchaser is at least 18 years of age. Similarly, if applicable law requires that a purchaser's identity be verified, you must verify the purchaser's identity. We will not be responsible for your failure to adequately verify your purchasers' identities or qualifications.

**Representation and Warranties.** Your use of the Services is subject to several important restrictions. Specifically, you represent and warrant to us that:

(a) Your use of the Services will not contravene any applicable international, Federal, State or local law or regulation, including applicable tax laws and regulations, and that your use of the Services will not violate the laws of the United States of America.

(b) Your use of the Services will not relate to sales of (i) narcotics, research chemicals or any controlled substances, (ii) cash or cash equivalents, including derivatives, (iii) items that infringe or violate any copyright or trademark, (iv) ammunition, firearms, explosives, weapons or knives regulated under applicable law, or (v) any services which compete with BitPay.

(c) Your use of the Services will not relate to transactions that (i) show the personal information of third parties in violation of applicable law, (ii) support pyramid or Ponzi schemes, matrix programs or other "get rich quick" schemes, (iii) are associated with purchases of annuities or lottery contracts, layaway systems, offshore banking or transactions to finance or refinance debts funded by a credit card, (iv) are associated with Money Service Business activities, as defined by the Financial Crimes Enforcement Network of the United States Department of the Treasury, or (v) provide credit repair or debt settlement services.

(d) Your use of the Services will not involve gambling or any other activity with an entry fee and a prize, including, but not limited to casino games, sports betting, horse or greyhound racing, lottery tickets, other ventures that facilitate gambling, and sweepstakes, unless you have obtained our prior approval and you and your customers are located exclusively in jurisdictions where such activities are permitted by law.

(f) You have the right, power and ability to enter into and perform under these Terms.

**Our Right to Reject.** We reserve the right to decline to process a sale if we believe that it violates these Terms or would expose you, other merchants, purchasers, or other parties to harm. If we reasonably suspect that your BitPay account has been used for an illegal purpose, you authorize us to share information about you, your BitPay account, and your account activity with law enforcement.

**Our Right to Inspect.** We may ask for permission to inspect your business location, in connection with your use of the Services or specific transactions. If you refuse our request, we may suspend or terminate your BitPay account.

**Third Parties.**

**Your Use of Third-Party Services.** In using the BitPay Web site or the Services, you may be offered services, products and promotions provided by third parties. If you decide to use these third-party services, you do so at your own risk and are solely responsible for reviewing, understanding and complying with the associated terms and conditions. We expressly disclaim any liability for the third-party services and are not responsible for the performance of the third-party services or servicers.

**Security.** We have implemented security measures designed to secure your information from accidental loss and from unauthorized access, use, alteration or disclosure. However, we cannot guarantee that unauthorized persons will never gain access to your information, and you acknowledge that you provide your information at your own risk, except as otherwise provided by applicable law.

**How we Collect, Use and Share Information.** In order to provide the Services, we may share information about you and your BitPay account with third parties, including but not limited to your bank and purchasers.

**Our Ownership of the Services and the BitPay Website.** You agree and acknowledge that we own all right, title and interest to and in the Services, the associated software, technology tools and content, the BitPay Web site, the content displayed on the Web site, and other materials produced by and related to BitPay (collectively, the BitPay IP). You are only permitted to use the Services and the BitPay IP to accept and receive payments, according to these Terms. When you accept the Terms, we grant you a personal, limited, revocable and nontransferable license to use the BitPay IP, without the right to sublicense. You shall not rent, lease, sublicense, distribute, transfer, copy, reproduce, download, display, modify or timeshare the BitPay IP or any portion thereof, or use the BitPay IP as a component of or a base for products or services prepared for commercial sale, sublicense, lease, access or distribution. You shall not prepare any derivative work based on the Company IP, nor shall you translate, reverse engineer, decompile or disassemble the Company IP.

**Advertising.** By mutual consent, we may publish your corporate name, artwork, text and logo **(Merchant Content)** on the BitPay Web site and promotional materials to acknowledge you as our customer. You represent and warrant to us that you have the right to provide the Merchant Content to us, and that the use, copying, modification and publication of the Merchant Content by us: (a) will not infringe, violate or misappropriate any third party copyright, patent, trade secret or other proprietary rights, (b) will not infringe any rights of publicity or privacy, and (c) will not be defamatory or obscene or otherwise violate any law.

**Fees & Settlement.**

**Invoice Generation and Exchange Rate Guarantee.** To create an invoice, you may post a request to BitPay to collect a specific amount in your local currency, such as dollars or euros, or in Bitcoin. BitPay will pull the exchange rate and provide the Bitcoin payment instructions to the pur-

chaser. We guarantee the exchange rate to you as long as the purchaser pays within the proper time window after the invoice is created. Invoice timeout information is clearly displayed on each BitPay invoice. While we guarantee the exchange rate as long as the purchaser pays within such time window, you agree that you assume the volatility risk of your local currency or Bitcoin, as applicable. For instance, if you ask us to collect USD $150, and the purchaser sends the payment within the time window, we guarantee you will receive exactly USD $150, minus our fee, but do not guarantee the value of the U.S. dollar.

**Fees.** We charge a processing fee on all transactions. The proceeds payable to you will equal the amount of the invoice (assuming that we have received the full amount of the invoice from the purchaser), unless you agree to accept less than the amount of the invoice, minus the processing fee. We reserve the right to change our fees and will give you 30 calendar days' prior notice of any fee increase. Your continued use of the Services after we notify you of any increase in our fees constitutes your acceptance of such change. Current pricing information is provided on the BitPay Web site at *https://bitpay.com/pricing*.

**Methods of Settlement.** We will clear the payments over the Bitcoin peer-to-peer payment network and post the balance to your accounting ledger, according to your preference settings.

The debits and credits to your accounting ledger are funds temporarily held by BitPay until settlement to your bank account can take place. You can receive a settlement in your local currency, in bitcoins, or in a mixture of both. You assume volatility risks of the currency in which you choose to be settled. If you choose to keep bitcoins, then you assume the volatility risk of the Bitcoin value.

**Settlements in Local Currencies.** Direct deposit to a bank account in a local currency is available to merchants located in certain countries. Please refer to Please refer to *https://bitpay.com/bitcoindirectdeposit* for a list of those countries. If you wish to receive direct deposit, you must provide us with valid bank account information and keep such information current. We will send a direct deposit to your bank account to clear out your accumulated balance. Minimum settlement amounts apply; please refer to *https://bitpay.com/bitcoindirectdeposit* for information related to minimum settlement amounts and deposit frequency.

**Your Bank Account.** You must provide us with written notice at least 1 business day prior to closing your bank account. If you wish to continue to receive direct deposits, you must provide us with information for a substitute bank account. You are solely liable for all fees and costs associated with your bank account and for all overdrafts. You authorize us to initiate electronic credits to your bank account at any time, as necessary to process your transactions. We will not be liable for any delays in receipt of funds or errors in bank account entries caused by third parties.

**Settlements in bitcoins.** Payments in bitcoins are sent to the Bitcoin address of your choice, at least once per calendar day. BitPay does not operate a Bitcoin wallet and funds must be moved to your wallet address.

**Certain Deferrals.** If we need to conduct an investigation or resolve any pending dispute related to your BitPay account, we may delay settlement or restrict access to your funds while we do so. Additionally, we may delay settlement or restrict access to your funds if required to do so by law, court order or at the request of law enforcement.

**Account Statements.** On demand, we will provide you with a statement detailing your account transaction and settlement history. Should you identify an error in the statement, you must notify us of such error within 30 calendar days.

**Refunds and Adjustments.**

**Refund Procedures.** In the event that you wish to issue a refund to a purchaser, BitPay can handle this. You can decide to issue a partial refund or the full amount of the initial purchase.

You can also decide whether to issue the original amount of the invoice in your local currency or in the number of bitcoins paid. If you do not have enough funds in your BitPay account to cover the refund, BitPay may require you to deposit bitcoins into your BitPay account to cover the refund to the purchaser. Any required currency conversion during the refund proc-

ess will be calculated at a spot rate determined by BitPay, following the guidelines found here: *https://bitpay.com/bitcoin-exchange-rates.*

**Disclosure of Your Refund Policy.** Merchants are required to have a clear refund policy for their customers. We recommend you refund the amount of the initial purchase in the currency in which the item was priced.

**Purchaser Complaints.** Purchasers filing complaints about a purchase will be forwarded to you for resolution. BitPay reserves the right to terminate accounts which receive excessive complaints.

**Account Termination.**

**Your Right to Close Your Account.** You may close your BitPay account at any time. You will still be obligated to us for any fees incurred before the closure and we will remit to you funds not yet paid to you and associated with preclosure sales. If your account balance is below our documented minimum transfer amount, you may be responsible for any transactions fees that may be incurred in the funds transfer.

**Our Right to Close or Suspend Your Account.** We may terminate these Terms and close your account, at our discretion, upon notice to you via email or phone communication. We may also suspend your access to the Services if we suspect that you have failed to comply with these Terms, pose an unacceptable fraud risk to us, or if you provide any false, incomplete, inaccurate or misleading information. We will not be liable to you for any losses that you incur in connection with our closure or suspension of your account.

**Effect of Account Closure.** If your BitPay account is closed, you agree: (a) to continue to be bound by these Terms, (b) to immediately stop using the Services, (c) that the license provided under these Terms shall end, (d) that we reserve the right (but have no obligation) to delete all of your information and account data stored on our servers, and (e) that we shall not be liable to you or any third party for termination of access to the Services or for deletion of your information or account data.

**Indemnification.** You agree to indemnify BitPay, its affiliated and related entities, and any of its officers, directors, employees and agents from and against any claims, costs, losses, liabilities, damages, expenses and judgments of any and every kind (including, without limitation, costs, expenses, and reasonable attorneys' fees) arising out of, relating to, or incurred in connection with any claim, complaint, action, audit, investigation, inquiry, or other proceeding instituted by a person or entity that arises or relates to: (a) any actual or alleged breach of your representations, warranties, or obligations set forth in these Terms; (b) your wrongful or improper use of the Services; (c) the products or services sold by you through the Services, including but not limited to any claims for false advertising, product defects, personal injury, death or property damage; or (d) any other party's access or use of the Services with your account information.

**No Warranties.** WE PROVIDE THE SERVICES ON AN "AS IS" AND "AS AVAILABLE" BASIS, AND YOUR USE OF THE SERVICES IS AT YOUR OWN RISK. TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, WE PROVIDE THE SERVICES WITHOUT WARRANTIES OF ANY KIND, WHETHER EXPRESS OR IMPLIED (INCLUDING, WITHOUT LIMITATION, WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NONINFRINGEMENT). WITHOUT LIMITING THE FOREGOING, WE DO NOT WARRANT THAT THE SERVICES (AND OUR WEBSITE): WILL OPERATE ERROR–FREE OR THAT DEFECTS OR ERRORS WILL BE CORRECTED; WILL MEET YOUR REQUIREMENTS OR WILL BE AVAILABLE, UNINTERRUPTED OR SECURE AT ANY PARTICULAR TIME OR LOCATION; ARE FREE FROM VIRUSES OR OTHER HARMFUL CONTENT. WE DO NOT ENDORESE, WARRANT, GURANTEE OR ASSUME RESPONSIBILITY FOR ANY PRODUCT OR SERVCE OFFERED OR ADVERTISED BY A THIRD PARTY THROUGH THE SERVICES OR THROUGH OUR WEBSITE, AND WE WILL NOT BE A PARTY TO NOR MONITOR ANY INTERACTIONS BETWEEN YOU AND THIRDPARTY PROVIDERS OF PRODUCTS OR SERVICES.

**Limitation of Liability.** IN NO EVENT WILL WE BE LIABLE TO YOU OR ANY THIRD PARTY FOR ANY DIRECT, INDIRECT, SPECIAL, INCIDENTAL, CONSEQUENTIAL, EXEMPLARY OR PUNITIVE DAMAGES OR ANY LOSS, THEFT, DISAPPEARANCE, OR DAMAGES FOR LOST PROFITS, LOST REVENUES, LOST DATA OR OTHER INTANGIBLE LOSSES THAT RESULT FROM

THE USE OF, INABILITY TO USE, OR UNAVAILABILITY OF THE SERVICES, REGARDLESS OF THE FORM OF ACTION AND WHETHER OR NOT WE KNEW THAT SUCH DAMAGE MAY HAVE BEEN INCURRED. IN NO EVENT WILL WE BE LIABLE TO YOU OR ANY THIRD PARTY FOR ANY DAMAGE, LOSS OR INJURY RESULTING FROM HACKING, TAMPERING, VIRUS TRANSMISSION OR OTHER UNAUTHORIZED ACCESS OR USE OF THE SERVICES, YOUR BITPAY ACCOUNT, OR ANY INFORMATION CONTAINED THEREIN. IN NO EVENT WILL OUR LIABILITY FOR ANY DAMAGES ARISING IN CONNECTION WITH THE SERVICES EXCEED THE FEES EARNED BY US IN CONNECTION WITH YOUR USE OF THE SERVICES DURING THE 6 MONTH PERIOD IMMEDIATELY PRECEDING THE EVENT GIVING RISE TO THE CLAIM FOR LIABILITY. THE FOREGOING LIMITATIONS OF LIABILITY SHALL APPLY TO THE FULLEST EXTENT PERMITTED BY LAW IN THE APPLICABLE JURISDICTION.

**Miscellaneous.**

**Taxes.** You are responsible for determining any and all taxes assessed, incurred, or required to be collected, paid, or withheld for any reason in connection your use of our software and services (Taxes). You also are solely responsible for collecting, withholding, reporting, and remitting correct Taxes to the appropriate tax authority. We are not obligated to, nor will we determine whether Taxes apply, or calculate, collect, report, or remit any Taxes to any tax authority arising from any transaction.

If in a given calendar year you receive (i) more than $20,000 in gross amount of payments and (ii) more than 200 payments, BitPay will report annually to the Internal Revenue Service, as required by law, your name, address, tax identification number (such as a social security number, or employer identification number), the total dollar amount of the payments you receive in a calendar year and the total dollar amount of the payments you receive for each month in a calendar year.

**Privacy Policy.** Please see our Privacy Policy for information regarding how we collect and use information. The Privacy Policy is part of these Terms, so please make sure that you read it.

**Assignment.** You may not transfer or assign these Terms, or any rights granted by these Terms. You agree and acknowledge that we may assign or transfer these Terms.

**Severability.** Should any provision of these Terms be determined to be invalid or unenforceable under any law, rule, or regulation, such determination will not affect the validity or enforceability of any other provision of this Agreement.

**Waivers.** Our failure to assert any right or provision in these Terms shall not constitute a waiver of such right or provision, and no waiver of any term shall be deemed a further or continuing waiver of such or other term.

**Entire Agreement.** These Terms, including the Privacy Policy referenced herein, represent the entire understanding between us and you with respect to the matters discussed. Headings are included for convenience only, and shall not be considered in interpreting these Terms.

**Notices.** You agree to accept communications from us in an electronic format, and agree that all terms, conditions, agreements, notices, disclosures or other communications that we provide to you electronically will be considered to be "in writing."

**Governing Law; Arbitration.** These Terms will be governed by and construed in accordance with the laws of the State of Georgia without reference to conflict of law or choice of law provisions, and applicable Federal law (including the Federal Arbitration Act). If a disagreement or dispute in any way involves the Services or these Terms and cannot be resolved between you and us with reasonable effort, the disagreement or dispute shall be resolved exclusively by final and binding administration by the American Arbitration Association (AAA), and will be conducted before a single arbiter pursuant to the applicable Rules and Procedures established by the AAA. You agree that the arbitration shall be held in the State of Georgia, or at any other location that is mutually agreed upon by you and us. You agree that the arbiter will apply the laws of the State of Georgia consistent with the Federal Arbitration Act, and will honor and agree to all applicable statutes of limitation. You agree that, unless prohibited by law, there shall be no authority for any claims to be arbitrated on a class or representative

basis, and arbitration will only decide a dispute between you and us. Arbitration proceedings must be initiated within 1 year after the disagreement or dispute arises. If any part of this Arbitration clause is later deemed invalid as a matter of law, then the remaining portions of this section shall remain in effect, except that in no case shall there be a class arbitration.

**Amendment.** We may update or change these Terms from time to time. Except as otherwise provided in these Terms, we will notify you of any changes by electronic mail or by posting a link to the amended Terms on our Web site. If you continue to use the Services after we provide notice of such changes, your continued use constitutes an acceptance of the amended Terms and an agreement to be bound by them. If you do not agree to the amended Terms, you must close your BitPay account and discontinue your use of the Services.

**Force Majeure.** Neither you nor we will be liable for delays in processing or other nonperformance caused by such events as fires, telecommunications, utility, or power failures, equipment failures, labor strife, riots, war, nonperformance of our vendors or suppliers, acts of God, or other causes over which the respective party has no reasonable control; provided that the party has procedures reasonably suited to avoid the effects of such acts.

**Survival.** The provisions of Sections 2.2, 3.3, 3.4, 4.2, 5, 6, 7, 8.1, 8.5, 8.7, 8.8, 9 (including all subsections), 11, 12, 13, and 14.7 shall survive the termination of these Terms.

You agree that the person signing below has the authority to sign the Terms and to bind you, and you acknowledge and agree that you: (a) have read and understand the Terms; (b) intend to form a legally binding contract; and (c) will abide by all the Terms.

## RESPONSE TO WRITTEN QUESTIONS OF SENATOR KIRK FROM JENNIFER SHASKY CALVERY

**Q.1.** I want to start off with a question about the Silk Road. In the case of the Silk Road, it was the FBI that was able to target, and eventually bring down the major players in the case. I have been told that a new "Silk Road" emerged just a month after the former Silk Road was shut down. In fact, the site administrator of this new site who goes by the moniker, "Dread Pirate Roberts" wrote, "It took the FBI two and a half years to do what they did . . . but 4 weeks of temporary silence is all they got".

Can you tell me what, if anything FinCen can and does provide to law enforcement in monitoring illicit actors such as those using the Silk Road? Is there coordination between FinCen, other financial regulators and law enforcement in these cases?

**A.1.** As mentioned in my written testimony, shortly after we issued our March 2013 guidance on virtual currency, FinCEN also issued a Networking Bulletin on crypto-currencies to provide a more granular explanation of this highly complex industry to law enforcement and assist in following the money as it funnels between virtual currency channels and the U.S. financial system. Among other things, the Bulletin addresses the role of traditional banks, money transmitters, and exchangers that come into play as intermediaries by enabling users to fund the purchase of virtual currencies and exchange virtual currencies for other types of currency. The Networking Bulletin has proved especially useful in the context of Silk Road because, as the Department of Justice has alleged, customers of Silk Road were required to pay a decentralized virtual currency to help both the operator of Silk Road and its sellers evade detection and launder hundreds of millions of dollars. Beyond the Networking Bulletin, FinCEN delivers its expertise to law enforcement on an ongoing basis by directly collaborating on criminal investigations, producing an ongoing series of analytical reports, and conducting training on the evolution in thevirtual currency sphere.

Equally important to our ongoing efforts to deliver expertise to our law enforcement partners is FinCEN's coordination with our regulatory counterparts to ensure they are kept apprised of the latest trends in virtual currencies and the potential vulnerabilities they pose to traditional financial institutions under their supervision. In addition, FinCEN plans to work with our law enforcement partners to produce a Webinar on FinCEN requirements for the virtual currency community.

**Q.2.** Is there or should there be a task force within the Administration or between Federal financial regulators to determine what risks are posed by virtual currencies and to contemplate possible coordination and collaboration of efforts?

**A.2.** While not labeled "taskforces," the Administration has established a number of high level virtual currency working groups that encompass the entire spectrum of regulatory and law enforcement agencies with technical expertise in virtual currency benefits, risks, threats, and vulnerabilities. The various working groups studying virtual currencies all approach the topic from different perspectives, which brings together a diversity of mandates, skill sets, and operational concerns on the subject matter. This approach fosters strong coordination and collaboration, and positively challenges opinions and informs the outcome of each working group's findings and deliverables. To help foster this interagency synergy, FinCEN continues to maintain a strong nexus with its external partner agencies in sharing multi-faceted knowledge bases and observations.

**Q.3.** Who do you see as taking the lead role in the U.S. Government in monitoring and reporting illicit activities being done through virtual currencies?

**A.3.** Since the issue of virtual currency is an Administration priority, the Administration itself is already taking a leading role by providing the necessary guidance and direction to ensure all relevant departments and agencies are maximizing their abilities and resources to safeguard the U.S. financial system from illicit activities posed by this emerging payment method. Through this guidance, those agencies at the operational level, such as FinCEN, leverage their equities and expertise to disrupt illicit activities conducted through virtual currencies.

**Q.4.** Knowing that a new "Silk Road" emerged just a month after the former Silk Road was shut down is there a way to ultimately bring down a particular site such as the Silk Road—and to eliminate users from creating another?

**A.4.** Since the circumstances surrounding the Silk Road matter are primarily a law enforcement concern, I would have to defer to my colleagues at the Departments of Justice and Homeland Security for their perspectives on permanently shutting down such criminal enterprises. However, for our part, FinCEN uses its existing regulatory authorities to disrupt and dismantle virtual currency exchanges in relation to and in conjunction with criminal investigations. Such was the case in May 2013, when FinCEN named Liberty Reserve—a Web-based virtual currency provider specifically designed and frequently used to facilitate money laundering in cyber space—as a financial institution of primary money laundering concern under Section 311 of the USA PATRIOT Act. FinCEN also strives to stay current on how money is being laundered in the United States, including through new and emerging payment systems like virtual currency and what investigative resources may be available, so that we can share this expertise with our many law enforcement partners to positively contribute to ongoing and future investigations. We meet this obligation by drawing from the knowledge we have gained through our regulatory efforts, use of targeted financial measures, analysis of the financial intelligence we collect, independent study of virtual currency, outreach to industry, and collaboration with our many partners at all levels of Government.

**Q.5.** There are some academics & policymakers that have suggested that the "Know your Customer" rule should apply to virtual currencies. What are your thoughts on this?

**A.5.** FinCEN's Customer Identification Program (CIP) rule applies to specific types of financial services providers, including depository institutions and securities broker-dealers. Because these entities originate and maintain what can be long-term relationships with their customers, it is imperative that they know who their customers are and the types of transactions that are consistent with their profile. Moreover, we believe that this current CIP rule already acts as an important choke point for virtual currency providers, since as my written statement illustrates, banks are oftentimes either the originating or terminating point for virtual currency transactions.

FinCEN works hard to strike the correct balance between smart regulation and industry burden, and at this time we believe mandating a CIP rule for virtual currency providers would be problematic, both from a privacy and cost/benefit perspective. It would require information collection and retention from every customer, even for one-time transactions, without generating the net tangible benefits realized from CIP obligations borne by other financial institutions.

**Q.6.** Just last week, the Federal Election Commission seriously considered letting candidates and committees accept bitcoins as in-kind contributions. Do you think since this is a Federal agency, that it gives legitimacy to our Government recognizing this virtual currency—or at least bitcoins, as a valid currency?

**A.6.** Since FinCEN's mission and mandate falls outside the scope of monetary policy, as a practical matter we do not offer opinions or perspectives on the validity or legitimacy of Bitcoin or any other virtual currency. However, as a store of value with funds transmission capabilities, FinCEN does focus on Bitcoin's potential to be exploited for money laundering or terrorist financing, and our focus on these vulnerabilities will continue to grow in concert with virtual currency's popularity, acceptance, and expanded use both domestically and internationally.

---

## RESPONSE TO WRITTEN QUESTIONS OF SENATOR KIRK FROM PAUL SMOCER

**Q.1.** Ms. Tunstall notes in her testimony that "virtual currencies could be attractive to large financial institutions if the fees associate with virtual currency transactions, including the exchange fees, are lower than the fees accompanying other payments (*i.e.,* interchange fees). What do you anticipate would give mainstream financial service providers and other electronic payment systems the comfort to enter into the digital currency space?

**A.1.** At this time, we are not seeing financial institutions moving to digital currencies. This can mostly be attributed to the number of potential fraud and security risks due to the lack of oversight of the entities participating in this space. Once the currencies are able to prove their ability to operate in a safe environment with the

ability to mitigate their risks, we may see a move to virtual currencies.

**Q.2.** Do you believe that, as with mobile payments and other new technologies, companies will become more comfortable with digital currencies in other countries before working to adopt them in the United States?

**A.2.** Often the reason these new technologies are adopted in other countries is their lack of banking and consumer protection regulations. This allows companies to experiment more with new technologies. Given the mature regulatory environment in the United States, we are likely to see a delay in the adoption of these types of technologies. Though, by having this delay, we will be able to make sure technologies protect consumers and ensure the safety and soundness of our financial markets.

**Q.3.** Where do you think the financial services industry is in terms of its own understanding, appreciation or lack thereof for virtual currencies?

**A.3.** The financial services industry has watched this market grow since its inception, so I think there is an understanding of virtual currencies. We continue to identify ways to leverage the currency meet consumer needs while ensuring appropriate protections. This we are still trying to understand and will require much more time to make sure we get it right.

**Q.4.** Is there a working group, taskforce or public-private group that industry is participating with to develop best practices or standards? Do you think there is a willingness of industry to participate with Government on such taskforces to study and better understand how to promote the good within the industry and further hamper the bad?

**A.4.** I am not aware of any existing efforts to develop best practices or standards. The sector would be willing to participate with the Government as this area expands. We'd be happy to facilitate any discussion that may need to take place.

---

**RESPONSE TO WRITTEN QUESTION OF SENATOR KIRK FROM SARAH JANE HUGHES**

**Q.1.** In your testimony, you recommend that we retain the current division of regulation between the States and the Federal Government—with prudential regulation of the nondepository providers of new payments systems with the States and retaining the anti-money laundering, anti-terrorism and economic sanctions regulations with the Federal Government. How do States ensure that they are coordinating the oversight of these new developing industries with other States and also that the Federal Government is able to track the illicit activities in new technologies such as virtual currencies?

**A.1.** Thank you, Senator Kirk, for this interesting question.

I remain persuaded that the current division of regulatory authority between the States and Federal Government that I mentioned in my testimony is the correct alignment of responsibilities for licensure, supervision and examination of nondepository pro-

viders, including providers of virtual currencies. Looking back at the record that FinCEN has had over the past decade in connection with the regulation of emerging payments systems for AML purposes, FinCEN has shown a careful development and articulation of standards for stored value devices and, more recently, for virtual currencies. I certainly think, and FinCEN Director Jennifer Calvery Shasky did not dispute, that FinCEN has all of the authority it needs to continue to monitor, supervise and issue guidance for virtual currencies consistent with its mandate from Congress. Although no representative from OFAC testified at the November 19, 2013 hearing, based in part on my knowledge of and confidence in OFAC's remarkable staff, I would think OFAC also has all of the authority it would need to handle the enforcement of economic sanctions against any virtual currency provider or exchange that violated U.S. economic sanctions law.

The prudential regulation of nonbank providers of financial products and services has long been the province of the States. The States generally assign responsibility for prudential regulation and supervision of nonbank providers to the same agency or department that serves as the prudential regulator for State-chartered banks and credit unions, as well as nondepository providers. In Illinois, the Department of Financial & Professional Regulation has responsibilities for all of these providers. In Indiana, the Indiana Department of Financial Institutions performs these functions. And, in New York, the newly renamed Department of Financial Services, has these responsibilities, as well as prudential regulation and supervision of insurance companies.

These departments and agencies have powers—not unlike those of Federal bank regulators—to examine the books and records of the providers they license and to impose corrective action measures on their licensees that are comparable to the powers exercised by Federal bank regulators. They also tend to have more "boots on the ground" and regular contact with nondepository providers than a Federal agency is likely to provide. This was made clear to me early in my career when I worked for the Federal Trade Commission, which had jurisdiction over 1.5 million nondepository providers of consumer credit products, including a far more decentralized consumer credit reporting industry than today, and about 20 attorneys nationwide to handle their compliance with Federal consumer credit protection laws.

The various State regulators work bilaterally and regionally with each other and have for many decades, including their regional compacts that presaged interstate banking and branching in the 1980s. At the national level, the widely regarded Conference of State Bank Supervisors with which Members of the Committee are familiar provides a variety of services to State bank supervisors. Prominent among their more recent services is a multi-State licensing service, in response to the Secure and Fair Enforcement of Mortgage Licensing Act of 2008 (SAFE Act), that handles licensing of mortgage originators and additional types of nondepository providers at the request of the States. States have been joining this service in the past year, and not only for mortgage originators but also for other nondepository providers. With the type of successes

this program has had, I am firmly of the view that Congress should not fix what is not broken.

Moreover, and thinking specifically about virtual currencies, without a widespread adoption of a payment system—and virtual currencies are not yet widely adopted—it is too early to add regulatory requirements for them. A more measured approach, such as FinCEN has taken with respect to its guidance to virtual currency participants in 2013 and 2014, has the benefit of addressing emerging areas of concern in a new payment mechanism and allowing suitable innovations to occur. The current approach—of registration with FinCEN and licensure from the States—is more than adequate regulation of the emerging field of virtual currencies at this time in my opinion. FinCEN's work is complemented by State "money transmitter" licensing and prudential regulation for providers of virtual currencies, mobile payments, and PayPal, just to name a few examples with which readers of the hearing's proceedings are likely to be familiar.

Several reporters have pressed me for ideas about what types of "consumer protections" Congress should adopt for virtual currencies. I have told each what I said in my prepared testimony: that it is early days for regulating virtual currencies for consumer protection purposes beyond the FinCEN and State-based regulations already in place. I would expand my prepared testimony to highlight that "early days" occasionally last a long time. For example, travelers' checks were first issued about 100 years ago. Only in the 1980s did the States begin to include them under State payments law, their versions of Article 3 of the Uniform Commercial Code. Similarly, "wire transfers" closely followed the advent of the telegraph but were not governed by law—as opposed to bilateral contracts or system rules until the 1980s.

Additionally, so far, we have few examples of problems with bitcoins transactions. This was truer 6 months ago than it is today—following announcement of exchange closures or disappearances, or of freezes on withdrawals for customers by exchange operators.

In the United States, and also elsewhere in the world, governments have decades of examples of ways to regulate payments, including electronic payments. So, I would like to see us use existing laws and frameworks, including system rules, bilateral contracts, and State law prudential regulation as well as the steps FinCEN has already taken before we write new rules for currencies that, like those of the mid-1990s, might sound great today and be gone tomorrow.

Last, if the United States were to move beyond our current mix of registration with FinCEN and compliance with licensure and prudential regulation by the States, and whatever bits of "law" in the United States cover the type of problem being seen, we may have to recognize that a domestic solution may not suffice in an arena that includes significant players abroad. With more than 50 percent of the bitcoins held in exchanges whose "locations" are abroad, domestic consumer protections could prove too difficult for consumers to enforce, but their expectations of enforcement help would have been raised.

**RESPONSE TO WRITTEN QUESTIONS OF SENATOR KIRK FROM ANTHONY GALLIPPI**

**Q.1.** Is BitPay synonymous with a Paypal but for Virtual Currency?

**A.1.** BitPay is strictly a merchant service, so a better analogy would be the "First Data" or the "Authorize.net" of virtual currency. BitPay does not have any consumer facing products. The company only clears and settles payments for merchants who want to accept virtual currency as a payment option.

**Q.2.** Is BitPay registered as a Money Service Business (MSB) with FinCen?

**A.2.** FinCEN's guidance that "virtual currency" is a type of money and should be treated like "real currency" is a step in the right direction. We have always worked under the impression that virtual currency is money, so we are glad that FinCEN now agrees with that position.

The heart of FinCEN's guidance recommends that activities which are classified as Money Services Businesses (MSB) or Money Transmission Businesses (MTB) should be applied equally to both real currency and virtual currency. Therefore activities such as remittance and check cashing would be regulated whether the type of money is real or virtual.

We should pay close attention to footnote #10 of the March 2013 FinCEN guidance, which states:

> 10 FinCEN's regulations provide that whether a person is a money transmitter is a matter of facts and circumstances. The regulations identify six circumstances under which a person is not a money transmitter, despite accepting and transmitting currency, funds, or value that substitutes for currency. 31 CFR § 1010.100(ff)(5)(ii)(A)–(F).

Looking up the six exemption circumstances in 31 CFR § 1010.100(ff)(5) will return the following:

(ii) Facts and circumstances; Limitations. Whether a person is a money transmitter as described in this section is a matter of facts and circumstances. The term "money transmitter" shall not include a person that only:

(A) Provides the delivery, communication, or network access services used by a money transmitter to support money transmission services;

**(B) Acts as a payment processor to facilitate the purchase of, or payment of a bill for, a good or service through a clearance andsettlement system by agreement with the creditor or seller;**

(C) Operates a clearance and settlement system or otherwise acts as an intermediary solely between BSA regulated institutions. This includes but is not limited to the Fedwire system, electronic funds transfer networks, certain registered clearing agencies regulated by the Securities and Exchange Commission ("SEC"), and derivatives clearing

organizations, or other clearinghouse arrangements established by a financial agency or institution;

(D) Physically transports currency, other monetary instruments, other commercial paper, or other value that substitutes for currency as a person primarily engaged in such business, such as an armored car, from one person to the same person at another location or to an account belonging to the same person at a financial institution, provided that the person engaged in physical transportation has no more than a custodial interest in the currency, other monetary instruments, other commercial paper, or other value at any point during the transportation;

(E) Provides prepaid access; or

**(F) Accepts and transmits funds only integral to the sale of goods or the provision of services, other than money transmission services, by the person who is accepting and transmitting the funds.**

We have highlighted exemptions (B) and (F) which describe the activities performed by BitPay. The IRS has defined rules for classifying Payment Processors, or Payment Settlement Entities (PSE) in 2008 with the Internal Revenue Code 6050W. This ruling and others clearly state that Payment Processors and Payment Settlement Entities are not Money Transmitters.

BitPay has a contractual agreement with our sellers for transaction processing, clearance, and settlement of funds that arrive for a given merchant account. BitPay does not have any contractual agreement with any sender of funds, and does not engage in any activities that would be considered Money Transmission activities.

**Q.3.** You are obviously on the forefront of these technologies—do you think that it is the anonymity or the privacy that is so attractive to virtual currencies? Would it not make more sense to ensure privacy (account information, *etc.*) but not grant total anonymity? Where is the industry heading on the issue of anonymity?

**A.3.** Bitcoin transactions and the Bitcoin network operate differently than traditional banking products. With a traditional banking product, the user expects a level of privacy where their bank is not broadcasting all of the users transactions to the outside world. With Bitcoin, every transaction is broadcast to the whole world, and remains public record on the Bitcoin blockchain indefinitely. The public blockchain is the cornerstone of Bitcoin.

Because every transaction is public record, users of Bitcoin must maintain their privacy. This is important for both individuals and businesses. For example, if a company is paying one of their suppliers with bitcoin, the company will not want their competitor to be able to reverse engineer their funds flows. Another example is an employee that receives payment from his employer in bitcoin has an expected level of privacy where his employer cannot see where the money is spent.

Given all of the benefits of bitcoin and virtual currencies, we think that the anonymity is not the main factor driving its adoption (because it is not really anonymous). All of our businesses clients prefer bitcoin because it is a far lower risk and lower cost form

of payment, compared to credit cards and the other options they have today.

**Q.4.** Ben Lawsky, the Superintendent of the NY Department of Financial Services was recently interviewed talking about the hearing that his department planned to hold on reviewing interconnection between money transmission regulations and virtual currencies and possibly considering a "BitLicense" specific to virtual currency transactions and activities. While he said that he did not think that this license and regulation would kill the industry he also noted that it was not his intent. Do you think that this is something that would potentially kill or severely impede this industry?

**A.4.** Money Transmission activities are currently regulated by the States. I think the existing laws are adequate. If a company is doing Money Transmission or Money Service activities, they need a license. If they are not doing those activities, they do not. The key criteria to determine whether an activity is considered money Transmission, as outlined by FinCEN and the States, covers two requirements: 1) is the consumer at risk of loss? and 2) is the product coming out the other end a form of money or currency? In addition, I feel that any type of license that would be discriminatory toward one type of business would probably impede the industry.

**Q.5.** While Tor was created by the U.S. Government and has been used in the past for good purposes—such as anonymizing financing of revolutions against tyrannical oppressive regimes, do you believe that it (Tor) is still necessary?

**A.5.** We believe Tor has a right to exist and people have the choice to use that product or use a different Web browser.

**Q.6.** Just a little over a week ago, there was a report from an Australian man that he had 4,100 bitcoins, worth more than $1.1 million, stolen from him. This alleged theft is one of the largest since Bitcoin was created 4 years ago. I know that Bitcoin developers and others have worked to put into place safe guards and have worked to prevent incidents such as this—but with this recent event can you tell us how progress on that front is going?

**A.6.** The security around Bitcoin is extremely important. New features such as multi-signature transactions will greatly reduce the risk of thefts. With a multi-signature transaction, funds are locked with a minimum of 3 keys (could be more) and a minimum of 2 keys are required to move the funds. If a hacker were to gain access to one private key, they could not steal the funds. We believe the technical solution of multi-signature will solve this problem, and I expect its use to be more widespread in 2014, reducing thefts.

**Q.7.** Is there a working group, taskforce or public-private group that industry is participating with to develop best practices or standards? Do you think that there is a willingness of industry to participate with government on such taskforces to study and better understand how to promote the good within the industry and further impede the bad actors?

**A.7.** We share the Committee's goals to develop best practices and prevent the bad actors from using our service. Many lessons and practices from the banking and credit card industry apply to vir-

tual currencies, and those practices are being adopted. There are several groups that are working to bring these experiences into the startup companies: The Bitcoin Foundation and DATA are two that our company is involved with. I believe the many years of experience that our banks and processors have in compliance and antimoney laundering policies will greatly assist the startup companies.

# Additional Material Supplied for the Record

WRITTEN STATEMENT OF

AARON J. GREENSPAN
CHIEF EXECUTIVE OFFICER, THINK COMPUTER CORPORATION

BEFORE THE

U.S. SENATE COMMITTEE ON BANKING, HOUSING AND URBAN AFFAIRS

NOVEMBER 19, 2013

Mr. Chairman and members of the Committee, thank you for this opportunity to contribute my thoughts on a topic that I believe is of great importance to our nation's economic future.

**Introduction**

I am the founder of a startup technology company located in Mountain View, California called Think Computer Corporation ("Think"). Think began developing its patented FaceCash® mobile payment system, which uses a digital image of a consumer's face to reduce fraud and lower interchange fees at the point of sale, in 2009.[1] FaceCash was operational at a number of retail merchants in the Bay Area until July 1, 2011, when Think was forced to shut it down due to passage of the California Money Transmission Act ("MTA"), one of approximately forty-seven state money transmission laws ("MTLs") implicitly authorized by Congress pursuant to 18 U.S.C. § 1960 ("Section 1960"), an anti-drug statute introduced in 1992 long before the commercial internet—let alone mobile payments or virtual currencies—even existed. Section 1960 has since been updated by the USA PATRIOT Act to address concerns regarding terrorism, but not technology.

[1] Think does not have venture capital backing, which became a material factor as the controversy described herein developed. I was fortunate enough to attend Harvard College from 2001-2004, where I designed and developed the predecessor to Facebook, Inc. Think reached a confidential settlement agreement with Facebook, Inc. in 2009. Since then, I have also spent time as a CodeX Fellow at Stanford Law School's Center for Legal Informatics.

With its new authority under Section 1960 and the MTA, the California Department of Financial Institutions ("DFI", since merged into the California Department of Business Oversight, or "DBO") required me to appear at a mandatory pre-application interview at the DFI's San Francisco offices after I made a timely inquiry about the process of applying for a license. At that meeting, the Deputy Commissioner for Money Transmission, Robert Venchiarutti, threatened both Think and me personally in a variety of ways, including incarceration, thanks to my questions about the new law and an unwritten departmental standard (what the California Office of Administrative Law calls an "underground regulation"). The Deputy Commissioner strongly implied that he would refuse to grant Think a license under the MTA, which would cause Think to violate the law if it continued to operate FaceCash. Even after protracted attempts—including appeals to DFI's parent agency, the Governor of California, both houses of the California legislature, and Congress—to secure the information necessary to apply for a license, such as the *true* (and still unwritten) capital requirement under the new law, Think was unable to determine the DFI's demands, and Think eventually filed a federal lawsuit against the Governor of California and the DFI in November, 2011. The lawsuit is still pending.[2] All of Think's employees were laid off.

To be clear, FaceCash was a legitimate and well-received initiative about which no complaints were ever filed with any agency, state or federal. FaceCash did not and does not make use of bitcoin or any other so-called virtual currencies. At the time that this dispute arose over the MTA's requirements, FaceCash could only be used to process United States Dollars, which was a deliberate decision on my part to minimize financial risk. Nonetheless, as has been clarified by FinCEN Guidance FIN-

---

[2] See https://www.facecash.com/legal/brown.html for correspondence regarding Think's attempts to obtain a license under the MTA, and http://www.plainsite.org/flashlight/case.html?id=716056 for the latest docket information concerning the lawsuit, Case No. 5:11-cv-05496-HRL in the Northern District of California. Think has been waiting on Magistrate Judge Howard R. Lloyd to rule upon the State of California's motion to dismiss for 643 days—nearly two years—as of the date of this hearing. In the motion hearing on April 17, 2012, Judge Lloyd remarked, "I think that the situation cries out for some more legislative solution."

2013-G001 issued on March 18, 2013, the same state MTLs apply to virtual currency operators as apply to money transmitters running mobile payment systems. Therefore, the discussion about bitcoin and virtual currency really boils down to a discussion of the effectiveness of state MTLs and Section 1960, which authorizes them.

FaceCash could have been of immense benefit to businesses, consumers and government had it been allowed to flourish, and it can still be with appropriate legislative action. A modern replacement for plastic payment cards that makes point of sale transactions more secure, FaceCash is more convenient and less expensive than just about any other payment system. In place of the traditional card signature on the back of the card, a digital image of the consumer's face is used to verify identity, and because Think developed its own network based on modern technologies, there is no need to use the aging plastic card technology infrastructure, saving on costs. Importantly, FaceCash can capture line item-level transaction data, which even the most exclusive and expensive plastic payment cards cannot. This alone has enormous implications for businesses large and small, who could use such data to automate accounting functions, including tax preparation.

## I. Problems with State Money Transmission Laws Generally

### A. The State Money Transmission Patchwork Protects Large Financial Companies, While Disproportionately Harming Low-Income Consumers and Small Businesses Through the Imposition of Monopoly Pricing

Setting out the nominal purpose of the MTA, which is generally no different from that of other states' money transmission statutes, California Financial Code § 2001(d) states:

> "To protect the interests of consumers of money transmission businesses in this state, to maintain public confidence in financial institutions doing business in this state, and to preserve the health, safety, and general welfare of the people of this state, it is necessary to regulate money transmission businesses in this state."

This text was drafted by a lobbying group comprised of several multi-billion dollar financial

institutions calling itself The Money Services Round Table ("TMSRT")[3], acting through its chief lobbyist, Ezra Levine (formerly of the defunct Howrey LLP, now with Morrison & Foerster LLP), with the additional frequent help of the California DFI. According to TMSRT's August 18, 2006 comment letter to FinCEN and the Federal Reserve System, the members of TMSRT are, "the leading national non-bank funds transmitters in the United States including:Western Union Financial Services, Inc., MoneyGram International, Travelex Currency Services, Inc., Integrated Payment Systems, American Express Travel Related Services, RIA Financial Services, Comdata Network, Inc. and Sigue Corporation."[4]

For roughly the past decade, Mr. Levine has literally made it his business to pass laws similar to the MTA in states throughout the nation, slightly modifying them in each instance to suit the particular fears of state legislators and bureaucrats—but most of all, to suit the needs of his clients, the member companies of TMSRT. According to Mr. Levine's biography as prepared for the 2006 Global Consumers Money Transfer Conference, "He has had an active role in the enactment of the money transmitter laws in Oregon, Minnesota, Washington, Iowa, West Virginia, Illinois, Wyoming, North Carolina, Florida, Idaho, North Dakota, New Jersey, Tennessee, Maine, Vermont, Arizona, the District of Columbia and Indiana." Since that biography was written, he and his clients have also succeeded in constructing unconstitutional laws in Hawaii, and now, California.

As concerned as these multi-national conglomerates may be about consumers—and there is no evidence whatsoever that they actually are concerned—they are also clearly concerned about themselves, which is why they pay Mr. Levine to ensure that no new competitors with more advanced technologies are permitted to enter the payment industry and render their overpriced

---

[3] TMSRT, formerly known as the Non-Bank Funds Transmitters Group, was the sole sponsor of the MTA.

[4] According to a February 22, 2001 comment letter, members of the Non-Bank Funds Transmitters Group at that time also included Citicorp Services, Inc. and Thomas Cook, Inc.

services obsolete. In other words, the thinly-veiled core purpose of modern MTLs is economic protectionism, and nothing more.

The effects of money transmission laws are mostly felt by low-income consumers, and especially immigrants, who have almost no choice but to patronize members of TMSRT when they send or receive money from foreign countries. The prices of funds transfers and currency conversion are considerably higher than they would otherwise be due to these laws.[5]

The laws also have a disproportionate effect on small businesses, who lack the bargaining power necessary to force credit and debit card issuers to lower interchange fees. This problem has recently been so pronounced that Congress enacted the Durbin Amendment to the Dodd-Frank Wall Street Reform and Consumer Protection Act of 2010 to lower debit (but not credit) card interchange fees, perhaps not fully realizing the role of state laws in contributing to the unusual upward trend in interchange pricing. The most promising new payment models that compete with credit and debit cards necessarily involve money transmission.

Of course, when businesses are forced to charge higher prices to cover their payment processing costs, as many often do, average consumers end up hurt as well. In a time of economic instability, this is most unfortunate.

### B. Member Companies of TMSRT, Which Sponsored Several MTLs, Have Repeatedly Engaged in Criminal Activity Involving Money Transmission, Illustrating the Ineffectiveness of MTLs

On November 9, 2012, the United States Department of Justice ("USDOJ") filed criminal felony charges against MoneyGram International, Inc. ("MoneyGram") in Pennsylvania Middle District

[5] See "New Rules for Money Transfers, but Few Limits," Jessica Silver-Greenberg, *The New York Times*, June 1, 2012, http://www.nytimes.com/2012/06/02/business/new-rules-for-money-transfers-but-few-limits.html.

Court, Case No. 1:12-cr-00291-CCC.[6] MoneyGram is one of approximately six members of TMSRT, the lobbying group that was the sole sponsor of the MTA. The USDOJ accused MoneyGram of perpetrating a fraud costing the American public approximately $120 million over a period of almost a decade. Three weeks after the USDOJ filed charges, MoneyGram agreed to settle the allegations for $100 million. A division of MoneyGram, MoneyGram Payment Services, Inc., is still in possession of California Money Transmission License No. 1910 despite the USDOJ's serious allegations. In fact, no state regulator of money services businesses has ever taken any action at all against MoneyGram as a result of this nationwide fraud.

Similarly, in 2008, Sigue Corporation, another member of TMSRT, entered into a deferred prosecution agreement with the USDOJ and agreed to forfeit $15 million due to Bank Secrecy Act violations.[7] Despite these serious transgressions, it still possesses California Money Transmission License No. 2062.

These alleged criminal actions and the resulting federal investigations reinforce three points. First, state regulators have effectively failed to enforce the laws they are charged with enforcing. Second, the federal government is in a far better position to investigate and regulate money transmission activity, both because the federal government has more resources, and because money transmission by its very nature crosses state lines. Third, in addition to being unconstitutional on their face and as applied, state MTLs are ineffective at both preventing illegal activity and protecting consumers. This is especially evident now that a number of well-publicized failures of and thefts from bitcoin exchanges have transpired. In effect, the state MTL patchwork forces consumers into the arms of criminals, some of whom are rich enough to possess licenses, but most of whom are not.

---

6 See http://www.plainsite.org/flashlight/case.html?id=2334104 for docket information.

7 See http://www.justice.gov/opa/pr/2008/January/08_crm_068.html for more information.

### C. Direct Conflicts with the United States Constitution in the Internet Age

Since the pioneers of traditional money orders began moving funds from place to place in the nineteenth century, the country has changed considerably. Today, the internet permits instant electronic funds transfers that until recently were inconceivable. Virtual currencies such as bitcoin are merely the latest iteration in the long history of electronic funds transfer, but are hardly novel from an accounting or regulatory perspective. Bitcoin's main notable attribute is the nature of its supply, which is to say that it is obtained through so-called "mining," or the computation of mathematical problems of increasing difficulty. Regulation comes into play because once mined, even despite the lack of a central authority to govern supply (which is fixed instead), a bitcoin can be exchanged for value electronically over the internet, just like a dollar on FaceCash or PayPal.

MTLs started to come into being on a state-by-state basis in the 1960s in response to localized crises involving fraud. Federal law bolstering those state laws, in the form of 18 U.S.C. § 1960, came into being in 1992 as part of H.R. 5334, the Housing and Community Development Act.[8] It was not until 1995 that the National Science Foundation allowed the commercialization of the internet, meaning that the majority of today's regulatory regime concerning money transmission is obsolete, failing to account for massive changes in market conditions.

Fundamentally, in an environment where money can and often does change hands electronically in the blink of an eye, whether across a distance measured in feet or thousands of miles from coast to coast, there is no role for state regulation. According to Article I, Section 8, Clause 3 of the United

[8] Before and after the creation of 18 U.S.C. § 1960, several attempts were made in Congress to pass legislation that would have directed states to standardize money transmission laws, with the Treasury reporting to Congress on their progress. Such language is found in § 10 of H.R. 26, the Money Laundering Enforcement Amendments of 1991 ("Uniform State licensing and regulation of check cashing services."); § 7 of H.R. 3235, the Money Laundering Suppression Act of 1994 ("Uniform State licensing and regulation of check cashing, currency exchange, and money transmitting businesses."); and Title IV, § 407 of H.R. 3474, the Community Development Banking Act of 1994 (identical heading). Some of these bills passed in the House or the Senate, but not both simultaneously.

States Constitution (commonly referred to as the Commerce Clause) and court decisions rendered relatively recently such as *American Libraries Assn. v. Pataki*, 969 F. Supp. 160 (S.D.N.Y. 1997), it is within Congress's purview—and only Congress's purview—to regulate internet commerce.[9] The reason why can be illustrated with a simple analogy.

Commercial air traffic is regulated by the Federal Aviation Administration (FAA) because air travel almost by definition requires that aircraft cross state borders, and sometimes, international borders as well. Until the advent of the Global Positioning System, it was not always immediately clear which state a particular aircraft was in at any given time. Had states insisted on regulating the skies, airlines and pilots would have been subject to a system of regulatory chaos, endangering the lives of passengers.

Today, commercial internet traffic involving payments (also known as money transmission) is regulated by precisely such a system of regulatory chaos.[10] Virtual currencies aside, it is frequently unclear where a given sender or recipient of funds is physically located, even with available Internet Protocol (IP) address information; it is furthermore difficult to determine where the funds themselves, which are symbolic representations of value, are physically located. This problem is

---

[9] Although Congress is permitted to delegate its authority to regulate commerce to the states, and Congress may have done so implicitly via 18 U.S.C. § 1960, its delegation power is curtailed by the fact that for purposes of regulation, the internet is a "national preserve." *American Libraries Assn. v. Pataki*, *supra*. Even if delegation to the states did occur, it took place three years before the existence of the modern internet, which has come to dominate money transmission—especially those "emerging" forms of money transmission the MTA now restricts. (FaceCash, in fact, completely *depends* upon the internet to transfer the image of each consumer's face to internet-connected cash registers.) Although Congress's delegation may have been legitimate in 1992 when it was hardly considering mobile payments, the heavy involvement of internet traffic today makes any supposed delegation presently unconstitutional.

[10] On June 21, 2012, Mr. Levine *and* one of his clients, Western Union, each appeared before the United States House Committee on Financial Services at a hearing entitled, "Safe and Fair Supervision of Money Services Businesses." The attorney-client relationship was not explicitly disclosed, nor were any technology companies heard from. At the hearing, both Mr. Levine and his client lamented the absurd complexity of the regulatory system that they built, and unsurprisingly encouraged Congress to do nothing but further entrench the role of the states.

exacerbated by the steady march of internet-enabled devices in the direction of mobility. Cellular mobile devices rely on networks with pooled IP addresses that do not reveal the location of a user. (Every iPhone and Android device on the Sprint network appears to be in Kansas, for example. BlackBerry traffic worldwide often seems to originate in Canada.) In addition, TCP/IP packets representing transactions cross multiple state lines routinely within milliseconds, millions (if not billions or trillions) of times per day. Accordingly, the burden on emerging money transmitters, who must comply with the arcane and anachronistic regulations of some forty-seven geographies who are themselves scarcely able to monitor such activity, is immense. The only way to effectively monitor a modern-day money transmitter is in real-time, electronically, which not one government agency actually does.

Therefore, states lack not only the legal jurisdiction and authority to regulate money transmission in the modern world; they also lack the expertise and equipment necessary to track it. That is part of the reason why some states that have MTLs have long admitted to prospective applicants that they do not even bother enforcing them unless an applicant has a physical presence in the state.

### D. Wasteful Spending

On average, no state has more than one hundred registered money transmitters. (According to the DBO web site, California has roughly sixty-five, a relatively high number given the number of publicly-traded technology companies in the state. Of those sixty-five, nine are now or at some point have been connected to TMSRT.) Despite the small scale of each state's licensing program, each money transmitter is subject to a complex litany of requirements that the state agency charged with enforcing the law must monitor. Such monitoring, usually conducted quarterly, requires manpower, and that manpower costs money.

Furthermore, due to the sweepingly broad scope of MTLs and the aforementioned constitutional

issues, keeping such laws on the books requires funding for state Attorneys General to defend against lawsuits challenging their validity. As previously mentioned, Think is presently engaged in one such federal lawsuit against the California DBO. Even though the MTA was largely written by enormous financial conglomerates, the law is actually defended by the California Attorney General *using taxpayer dollars*, making the extra budgetary strain on the state government particularly egregious. In effect, the large financial institutions (whose own legal budgets are plenty large) have figured out a way not only to protect their own economic interests, but to charge the taxpayer and the state for defending those interests in court as well.

Laws that cost society more than they benefit society fail the test for constitutionality set out by the Supreme Court in *Pike v. Bruce Church, Inc.*, 397 U.S. 137 (1970). Here, the costs of money transmission laws are felt by countless consumers, businesses, and state governments. The benefits accrue to less than ten companies.

For all of these reasons, the Commerce and Consumer Affairs Committee of the State of New Hampshire House of Representatives recently concluded a study of a bill, H.B. 1700 (2012) that would completely repeal that state's own money transmission law, Chapter 399-G. As of October 2, 2012, the bill to repeal the law has been recommended for legislation in 2013 by a vote of 8 in favor, 3 against.

Before Mr. Levine and local attorney Marvin S.C. Dang began their extensive lobbying efforts in Hawaii on behalf of TMSRT in 2006, the Auditor of the State of Hawaii issued a report to the Governor and the Legislature of that state entitled, "Sunrise Analysis: Money Transmitters," regarding H.B. No. 2428 of the 2004 Regular Session. The report's conclusion was clear: "Money transmitters pose little risk of harm to consumers and the public. Some protections already exist, and regulation would likely benefit certain money transmitters more than consumers. We conclude that the bill

should not be enacted."

Once TMSRT's Act 153 was signed anyway in 2006, the *Honolulu Star Bulletin* wrote about the new law, which was passed without Mr. Dang being able to cite even a single complaint about money transmitters:[11]

> "Sen. Gordon Trimble (R, Downtown-Waikiki) cast the sole dissenting vote against Hawaii's first regulation of the money transmitters industry because he said he felt it would raise costs for consumers and put some small operations out of business.
>
> 'Many people chose to use unregulated money transmitters because they provide better service for a lower price,' said Trimble, who first got exposed to the cottage side of the industry while serving as a peace corps volunteer in the Philippines. 'This legislation is only going to force people to pay a lot more to send money home.'"

Today, as residents of the Philippines suffer the cataclysmic aftermath of Typhoon Haiyan, it costs more for Americans to send them much-needed funds than it otherwise would have, thanks to TMSRT's MTL.

Bitcoin exchanges especially are more risky than typical money transmitters because the use of bitcoin is presently limited for the most part to extremely high-risk goods and services such as gambling and illegal drugs. By design, bitcoin is also decentralized, which means that like cash stuffed in a mattress or a poorly-protected vault, it can easily disappear. Not a single bitcoin exchange is properly licensed nationwide in each state with MTLs; most exchanges have no state licenses at all. Many are located overseas to avoid MTLs entirely. This does not mean that all money transmitters are inherently high-risk or that bitcoin's risk profile will never change (it may or may not for a host of reasons). Rather, bitcoin's high risk profile should be viewed as the symptom of an ailing and outdated regulatory structure unable to adapt to changes in the market. If anything, bitcoin proves the need for a comprehensive federal money transmission regulatory framework that does

---

[11] See "New law regulates transmitters of money," Allison Schaefers, *Honolulu Star Bulletin*, June 7, 2006, http://archives.starbulletin.com/2006/06/07/business/story02.html.

not increase the risk to consumers by driving new technologies underground or out of business, and that is capable of keeping up with quickly-changing technological trends, whether they involve bitcoin or something new.

### E. Distortions in the Competitive Market for Payments

#### 1. Spotty Enforcement Causes a Tilted Playing Field

Except on extremely rare occasions, state agencies rarely take action against unlicensed money transmitters. If they do take action, not all states bother, because doing so would be require duplicative effort, and they instead allow one state agency to take the lead. This model is nonsensical. Even with coordinating groups such as the Money Transmission Regulators Association (MTRA) in place, it means that the same entity is often monitored by more than forty separate agencies so that only one may ultimately act, almost at random. State regulators proudly declare this to be evidence of coordination; really, it is evidence of a broken system with gaping holes that allows financial fraud and narcotics trafficking to go undetected.

It has been well known for years in the payments community that Dwolla, Inc., a company that purports both to be an "agent" of a credit union in Iowa, which it is not,[12] and a "mobile payments" company, which is true only from a purely technical perspective, mostly facilitated the exchange of bitcoins which were frequently used for illegal activity, such as buying and selling drugs on underground Tor sites such as The Silk Road. Not a single state regulator has ever taken any action against Dwolla, Inc., although the State of New York Department of Financial Services did issue Dwolla, as well as many other bitcoin-related entities, subpoenas in August, 2013 due to their lack of compliance with MTLs, which caused Dwolla to abandon its involvement with bitcoin as recently

[12] See "Dwolla, Veridian CU Describe and Defend Their Strange Symbiosis," Bailey Reutzel, *PaymentsSource*, November 6, 2012, http://www.paymentssource.com/news/dwolla-veridian-cu-describe-and-defend-their-strange-symbiosis-3012326-1.html?zkPrintable=1&nopagination=1, also available at http://www.themembersgroup.com/news/tmg-in-the-news/dwolla-veridian-cu-describe-and-defend-their-strange-symbiosis/.

as October 28, 2013. Think is actively engaged in an unfair competition lawsuit[13] against Dwolla and many of these entities, which have, with the help of their venture capital and angel investors, knowingly exploited the regulatory chaos to profit from as much illegal activity as possible.

### 2. Investors Who Cheerlead and Profit From Criminal Activity

Some of these investors have been forthright about their views on financial regulation: they believe that MTLs are simply a game where the potential rewards of "winning" far outweigh the costs. At an invite-only dinner that was videotaped, Marc Andreessen, principal of the leading venture capital firm Andreessen Horowitz that has invested millions upon millions of dollars in illegal money services businesses, gleefully recalled the advice of his lawyer on the topics of bitcoin and its regulators, "The good news is they're going over who gets to regulate it. Um, and so your job is to *sneak through the fight*, while they're battling it out to see who's in charge!" (emphasis added). Laughter ensued.[14]

Yishan Wong, an early PayPal, Inc. employee well-versed in the complexity of MTLs, Chief Executive Officer of Reddit, and an angel investor in at least one money services business, stated publicly on March 2, 2011, "if you are a startup who feels that the violation of a law (or an excursion into a grey and questionable/undefined area of the law) will allow you to create a business that provides enormous value to people, the tactically wise thing to do is to move forward and try to build the business. Moreover, if your business is not doing something morally egregious (e.g. killing people) but simply violating the law in a somewhat more minor way, the officers of the company bear little more risk than the company being sued out of existence..."[15]

Mr. Andreessen's and Mr. Wong's views are shared by an overwhelming majority of wealthy

---

[13] For docket information see http://www.plainsite.org/flashlight/case.html?id=2434524, Case No. 5:13-cv-02054-EJD, Northern District of California.

[14] See http://pandodaily.com/2013/10/03/andreessen-bitcoin-is-like-the-early-internet/.

[15] See Yishan Wong's answer to "Airbnb: Why has Airbnb not been sued or regulated out of existence?", https://www.quora.com/Airbnb/Why-has-Airbnb-not-been-sued-or-regulated-out-of-existence.

technology investors who have placed investments in the most popular brands in the payments space. In private conversations, some have confided that although they believe federal regulation of money transmission is the right and only answer to the problem of inconsistent, ineffective and onerous state MTLs, they will not speak up, effectively because the potential profits to be made from simply ignoring the current, broken system are too lucrative to sacrifice. The fact that consumers and their law-abiding competitors are injured by their deliberately unlawful approach does not concern them in the least. The message from these respected investors is clear: success at any cost is fine; laws are for other people.

### 3. "Consultants" Who Were "Regulators" The Day Before

At least in California, it is not a mere coincidence that enforcement of MTLs had been so spotty and lackluster while high-profile startups with millions of dollars publicly announce their intent to violate the law practically weekly. Consulting firms such as Promontory Financial Group lead the way in helping their elite clients evade MTLs. The most glaring example of this was visible on October 17, 2013 when the Financial Women of San Francisco held an event called "New Payments Networks and Virtual Currencies: Are They the Future of Payments?" at which virtual currency entrepreneurs from Ripple Labs, Coinbase and Dwolla presented their views on a panel. (Dwolla cancelled at the last minute.) All three companies, none of which have even applied for a license under the MTA in California (making their founders and investors federal felons), share more than just an interest in financial technology—they also have a common investor: Andreessen Horowitz. The panel's moderator was none other than William Haraf, until recently Commissioner of the California DFI, on whose watch the MTA was implemented. Mr. Haraf is now Managing Director at Promontory Financial Group. It was suggested by a former Promontory Director in attendance at the event that the panelists were also Promontory clients. That individual was a former Director, and not still a Director, because he had been forced to resign from Promontory when he decided

to join the team at one of the panelist's companies, a Promontory client, which focuses on virtual currency.

F. **Redundancy**

The federal prosecutors who most often handle cases involving complex financial crimes already have an arsenal of statutes at their disposal. State MTLs, and even Section 1960, are rarely invoked and generally redundant in the context of these other statutes. Covering a roughly twenty-year period, nationwide case data from PlainSite (http://www.plainsite.org) show:

- **18 U.S.C. § 1341 (Frauds and swindles):** 3,545 cases
  *See http://www.plainsite.org/laws/index.html?id=14176*
- **18 U.S.C. § 1343 (Fraud by wire, radio, or television):** 2,591 cases
  *See http://www.plainsite.org/laws/index.html?id=14178*
- **18 U.S.C. § 1956 (Laundering of monetary instruments):** 3,306 cases
  *See http://www.plainsite.org/laws/index.html?id=14422*
- **18 U.S.C. § 1957 (Engaging in monetary transactions in property derived from specified unlawful activity):** 756 cases
  *See http://www.plainsite.org/laws/index.html?id=14423*
- **18 U.S.C. § 2314 (Transportation of stolen goods, securities, moneys, fraudulent State tax stamps, or articles used in counterfeiting):** 915 cases
  *See http://www.plainsite.org/laws/index.html?id=13668*
- **31 U.S.C. § 5324 (Structuring transactions to evade reporting requirement prohibited):** 354 cases
  *See http://www.plainsite.org/laws/index.html?id=30138*

Compare these figures to:

- **18 U.S.C. § 1960 (Prohibition of unlicensed money transmitting businesses):** 66 cases
  *See http://www.plainsite.org/laws/index.html?id=14426*

Of the few cases invoking Section 1960, many already invoke at least one of the other statutes listed above. Clearly, prosecutors can still easily do their jobs when it comes to financial crime without state money transmission laws. Most would likely agree that their jobs would be easier with a single, updated federal statute.

### G. Surety Bonds are Ineffective, Inefficient and Costly Insurance Mechanisms That Will Become Increasingly Insufficient with the Rise of Mobile Payments

A money transmitter wishing to do business in the United States of America must presently pay for almost fifty surety bonds of varying amounts with a total worth of approximately $20 million—annually. Even at a premium rate of 5%, this represents a $1 million annual expenditure. Aside from being impossible to afford for most startups, who might be lucky to raise a fraction of that amount in angel or venture capital financing, the insurance mechanism doesn't even make sense.

The California MTA's maximum bond requirement is $9 million according to Financial Code § 2037(f), which explicitly combines the $2 million maximum for "stored value" with the $7 million maximum for "receiving money for transmission." Aside from the fact that these numbers are totally arbitrary, they are also far too small. A large money transmitter such as PayPal holds far more than $9 million in consumer funds. If PayPal's parent company, eBay, Inc. were to suffer a sudden collapse for whatever reason, the funds held by PayPal's customers would be mostly uninsured. PayPal customers would be lucky to receive pennies on the dollar.

Contrast this to FDIC insurance, which presently covers every bank account in the United States up to $250,000. All banks pay premiums to the FDIC based on risk, and those pooled premiums serve as insurance. This system works because the risk of one bank failing is spread out across all banks.

For money transmitters, each entity is required to shoulder the full burden of its own potential failure. Even though an insurance provider backing surety bonds can collect premiums from multiple money transmitters, offsetting that *provider's* own risk, this does little to offset the risk to *customers* of any one failure, because the bonds only insure one party each.

In short, the surety bond system used in place of FDIC insurance for money transmitters is hardly

more than smoke and mirrors. It offers too little protection for large players, and is prohibitively expensive for vastly over-insured small ones. And for customers of the riskiest entities who have no licenses, e.g. bitcoin exchanges, it offers no protection at all.

As mobile payments and virtual currencies (and therefore money transmission) become more prevalent, more money will be entrusted with money transmitters, and less with chartered banks. *Under the current model, surety bonds alone, in any amount, will not be able to adequately protect increasing amounts of funds.* Government officials at all levels ignore this inevitable trend at their own peril.

### H. Capital Requirements Have Been Repeatedly Proven Ineffective as Regulatory Safeguards in Non-Banking Contexts

Banks (which have the option of obtaining national charters) require minimum levels of capital because they make loans. If too much money has been loaned out at the same time by a bank and there is a spike in demand for deposits on hand at that bank, a run can result, leaving the bank insolvent.

Money transmitters do not make loans. Money transmitters therefore do not suffer from the same type of problem as banks, and capital requirements must be evaluated in a different light. Every dollar entrusted to a money transmitter is available to its holder at all times. The key regulatory objectives are merely ensuring that customer funds are not co-mingled with the money transmitter's operational funds, and that customers have access to their funds as needed. In essence, maintaining the distinction between consumer accounts and operational accounts is a matter of good record keeping.

Nonetheless, ignoring this logic, many (but not all) money transmission laws regulate commercial activity on the basis of surety bonds, as previously discussed, and capital requirements. The conventional wisdom is that financial institutions with greater levels of capital are more trustworthy,

Simply put, this conventional wisdom is wildly wrong.

One only need recall the events of 2008 to see that capital amounts in absolute terms (as opposed to reserve ratios) only go so far. The creditors of Lehman Brothers, an entity once managing $600 billion of assets, were hardly protected by the firm's immense reserves of capital when it declared bankruptcy on September 15, 2008. Bear Stearns suffered a similar fate. Bernard Madoff's investment firm had many millions of dollars in its accounts before it was discovered to be a Ponzi scheme of unprecedented scale.[16] Although these entities were not money transmitters and in many cases used leverage to attempt to bolster their returns, extremely large companies such as MF Global (with $41 billion in total assets and $39.7 billion of debt according to its bankruptcy filing)[17] and Peregrine Financial Group operated much more like money transmitters (not making loans) and suffered the same fate.[18] Yet financial regulators continue to place trust in capital alone when it is a totally irrelevant factor for money transmitters.

At least in the case of MF Global, wire transfers of *hundreds of millions of dollars* were made without any regulators noticing that customer funds and operational funds were being co-mingled.[19] Were MF Global a money transmitter instead of a futures brokerage, under the MTA, it would have had no problem obtaining a money transmission license given the original written $500,000 tangible

---

16 MTLs are also flawed in that they rely heavily on third-party audits to assess capital levels, *paid for by the applicant, the same entity being audited*. This perverse incentive structure gives the auditor a strong desire to please its customer, not the government, lest it not get paid. It partially explains how Madoff was able to hide his fraud for so long. It also makes compliance that much more expensive: Think paid $18,000 for useless MTA audits.

17 See "MF Global Holdings Amends Agreement to Use JPMorgan Cash," Tiffany Kary, *Bloomberg*, http://www.bloomberg.com/news/2012-09-07/mf-global-holdings-amends-agreement-to-use-jpmorgan-cash.html.

18 See "MF Global redux as regulator says PFGBest client funds missing," *Reuters*, July 10, 2012, http://www.reuters.com/article/2012/07/10/us-broker-pfgbest-mfglobal-idUSBRE86905120120710.

19 See "Investigators Scrutinize MF Global Wire Transfers," Azam Ahmed and Ben Protess, *The New York Times*, February 26, 2012, http://dealbook.nytimes.com/2012/02/26/investigators-scrutinize-mf-global-wire-transfers/.

net worth requirement, or even the unwritten $1 million-plus tangible net worth requirement. Nonetheless, its management would not have been any more trustworthy.

This all goes to show that there is no relationship between capital and trust. Even if such a relationship did exist, the actions of large banks in the 2008 financial crisis suggests that it would be inverse and certainly not strong enough for policy to be based on its existence. Therefore, basing the licensure process on absolute amounts of capital, as most MTLs do, accomplishes nothing except to discriminate against small firms just starting out who inevitably cannot meet the requirements on day one of business.

### I. The Domino Effect

Virtually every state money transmission application asks the applicant to present a list of all other states in which licenses have been obtained or applied for. Rejections must also be noted, often in answer to a yes-or-no question asking whether the applicant has ever been rejected for a money transmission application in any other state. If the answer to this question is "yes," then the chances that the instant application will also be rejected increase dramatically. (This question is often next to other questions concerning whether any of the applicants' officers have criminal records.)

As a result of the domino effect, applicants cannot risk applying for licenses in states where it seems possible that their application might be rejected for any reason, including insufficient capital. Applying anyway could easily and irreversibly jeopardize that applicant's chances at doing business nationwide.

### J. Nervous Banks

Many bitcoin exchanges are poorly-run, fly-by-night operations that should not be able to obtain banking services in the United States. Yet many money transmitters having nothing to do with virtual currency are legitimate, and these companies also increasingly have trouble obtaining banking

services. Banks are required to comply with the Bank Secrecy Act (BSA), and many fear penalties for associating with the wrong money transmitters given the regulatory complexity inherent in the present system..

### K. Criminalization of Legitimate Entrepreneurship

Perhaps the most counter-productive aspect of Section 1960 is part (a), which reads:

> Whoever knowingly conducts, controls, manages, supervises, directs, or owns all or part of an unlicensed money transmitting business, shall be fined in accordance with this title or imprisoned not more than 5 years, or both.

In effect, while the CEOs of failed banks that caused the 2008 financial crisis walk free, entrepreneurs trying to improve upon the enormous mess they have left behind are told that if they do not comply perfectly with forty-seven incredibly confusing and contradictory state laws (as explained in part (b)), they might well go to jail, along with their investors, directors, and even shareholders. Never has there been such a stark disincentive to enter an industry.

The fact that failing to comply with *any* state law is a federal crime, combined with the naturally interstate nature of money transmission, means that compliance with *all* state laws is required at all times, even if it is not clear which states regulate which aspects of commerce (which it is not, as applicants for licenses are frequently told to write to state agencies for determination letters, which can take months or years to receive). Compliance with even a few state laws can be prohibitively expensive for a new entrant, which typically must hire an army of lawyers to explain forms, compile documentation, assemble notarized affidavits, etc.

In the end, the result is that fewer law-abiding entrepreneurs have any interest in entering an industry where punishments are plentiful and rewards are hard to come by. Suffice it to say that PayPal would not have been able to succeed as quickly as it did, if at all, had a law such as the MTA existed in California in 1999. (Those MTLs that did exist ended up being an enormous challenge

for PayPal in its early days.)

Most states are hardly in a position financially to crush non-polluting, efficiency-driving businesses who hire workers and pay taxes. Yet that is exactly what they have done with MTLs.

### I. The Money Services Round Table Presents MTLs to State Legislatures Under the False Pretense of "Consumer Protection"

That the interests of large financial companies are really the motivating force behind MTLs' myriad restrictions is self-evident from the bulleted prospectus that Mr. Levine and his colleagues supplied to the California DFI in late February, 2010. Under the bold heading of "ADVANTAGES," this unsigned document on no letterhead states that the new proposed law would reduce administrative burden for DFI and "industry;" would bring California's financial laws "into the mainstream;" would give DFI more power (to harass the competitors of TMSRT's members); and apparently reflects "a DFI-Industry consensus." This last statement is blatantly false unless the capitalized "Industry" is a code word for TMSRT. Consumers are mentioned only in passing as the supposed beneficiaries of additional disclosures required by statute "with regard to emerging electronic technologies"—obstacles clearly targeted at technology startups that naturally threaten TMSRT members.

Conspicuously missing from TMSRT's bulleted list was a mention of any specific event or reputable study (or any study at all) that would have suggested that more state MTLs were necessary in the first place. This is because the MTA represented nothing more than a naked power grab on behalf of both TMSRT and the DFI.

This is not to say that consumer protection is not a legitimate state interest, for it clearly is. Unfortunately, the MTA and other MTLs lack any effective means by which consumers would actually be protected, and even if they did contain such effective means, state regulators have shown time and again that they have little to no intention of actually enforcing the law in a manner that

would protect consumers.

### M. Some MTLs Are So Broad as to Encompass Virtually All Aspects of Routine Commerce

Under the California MTA, every law firm that maintains a trust account or remits funds to government agencies on behalf of clients is a money transmitter. Every payroll company that drafts and holds onto client funds is a money transmitter. (Consequently, the payroll industry lobbied for an exemption from the MTA and got one in October, 2013.) Every private university that operates a pre-paid debit system for students, allowing them to purchase goods and services at on-campus third-party merchants, is a money transmitter. Every construction company, real estate agency, escrow service, and political donation aggregator is a money transmitter. The definition of "money transmission" in Financial Code § 2003(o) is so absurdly broad as to encompass much of the daily activity that keeps California's economy running. Of course, a good number of technology startups are also unwittingly money transmitters under this definition, even if their core business has nothing to do with payments.

Almost none of these types of entities listed above have licenses, let alone licenses nationwide; after all, California only has sixty-five licensed companies[20] with the MTA having been in effect for slightly more than two years. Meanwhile, as the MTA claims to regulate everything, the DBO does almost nothing to enforce it, save for threatening those prospective applicants who dare to ask questions.

### N. MTLs Are Completely Inconsistent with Each Other

Despite the nominally common goal of consumer protection, MTLs each have requirements that are considerably different. There does not appear to be any particular logic to the original or amended

[20] This represents $325,000 of application fee revenue for the DFI, enough to cover the salary and benefits of only 1-2 bureaucrats to oversee the program. Yet the sacrificed tax revenues are in the tens of millions.

figures in the MTA ($500,000, amended to $250,000[21]; $2 million; $7 million) except that they are big, round numbers.

In contrast to the California MTA's original $500,000 (but really not) minimum tangible net worth requirement and $750,000 aggregate surety bond requirement, Alabama requires $5,000 in minimum tangible net worth and a surety bond anywhere from $10,000 to $50,000. The MTA's non-refundable application fee is $5,000; in Alabama, the total fee is $500.

Ohio requires a minimum net worth of $25,000 but a $300,000 surety bond. Oregon requires $100,000 in net worth but a $25,000 minimum surety bond—except that it defines "money transmission" in a way that exempts payment processors such as FaceCash.[22] Maryland's application fee changes depending upon whether one applies in an even-numbered or odd-numbered year.[23] Clearly it is impossible to find much consistency between the various laws, but even given the variation built into the regulatory regime, the MTA is an order of magnitude more expensive to comply with, and therefore more restrictive. Unfortunately in these circumstances, Silicon Valley is in California.

State laws that are completely inconsistent with one another are often found to be unconstitutional by federal courts as they tend to impede interstate commerce.

---

21 With Assembly Bill 786 (2013), in response to pressure from Think and others, the California legislature decided to lower the MTA's minimum tangible net worth requirement by half. Then it gave the DBO the statutory power to raise it up again to infinity, based on any factor at all, accomplishing nothing.

22 According to FinCEN, money transmitters are distinct from payment processors. Even though this distinction is embodied in the Code of Federal Regulations, the DBO and certain other state agencies choose to actively ignore it. See FinCEN Rulings 2003-8; FIN-2008-R005; FIN-2009-R001; and FIN-2009-R004.

23 See "Held Hostage: How the Banking Sector Has Distorted Financial Regulation and Destroyed Technological Progress," Aaron Greenspan, Think Computer Corporation, August 15, 2011, http://www.thinkcomputer.com/corporate/whitepapers/heldhostage.pdf.

## II. Think's Experience in California

### A. State Regulators Abused Their Discretion Under the MTA

Both before and after the passage of California Assembly Bill 786, which Governor Brown signed into law in October, 2013, the MTA gave, and now to an even greater extent gives, the DBO *carte blanche* to do whatever it wants with respect to money transmission licensure. Applicants are now to be assessed on the "quality of their management" (whatever that means) and "any other factor," according to the statute. The issuance of licenses can be put on hold for up to a year, giving an applicant's competition more than enough time to gain traction illegally. Or, as happened to Think, applicants can be told that they will simply never be granted a license, no matter what—but that they could try applying anyway, so long as they remember that the application fee is non-refundable.

#### 1. The DFI Invented Its Own Set of Illegal Underground Regulations Not Subject to a Notice and Comment Period in Violation of California Government Code § 11346.8(c) and 1 C.C.R. § 44

Relying on what he called his "personal experience," DFI Deputy Commissioner Venchiarutti explained at Think's mandatory pre-application interview, held at the DFI's San Francisco office on June 14, 2011, that the MTA gave him unbridled discretion to set the tangible net worth requirement as high as he desired so long as it exceeded the $500,000 statutory figure. During the meeting, he cited a minimum net worth requirement of $1 million, $2 million, $20 million, and as high as *$80 million* as potentially necessary to obtain a license. When Ms. Eileen Newhall, Staff Director of the California Senate Banking, Finance and Insurance Committee inquired again on behalf of Think after the meeting, the Deputy Commissioner told her that the number was $1.5 million, but did not put this statement in writing. Without clarity as to the *actual* threshold used to evaluate applications, Think was unable to apply for a license without running a significant risk of rejection that would ultimately trigger irreversible nationwide ramifications, due to the aforementioned domino effect.

Although the Commissioner (or practically speaking, the Deputy Commissioner) can increase the tangible net worth requirements on any given licensee pursuant to Financial Code § 2081(b), there is no direct oversight mechanism that would prevent a DBO Commissioner or subordinates from picking "favorites" and selectively raising the capital requirements of particular companies for little to no reason at all, as the DBO appears to already be doing.

Courts tend to look rather unfavorably on statutes that grant unfettered discretion to bureaucrats, or even elected officials. "We hold those portions of the Lakewood ordinance giving the mayor unfettered discretion to deny a permit application and unbounded authority to condition the permit on any additional terms he deems 'necessary and reasonable,' to be unconstitutional." *City of Lakewood v. Plain Dealer Publishing Co.*, 486 U.S. 750 (1988).

After Think filed suit against the DFI, an undated "Money Transmitters FAQ" page spontaneously appeared on the DFI web site to supposedly clarify the following (emphasis added):

> "**Q.** What is the capital requirement?
>
> **A.** The capital requirement *varies based on the licensee's plan of operation and risk profile*. The amount of tangible net worth stated in the Financial Code, $500,000, is *not* the amount required for licensing, but rather the *minimum* allowed for existing licensees. A new licensee would typically be required to have more tangible net worth, *at least* $1 million, to offset the *expected losses* of a new transmitter and support its operational needs at all times."

The DBO therefore pre-supposes that all applicants will immediately lose more than $1 million. This is simply not so. The web page has since been modified and this language has been removed.

When questioned by Magistrate Judge Howard R. Lloyd about the ever-changing requirements for licensure during oral argument on April 17, 2012, according to the official transcript Deputy Attorney General Ryan Marcroft, representing the DFI, stated, "As far as that issue goes, it's kind of a confusing issue, it was to me at least."

In essence, the DBO's interpretation of the MTA requires that applicants pay a non-refundable fee of $5,000 and risk nationwide rejection *before* learning what the requirements even are to apply for a money transmission license in California. This is a gross perversion of due process, rendering the MTA unconstitutional for yet another reason.

Think is not the only company that has expressed concern over the DBO's handling of the MTA. On July 23, 2013, Thomas P. Brown, an adjunct faculty member at the University of California, Berkeley School of Law and partner in the San Francisco office of Paul Hastings LLP (who has testified before the U.S. Senate Committee on Banking, Housing and Urban Affairs about mobile payments and happens to represent many of the unlicensed entities that Think is suing), quietly filed a petition with the California Office of Administrative Law ("OAL") expressing concern that the DBO was attempting to enforce underground regulations. He cited Think's experience but added his own concerns as well. According to counsel at OAL, Mr. Brown withdrew the petition just before the OAL would have issued an acceptance or denial, after a private telephone conversation in which DBO officials promised to issue regulations concerning the MTA. In this conversation, the DBO claimed that it was "unaware" that it had to issue formal regulations, even though this had been a major topic of concern at the March, 2013 oversight hearing before the California General Assembly Committee on Banking and Finance at which the then-DFI Commissioner testified and at which Deputy Commissioner Venchiarutti was present.

### 2. <u>The DBO Has Threatened to Bankrupt Applicants via the Audit Power Granted by the MTA</u>

In the past, the DFI has specifically threatened that it can abuse its audit power pursuant to Financial Code § 2120 to drive an applicant into bankruptcy if that applicant attempted to apply for a license and managed to somehow be successful in obtaining one. Undoubtedly, the DFI was referring to the fact that licensees are required to pay for the "reasonable costs" of audits. (Of course, no cost is

really reasonable because such audits could be conducted for the most part electronically at no cost if the regulator were properly equipped to regulate modern money transmission.)

### 3. The DBO Bases Policy on a Magic Number with No Foundation

As the basis for many assertions and rationales, then-DFI personnel stated that as a rule it took three years for money transmitters to become profitable. These staff members offered no justification for this arbitrary figure other than personal experience. The three-year rule was repeated in discussions between Think and DBO Senior Counsel Tony Lehtonen. No authoritative source for the rule was ever provided.

## B. The MTA's Geographic Scope is Unconstitutional On Its Face and As Applied

On October 13, 2011, in response to Think's repeated inquiries about the actual tangible net worth requirement and the potential liability that Think would assume as a California company conducting *licensed* money transmission activity outside of California (in Alabama and Idaho specifically, where Think held valid licenses), the DFI issued an Order exempting Think from the MTA so long as it effectively promised not to do business as a money transmitter in California. This necessarily implies that the MTA polices the entire United States of America outside of California, which is not possible or permissible given that the MTA is a state, and not federal, law.

To the extent that any state MTL polices money transmission activity anywhere outside of its respective jurisdiction, that MTL is unconstitutional.

## C. The DBO Has Enforced the MTA in an Arbitrary and Capricious Manner

Adding insult to injury, the DFI seems indifferent toward the countless companies violating the MTA on a daily basis.

### 1. The DBO Has Failed to Respond to Formal Complaints

Think filed no less than thirty-four (34) different formal complaints with the DFI in November, 2011, referenced in the lawsuit. No action that has been made public has resulted from their investigation. Namely, many of the startup companies conducting money transmission in California in violation of the MTA are still conducting money transmission in California in violation of the MTA. Meanwhile, Think's inability to operate FaceCash means that its competitors have an unfair advantage in the marketplace. Think intends to re-start FaceCash once a viable regulatory framework is in place, but when that happens, it will find the market already saturated by companies who deliberately broke state and federal laws for years to achieve their positions of dominance.

The DBO has now had a full two years to act since the complaints were filed in or before November, 2011.

### 2. The DBO Has Made False Statements to the Press Concerning the Existence of the Complaints

In a July 11, 2012 article by Owen Thomas on the *Business Insider* web site entitled, "This Innovation-Killing California Law Could Get A Host Of Startups In Money Trouble" (http://www.businessinsider.com/california-money-transmitter-act-startups-2012-7), DFI spokesperson Alana Golden was quoted as saying, "Thankfully, none," in response to the reporter's question about how many formal complaints the DFI had received about unlicensed money transmitters. Ms. Golden's statement is demonstrably false.

Approximately two months prior, on April 17, 2012 at oral argument, Deputy Attorney General Marcroft stated, "Well, to answer Your Honor's question, my client mentioned this morning they are looking into those complaints," in response to the Judge Lloyd's question as to what had happened to Think's thirty-four formal complaints.

### 3. The DBO Granted License Applications in Record Time to Entities in Active Violation of the MTA While Delaying Others

Facebook Payments, Inc., a wholly-owned subsidiary of Facebook, Inc. began conducting money transmission through its Facebook Credits program sometime in early 2011, but did not apply for a money transmission license until after Think filed a formal complaint about its activity in November 2011. This is significant insofar as Facebook missed the application cutoff date of July 1, 2011 prescribed by Financial Code § 2172(a)[24] that would have allowed it to continue operating legally as a money transmitter. In other words, it broke the law, fully aware of its existence.

Nonetheless, the DFI looked the other way, ignoring Facebook's illegal activity, and approved its application for a license in just three months, leaving plenty of time before the company's initial public offering in May, 2012 when it would undergo extreme scrutiny by the United States Securities and Exchange Commission. A cursory review of public records concerning license applications reveals that most are not approved within less than six months, while many take a full year (or two years) to review. Since there are no published standards outlining the DFI's application review process, it is not clear why such discrepancies exist. At an oversight hearing before the California Assembly Committee on Banking and Finance in March, 2013, former DFI Commissioner Teveia Barnes claimed that the agency's internal target for application processing is 90 days, but there is absolutely no evidence of such a policy in the actual data. Former Commissioner Barnes also stated, "we don't treat every applicant—it's really an art form in the sense that we don't treat every applicant exactly the same."[25]

---

[24] According to the official text provided by the State, Financial Code § 2172 was not properly re-numbered, and still references pre-2012 section numbers in the text of the statute itself.

[25] See http://www.plainsite.org/flashlight/download.html?id=31313747&z=395adb4e, Case No. 5:11-cv-05496-HRL, Docket No. 47, Page 46.

### D. The DBO's Own Lawyers Are "Appalled At" the MTA

In speaking with Think, DBO Senior Counsel Tony Lehtonen remarked that he was surprised by the reasonableness of Think's requests. On September 13, 2011, he admitted that his own personal view, shared by other legal staff, was that, "We have been appalled at the new law. Even though some of us may have been complicit in it, the view from Legal is: what are we doing here?"

On October 17, 2011, Mr. Lehtonen refused to communicate with Think any further, despite his earlier promise that he would be glad to talk any time. Given the DFI's open hostility, this left Think with no channels of communication to its financial regulator.

### E. The MTA and DBO Have Engendered a Culture of Fear, Making Money Transmission More Dangerous

Institutional investors are not the only ones who have taken note of the DBO's arbitrary and capricious actions with respect to the MTA, not to mention the Byzantine and draconian nature of the MTA itself. Entrepreneurs are very much aware of the DBO's antipathy towards their work on improving payments. Consequently, those entrepreneurs most affected by the MTA are afraid to come forward, for those who identify themselves are most likely to be targets of reprisals (as Think has been).

Further aware of the DBO's lackluster record in enforcing the MTA, many entrepreneurs also correctly calculate their risk of being prosecuted for running an unlicensed money transmission business as being low if they simply stay quiet, and proceed with money transmission activities regardless. This has the ironic effect of endangering consumers, who may be able to turn to the DBO for help with a handful of giant, licensed conglomerates, but not for help with most other smaller businesses of which the DBO is unaware. For example, in the past few months alone, several unlicensed bitcoin startups have cost consumers hundreds of thousands, if not millions, of dollars.

Were there reasonable federal money transmission regulations in effect, these consumers might have some recourse, but alas, they do not.

Ironically, the 2006 version of Mr. Levine would agree here. As he wrote in that same comment to FinCEN and the Federal Reserve in which he disclosed TMSRT's members, "The bottom line is that from the standpoint of law enforcement and for national security, it is far better for all financial transactions to be conducted through legitimate financial institutions rather than illicit operators who maintain no transaction records accessible to law enforcement, file no reports and have no BSA compliance costs. Therefore, neither law enforcement nor the overall security of the United States is served by promulgating regulatory requirements which have the effect, at least insofar as MSB customers are concerned, of driving funds underground by providing an unintentional incentive for customers to use these illicit channels."

This is exactly what Mr. Levine's state MTLs do. They raise prices on the services provided by "legitimate financial institutions" and render all other channels "illicit."

## III. Proposed Solutions

### A. Federal Harmonization of MTLs

As described herein, state MTLs are fundamentally flawed and cannot be salvaged, nor would there be any point in trying to do so. No level of surety bonds or capital requirements can actually keep consumers safe; insurance only truly works in pooled networks. What *will* ensure that consumers funds are in safe hands are comprehensive background checks, character assessments, and real-time electronic auditing of money transmitters by a federal agency that collects insurance premiums *based upon the quantity of deposits held in trust*. There is no role for any state in such a regulatory regime, just as there is no role for any state in policing interstate commercial airline travel.

Notably, the steps for starting a money services business in Canada are much more straightforward,

and Canada is hardly known as a hotbed of financial crime. It requires registration with one federal agency, the Financial Transactions Reports Analysis Centre (FINTRAC). There are no up-front fees, no surety bonds, and no capital requirements for money transmitters to register.

Here in the United States, the Consumer Financial Protection Bureau (CFPB) has expressed an interest in regulating non-banking entities such as money transmitters on a federal level. FinCEN already coordinates the registration of money services businesses for Bank Secrecy Act purposes. The FDIC has considerable expertise in the area of financial account insurance. Congress should choose an agency to house the comprehensive regulatory framework needed to manage money transmitters, including virtual currency operators, in a responsible manner reflecting the concerns raised in these comments, as soon as possible.

### B. Virtual Currencies Should Not Be Regulated Separately

Recently the State of New York Department of Financial Services proposed a new kind of separate "BitLicense" for virtual currency operators. The notion that specific branches of mathematics should require licensure under any regime is ludicrous. Furthermore, the regulatory landscape is already unfathomably complex. New York's proposal, however well-intentioned, would only worsen an already serious problem and achieve very little to help protect consumers. Separate regulation might give entrepreneurs perverse incentives to classify their financial products as "virtual currency" products just to fall within or outside of a more or less favorable regulatory regime. It may very well also prove useless, as technology could quickly move on from bitcoin as we know it today. The abrupt rise in the price of one bitcoin, even factoring in the system's deflationary design, suggests that a combination of market manipulation, media hype and general confusion may be fueling a spike in interest that is not necessarily warranted given the technology's extremely sparse uptake and severe security limitations. Bitcoin is one of the few financial technologies developed wherein it is possible to actually delete one's wallet by mistake.

### C. Money Transmitter Deposit Insurance Should Be Modeled Upon the FDIC

For these reasons and others, it is true that virtual currency operators have a higher risk profile than most other money transmitters. The sensible approach to this problem would be to multiply the premium paid into an FDIC-like insurance pool by such high-risk entities (whether bitcoin exchanges, on-line casinos, or otherwise) for money transmitter deposit insurance. In other words, using arbitrary figures for illustrative purposes only, low-risk money transmitters might pay in $0.005 per dollar held for deposit insurance, while high-risk money transmitters might pay in $0.05 per dollar held. Risk would be best defined by federal agency regulations in order keep up with changing technology.

Deposit insurance up to a limit of $10,000 (as opposed to the $250,000 FDIC/NCUA limit) should be more than sufficient for most money transmitters' client accounts.

### D. Stop The Revolving Door

The actions of "consulting" companies such as Promontory Financial Group are inexcusable. Former senior-level financial regulators should not be permitted to earn salaries for helping their clients evade the laws they enforced only weeks or months before. Congress should specifically outlaw such activity for at least a period of ten years and impose severe criminal penalties for former financial regulators who hope to profit from helping others evade or outright violate the law.