House Financial Services Committee

Hearing entitled "Virtual Currency: Financial Innovation and National Security Implications"
Thursday, June 8, 2017 10:00 AM in 2128 Rayburn HOB
Terrorism and Illicit Finance

Prepared Testimony
Scott Dueweke
President, The Identity and Payments Association (IDPAY)
President, Zebryx Consulting

Esteemed members of the House Financial Services Committee,

I am honored to be testifying before you today on the important topic of virtual currencies and their role in enabling terrorism and illicit financial transactions.

I have been involved in identifying security concerns of Internet payments and their use by criminals and terrorists since presenting on the topic at the first Internet World conference in 1994. Since that time we have seen the scope and scale of Internet payments 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 are transforming economies through their use – especially in African 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.

The Financial Action Task Force (FATF) defines virtual currencies much more broadly than bitcoin, or even cryptocurrencies more generally. In their report "Virtual Currencies: Key Definitions and Potential AML/CFT Risks", June 2014, they 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 a Dark Web site which sold drugs online anonymously for bitcoin to more than a million customers around the world, and many other cases including the use of WebMoney for wholesale purchases of stolen Target credit cards and personally identifiable information (PII), criminals find the relative anonymity of these systems to be a boon.

Today's financial technologies (FinTECH), remittance and virtual currency ecosystem is indeed borderless, making them difficult to control simply through national legislation, regulation, and policymaking. The opportunity for the US, due to its size, financial power, and economic influence, to play a leading role in shaping international rulesets. Indeed, this has already occurred with FinCEN's treatment of virtual currency providers as money service businesses (MSBs) that has had a global impact with the establishment or pending establishment of similar regulations. 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, it's impact, it's 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. I am working with St. Luke's University Healthcare Network, for example, to implement the blockchain

to enhance the patient experience and to create a more secure and convenient experience. 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 per cent 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. One example is the Irish start-up Aid:Tech which is trying to work with the UN and the International Red Cross to make aid entirely transparent, using blockchain technology. Aid:Tech has already rolled out a trial project in Lebanon to help Syrian refugees with the Irish Red Cross, using mobile phones and the blockchain to identify people and replace easily falsified vouchers to deliver aid directly. Blockchain could be applied to many foreign aid projects to allow full transparency and accountability.

Mobile phone penetration is also enabling the unbanked and underbanked to be reached throughout the developing world. Global mobile phone penetration in Africa for example is about 60% and about 30% of them use their phones for mobile money transfers. In East Africa the MPesa success is well known, but has grown in the last decade to include more than 30 million users in 10 countries. Through systems like Clam, you can convert digital payment providers like PayPal into MPesa. Focusing only on cryptocurrencies, and not considering mobile payments and stored value systems is a very limiting and misleading mistake.

Although mobile payment systems are not all considered virtual currencies by the FATF definitions, they are part of the same alternative payments ecosystem. Internet-based currency exchanges allow you to convert virtual currencies, mobile payment systems, stored value cards, fiat currencies and even precious metals to and from each other. Actions and regulations against this ecosystem could have broad unintended consequences that could hurt the most vulnerable and derail growing new financial solutions that are meeting their needs where traditional financial systems have failed them. However, the most anonymous of these exchanges are critical nodes in a criminal relationships and transactions exploiting this ecosystem. We must find a way to target these criminal currency exchanges, often sheltered in countries where officials protect and even profit from them.

There are plenty of reasons to be concerned about the enabling effects of virtual currencies on criminal activities. This is not a new trend. It did not begin with bitcoin. Since at least the early 2000s with the use of eGold, anonymous payment systems have been used not only to protect privacy but also to support criminal activities. Child pornography, money laundering, drug sales, weapon sales, slavery rings, zero day exploits, hackers for hire, murder for hire, mercenaries for hire, credit and debit cards, personally identifiable information, synthetic identities,

identity documents such as passports, drivers licenses, and all the components needed to create them, have all been available on the regular internet and the Dark Web as well as much more. The advent of these criminal markets enabled by anonymous virtual currencies have created a global bazaar for criminals and organized crime to reach a mass global market.

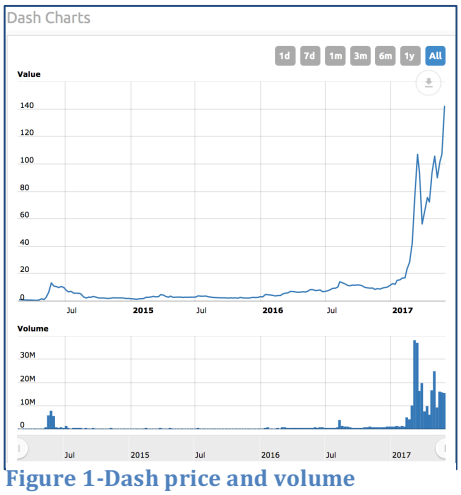

Figure 1-Dash price and volume

While most of the transactions of the Dark Web markets such as Silk Road and those that followed in its footsteps have used bitcoin, this is beginning to change. New, more anonymous cryptocurrencies such as Monero, Dash and Zcash are beginning to gain marketshare. These systems now account for about 1% of cryptocurrency usage on the Dark Web and are increasing rapidly. As these systems increase in usage existing blockchain analysis tools will be challenged to continue to be relevant, as these "dark" cryptocurrencies are designed to avoid the tracking of transactions whereas bitcoin was designed to be transparent.

The Russian central bank on June 3 announced that they will be creating a national cryptocurrency. Considering that a large percentage of the global criminal hackers and many cyber-criminals are Russian or speak 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 it even be considered a virtual currency since it will likely be tied to the ruble? How this cryptocurrency is set up will be telling. Will it have a publically 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.

WebMoney is a Russian global settlement system established in 1998. In general, this is 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 on Dark Web 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 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.
- 2004 - Officials with the U.S. Postal Inspection Service worked with Eastern European authorities to shut down two cybergangs, known online as dumpsmarket and carderportal. According to the postal inspectors, the gangs had laundered proceeds from the sale of stolen credit cards through two digital currencies, including WebMoney.

WebMoney in the past several years 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 and 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 and is distinctly marketed towards 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 many thousands of sites and companies and services that are part of the alternative/anonymous payments ecosystem, PerfectMoney is the centralized virtual currency most completely focused on criminal uses.

Taken together, these Russian 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 and 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 like there would be 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 US 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 off shore – the next "Panama Papers" scandal could well be focused on these systems
- Funding the virtual army of proxy hackers to do their "patriotic" duty

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 understand the scope and scale of these systems outside of those systems they know within the USA 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 to attempt to provide a public/private partnership 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. I will be at the United Nation's Global Family Remittance Day next week at UN headquarters to encourage participation in this NGO. 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. Working with foreign governments and 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 is 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 and "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, such as the Dark Web. Ultimately, through research grants and contracts, the US Government could enable international transparency in foreign aid, tax payments, government grants, and other payments. Such research should include both great scrutiny of the trajectory of illicit uses, including recognizing the direction that the criminal, terrorist, and illicit users are taking -- and developing an "early warning system" to identify new illicit uses as they gain interest -- while also encouraging the development of digital services and technologies that enable valid uses while improving the tracking of improper uses. This type of approach is needed; it is no less important to the future of the Internet than was the original Advanced Research Projects Agency Network (ARPANET), which created the protocols and packet switching technologies that originally gave birth to the Internet.

Together we can help drive technical innovation, encourage economic growth by helping the disconnected become connected and help themselves. Helping to reduce

the de-risking of virtual currency and other alternative payment providers we can spur technical innovation, economic growth, reduce poverty, and allow the US to stay central to a rapidly morphing world financial system. By enabling the unbanked and underbanked to raise their standard of living while driving economic development organically, not through handouts riddled with corruption, we can undermine one of the key recruiting rationales of terrorist organizations while simultaneously limiting criminal abuse of these systems. This approach cannot be limited only to bitcoin and other cryptocurrencies. There is a shadow financial system that is thriving outside of our control. We need to take strong steps to understand, control and counter it while encouraging the growth of new alternative payment and virtual currency systems that are governed by the rule of law.

Thank You,

Scott Dueweke