ELLIPTIC

House Foreign Affairs Committee
Tom Lantos Human Rights Commission

Hearing
on
The Trafficking Victims Protection Act at 20:
A Look Back – and a Look Ahead

Wednesday, January 15, 2020, 2:00 p.m.
2200 Rayburn House Office Building

Statement of Ms. Liat Shetret, CAMS
Senior Advisor - Crypto Policy and Regulation
Elliptic

Good Afternoon. Co-Chairman McGovern, Co-Chairman Smith, members of the committee. Thank you for the invitation to testify today. I am honored and privileged to be here on this 20th anniversary of the Trafficking Victims Protection Act (TVPA), a landmark piece of legislation.

My name is Liat Shetret. I am a Senior Advisor - Crypto Policy and Regulation at Elliptic, a provider of cryptocurrency anti-money laundering tools. We equip the world's leading financial institutions and cryptocurrency businesses with the software and insights they need to identify and act upon illicit cryptocurrency transactions, including those associated with human trafficking. We also work with law enforcement agencies in the US and around the world, helping them to investigate criminal activity involving the use of cryptocurrency.

Human trafficking is one of the most heinous types of criminal activity, exploiting some of the most vulnerable in society. It is also one of the most lucrative. Over the past decade, the proceeds generated by human trafficking have soared from 30 billion dollars to over 150 billion dollars per year[1].

The large sums involved provide law enforcement with the opportunity to work with financial institutions to detect human trafficking through distinctive patterns in

[1] International Labour Office, "PROFITS AND POVERTY: The economics of forced labour," May 20, 2014, https://www.ilo.org/wcmsp5/groups/public/---ed_norm/---declaration/documents/publication/wcms_243391.pdf

financial transactions. These patterns have been used to identify perpetrators and victims of human trafficking for sexual exploitation, for example based on unusual and sustained expenditure on travel, accomodation, or sustenance. The proceeds of this activity must also be reintroduced into the financial system, and transactions indicative of money laundering can be used to identify human trafficking and "follow the money" from lower level operatives to the greater criminal enterprise[2].

Human traffickers use a variety of techniques to mask their activity when engaging in these transactions. These include the use of online payments, prepaid cards, informal banking systems, anonymous shell companies and real estate transactions. Human trafficking is an agile criminal enterprise, constantly adapting to the regulatory environment, the capabilities of law enforcement and the new technologies at their disposal. Over the past few years, cryptocurrency has been one of the new technologies that human traffickers have begun to exploit.

Cryptocurrencies such as bitcoin can be thought of as digital cash[3]. Like cash they have properties that make them attractive to criminals - such as the lack of a central authority that can block transactions or seize funds. There is also the perception that cryptocurrency transactions are anonymous and untraceable, although as we will see this is not entirely true. In a small number of known cases, criminals have exploited these characteristics and cryptocurrencies have been used to facilitate human trafficking.

In 2015, Visa and Mastercard cut off payment services to Backpage.com, the largest online marketplace for buying and selling sex in the US, leaving it unable to accept payments from those purchasing ads on its platform[4]. In response, Backpage turned instead to accepting payments in bitcoin[5], in the knowledge that they could not be prevented from doing so. In 2018 the co-founders and others associated with

---

[2] FATF, "Financial Flows from Human Trafficking," July 2018, https://www.fatf-gafi.org/media/fatf/content/images/Human-Trafficking-2018.pdf

[3] Satoshi Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System", October 31, 2008, https://bitcoin.org/bitcoin.pdf

[4] The Washington Post, "MasterCard cuts ties with Backpage.com after pressure from law enforcement", July 1, 2015, https://www.washingtonpost.com/news/morning-mix/wp/2015/07/01/mastercard-cuts-ties-with-backpage-com-after-pressure-from-law-enforcement/

[5] NPR, "For Sex Industry, Bitcoin Steps In Where Credit Cards Fear To Tread", December 15, 2015, https://www.npr.org/sections/alltechconsidered/2015/12/15/456786212/for-sex-industry-bitcoin-steps-in-where-credit-cards-fear-to-tread

Backpage were indicted, accused of earning hundreds of millions of dollars from facilitating prostitution and sex trafficking[6].

Until early 2018, Welcome to Video was the largest child sexual exploitation market on the dark web[7]. It sold access to 250,000 videos portraying child sexual abuse, which were downloaded over a million times. Payment was accepted in bitcoins, presumably to make it difficult to trace the transactions of the buyers and sellers of this material and identify them.

However, cryptocurrencies such as bitcoin are not in fact anonymous[8]. Transactions take place between wallets that are identifiable through their "address", which is similar to an account number. The blockchain ledger behind a cryptocurrency such as bitcoin lists the details of all transactions between these addresses, including the sending and receiving wallets. Blockchain analytics techniques have been developed by Elliptic and others to link these addresses to real life identities. Tools based on these techniques are used by law enforcement agencies in the US and elsewhere to trace proceeds of crime and identify victims and perpetrators[9].

In fact these tools were used in both the Backpage[10] and Welcome to Video[11] cases that I just described. Law enforcement used blockchain analytics to help to identify and bring to justice the buyers and facilitators of human trafficking for sexual exploitation.

---

[6] United States Department of Justice, "Justice Department Leads Effort to Seize Backpage.Com, the Internet's Leading Forum for Prostitution Ads, and Obtains 93-Count Federal Indictment", April 9, 2018, https://www.justice.gov/opa/pr/justice-department-leads-effort-seize-backpagecom-internet-s-leading-forum-prostitution-ads

[7] United States Department of Justice, "South Korean National and Hundreds of Others Charged Worldwide in the Takedown of the Largest Darknet Child Pornography Website, Which was Funded by Bitcoin", October 16, 2019, https://www.justice.gov/opa/pr/south-korean-national-and-hundreds-others-charged-worldwide-takedown-largest-darknet-child

[8] Elliptic, "Bitcoin Is Not Anonymous", June 17, 2015, https://www.elliptic.co/our-thinking/bitcoin-transactions-money-laundering

[9] The Next Web, "Here's how law enforcement catches cryptocurrency criminals", December 26, 2019, https://thenextweb.com/hardfork/2019/12/26/bitcoin-cryptocurrency-criminals-law-enforcement/

[10] UC Berkeley, "In a step toward fighting human trafficking, sex ads are linked to Bitcoin data", August 16, 2017, https://news.berkeley.edu/2017/08/16/in-a-step-toward-fighting-human-trafficking-sex-ads-are-linked-to-bitcoin-data/

[11] United States Department of Justice, "South Korean National and Hundreds of Others Charged Worldwide in the Takedown of the Largest Darknet Child Pornography Website, Which was Funded by Bitcoin", October 16, 2019, https://www.justice.gov/opa/pr/south-korean-national-and-hundreds-others-charged-worldwide-takedown-largest-darknet-child

Huge strides have been made in combating all types of financial crime in cryptocurrencies over the past decade, both through the development of law enforcement capabilities, and through regulation. It is important to take note of these efforts and their achievements. In 2013 Financial Crimes Enforcement Network (FinCEN) issued guidance stating that certain types of cryptocurrency businesses, including exchanges, would be treated as money transmitters and were subject to the requirements of the Bank Secrecy Act[12]. This obligates them to aid government agencies in detecting and preventing the laundering of the proceeds of criminal activity including human trafficking.

Cryptocurrency exchanges act as key gateways to the crypto economy, allowing the purchase and sale of cryptocurrencies. Thanks to the inclusion of these businesses within the scope of the Bank Secrecy Act, the vast majority of exchanges operating in the US enforce stringent anti-money laundering programs. These programs include customer identification, the use of blockchain monitoring to identify high risk transactions, and the filing of suspicious activity reports that provide law enforcement with valuable intelligence. Elliptic has also worked with cryptocurrency businesses to develop a library of typologies that can be used to detect cryptocurrency transcations that might be associated with human trafficking[13].

The regulatory regime for anti-money laundering in the US holds cryptocurrency businesses to the same standard as comparable traditional financial institutions, and has helped to deny criminals a means to cash out their proceeds. In fact our analysis shows that in 2019, less than 0.5% of all bitcoin transactions were associated with the purchase of illicit goods or services on the dark web, and we expect this to continue to fall[14].

However, some risks do remain. First, cryptocurrency does not respect borders. It is very easy for criminals to cash-out or launder funds by sending them to an exchange overseas that does not perform anti-money laundering checks. Anti-money laundering regulations must be applied globally in order to be truly

[12] FinCEN, "Application of FinCEN's Regulations to Persons Administering, Exchanging, or Using Virtual Currencies", March 18, 2013, https://www.fincen.gov/sites/default/files/shared/FIN-2013-G001.pdf
[13] Elliptic, "Money Laundering & Terrorist Financing Typologies In Cryptocurrencies", November 2018, https://www.elliptic.co/white-papers-and-reports/money-laundering-guide-terrorist-financing-typologies-cryptocurrencies-report
[14] Elliptic, "Bitcoin Money Laundering: How Criminals Use Crypto", September 18, 2019, https://www.elliptic.co/our-thinking/bitcoin-money-laundering

effective, and the recent work of the Financial Action Task Force (FATF)[15] is a good first step towards this. The US delegations to the FATF, the Egmont Group and other international forums have a central role in advocating for the adoption, implementation and application of the June 2019 FATF guidance on virtual currencies, around the globe.

To that end, Congress should ensure that attention is drawn to jurisdictions that fail to implement the FATF guidance on the regulation of cryptocurrency service providers. Through its Mutual Evaluation process[16], the FATF will soon begin to publish information about whether, and how effectively, countries are implementing its cryptocurrency standards. Based on that information, Congress should call for accountability from those countries that the FATF finds are imposing inadequate measures**.**

Second, a new type of cryptocurrency, collectively known as "privacy coins", has emerged[17]. Privacy coins are far less traceable than the likes of bitcoin. Indeed, tools allowing law enforcement or financial institutions to trace payments in privacy coins simply do not exist. At Elliptic we respect every individual's right to financial privacy, and privacy coins have societal value, especially for the millions of people living under authoritarian, corrupt regimes[18]. However, they are also being exploited by criminals, with the majority of dark marketplaces now accepting one or more privacy coins as a payment option[19]. Regulators should ensure that cryptocurrency businesses that support privacy coins enforce anti-money laundering policies that are appropriate to the lack of traceability inherent to them.

In May 2019, FinCEN issued guidance on cryptocurrencies that importantly stated that businesses handling privacy coins are not exempt from anti-money laundering requirements merely because privacy coins are impossible to trace.[20] However,

---

[15] Financial Action Task Force, "Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers", June 21, 2019, https://www.fatf-gafi.org/publications/fatfrecommendations/documents/guidance-rba-virtual-assets.html

[16] http://www.fatf-gafi.org/faq/mutualevaluations/

[17] Cointelegraph, "Privacy Coins in 2019: True Financial Freedom or a Criminal's Delight?", January 2, 2020, https://cointelegraph.com/news/privacy-coins-in-2019-true-financial-freedom-or-a-criminals-delight

[18] Coin Center, "The Case for Electronic Cash", February 6, 2019, https://coincenter.org/entry/the-case-for-electronic-cash

[19] Elliptic research.

[20] FinCEN, "Application of FinCEN's Regulations to Certain Business Models Involving Convertible Virtual Currencies", May 9, 2019,

because transaction tracing solutions are unavailable for privacy coins, cryptocurrency businesses require further guidance from regulators specifying the types of control measures that they could apply to transactions in privacy coins. There remains continuing confusion among cryptocurrency businesses as to how, or whether, they can handle privacy coins while meeting regulatory expectations.

To that end, Congress should call on FinCEN to issue additional guidance providing further clarity on its expectations of US cryptocurrency businesses that enable the use of privacy coins. Any additional guidance should also clarify that US cryptocurrency businesses should deploy tracing solutions for any coins they offer where those solutions exist. Congress can also play an important role in this effort by soliciting future testimony from experts on the risks presented by privacy coins, offering a forum for discussion on appropriate policy and regulatory responses.

Finally, the boundary between cryptocurrencies and mainstream finance is beginning to blur. Knowingly or not, banks and other financial institutions are enabling the movement of funds into or out of cryptocurrency. This may involve cryptocurrency exchanges in jurisdictions where anti-money laundering regulations do not yet apply to cryptocurrency businesses, and which may be enabling the laundering of criminal activities such as human trafficking. Financial institutions in the US must do better at assessing whether they are exposed to this kind of activity and implement adequate measures aligned with a risk-based approach, which begins with institutional risk assessments[21].

Congress should insist that US banking regulators, and banks, undertake additional efforts to mitigate mainstream financial sector exposure to cryptocurrency-related risks. This should include calling on US banking regulators to issue formal guidance clarifying their expectation that US banks must be able identify and manage cryptocurrency risk exposure. Congress should also convene future hearings to explore the role that banks can play in preventing cryptocurrency-related risks, and to insist on accountability from banks in managing those risks.

---

https://www.fincen.gov/sites/default/files/2019-05/FinCEN%20Guidance%20CVC%20FINAL%20508.pdf, p. 19.

[21] FinCEN, "Prepared Remarks of FinCEN Director Kenneth A. Blanco, delivered at the American Bankers Association/American Bar Association Financial Crimes Enforcement Conference", December 10, 2019, https://www.fincen.gov/news/speeches/prepared-remarks-fincen-director-kenneth-blanco-delivered-american-bankers

Cryptocurrencies have the potential to create a secure, open financial system that will promote innovation, competition and access to financial services around the world. However, it can take time for law enforcement capabilities and financial regulations to catch up with new financial innovations. In the interim these technologies can be open to criminal exploitation, including by human traffickers. This has been the case with cryptocurrencies and challenges still remain, but in the US we now have powerful tools and a strong regulatory framework in place, which will help to ensure that this activity can be detected and prevented.

Thank you again for the opportunity to speak here today and I welcome your questions and follow up.