Senate Judiciary Committee

Hearing entitled "Protecting Our Elections: Examining Shell Companies and Virtual Currencies as Avenues for Foreign Interference**"**
Subcommittee on Crime and Terrorism
DATE: Tuesday, June 26, 2018
TIME: 02:30 PM
LOCATION: Dirksen Senate Office Building 226

Prepared Testimony
Scott Dueweke
President, The Identity and Payments Association (IDPAY)
Director, DarkTower

Esteemed members of the Senate Judiciary Committee,

I am honored to be testifying before you today on the critical topic of how to protect our elections from foreign interference through the use of virtual currencies and shell companies. The relevance of focusing on virtual currencies and shell companies is, of course, their frequent usage in an attempt to shield the identities of those using them. Foreign parties, state actors and potentially others interested in affecting the U.S. political process need anonymity or mis-attribution to appear to be valid members of the community. For this, virtual currencies are tailor made.

We have seen the scope and scale of these systems grow exponentially and reach every corner of the world. Now, billions of people use virtual currencies and other alternative payment and remittance systems for legitimate purposes and they are transforming economies through their use – especially in Africa and Asia. These systems now represent a major force for the financial inclusion of the more than 3 billion unbanked and underbanked around the world. That is an important point I hope you will remember as you examine the negative uses of these systems. However, that same scope and reach also bring risk as these conduits lead through a web of thousands of exchange points that connect every corner of the world to the United States, and potentially into the coffers of political candidates.

First, though, it is important to acknowledge that virtual currencies are about much more than cryptocurrencies such as Bitcoin. The Financial Action Task Force (FATF), in their report "Virtual Currencies: Key Definitions and Potential AML/CFT Risks", June 2014, define virtual currencies as:

"….a digital representation of a medium of exchange; and/or a unit of account; and/or a store of value, but does not have legal tender status (i.e., when tendered to a creditor, is a valid and legal offer of payment) in any jurisdiction. It is not issued

nor guaranteed by any jurisdiction, and fulfills the above functions only by agreement within the community of users of the virtual currency. Virtual currency is distinguished from fiat currency (a.k.a. "real currency," "real money," or "national currency"), which is the coin and paper money of a country that is designated as its legal tender; circulates; and is customarily used and accepted as a medium of exchange in the issuing country."

The report goes on to include many different types of virtual currencies including decentralized systems such as cryptocurrencies (Bitcoin, Litecoin, etc), as well as centralized systems (WebMoney, Second Life Linden Dollars). There are thousands of these systems, although less than 100 are relevant due to a lack of liquidity. These systems do not stand in isolation but rather are part of a thriving ecosystem of not only virtual currencies but also other digital, mobile and stored value systems that cumulatively number in the thousands. These systems are collectively revolutionizing payments in many parts of the world, especially south Asia and Africa, providing opportunities for financial inclusion and growth. Taken together this alternative payments ecosystem is creating a viable alternative to the traditional western-dominated financial system. Most of these systems adhere to established Know Your Customer (KYC) and Anti-Money Laundering (AML) rules and regulations, but not all. As we saw with the Silk Road case, where Ross Ulbrecht created aDarknet site which sold drugs online anonymously for Bitcoin to more than a million customers around the world, criminals find the relative anonymity of these systems to be a boon.

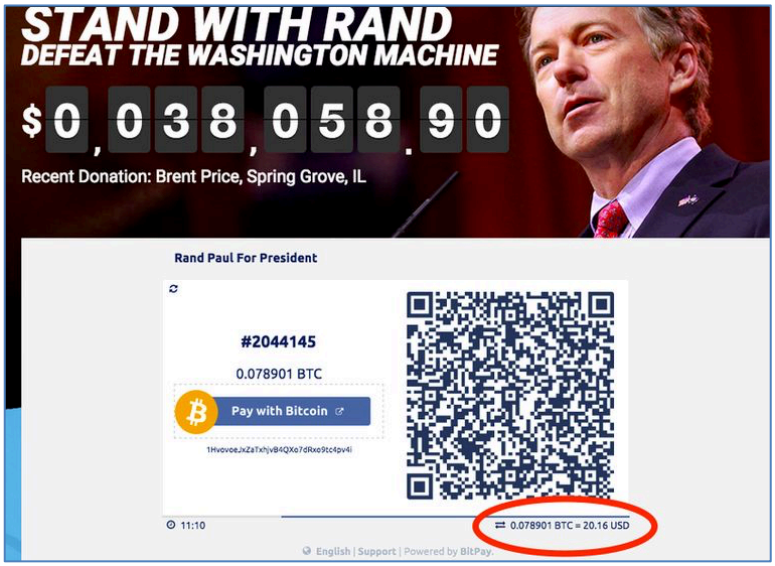
Status of Virtual Currencies as Political Contributions

Bitcoin, ether, and other cryptocurrencies are now finding their way into U.S. political campaigns. Every state except for Kansas allows Bitcoin contributions. In 2014 the Federal Elections Committee (FEC) first allowed the use of cryptocurrencies in small individual amounts of no more than $100, as opposed to the regular donation limit of $2,700, noting that Bitcoin contributions should be treated as "in-kind donations". [VS1]The FEC ruled that campaigns and PACs could accept Bitcoin, as long as they exchange the donations for U.S. dollars and verify the donor's identity; however, this reasonable approach left open a critical opportunity for abuse: unlimited cryptocurrency donations to super PACs. This makes it all the more important to understand who the cryptocurrencies are coming. Unlike bank records, the origin of cryptocurrencies (especially when converted in and out of other virtual currencies) can become opaque quickly and efficiently. Understanding who the middlemen are (those who consolidate political money before it reaches the super PACs) is critical but extremely difficult.

Adav Noti, Senior Director at the Campaign Legal Center and former associate general counsel for policy at the FEC, told Bloomberg Law "It's much easier to give false information in the Bitcoin context. As long as the amounts are small, it's not a big deal, but if you start getting maxed-out donors through Bitcoin, it becomes potentially a very big deal". The FEC currently does not have the ability to require

the disclosure of identity to the degree required to understand the full source of funds.

This has led to a growing number of candidates from across the political spectrum to accept cryptocurrencies, most commonly Bitcoin but also ether, to fund their campaigns. Rand Paul famously became the first presidential candidate to embrace cryptocurrency donations when he announced his bid for the 2016 election. Currently, Brian Forde, a former Obama White House aide is running for Congress and is accepting Bitcoin. Since announcing his candidacy last year for a Southern California seat, Forde has embraced cryptocurrency donations: according to FEC records, Forde's campaign has raised nearly $200,000 through virtual currencies. Of the approximately $1.2 million he raised by the end of March 2018, $192,000 (or 16%) came through Bitcoin donations. This is in spite of the Fair Political Practices Commission in California recommending campaigns to not accept cryptocurrencies because their transactions are considered "virtually impossible to trace."



Other countries have seen the impact of virtual currencies, especially Bitcoin. In Iceland the Pirate Party runs on a cryptocurrency funded platform and succeeded in Iceland's last national election. In Colombia Mauricio Toro won a seat in their House of Representatives while accepting Bitcoin and Ether contributions to his campaign. According to media reports, his cryptocurrency wallet addresses are not available publicly, which is alarming. Instead, there is a message on his website asking potential cryptocurrency donors to contact his campaign directly to donate, due to "compliance with AML norms." Without oversight or reporting of the verified identities behind these payments, this would an opportunity for illicit campaign funding.

Non-cryptocurrency virtual currencies have been used in U.S. elections since at least 2008 when 8 of 9 presidential candidates accepted PayPal donations. This has not been a problem as PayPal is thorough in their authentication of identities. Any acceptance of foreign virtual currencies, especially those that do not meet the requirements of FinCEN's Money Service Business (MSB) regulations, would be of far greater concern.

Foreign Capabilities to Influence our Elections using Virtual Currencies

New reports indicate that state actors are actively pursuing the value of these systems not only for their anonymity, which might be selectively present but simply as an alternative to the Western financial system and its KYC and AML controls. A recent example is Venezuela's launching of their Petro, in February 2018. Petro coin is claimed to be backed by the country's oil and mineral reserves, to circumvent U.S. sanctions and access international financing. President Madura proudly claimed @$300M in proceeds (although this figure is widely viewed as false). President Trump signed an executive order prohibiting transactions in any Venezuelan government-issued cryptocurrency by a United States person, effective March 19, 2018. According to Time, Russia helped Venezuela set up and launch the Petro. It does not appear their investment has paid off.

The Russians, while apparently initially viewing Bitcoin as competition to their centralized virtual currencies like WebMoney, have begun to embrace cryptocurrencies. The first ruble-to-Bitcoin virtual currency exchanger as opened this year in Moscow. Russian legislators are also considering a tax of roughly 13 percent on all cryptocurrency investing or trading profit, potentially placing them in the position to benefit from money laundering using Bitcoin and other cryptocurrencies. The Russian central bank on June 3, 2017, announced that they will be creating a national cryptocurrency. In the Russian online news outlet *Fontanka.ru,* a 2017 interview described how the Kremlin "is considering cryptocurrencies as a way of bypassing the international sanctions that are affecting the country's defense capabilities." This was illustrated last Fall when Ethereum founder Vitalek Buterin struck a deal to create Ethereum Russia, with Russia's state-owned Bank for Development and Foreign Economic Affairs, otherwise known as Vnesheconombank (VEB), to explore new opportunities to apply blockchain technology.

Considering that a large percentage of global criminal hackers and many cyber-criminals are Russian or speak Russian (it is estimated that 25% of Darknet content is Russian), and given Russia's current state of tension with the United States and Europe, this development should be closely monitored. Given current FATF definitions (see above) will such a fiat-linked cryptocurrency even be considered a virtual currency since it will likely be tied to the ruble? This could be critical wording in any future legislation. How this cryptocurrency is set up will be telling. Will it have a publicly available and verifiable blockchain like Bitcoin, or will it be a private or permissioned blockchain and be opaque to Western observers and regulators? If private it could be used to circumvent KYC and AML, and even be used to support proxy "patriotic" hackers, as Vladimir Putin referred to them last week. This possibility already exists with Russian-language centralized systems, especially WebMoney.

Russia does not need cryptocurrencies to influence our elections, however. Facebook disclosed in September 2017 that it had discovered more than 3000 ads bought by 470 accounts run by a Russian troll farm in St. Petersburg, reaching more than 11.4 million people who saw the ads, as reported in the media. The goal of these Facebook ads was to divide us and inflame passions. They worked. But how were these ads paid for? As The Washington Post reported, many of the ads placed by Russians aimed at influencing the U.S. election were paid for through the Russian centralized virtual currency, Qiwi. Visa, the credit card giant, partnered with Qiwi on a virtual wallet in 2011. There are approximately 18.5 million Visa Qiwi wallet accounts and they are a relatively easy way for Russians to send money internationally.

Facebook's global aspirations to keep elections honest is still out of reach for the social network, despite the prominent role its service has come to play in many societies. Combining better forensics to understand the source of funds, tied to stronger identity attribution for those placing political ads is critical. While the partnership with Visa made it convenient and easy to spend relatively small amounts of Russian troll's rubles as dollars for Facebook ads, there are far better ways to transfer greater amounts with greater anonymity. Without stronger identity attribution and understanding of the digital payments ecosystem, this type of "disinformatsia" will continue. In the proposed Honest Ads Act – S.1989, two of its goals require KYC of advertisers:

- free and fair elections require both transparency and accountability which give the public a right to know the true sources of funding for political advertisements in order to make informed political choices and hold elected officials accountable; and
- transparency of funding for political advertisements is essential to enforce other campaign finance laws, including the prohibition on campaign spending by foreign nationals.

Understanding where the money is coming from should be another requirement.

Another major centralized virtual currency to be aware of is WebMoney. Using well-protected servers, not a public blockchain, this service is chief amongst channels for Russian funds to flow to their "patriotic hackers" or other cooperating actors. WebMoney is a Russian global settlement system established in 1998, an e-wallet solution that supports different currencies, including dollars, rubles, Bitcoin, gold and many other currencies and forms of value. Currency exchange and asset storage

is organized via a network of so-called "guarantors" from various jurisdictions. This system has been implicated many times over during the past 19 years in criminal activities. A few examples:

- December 2013 – In the infamous breach of the US retailer Target, which resulted in between 1-3 million credit and debit cards being sold onDarknet sites including on the carder site Rescator, Russian centralized virtual currency services WebMoney and PerfectMoney, as well as cyrptocurrencies and other payment systems, were used by criminals to make purchases of stolen cards and Personally Identifiable Information (PII). This resulted in total losses of hundreds of millions of dollars.
- November 2013 - Fraudcheck.cc, an anti-fraud service for criminal spammers exclusively used WebMoney for payment for its services.

In the past several years WebMoney has become not only ubiquitous in Russian-language speaking countries, but also in countries like Mexico where you can add funds to your WebMoney accounts at over 15,000 OXXO 7/11 stores.

This type of service is not limited to WebMoney. Yandex.Money is a payments solution from Russian search engine giant Yandex. The account can be topped up with cash, bankcards, and virtual currencies. Additionally, every Yandex.Money account can be connected to a bank account. It is also an e-wallet solution similar to Paypal. Yandex.Money can be used to pay for mobile services, Skype, online games and different goods. You can also transfer money between two accounts, for example sending money to friends or business associates.

PerfectMoney is perhaps the most anonymous centralized virtual currency and is distinctly used primarily by criminals. It is clearly run by Russian language speakers and has a business address in Hong Kong that is an empty office. In my analysis of thousands of sites and companies and services that are part of the alternative/anonymous payments ecosystem, PerfectMoney is the centralized virtual currency most focused on criminal uses.

Taken together, these Russian language speaker-managed centralized virtual currencies represent a vibrant and growing set of services that are not only serving the ecommerce needs of Russian-speaking legitimate customers but also the criminal underground. Why? In 2015 Ed Lowery, U.S. Secret Service Deputy Assistant Director said that criminals are less likely to utilize crypto-currencies like Bitcoin, since Bitcoin displays all of its transaction data in the public ledger of the blockchain, making it possible to follow its movement.

"They've been more likely to use digital currency: WebMoney, a Liberty Reserve, or going back a few years to EGold," Lowery said. "It's the anonymity it provides. Most of these currencies have very, very lax Know Your Customer' standards. They are

specifically built to get around the banking regulations from the various international regulators that are out there."

These centralized virtual currencies, as well as many of the thousands of sites and services that buy, sell and accept decentralized virtual currencies like Bitcoin, lie outside of the Western financial system's network of detection points. When someone buys WebMoney credits, or PerfectMoney, or AliPay in China, and identities are not established, or suspicious transactions occur, no Suspicious Activity Report (SAR) is generated as would be required here or in Europe. However, since no SARs are generated, often there is a lack of appreciation for the scale of the potential, the probable use of these systems for transactions which are criminal, or for transactions for which there is an incentive for nation states to keep hidden from the prying eyes of U.S. law enforcement and regulators.

Hypothetically, what could these virtual currency systems be used for? I'm especially referring now to the centralized virtual currency systems that are not exposed on a public blockchain, and have the capability to move unlimited amounts of funds completely outside of the Western financial system and would never be detected by our traditional detection systems:

- Balance of payment transfers between criminal organizations such as organized crime and drug cartels
- Funds transfers between countries doing business with pariah states
- Transfers to and from terrorist organizations, especially as part of a trade-based money laundering scheme to cause investigators to lose their money trail
- Enabling kleptocrats to move funds from their country's coffers offshore – the next "Panama Papers" scandal could well be focused on these systems

For cryptocurrencies, the greatest emerging threat of foreign funds reaching the coffers of political candidates, or to be used to fund other influence operations, are the increasing number and liquidity of "privacy coins." These are cryptocurrencies that seek to evade efforts to identify their users. Due to the permanent nature of the blockchain, if at any point your true identity is linked to a wallet address, then the whole history of your transactions then becomes public knowledge. Companies like Chainalysis, Elliptic and CipherPoint have been created to mine the public blockchains for purposes of tracking tax evaders and other criminal activity. Privacy coins, like Monero and many others sprouting out of the blockchain, have sought to evade transactional visibility by having enhanced levels of privacy, and many strive for complete anonymity. Criminals are rapidly improving their tradecraft - increasingly they use escrow services, mixers and tumblers to defeat the geospatial and temporal analysis performed through blockchain analysis. At DarkTower we defend companies and other institutions against those criminals who use these environments and the life-blood of the digital criminal underground - virtual currencies. We have seen the damage done by human traffickers, credit card

thieves, purveyors of ransomware, and nation states seeking to damage our democracy and we are working hard to deter them.

The Virtual Currency Ecosystem

These funds do not need to stay in their virtual currency of origin. Digital money can move through a huge matrix of exchangers, converting from fiat-to-centralized virtual currencies-to-cryptocurrencies and so on from any part of the planet to another. These systems can effectively be used as virtual money laundering nodes, and tracking a knowledgeable user through these systems (especially if outside of Western regulation) can quickly become impossible.

Today's financial technologies (FinTECH), remittance and virtual currency ecosystem are indeed borderless, making them difficult to control simply through national legislation, regulation, and policymaking. The opportunity for the U.S., due to its size, financial power, and economic influence, to play a leading role in shaping international rulesets should not be missed. Indeed, FinCEN's treatment of virtual currency exchangers and providers such as money service businesses (MSBs) has had a positive global impact with the establishment or pending establishment of similar regulations in many countries. The Committee would do well to set as a goal for itself to maintain and continuously establish the United States as the world's leading advocate of Internet payment systems, virtual currencies, and their use. Doing so would help to ensure that we have the reach to properly manage the growth and uses of these systems and ensure that they remain legal, transparent, and run to internationally-accepted standards of behavior – thus maintaining our position at the heart of a modernizing global financial system.

Therefore we are faced with a dilemma. How do we balance the profound benefits of new FinTECH against the criminal use of these systems? It is critical that the entire scope of this ecosystem be considered - its impact, uses, and structure - before making judgments or creating laws and regulations that might have broad unintended consequences. Included in this ecosystem, beyond the virtual and alternative payments providers themselves and the virtual currency exchangers who connect them, I would also recommend understanding the incredible possibilities of the technology which enables Bitcoin and other cryptocurrencies – the blockchain.

The impacts of the blockchain are being felt far beyond Bitcoin. The blockchain is being implemented in financial institutions to transfer funds, the NYSE to modernize the trading of stocks and many other applications. It can also be applied to reduce

fraud and graft in foreign aid while increasing its reach and impact. In 2012, UN Secretary General Ban ki-Moon said "Last year, corruption prevented 30% of all development assistance from reaching its final destination. This translates into bridges, hospitals and schools that were never built, and people living without the benefit of these services," Mr. Ban said. "This is a failure of accountability and transparency. We cannot let it persist." Accountability and transparency are precisely why the blockchain is being applied in the industries previously mentioned. The blockchain has the ability to revolutionize and secure the voting process, as well as campaign financing, adding a level of security and transparency unthinkable until now.

Embracing New FinTech while Balancing Risk

So how do we cope with these daunting law enforcement and regulatory challenges while acknowledging the significant positive role that these systems play in the economy and the potential to use these systems to help connect the unbanked, underbanked and those in need of aid?

Education is, of course, the first step. Helping regulators and law enforcement understands the scope and scale of these systems outside of those systems they know within the U.S. is critical, including at the state and local levels. Understanding the role these systems play in the purchase of illicit goods and services, as well as their positive uses in enabling global remittances between foreign workers and their families is important. These systems are not inherently bad, no more so than using cash or credit cards, and should not have a stigma attached to them.

At the Identity and Payments Association (IDPAY) we have launched a global non-profit that provides a public/private partnership model to provide not only education but a platform to enable a market-driven approach to self-regulation. This is of critical importance because of the pressing problem of the "de-risking" of the accounts of virtual currency, FinTECH, and remittance service providers around the world. US Government agencies need to join us - as well as large US companies such as PayPal, WesternUnion, Bank of America, and others who want to be part of the solution.

Together, public and private entities can work aggressively to promote and coordinate mutually beneficial uniform legal, regulatory, and policy solutions for the management and oversight of virtual currencies and other payments systems. We must work with foreign governments, law enforcement, and intelligence community players to create a uniform, level-playing field that ensures that bad actors cannot find and exploit the seams and gaps between the various national regulatory and legal frameworks and policies to undertake and hide their illicit activities. This includes reaching out on multiple levels, on a government-to-government basis, and through a public/private partnership, to facilitate market conscious policies and regulations which extend beyond national borders which are critical given the new payment ecosystem's transnational nature. Given the rapid pace of development of

these systems and the fact that they are almost all developed by private companies and individuals -- not governments (with the exception of the recent Russian central bank's cryptocurrency announcement) it is essential that whatever approaches are made are based on a public/private partnership rather than a government-only approach to the problem.

It is also critical to create transparency regimes and technologies that are publicly sponsored and funded so that the role of government is not strictly in monitoring illegal, illicit, criminal, and terrorist misapplications of these systems, but also establishing internationally accepted methodologies and transparent solutions that are required for all. Building trust in these systems is critical. This would be a natural and timely development and is an ideal focus for government action as it pertains to payment systems and virtual currencies. This can begin by developing an internationally accepted set of terms, "best practices" and transparency requirements that all governments can agree to adhere to in regulating these systems. Thus, the role of government can be focused where it can both do the most good in encouraging the positive applications of these new technologies as well containing the illicit uses of these systems to more obvious areas of illicit activity and protecting our democratic institutions against hidden influences bought with virtual currencies.

Recommendations

Identity is the key. International cooperation is critical. Providing a cooperative environment, through Interpol or some other multinational law enforcement/regulatory body, or optimally through a public/private partnership focused on establishing identity and seizing criminal virtual currency assets, will help protect our institutions and industries from the illicit use of virtual currencies.

The answer to managing the opportunities and risks associated with the use of virtual currencies as political contributions, or as funding mechanisms for influence operations, can be answered through the authentication and reporting of identities. This approach cannot be limited only to Bitcoin and other cryptocurrencies as there is a shadow financial system that is thriving outside of our control, reaching every country, and using systems that range from meeting our KYC/AML requirements to those that are opaque to our view. We need to take strong steps to understand, control and counter the risks while encouraging the growth of new virtual currency systems that are governed by the rule of law. The world is changing and we must change with it. Identity is the key.

Thank You,

Scott Dueweke