FINANCIAL INTEGRITY
NETWORK

Human Trafficking and its Intersection With the Financial System

September 3, 2019

David Murray
Vice President
Financial Integrity Network

Thank you, Chairman Sasse and Ranking Member Warner, for convening this hearing to discuss human trafficking and its intersection with the financial system. And thank you for the invitation to testify. It is an honor to be before this subcommittee. Human trafficking is the most heinous form of transnational criminal activity, and we are fortunate for your attention to this threat.

Human trafficking is highly profitable, generating $150.2 billion in annual profits as of 2014, according to the International Labour Organization, a U.N. agency that brings together governments, employers, and workers in 187 member states.[1] Developed economies are the most profitable for human traffickers, with criminal organizations earning more than $34,000 annually in profit from each victim in North America.[2]

Human trafficking interacts extensively with the financial system, in contrast to other types of criminal activity, whose touch points are usually more discrete. Drug trafficking is principally a cash business, and the proceeds of the crime are held as cash well into the money laundering cycle.[3] Fraud typically targets money that is already in the financial system through transactions that are designed to appear legitimate.[4] Human traffickers may receive money from buyers either in cash or through electronic means, and the transactions that are vital to operating their businesses may be small or large.[5]

As a result, human trafficking has many intersections with the financial system. At lower levels of human trafficking organizations, human traffickers have used cash, retail payment systems, online payment systems, and cryptocurrencies.[6] At higher levels of human trafficking organizations, human traffickers have exploited anonymous companies to conceal their activities.[7]

Federal, state, and local officials have worked with the financial industry to disrupt human trafficking organizations and push them out of the financial system.[8] But human trafficking is difficult to combat, because the financial transactions associated with human trafficking dwell in parts of our financial system where transparency may be poor: small payments carried out through retail payment systems, online payment systems, and cryptocurrencies, and large payments carried out through anonymous companies.[9]

I make three recommendations to disrupt human trafficking organizations by increasing financial transparency:

- *Pass legislation that bans anonymous companies.* The Improving Laundering Laws and Increasing Comprehensive Information Tracking of Criminal Activity in Shell Holdings (ILLICIT CASH) Act is one legislative initiative under consideration that would ban anonymous companies.[10]

- *Strengthen cryptocurrency regulations by creating a new class of financial institution: virtual asset transaction validators.* For these essential actors in cryptocurrency transactions, such a regulatory regime would emphasize counterparty financial institution due diligence. The lack of system-wide financial crimes compliance (FCC) governance for some existing cryptocurrencies allows criminals space to operate and makes it difficult for the United States to isolate rogue service providers from the U.S. financial system.[11]

- *Improve transparency of retail and other consumer payments.* Changes in the payments industry are reducing transparency of retail and other consumer payments throughout the value chain, making it difficult for downstream financial institutions to understand their customers' sources of funds and the illicit finance risk that each customer poses to the financial institution.[12]

Human Trafficking's Intersection with the Financial System

Nearly three quarters of human trafficking victims brought to North America are trafficked for the purpose of sexual exploitation.[13] The predominant business model for human trafficking therefore requires human trafficking organizations to manage three primary funds flows in the United States: money for logistics such as transportation and lodging, money paid by purchasers of sex to low-level operatives, and money transferred from low-level operatives to the larger organization.[14]

Paying for logistics leaves a financial trail. Financial transactions may be most readily associated with human trafficking when they are carried out by victims and low-level operatives, according to the Financial Action Task Force (FATF).[15] Victims have been identified when they incurred unusually high lodging, sustenance, or transportation charges.[16] Low-level operatives have been identified by connecting them to the purchase of advertisements for prostitution.[17] The amounts paid for lodging, transportation, and advertisements tend to be small, well under the $3,000 recordkeeping threshold and the $5,000 suspicious activity report (SAR) threshold. Traffickers also are now turning to payment tools that allow them to remain anonymous, such as prepaid cards and cryptocurrencies, for purchases of advertisements and websites.[18]

Purchasers of sex tend to pay in cash, which means that human trafficking for sexual exploitation generates high volumes of cash, according to the FATF.[19] Purchasers of sex may also use cryptocurrencies to pay for premium memberships on websites that they use to review services.[20] When human trafficking organizations use fronts such as massage parlors, they may accept credit cards.[21]

At higher levels, human trafficking organizations are sophisticated transnational criminal organizations that prey upon vulnerable people.[22] As money moves from lower levels of an organization to higher levels of an organization, techniques for moving funds are consistent with those employed by other dangerous transnational criminal organizations. Human traffickers have used money transmitters, shell companies, and unregulated money services businesses to send money upstream.[23] The large profits suggest that human trafficking organizations' funds flows may have a strong signal in the international financial system, but, according to the FATF, they are not readily distinguishable as the proceeds of human trafficking once they move upstream.[24]

The U.S. Policy Response

Federal, state, and local authorities are working closely with the financial sector to detect human trafficking networks operating in the U.S. financial system.[25] Visa and Mastercard have banned customers whose businesses are at high risk for human trafficking from their networks,[26] as have leading fintech firms such as PayPal[27] and Stripe.[28] Iowa-based MetaBank developed a prepaid card monitoring effort that enables identification of suspicious activity with resulting referrals to law enforcement.[29]

Regulators have been active in warning financial institutions about illicit finance risks related to human trafficking. In 2014, the Treasury Department's Financial Crimes Enforcement Network (FinCEN) issued guidance to financial institutions that included more than a dozen red flags for human trafficking.[30] In 2018, the FATF issued its second report on human trafficking, which also included red flags.[31]

In 2017, FinCEN announced the FinCEN Exchange program.[32] The FinCEN Exchange program is a public-private sector partnership in which FinCEN, in close coordination with law enforcement, convenes regular briefings with financial institutions to exchange information on priority illicit finance threats, including human trafficking.[33] In August 2019, FinCEN announced a new division, the Global Investigations Division, focused on "identifying primary foreign money laundering threats."[34] The new division will be dedicated to strategic use of FinCEN's Section 311 authority and to FinCEN's targeted information collection authorities.[35]

Nonetheless, gaps in our financial transparency regime make investigating human trafficking difficult for both financial institutions and law enforcement. Payments involving human trafficking victims and low-level operatives tend to involve small amounts, well below the $5,000 SAR threshold,[36] challenging financial institutions' anti-money laundering (AML) programs, which are geared primarily toward detecting larger payments.[37] At higher levels of human trafficking organizations, criminal organizations employ sophisticated money laundering techniques to evade detection, including by exploiting anonymous shell companies to conceal their activities.[38] As a result, investigations can be lengthy.

Strengthening Financial Transparency to Combat Human Trafficking

The heinousness of human trafficking demands a swift response that enables financial institutions to prevent financial transactions related to human trafficking or to detect them quickly once they have occurred. We can better protect our financial system by banning anonymous companies, strengthening cryptocurrency regulation, and improving transparency of retail and other consumer payments.

Anonymous Companies

Congress should ban anonymous companies.

The ILLICIT CASH Act that U.S. Senators Tom Cotton, Mark R. Warner, Doug Jones, and Mike Rounds released in June is one of several legislative efforts to eliminate the leading vulnerability in the U.S. financial transparency regime: anonymous companies. Such companies have been a persistent weak spot in our efforts to prevent money laundering and disrupt criminal organizations. They were mentioned in the first-ever National Money Laundering Strategy in 1999[39] and highlighted as a major vulnerability in the National Money Laundering Risk Assessment in 2015[40] and again in the National Money Laundering Risk Assessment in 2018.[41]

Anonymous companies may present themselves in one of two forms: Anonymous shell companies or anonymous front companies. Shell companies are legal entities without active business operations or a physical presence.[42] They often lack employees.[43] They have some legitimate business purposes because they can be formed cheaply and have little or no overhead.[44] But those same characteristics make them very attractive for illicit actors.

Alternatively, anonymous companies may take the form of front companies. Front companies have real, licit business operations that provide cover for illicit activity.[45] Front companies' licit business operations makes illicit activity even more difficult to detect and investigate.[46]

Regardless of whether they are established as shell companies or front companies, anonymous companies are the ultimate utility player in a money laundering operation. Their primary role is to conceal criminals' identities. But they can do much more. Anonymous companies can conceal relationships among the parties to a transaction, as in the case of the Russian Laundromat scandal,[47] to defeat financial institutions' anti-money laundering detection systems. They also can conceal sanctions evasion, as in the case of ZTE[48] or North Korea.[49] And they can hide a politically exposed person's interest in a transaction, as seen in the behavior of corrupt officials in Venezuela[50] and throughout the world.[51]

Human trafficking organizations and other transnational criminal organizations have exploited anonymous companies for decades.[52] In many places in the United States, obtaining a library card requires more documentation than forming a legal entity.[53] The ease with which anonymous companies can be formed makes identifying criminals more difficult, lengthening the time that it takes law enforcement to disrupt human trafficking networks if they can disrupt them at all.[54] In 2016, the FATF took the United States to task for failing to ensure that accurate ownership information is available for legal entities formed in the United States.[55]

Convertible Virtual Currencies

Congress should create a new class of financial institution under the BSA to cover firms involved in convertible virtual currency transactions: virtual asset service providers (VASPs), which are firms involved in convertible virtual currency transactions. VASPs should include cryptocurrency service providers that are already covered by the BSA as well as virtual asset services that currently fall outside the scope of the BSA.

A convertible virtual currency is a "medium of exchange that can operate like currency but does not have all the attributes of 'real' currency."[56] Bitcoin is a convertible virtual currency. Virtual assets are a class of financial assets that includes convertible virtual currencies.[57] They have proved vulnerable to criminal exploitation. According to one study, illicit Bitcoin transactions are on a pace to top $1 billion this year.[58] Protecting virtual assets from illicit finance will become even more important as virtual assets become more credible challengers to existing consumer payment tools.

Virtual assets are vulnerable to illicit finance because they offer rapid and irrevocable settlement and the potential for anonymity. Importantly, some virtual assets are traded through decentralized networks, with no central oversight body.[59] In other words, there is no entity performing a governance function and controlling admission to the payment system. In practice, the lack of a central oversight body means that anyone can create a VASP and begin facilitating transactions. As this committee considers how best to regulate VASPs, it should ensure that when U.S. authorities identify a rogue VASP, they can effectively prevent that VASP from exposing the U.S. financial system to illicit finance risk, because the trend toward decentralized and autonomous systems threatens our ability to control access to the U.S. financial system.

Effectively safeguarding virtual assets requires a regime that acknowledges that VASPs are not a unitary class of financial institutions and instead recognizes that VASPs play different roles in facilitating virtual asset transactions. Some VASPs are currently regulated as money transmitters under the BSA. Others are not regulated at all. Even for those VASPs currently regulated as money transmitters, the regulations are insufficient to protect virtual assets from exploitation. VASPs should be regulated based on the particular service or services that they provide, with an emphasis on promoting system-wide governance to prevent bad actors from establishing VASPs and connections to the international financial system.

- *Virtual Asset Exchangers*: Virtual asset exchangers dealing in convertible virtual currencies are currently regulated as money services businesses (MSBs) under the BSA. Virtual asset exchangers exchange fiat currencies for virtual assets and are the gateways for people and businesses who seek to transact in virtual assets. Virtual asset exchangers are required to keep records, maintain effective AML programs, and file SARs. They also should be required to establish risk-based customer identification programs and to conduct customer due diligence (CDD), because the transaction-based customer identification requirements currently in place under the existing MSB regime are insufficient to mitigate risk for account-based products and services.

- *Virtual Asset Issuers*: The initial issuance of virtual assets, including the initial offering a virtual coin, is money transmission under the BSA when an asset issuer sells a convertible virtual currency.[60] Virtual asset issuers should be subject to the same requirements as virtual asset exchangers, with a special emphasis on conducting enhanced due diligence on virtual asset buyers that are financial institutions, because virtual asset issuers are well positioned to play a strong governance role when creating new virtual assets.

- *Virtual Asset Custody Services*: Virtual asset custody services hold funds on behalf of customers and are currently MSBs under the BSA.[61] Virtual asset custody services are required to keep records, maintain effective AML programs, and file SARs. They also should be required to establish risk-based customer identification programs and to conduct CDD, because the transaction-based customer identification requirements currently in place under the existing MSB regime are insufficient to mitigate risk for account-based products and services.

- *Virtual Asset Transaction Validators*: Individuals and entities that validate virtual asset transactions are as critical to the success of virtual assets as credit card system operators are to credit cards because without transaction validation, the custody of a virtual asset cannot be assigned from one person to another. Virtual asset transaction validation – known alternatively as mining[62] – is not currently regulated under the BSA,[63] but virtual asset transaction validators could be gatekeepers for virtual asset systems if they are brought into the scope of the BSA. At minimum, virtual asset transaction validators should be required to govern participation in their validation systems, with well-designed programs for vetting the issuers, exchangers, and custodians that they serve.

- *Non-Custodial Virtual Asset Wallets*: Non-custodial virtual asset wallets allow virtual asset users to store their assets on a personal device rather than in a financial institution. Personal ownership and use of non-custodial wallets are not currently regulated under the BSA.[64] Strong consideration should be given to prohibiting virtual asset transaction validators from allowing non-custodial wallets to transact through their systems. Non-custodial wallets also should be subject to border declaration requirements, just as cash and other bearer instruments are. However, even with those safeguards in place, non-custodial virtual asset wallets would remain very attractive to people engaged in illicit activity.

Imposing regulations on people and entities who perform these functions almost certainly would make it difficult for some existing implementations of blockchain-based payments to continue operating as they do today. But it is not the purpose of the BSA or the global financial transparency regime to enable or accommodate all manner of financial products and services, regardless of the threat that they pose to financial transparency. Indeed, some financial products services have been deemed so risky that they have been banned.

- *Bearer Shares:* All 50 states prohibit the issuance of bearer shares,[65] and the ILLICIT CASH Act would ban bearer shares at the national level.[66] The FATF has recommended that countries ban bearer shares and convert any outstanding bearer shares into registered shares or immobilize them.[67]

- *Shell Banks:* The FATF recommends that regulators not license shell banks, and U.S. financial institutions are prohibited from entering into correspondent banking relationships with shell banks.[68]

- *Anonymous Accounts:* The FATF recommends that financial institutions should be prohibited from keeping "anonymous accounts or accounts in obviously fictitious names,"[69] and U.S. financial institutions that are covered by a customer identification program rule are prohibited from offering anonymous accounts.[70]

New York County District Attorney Cyrus Vance last year told the House Committee on Financial Services that some VASPs "appear to cater to traffickers who are trying to post advertisements."[71] Because of their potential for anonymity, virtual assets pose challenges for investigators. Even when a virtual asset has a public ledger that allows for transactions to be traced, connecting a transaction to an individual is difficult, unless that individual has been identified by a financial institution or has associated himself or herself with a wallet address through other means. Transaction data alone is of limited value, which is why anonymous accounts have been banned elsewhere in the financial system.

Consumer Payment Systems

Money transmission regulations should be revised to require that money transmitters that maintain accounts for their customers implement risk-based customer identification and CDD programs, and exclusions to the definition of money transmission should be narrowed.

The payments landscape has changed considerably during the past two decades, starting with the founding of PayPal in December 1998.[72] As Bank of England Governor Mark Carney recently said, "Retail transactions are taking place increasingly online rather than on the high street, and through electronic payments over cash. And the relatively high costs of domestic and cross border electronic payments are encouraging innovation, with new entrants applying new technologies to offer lower cost, more convenient retail payment services."[73]

As payments evolve, the BSA must evolve with them. The BSA regulations for money transmitters are insufficient to address the risk resulting from the evolution of consumer payments, because they do not adequately cover customer identification for account holders and because exclusions to the definition of money transmission under the BSA leave our payment systems exposed to illicit activity.

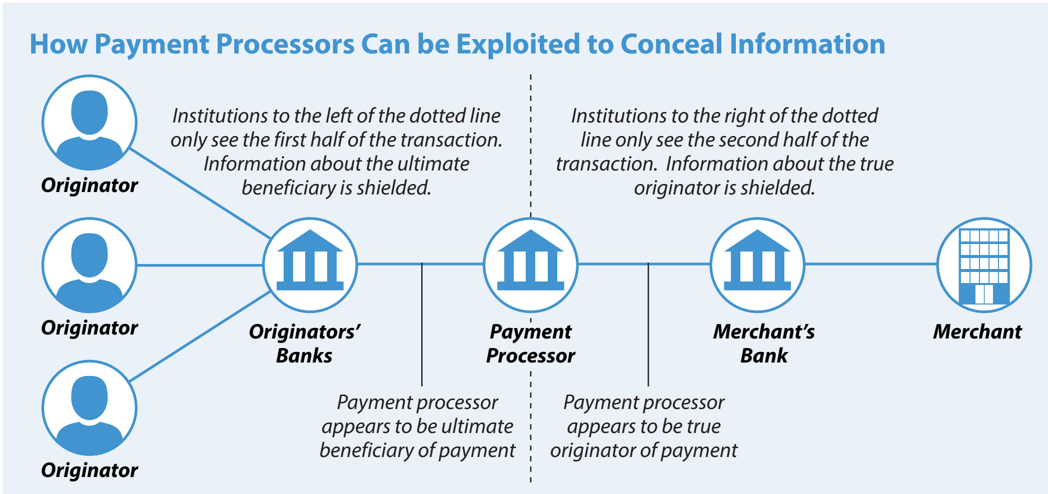
The first deficiency in our money transmission regulations arises from customer identification and CDD requirements. The money transmission regulations that cover an increasing number of consumer payments are geared toward financial institutions that serve occasional customers. This is most clear in the lack of customer identification and CDD rules governing account relationships with MSBs, even though many MSBs maintain accounts for their customers, especially in the online consumer payments and virtual assets segments. Instead, MSBs are only required to identify customers who carry out transactions worth $3,000 or more.[74] In contrast, banks must perform customer identification and CDD at account opening.[75] The opportunity for regulatory arbitrage is clear. Although many MSBs have implemented risk-based customer identification and CDD programs with thresholds below $3,000 that mirror those of banks, the lack of a legal requirement leaves bad actors space to operate.

The second deficiency in our money transmission regulations arises from exclusions from the definition of money transmission. In 2011, FinCEN issued a rule that added facts and circumstances limitations to the definition of money transmission.[76] One such limit on this definition is particularly noteworthy: Firms that act as a payment processor to facilitate payments through a clearance and settlement system by written agreement with the seller are excluded from the definition of money transmission and thus are not subject to the BSA.[77] FinCEN refers to this as exclusion as "the payment processor exemption."[78]

The 2011 rulemaking codified administrative rulings that FinCEN had issued since the early 2000s.[79] The payment processor exemption was initially intended to apply to payments that posed little illicit finance risk,[80] such as utility payments,[81] so the exemption made sense when FinCEN developed it.

But the effect of the payment processor exemption has outgrown its original rationale. The payment processor exemption is now being relied upon by fintech firms with more diverse and higher risk business models.[82] Moreover, the types of payments handled by payment processors have more explanatory power than was believed when the exemption was created, judging from the red flags published by FinCEN and the FATF. But the payment processor exemption allows payment processors to act as unregulated financial cutouts between buyers and sellers,[83] impairing visibility into merchant behavior and risk.[84]

In practice, this means that when a bank's merchant customer receives money through a payment processor that aggregates incoming payments and sweeps those funds into the merchant customer's account on a periodic basis, the merchant's bank has reduced visibility into that merchant's source of funds. The merchant's bank only sees large transactions coming from the payment processor to the merchant's account at the bank. In other words, the end-to-end payment chain, which includes the originator, intermediaries and ultimate beneficiary of the payment, is not seen by a single party with a transaction monitoring obligation, and the financial institution at the end of the payment chain may not be able to determine the source of funds for sanctions screening purposes.



The merchant's bank does not know whether its merchant customer is receiving funds from U.S. or foreign buyers, it does not know its customer's average retail transaction amount, and it does not know its customer's rate of returned or reversed transactions. These are key factors that banks use to risk rate their customers and to determine whether to file a SAR.

When payment chains become longer and banks lose visibility, they are not as well positioned to manage risk or assist law enforcement efforts to disrupt criminal activity. And as payment chains become longer, the payment processor, which may be excluded from the definition of money transmitter under the BSA, becomes the party with the best insight into a merchant's risk. It is therefore vital that payment processors be covered by appropriate financial transparency measures when they have the best insight into merchants' activities and risk.

Money launderers acting as payment processors have gained access to U.S. clearance and settlement networks, and the exclusions to the definition of money transmission probably gave the bad actors space to operate within the U.S. financial system for long periods of time. In 2016, the Treasury Department's Office of Foreign Assets Control (OFAC) sanctioned the PacNet Group, which was "the third-party payment processor of choice for perpetrators of a wide range of mail fraud schemes."[85] In 2019, OFAC sanctioned the Smile Group, which funneled drug proceeds to an Argentina-based online pharmacy.[86] The Smile Group offered international credit card payments, point-of-sale terminals, prepaid cards, and Bitcoin trading.[87] The Smile Group claimed to have relationships with major U.S.-based credit card system operators and online payment systems.[88] It courted customers engaged in high-risk businesses such as adult content, online gaming, health and wellness products, dating, and call centers.[89]

Many of the human trafficking red flags identified by FinCEN[90] and the FATF[91] rely on visibility into consumer payments. Therefore, maintaining and improving visibility into these payments is critical to detecting human trafficking activity. The gaps in the regulatory regime governing consumer payments should be closed, particularly the gaps in customer identification and the gaps in the definition of money transmission that allow some higher risk businesses to operate outside the BSA framework.

Endnotes

1 International Labour Office, "PROFITS AND POVERTY: The economics of forced labour," May 20, 2014, Page 13, https://www.ilo.org/wcmsp5/groups/public/---ed_norm/---declaration/documents/publication/wcms_243391.pdf.

2 International Labour Office, "PROFITS AND POVERTY: The economics of forced labour," May 20, 2014, Page 14, https://www.ilo.org/wcmsp5/groups/public/---ed_norm/---declaration/documents/publication/wcms_243391.pdf.

3 Treasury Department, "National Money Laundering Risk Assessment," June 12, 2015, Page 23, https://www.treasury.gov/resource-center/terrorist-illicit-finance/Documents/National%20Money%20Laundering%20Risk%20Assessment%20–%2006-12-2015.pdf.

4 Treasury Department, Treasury Department, "National Money Laundering Risk Assessment," June 12, 2015, Page 11, https://www.treasury.gov/resource-center/terrorist-illicit-finance/Documents/National%20Money%20Laundering%20Risk%20Assessment%20–%2006-12-2015.pdf.

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

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

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

8 FinCEN, "FinCEN Launches "FinCEN Exchange" to Enhance Public-Private Information Sharing," Dec. 4, 2017, https://www.fincen.gov/news/news-releases/fincen-launches-fincen-exchange-enhance-public-private-information-sharing.

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

10 Office of Tom Cotton, "Cotton, Colleagues Unveil Legislation to Combat Terror Finance, Money Laundering," June 10, 2019, https://www.cotton.senate.gov/?p=press_release&id=1151.

11 FATF, "Virtual Currencies Key Definitions and Potential AML/CFT Risks," June 2014, https://www.fatf-gafi.org/media/fatf/documents/reports/Virtual-currency-key-definitions-and-potential-aml-cft-risks.pdf.

12 Bloomberg, "After Danske, New Dirty Money Risk Seen in Payment Services," March 17, 2019, https://www.bloomberg.com/news/articles/2019-03-17/after-danske-next-dirty-money-route-gets-scrutinized-in-denmark.

13 United Nations Office on Drugs and Crime, "Global Report on Trafficking in Persons 2018," December 2018, Page 71, https://www.unodc.org/documents/data-and-analysis/glotip/2018/GLOTiP_2018_BOOK_web_small.pdf.

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

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

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

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

18 Cyrus Vance, House Financial Services Committee, January 30, 2018.

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

20 Cyrus Vance, House Financial Services Committee, January 30, 2018.

21 Yelp review of massage parlor whose owner was indicted on human trafficking charges.

22 International Labour Office, "PROFITS AND POVERTY: The economics of forced labour," May 20, 2014, Page 13, https://www.ilo.org/wcmsp5/groups/public/---ed_norm/---declaration/documents/publication/wcms_243391.pdf.

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

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

25 Cyrus Vance, House Financial Services Committee, January 30, 2018.

26 Cyrus Vance, House Financial Services

Committee, January 30, 2018.

27 PayPal, "Acceptable Use Policy," June 15, 2018, https://www.paypal.com/us/webapps/mpp/ua/acceptableuse-full.

28 Stripe, "Restricted Businesses," March 15, 2019, https://stripe.com/restricted-businesses.

29 Rick McDonnell, "Banks-The Unexpected Heroes In The War Against Human Trafficking," Fortune.com, July 17, 2018.

30 FinCEN, "Guidance on Recognizing Activity that May be Associated with Human Smuggling and Human Trafficking – Financial Red Flags," Sept. 11, 2014, https://www.fincen.gov/sites/default/files/advisory/FIN-2014-A008.pdf

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

32 FinCEN, "FinCEN Seeks to Strengthen Public-Private Partnership to Combat Financial Crime," Dec. 4, 2017, https://www.fincen.gov/news/news-releases/fincen-launches-fincen-exchange-enhance-public-private-information-sharing.

33 FinCEN, "FinCEN Seeks to Strengthen Public-Private Partnership to Combat Financial Crime," Dec. 4, 2017, https://www.fincen.gov/news/news-releases/fincen-launches-fincen-exchange-enhance-public-private-information-sharing.

34 FinCEN, "New FinCEN Division Focuses on Identifying Primary Foreign Money Laundering Threats," August 28, 2019, https://www.fincen.gov/news/news-releases/new-fincen-division-focuses-identifying-primary-foreign-money-laundering-threats.

35 FinCEN, "New FinCEN Division Focuses on Identifying Primary Foreign Money Laundering Threats," August 28, 2019, https://www.fincen.gov/news/news-releases/new-fincen-division-focuses-identifying-primary-foreign-money-laundering-threats.

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

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

38 Cyrus Vance, House Financial Services Committee, January 30, 2018.

39 Treasury Department and the Justice Department, "The National Money Laundering Strategy for 1999," September 1999, https://www.treasury.gov/press-center/press-releases/Documents/money.pdf.

40 Treasury Department, "National Money Laundering Risk Assessment," 2015, https://www.treasury.gov/resource-center/terrorist-illicit-finance/Documents/National%20Money%20Laundering%20Risk%20Assessment%20–%2006-12-2015.pdf.

41 Treasury Department, "National Money Laundering Risk Assessment 2018," Dec. 20, 2018, Page 28, https://home.treasury.gov/system/files/136/2018NMLRA_12-18.pdf.

42 FATF, "Transparency And Beneficial Ownership," October 2014, available at http://www.fatf-gafi.org/media/fatf/documents/reports/Guidance-transparency-beneficial-ownership.pdf.

43 Chip Poncy, "Beneficial Ownership: Fighting Illicit International Financial Networks Through Transparency," Feb. 6, 2018, available at http://www.financialintegritynetwork.net/uploads/8/7/8/0/87802750/2018.02.05_c.poncy_testimony_for_senate_judiciary_committee.pdf.

44 Jim Zarroli, "Want to Set Up a Shell Corporation to Hide Your Millions? No Problem," NPR, available at https://www.npr.org/2016/04/13/474101127/want-to-set-up-a-shell-corporation-to-hide-your-millions-no-problem.

45 Chip Poncy, "Beneficial Ownership: Fighting Illicit International Financial Networks Through Transparency," Feb. 6, 2018, available at http://www.financialintegritynetwork.net/uploads/8/7/8/0/87802750/2018.02.05_c.poncy_testimony_for_senate_judiciary_committee.pdf.

46 Chip Poncy, "Beneficial Ownership: Fighting Illicit International Financial Networks Through Transparency," Feb. 6, 2018, available at http://www.financialintegritynetwork.net/uploads/8/7/8/0/87802750/2018.02.05_c.poncy_testimony_for_senate_judiciary_committee.pdf.

47 OCCRP, "The Russian Laundromat Exposed," March 20, 2017, available at https://www.occrp.org/en/laundromat/the-russian-laundromat-exposed/.

48 Treasury Department, "Settlement Agreement between the U.S. Department of the Treasury's Office of Foreign Assets Control and Zhongxing Telecommunications Equipment Corporation," March 7, 2017, https://www.treasury.gov/resource-center/sanctions/CivPen/Documents/20170307_zte_settlement.pdf.

49 Financial Crimes Enforcement Network, "Advisory on North Korea's Use of the International Financial System," Nov. 2, 2017, available at https://www.fincen.gov/sites/default/files/advisory/2017-11-02/DPRK%20Advisory%20FINAL%20508%20C.pdf.

50 Financial Crimes Enforcement Network, "Advisory on Widespread Public Corruption in Venezuela," Sept. 20, 2017, available at https://www.fincen.gov/sites/default/files/advisory/2017-09-20/FinCEN%20Advisory%20FIN-2017-A006-508%20Compliant.pdf.

51 Financial Crimes Enforcement Network, "Advisory on Human Rights Abuses Enabled by Corrupt Senior Foreign Political Figures and their Financial Facilitators," available at https://www.fincen.gov/sites/default/files/advisory/2018-06-12/PEP%20Facilitator%20Advisory_FINAL%20508.pdf.

52 Treasury Department and the Justice Department, "The National Money Laundering Strategy for 1999," September 1999, available at https://www.treasury.gov/press-center/press-releases/Documents/money.pdf.

53 Joshua Kirschenbaum and David Murray, Bloomberg Opinion, "Do You Know Which Nations Own Your Data? The U.S. Government Doesn't," May 23, 2019, https://www.bloomberg.com/opinion/articles/2019-05-23/private-equity-hides-foreign-capital-from-u-s-scrutiny.

54 Cyrus Vance, House Financial Services Committee, January 30, 2018.

55 FATF, "United States Mutual Evaluation Report," December 2016, available at http://www.fatf-gafi.org/media/fatf/documents/reports/mer4/MER-United-States-2016.pdf.

56 FinCEN, "Application of FinCEN's Regulations to Certain Business Models Involving Convertible Virtual Currencies," May 9, 2019, https://www.fincen.gov/sites/default/files/2019-05/FinCEN%20Guidance%20CVC%20FINAL%20508.pdf.

57 Financial Actions Task Force, "The FATF Recommendations," June 2019, http://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF%20Recommendations%202012.pdf.

58 Bloomberg, "Bitcoin Criminals Set to Spend $1 billion on Dark Web This year," July 1, 2019, https://www.bloomberg.com/news/articles/2019-07-01/bitcoin-criminals-set-to-spend-1-billion-on-dark-web-this-year.

59 FATF, "Virtual Currencies Key Definitions and Potential AML/CFT Risks," June 2014, https://www.fatf-gafi.org/media/fatf/documents/reports/Virtual-currency-key-definitions-and-potential-aml-cft-risks.pdf.

60 FinCEN, "Application of FinCEN's Regulations to Certain Business Models Involving Convertible Virtual Currencies," May 9, 2019, https://www.fincen.gov/sites/default/files/2019-05/FinCEN%20Guidance%20CVC%20FINAL%20508.pdf.

61 FinCEN, "Application of FinCEN's Regulations to Certain Business Models Involving Convertible Virtual Currencies," May 9, 2019, https://www.fincen.gov/sites/default/files/2019-05/FinCEN%20Guidance%20CVC%20FINAL%20508.pdf.

62 FATF, "Virtual Currencies: Key Definitions and Potential AML/CFT Risks," June 2014, https://www.fatf-gafi.org/media/fatf/documents/reports/Virtual-currency-key-definitions-and-potential-aml-cft-risks.pdf.

63 FinCEN, "Application of FinCEN's Regulations to Virtual Currency Mining Operations," Jan. 30, 2014, https://www.fincen.gov/sites/default/files/administrative_ruling/FIN-2014-R001.pdf.

64 FinCEN, "Application of FinCEN's Regulations to Certain Business Models Involving Convertible Virtual Currencies," May 9, 2019, https://www.fincen.gov/sites/default/files/2019-05/FinCEN%20Guidance%20CVC%20FINAL%20508.pdf.

65 FATF, "United States of America Mutual Evaluation Report 2006," June 23, 2006, http://www.apgml.org/includes/handlers/get-document.ashx?d=f747d950-9e02-4cd8-a933-6916782a3aee. Nevada and Wyoming subsequently prohibited bearer shares.

66 Office of Tom Cotton, "Cotton, Colleagues Unveil Legislation to Combat Terror Finance, Money Laundering," June 10, 2019, https://www.cotton.senate.gov/?p=press_release&id=1151.

67 FATF, "Transparency and Beneficial Ownership," October 2014, http://www.fatf-gafi.org/media/fatf/documents/reports/Guidance-transparency-beneficial-ownership.pdf.

68 FATF, "Methodology for Assessing Technical Compliance with the FATF Recommendations and the Effectiveness of AML/CFT Systems," February 2019, http://www.fatf-gafi.org/media/fatf/documents/methodology/FATF%20Methodology%2022%20Feb%202013.pdf.

69 FATF, "Methodology for Assessing Technical Compliance with the FATF Recommendations

and the Effectiveness of AML/CFT Systems," February 2019, http://www.fatf-gafi.org/media/fatf/documents/methodology/FATF%20Methodology%2022%20Feb%202013.pdf.

70 31 USC 5318(l).

71 Cyrus Vance, House Financial Services Committee, January 30, 2018.

72 PayPal, "Who We Are," undated, https://www.paypal.com/us/webapps/mpp/about.

73 Bank of England, "The Growing Challenges for Monetary Policy in the current International Monetary and Financial System," Aug. 23, 2019, https://www.bankofengland.co.uk/-/media/boe/files/speech/2019/the-growing-challenges-for-monetary-policy-speech-by-mark-carney.pdf.

74 31 CFR 1010.415.

75 31 CFR Part 1020.

76 76 FR 43596, July 21, 2011.

77 31 CFR 1010.100(ff)(5)(ii)(B).

78 FinCEN, "Application of Money Services Business Regulations to a Company Acting as an Independent Sales Organization and Payment Processor," Aug. 27, 2014, https://www.fincen.gov/sites/default/files/administrative_ruling/FIN-2014-R009.pdf.

79 74 FR 22129, May 12, 2009.

80 74 FR 22129, May 12, 2009.

81 FinCEN, "Whether an Authorized Agent for the Receipt of Utility Payments is a Money Transmitter," May 21, 2008, https://www.fincen.gov/sites/default/files/administrative_ruling/fin-2008-r006.pdf.

82 Mayer Brown, "California to Clarify Money Transmission Act Exemption Through Rulemaking," March 8, 2019, https://www.mayerbrown.com/-/media/files/perspectives-events/publications/2019/03/californiaclarifymoneytransmissionactexemptionthroughrulemaking.pdf.

83 FinCEN, "Application of Money Services Business Regulations to a Company Acting as an Independent Sales Organization and Payment Processor," August 27, 2014, https://www.fincen.gov/sites/default/files/administrative_ruling/FIN-2014-R009.pdf.

84 Bloomberg, "After Danske, New Dirty Money Risk Seen in Payment Services," March 17, 2019, https://www.bloomberg.com/news/articles/2019-03-17/after-danske-next-dirty-money-route-gets-scrutinized-in-denmark.

85 Treasury Department, "Treasury Sanctions Individuals and Entities as Members of the Pacnet Group," Sept. 22, 2016, https://www.treasury.gov/press-center/press-releases/Pages/jl5055.aspx.

86 Treasury Department, "Treasury Sanctions Argentina-based Goldpharma," May 23, 2019, https://home.treasury.gov/news/press-releases/sm694.

87 Smile Payments, "Partner Program," undated, http://smilepayments.com/en/partner-proram/.

88 Smile Payments, "Partner Program," undated, http://smilepayments.com/en/partner-proram/.

89 Smile Payments, "Rates," undated, http://smilepayments.com/en/rates/.

90 FinCEN, "Guidance on Recognizing Activity that May be Associated with Human Smuggling and Human Trafficking – Financial Red Flags," Sept. 11, 2014, https://www.fincen.gov/sites/default/files/advisory/FIN-2014-A008.pdf.

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