U.S. DEPARTMENT OF THE TREASURY

Press Center

Remarks From Under Secretary of Terrorism and Financial Intelligence David S. Cohen on "Addressing the Illicit Finance Risks of Virtual Currency"

3/18/2014

As Prepared for Delivery

Good morning. It is a pleasure to join you today to discuss virtual currency. And I would like to thank Bloomberg News for hosting this event and providing a forum for this important conversation.

I should begin by admitting that I hesitated to draft written remarks for today. Developments in the virtual currency world occur so rapidly, I was concerned that anything I wrote would be overtaken by events before I got here. In fact, since this event was announced, Mt. Gox went under, Satoshi Nakamoto was identified – or maybe not – and Superintendent Lawsky announced that the New York Department of Financial Services will begin accepting applications to operate virtual currency exchanges.

But despite the pace of the developments in this incredibly innovative and fast-moving field, there are some core principles that guide how we think about virtual currencies and the illicit finance risks they pose. These core principles animate our regulatory approach, and are what I want to focus on this morning.

The Promises and Pitfalls of Virtual Currency

As you all know, there is intense, albeit perhaps not universally shared, enthusiasm for virtual currency.

That enthusiasm is based, in part, on its novelty, its tech roots, and its supposed distance from governments, central banks, and regulators.

It also flows from a belief – shared by consumers, businesses, and investors alike – that virtual currencies have enormous potential to empower users, lower transaction costs, increase access to capital, and bring financial services to many unbanked individuals all around the world.

Now, one often hears virtual currency compared to cash. And to an extent, this analogy has merit.

But one way virtual currency is different from cash, and different from other established payment mechanisms, is that users of virtual currency today can transfer value – around town, across the country, and over oceans – in the blink of an eye with comparatively little or, in some cases, no regulatory oversight.

This poses clear risks to consumers and investors alike. For consumers, anonymity and transaction irrevocability expose them to fraud or theft. And unlike FDIC insured banks and credit unions that guarantee the safety of deposits, there are no such safeguards provided to virtual wallets. Similarly, investors in virtual currency today lack the standard protections applied to the purchase of a security or a commodity.

There is no question that improved consumer and investor protections are sorely needed, and will be crucial to the long-term viability of virtual currency.

Nor is there any question that the long-term viability of virtual currency depends on addressing the risk that virtual currencies can be used to facilitate illicit finance.

Now, what do I mean by illicit finance?

The term refers to money that is illegally earned, transferred, or spent. Every year, hundreds of billions of dollars of illicit funds course through the international financial system. These flows serve disparate but dangerous functions: fundraising by terrorist organizations and their supporters; money laundering by drug cartels and transnational criminal organizations; financial transactions that facilitate nuclear and ballistic missile programs; the list goes on.

The office I lead in the Treasury Department – the Office of Terrorism and Financial Intelligence – is dedicated to combating these threats.

Along with an extraordinarily talented and skilled group of intelligence analysts, policy advisors, sanctions investigators, and anti-money laundering regulators, we work to disrupt these illicit networks, protect the integrity of the U.S. and international financial systems, and, in doing so, advance core national security and foreign policy interests of the United States.

Virtual currencies pose a variety of illicit finance risks. But perhaps the most significant one involves the potential for anonymity.

Illicit actors have always sought to exploit anonymity to hide their financial trails, making it more difficult for financial institutions to detect suspicious activity, identify those involved, and collect accurate transaction records – the basic tools used to weed out bad actors.

Virtual currency, as we all know, can offer a sort of anonymity that has been particularly useful for criminals.

These are not hypothetical risks.

The enforcement actions taken against Liberty Reserve last spring illustrate both the scale and scope of how criminals can abuse virtual currency. Working alongside U.S. Attorney Preet Bahara and his outstanding team from the Southern District of New York, the Treasury Department used Section 311 of the USA PATRIOT Act to help shut down Liberty Reserve – a virtual currency system used to facilitate $6 billion worth of illicit web-based activity, including identity fraud, credit card theft, online scams, and dissemination of computer malware.

The more recent actions against Silk Road and its operators, along with the money laundering indictments of two Bitcoin exchangers, shed more light on the criminal underworld transacting in virtual currency.

Much of the attention on the misuse of virtual currencies has focused on how criminals – from drug dealers to illegal weapons traffickers to computer hackers – have used virtual currencies for online trade in illicit goods and services. That attention is certainly well-deserved.

But less attention has been given to the potential national security risks posed by virtual currencies.

As I noted earlier, my office focuses on mapping the financial networks for terrorists, WMD proliferators, transnational organized criminals, drug kingpins, and rogue regimes, pinpointing their financial pressure points, and attacking their funding streams.

And over the past decade, we have used our array of powerful financial tools at the national and international level to make it harder than ever for many of these actors to raise, move, store, and use funds.

Because of our efforts, terrorist groups have been turned away by banks and other reputable financial institutions, and forced to turn to less regulated, and less desirable channels – including hawaladars, exchange houses, and cash couriers – to transfer funds.

So, for terrorist financiers, virtual currencies are understandably appealing: If funds could be swiftly sent across borders in a secure, cheap, and highly secretive manner, it would suit their needs well. Moreover, access to a fully anonymous – or even pseudonymous – currency would allow terrorists to better cover their tracks.

And just as terrorists could use virtual currencies to minimize exposure to the regulated global financial system, sanctions evaders conceivably could do the same.

The purpose of a financial sanction is to change behavior. Its underlying premise is straightforward: With enough financial pressure, we can influence the target's decision-making calculus. But sanctions only work if we can detect efforts to evade them and respond accordingly. If a sanctioned entity could use virtual currencies to transact anonymously, our sanctions would have a weaker bite.

To be clear, we do not currently see widespread use of virtual currencies as a means of terrorist financing or sanctions evasion. The volatility associated with virtual currency, combined with its low capitalization and liquidity, has limited its appeal to these illicit actors. Terrorists generally need "real" currency, not virtual currency, to pay their expenses – such as salaries, bribes, weapons, travel, and safehouses. The same is true for those seeking to evade sanctions.

But these are adaptable actors who are drawn to ungoverned spaces and so may increasingly look to this technology as an attractive way to transfer value.

Treasury's Goals: Fostering Innovation and Ensuring Transparency through Smart Regulation

So how are governments confronting these risks?

Some countries have already acted. China banned financial companies from Bitcoin transactions while Russia outright prohibited the use of all virtual currencies.

The U.S. posture has been more measured and, I'd submit, more sensible.

On the state level, regulators have begun exploring how virtual currencies fit into their existing statutory frameworks and whether they need new ones. The New York Department of Financial Services, as I noted earlier, has begun accepting applications to operate exchanges for Bitcoin and other virtual currencies as a means of adapting existing money transmission regulations to the world of virtual currency.

Federal regulators have also joined the mix. Agencies such as the CFTC, the IRS, the SEC, and the CFPB are assessing how they can address the challenges posed by virtual currency.

At Treasury, our approach to regulating virtual currency is rooted in two guiding principles: fostering innovation and ensuring transparency.

We place real value on the benefits of financial innovation. Advancements in technology that allow entrepreneurs and businesses to innovate, grow, and hire are crucial to our country's long term economic success. Financial innovation fosters financial inclusion – developing financial products and services to reach both the unbanked and underserved populations.

And so one of our core goals is to create an environment in which promising new financial technologies can flourish.

At the same time, we have a critical responsibility to protect the U.S. economy from illicit finance threats. And that is where our focus on transparency comes in.

We recognize that balancing these objectives is a challenge, and that there may be situations where we need to choose between innovation and transparency. Let me be clear: When forced to choose between the two, we will err on the side of transparency.

But, in the long run, financial transparency and financial innovation are mutually reinforcing. All responsible parties in the virtual currency industry should be able to agree to this proposition. In fact, many invested in the virtual currency space have argued that only through effective regulation can the technology gain mainstream acceptance and become a real part of global commerce.

Now, as we focus on the illicit finance challenge of virtual currencies – and how they can be used to perpetrate and facilitate financial crime, terrorist financing, and sanctions busting – it is worth remembering that virtual currency is not the first "new technology" illicit finance regulatory challenge we have confronted.

The Bank Secrecy Act (BSA) – the statutory foundation of much of what we do to combat illicit finance – was adopted in 1970 to bring transparency to what had been an opaque world of banking, where fraudsters and criminals were making use of effectively anonymous numbered accounts to launder the proceeds of crime.

Over the years, as financial services and payment technologies evolved and expanded, the regulatory reach of the BSA expanded as well, bringing financial transparency to the securities industry, to money transmitters – including online payments systems – and to prepaid programs.

So as we think about the illicit finance challenges of virtual currencies, we should bear in mind that we have been down this road before, and we know how to incorporate new financial products and financial institutions into the financial transparency framework.

Now, what do we mean by financial transparency? By financial transparency, we are not talking about the government snooping on financial transactions or erecting meaningless bureaucratic hurdles.

At its core, financial transparency requires financial institutions to implement certain basic controls: they must know who their customers are; they must understand their customers' normal and expected transactions; and they must keep the records and make the reports necessary for regulators and law enforcement to take action to hold accountable those who abuse the financial system.

The reason for this is clear. Any financial institution could be exploited for money laundering purposes. Therefore, all financial institutions must put controls in place to deal with these threats.

These controls are not just good practice -- they are good business. For financial institutions, reputation is sacrosanct. Those that disregard their responsibilities will be saddled with a financial scarlet letter as legitimate consumers and banks plainly prefer to transact with entities that have a reputation for integrity and transparency. And so, more than ever, controls are also necessary to preserve a company's bottom line.

We know that there is opposition to the regulation of virtual currencies.

Some of it stems from the view that the government has no business even trying to regulate in this realm – that the computer code that gives life to virtual currency was not created by the government, and so should be exempt from the government's attempts to regulate. Needless to say, we do not subscribe to that notion.

Others maintain that regulation will be so costly that any meaningful oversight will suffocate the industry.

But these people often forget that there was a time when there was little oversight over the financial system – and that was not such a good thing.

In the 1920's, the government had very little visibility or influence over financial firms. During that era, companies routinely cooked their books to induce gullible investors to purchase securities.

With barely any disclosure requirements, promises made by companies and brokers had little or no basis in reality and were often wholly fraudulent. Thousands of investors bought up stock in hopes of huge profits. The market was in a state of speculative frenzy that only ended on October 29, 1929, when the market crashed as panicky investors sold off their investments en masse.

In the wake of the crash and the ensuing Great Depression, President Franklin Delano Roosevelt called for new regulations that would let in "the light of day on issues of securities."

But this did not come without its share of critics. *Fortune* magazine, for instance, argued that new regulations would cause "American corporations to go abroad for capital." And the President of the New York Stock Exchange predicted "tremendous, if not universal, withdrawal" of public companies from American stock markets if new regulations were passed.

These critics were clearly wrong in their predictions. Yet, we are hearing very similar critiques today from those opposed to the regulation of virtual currencies.

Today's critics claim that regulation will push all the innovation and progress overseas, outside of the supposed stifling grip of American financial regulators. But, the opposite is true: Financial transparency can help bring stability to the virtual currency market and security to its users and investors. And that is what we are trying to do through sensible, flexible and – to use a word from the tech world – scalable regulation.

Treasury's Toolkit: Smart Regulation, Engagement, Intelligence, and Enforcement

Now, with innovation and transparency as our guiding principles, let me take a minute to discuss our regulations.
Exactly one year ago today, Treasury's Financial Crimes Enforcement Network (FinCEN), the agency charged with implementing the BSA, issued interpretive guidance to bring clarity and certainty to one aspect of the regulation of virtual currencies.

The guidance explains that administrators and exchangers of virtual currency are money transmitters under existing regulations, and thus must register with FinCEN, keep particular records, and report suspicious transactions to adequately guard against money laundering and terrorist financing abuse.

In essence, FinCEN's guidance clarifies that our illicit finance regulatory focus – at present – is on those who facilitate the entry and exit into a convertible virtual currency system.

Since FinCEN issued this guidance, dozens of virtual currency exchangers and administrators have registered with FinCEN, and FinCEN is receiving an increasing number of Suspicious Activity Reports (SARs) from these entities. It is encouraging to see players in the virtual currency industry taking their responsibilities seriously and modifying their businesses to comply with these transparency requirements.

But we know there are many virtual currency exchangers and administrators that have not registered with FinCEN and are not fulfilling their recordkeeping and reporting requirements. Those that do not comply with these rules should understand that their actions will have consequences. Not only are they subject to FinCEN civil monetary penalties, but the knowing failure to register a money transmitting business with FinCEN – or to fail to register with state authorities when required – can be a federal criminal offense.

Importantly, FinCEN's guidance also explains that those who simply use virtual currencies for transactions – such as buying goods or services online – are not subject to regulatory requirements.

In this way, virtual currencies are regulated like cash. Existing BSA regulations do not require any recordkeeping or reporting requirements for everyday purchases in either cash or virtual currency.

The regulations for the two, however, diverge when it comes to transactions over a certain dollar or dollar-equivalent threshold. Vendors processing cash transactions are required to report transactions involving more than $10,000 in cash to FinCEN, while those processing virtual currency transactions are not.

At present, the crux of FinCEN's regulatory framework for convertible virtual currencies focuses on the moment "real" money is exchanged into virtual currency, and when virtual currency is exchanged back into "real" money. As I noted earlier, we regulate the entries and exits of the virtual currency world. And at current adoption levels, we think that this type of oversight is sufficient to guard against money laundering and other illicit finance threats.

But we know that the virtual currency industry is quickly evolving. While we surely don't know where it will ultimately go, or even if one or more virtual currencies will really catch on, I can assure you that as the industry evolves we will continue to assess whether the regulatory steps we have taken to combat illicit finance are sufficient. And so, for instance, if virtual currencies achieve much greater adoption and it appears that daily financial life can be conducted for long stretches fully "within" a virtual currency universe, we will need to consider whether to apply "cash-like" reporting requirements to the virtual currency space.

That is because in a world where virtual currencies are pervasively accepted and used, illicit actors would never need to exchange their virtual funds back into “real” money, and terrorists, criminals, and sanctions evaders would be able to freely transfer and spend their funds without ever arousing the suspicions of law enforcement. And in that world, we may need some enhanced visibility into the virtual currency marketplace to effectively counter those illicit finance threats.

Now, while we know that domestic regulations are vital to establishing much-needed transparency, we also recognize that we cannot do this alone. The virtual economy is a global economy, and any value-transfer mechanism that transcends international borders needs a regulatory framework that does the same.

And so we are coordinating with others around the world to establish and maintain effective international standards to protect the global financial system from the illicit finance threats posed by virtual currencies, as well as other online payments methods.

Treasury primarily advances this strategic objective through the Financial Action Task Force (FATF), the global anti-money laundering and counter-terrorist financing standard-setting body. To this end, Treasury played a leading role in drafting the FATF guidance on new payments methods in June 2013. And just last month, we helped spearhead discussion of a FATF paper that proposes common definitions for the virtual currency world and describes the potential benefits and illicit finance vulnerabilities of virtual currencies. We anticipate that FATF will publish an updated paper on the topic later this year.

We also are actively engaging with other multilateral groups, including the European Commission, as well as with individual countries, to facilitate global understanding of the illicit finance threats associated with virtual currencies and regulatory approaches to confront them.

But while it’s up to regulators – both domestic and foreign – to apply and develop a suitable legal framework, this cannot be an insular process. Put simply, we must engage with all stakeholders to keep pace with this evolving sector.

My team and I have already had many productive conversations with members of the virtual currency community. We have expressed our hope that the industry’s great innovators extend their focus toward devising creative solutions for preventing the abuse of virtual currencies by criminals, and not toward creating technology that only further obscures financial trails.

And we will continue to engage in open dialogue. In that vein, I am pleased to announce that, for the first time, we will be including a member of the virtual currency community as part of the Treasury’s Bank Secrecy Act Advisory Group (BSAAG). The BSAAG consists of representatives from regulatory and law enforcement agencies, financial institutions, and trade associations who advise Treasury on anti-money laundering and counter-terrorist financing policy. We are hopeful that formally including the virtual currency community’s voice in the BSAAG will mean that our regulatory approach as a whole, including our approach to virtual currency regulation, is better informed and more effective.

Meanwhile, we will never lose sight of the fact that not everyone will comply with our regulations. And so we will continue to couple our engagement with a robust effort to identify and combat those using virtual currencies for illicit purposes. We have a dedicated team of analysts at FinCEN focused on tracking and developing investigative methodologies for virtual currency, including by partnering with law enforcement to stop illicit actors.

Treasury is also the only finance ministry in the world with an in-house intelligence shop. Our analysts have at their disposal information collected by their partners throughout the U.S. intelligence community. These resources, of course, are focused on non-U.S. persons who pose threats to our national security. To the extent that these actors use, or seek to use, virtual currency to engage in their threatening acts, we will seek to disrupt that activity as well.

Now, let me be clear: virtual currency providers that comply with the law have nothing to fear.

But, if and when appropriate, Treasury, working alongside our partners, will respond to the illicit use of virtual currency, including issuing advisories to financial institutions, taking action under Section 311 of the USA PATRIOT Act, imposing targeted financial sanctions, and taking civil enforcement actions.

Conclusion

Taking a step back, I have no idea whether virtual currencies will grow and thrive, or whether we are just witnessing a passing fad. The industry is still very young and there are many factors that will help determine its future.

But one can imagine a world where virtual currencies achieve large-scale adoption. That world, however, is a fantasy unless we effectively combat illicit finance threats through thoughtful and firm regulation.

We have now begun that process.

Thank you.

##