FINANCIAL INTEGRITY NETWORK

Protecting Our Elections: Examining Shell Companies and Virtual Currencies as Avenues for Foreign Interference

June 26, 2018

David Murray
Vice President
Financial Integrity Network

Thank you, Chairman Graham and Ranking Member Whitehouse, for convening this hearing to discuss protecting our elections from foreign interference through the exploitation of shell companies and virtual currencies. And thank you for the invitation to be here today. It is an honor to be before this subcommittee. Foreign interference in our democratic processes is a critical national security threat, and the American people are fortunate for your diligence in addressing this threat.

The concern about foreign interference in our elections predates the ratification of the Constitution. In 1788, Alexander Hamilton warned that "cabal, intrigue, and corruption" are the "most deadly adversaries of republican government" and that meddling by foreign powers was the chief threat to our new form of government.[1] Since then, Congress has acted to protect our elections and our campaigns from foreign interference. It has required agents of foreign governments to register[2] and lobbyists to disclose their activities.[3] And there is an entire title of the U.S. Code dedicated to voting and elections, a subtitle of which is dedicated to campaign finance.[4]

Despite these efforts, the United States remains vulnerable to foreign interference in our political and electoral processes, in part because of critical gaps in our financial transparency regime. Foreign adversaries can exploit companies formed in the United States and virtual currencies to defeat our campaign finance laws. Today, I will discuss how foreign actors have exploited these gaps to evade campaign finance laws. I will conclude by providing recommendations for strengthening financial transparency.

It is vital that we build a financial transparency regime that enables the exposure and interdiction of foreign covert influence campaigns in near real time, not merely a regime that enables investigation of them after the fact. I recommend three financial transparency measures to support interdiction:

- **Ban anonymous companies.** Much of the discussion surrounding company formation reform has focused on shell companies. Some shell companies serve perfectly legitimate purposes, and provided that they are formed in a transparent manner, they pose no threat to financial transparency.[5] But anonymous shell companies pose a particular danger and, along with anonymous front companies, are worthy of special attention.

- **Do not delay enforcement of the Customer Due Diligence (CDD) rule.**[6] The rule requires banks to identify the beneficial owners of companies that hold accounts and to make sure that their customers' activity is consistent with the banks' expectations, allowing illicit activity to be detected more quickly and more reliably.[7] A bill recently introduced in the House of Representatives

would delay enforcement of this rule.[8]

- **Require cross-border funds transfers to be reported.** As soon as possible, the Financial Crimes Enforcement Network (FinCEN) should require financial institutions to report international funds transfers. FinCEN proposed such a reporting requirement in 2010, but the proposal has not been finalized.[9] FinCEN already requires travelers to file reports when they cross the border with more than $10,000 in cash and other monetary instruments,[10] but a foreign adversary can transfer millions of dollars into the United States with no report required.

Funding for Covert Influence Campaigns

Foreign interventions in democratic processes are neither new nor limited to the United States.[11] Nor was the 2016 election cycle the first time the Soviet Union or Russia had attempted to influence a U.S. election.[12] During the Cold War, the Soviet Union attempted to prevent the election of President Truman in 1948 and of President Reagan in 1984.[13]

Indeed, as of 1984, the Soviet Union often employed covert influence – or "active measures" in the Soviet and Russian nomenclature – throughout the world to advance Soviet policy objectives, according to a National Intelligence Estimate (NIE) published that year.[14] "Active measures" mobilized "virtually every element of the Soviet party and state structure" to spread disinformation and support other political influence operations, according to the NIE.[15] In 1987, the FBI reported that the Soviet Union used front organizations in the United States to circumvent the Foreign Agents Registration Act and to conceal Soviet financial support for organizations in the United States.[16]

In 2016, Russian active measures blended covert intelligence operations with overt efforts by Russian Government agencies, state-funded media, third-party intermediaries, and paid social media users, according to a January 2017 Intelligence Community Assessment (ICA).[17] Though not novel, the Russian campaign was the "boldest yet" to target the United States and represented a "significant escalation in directness, level of activity, and scope of effort compared to previous operations aimed at US elections," according to the ICA.[18]

Because of the investigations into Russian interference that have been conducted during the past 18 months, we have much more granular detail available to us about the sources of, routes for, and efforts to conceal financing for Russian active measures than we have had in the past. According to a grand jury indictment, part of the Russian active

measures campaign targeting the 2016 U.S. elections was carried out by the Internet Research Agency LLC, a Russian firm whose operational hubs included an office in St. Petersburg, Russia.[19] As of September 2016, the Internet Research Agency's monthly budget was about $1.25 million, according to the indictment.[20]

According to the indictment, the Internet Research Agency bought political advertisements on U.S. social media websites in the names of U.S. persons and entities and solicited and compensated U.S. persons to promote or disparage candidates.[21] To pay for the advertisements, the Internet Research Agency used U.S. personas to establish Russian credit cards and bank accounts and to establish PayPal and cryptocurrency exchange accounts.[22] It also established bank accounts in the United States using stolen identities.[23] In addition, the Internet Research Agency purchased computer infrastructure located in the United States to conceal the organization's Russian origin and evade detection.[24]

Yevgeniy Prigozhin, a close confidante of Russian President Vladimir Putin,[25] funded the Internet Research Agency through companies that he controlled, according to the indictment.[26] The company that was the Internet Research Agency's primary source of funds labeled the payments as "related to software support and development" to conceal their true purpose.[27] Payments were funneled through 14 other entities to conceal their origin further.[28]

The outlays for the Internet Research Agency's operation were not large in the context of the Russian government's budget,[29] and only a fraction of the funds was spent in the United States, with the balance used to support operations in Russia.[30] Nonetheless, deliberate concealment was vital in order to prevent detection and defeat U.S. reporting requirements,[31] because covert influence requires dark funding in order to remain covert. If the funding trail led directly back to the Kremlin, this component of the active measures campaign would have unraveled.

In April, Facebook founder Mark Zuckerberg told the Senate's Commerce and Judiciary committees that his company would not be able to determine whether a U.S. shell company was actually a cutout for Russian intelligence services.[32] This is not a flaw in Facebook's vetting procedures. It is a flaw in our financial transparency regime. This very problem bedevils global financial institutions,[33] which have large investigative teams, and federal financial investigators,[34] who are the most sophisticated in the world. More importantly, this problem frustrates and ultimately undermines investigations by law enforcement and national security authorities across the full spectrum of illicit finance threats that we face.

The Russians' 2016 active measures were not the only attempt by a foreign actor to

intervene in a U.S. election in the past decade. Less well known is the case of Jose Susumo Azano Matsura, a wealthy Mexican businessman who between 2011 and 2013 tried to buy influence in San Diego through campaign spending.[35] In May 2012, Azano conspired with a U.S. person to form an independent expenditure committee, according to a criminal complaint filed in the Southern District of California.[36] Azano gave $100,000 to the independent expenditure committee, funneling the money through a U.S. shell company.[37] The committee spent $114,000 in support of a single mayoral candidate during the 2012 primary election.[38] In all, Azano spent $120,000 in support of the candidate.[39] Azano was convicted along with his U.S. co-conspirators in 2017.[40]

Our Financial Transparency Problem

Foreign adversaries have both low-tech and high-tech options for covertly funding interference operations that undermine democratic processes. Among the low-tech options, anonymous companies are the leading threat. Among high-tech options, virtual currencies are an emerging threat.

Anonymous Companies

The schemes described above illustrate how legal entities can be used to thwart our campaign finance laws. They were ultimately exposed, but not until after the elections. The lack of transparency deprived voters of facts that they deserved to have when casting their ballots.

Anonymous companies are our chief financial transparency challenge, affecting not only campaign finance, but the integrity of the U.S. financial system as a whole. It is not surprising that foreign actors would target this weak spot in our anti-money laundering regime as they seek to intervene in our domestic politics, because anonymous companies are a well-established money laundering vulnerability. They were mentioned in the first-ever National Money Laundering Strategy in 1999[41] and highlighted as a major vulnerability in the National Money Laundering Risk Assessment in 2015.[42]

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.[43] They often lack employees.[44] They are necessary for some legitimate business and can be formed cheaply with little overhead.[45] 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.[46] Front companies' licit business operations may provide more lead opportunities for investigators than shell companies, but their licit cover also makes illicit activity difficult to detect and investigate.[47]

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 so much more. Anonymous companies can conceal relationships among the parties to a transaction, as in the case of the Russian Laundromat scandal,[48] to defeat financial institutions' anti-money laundering detection systems. They can conceal sanctions evasion, as in the case of ZTE[49] or North Korea.[50] And they can hide a politically exposed person's interest in a transaction, as with corrupt officials in Venezuela[51] and throughout the world.[52]

Importantly, anonymous companies also can be used to conceal nationality, because a person from one country can form anonymous companies in many other countries.[53] This poses challenges to enforcing laws that proscribe foreign nationals' activities and to financial institutions attempting to determine the risk presented by a customer or transaction.

Anonymous companies adversely affect our national security in other ways as well. Transnational criminal organizations have exploited anonymous companies for decades.[54] Anonymous companies also undermine the effectiveness of U.S. sanctions,[55] because they make it difficult for banks to identify payments that should be blocked or rejected. In 2016, the Financial Action Task Force took the United States to task for failing to ensure that accurate ownership information is available for legal entities formed in the United States.[56]

Virtual Currencies

Virtual currencies are a newer financial transparency challenge. Some promote anonymity[57] and irreversible settlement,[58] two traits that are particularly attractive to criminals. They also facilitate peer-to-peer transactions, meaning that there is no financial institution between the sender and receiver of the transaction.[59] They have emerged as the chosen medium of exchange for people trafficking in illicit drugs online,[60] malware,[61] and child pornography.[62]

The Treasury Department has aggressively sought to curb the illicit use of virtual currencies. In 2013, FinCEN issued guidance clarifying that virtual currency exchangers are money services businesses subject to the Bank Secrecy Act (BSA).[63] FinCEN has

backed up that guidance with enforcement actions. In 2015, FinCEN cited Ripple Labs for failing to register with FinCEN, failing to implement and maintain an adequate anti-money laundering program, and failing to report suspicious activity related to several financial transactions.[64] In 2017, FinCEN brought an enforcement action against a foreign-located virtual currency exchanger, BTC-e.[65] FinCEN cited BTC-e for failing to register, failing to establish internal controls, and failing to collect CDD information.[66] BTC-e was assessed a $110 million civil monetary penalty.[67]

FinCEN guidance and enforcement actions made clear that the BSA covers virtual currency exchangers, even foreign-located virtual currency exchangers when they serve U.S. customers. Nonetheless, virtual currency exchangers remain vulnerable to illicit finance. Exchangers can hop from jurisdiction to jurisdiction in pursuit of favorable regulatory regimes,[68] and the anonymity that they afford users[69] could be attractive to foreign adversaries seeking to thwart campaign finance laws.

Campaigns may accept donations denominated in virtual currencies.[70] The Federal Election Commission requires donor attestations in these cases, as with other types of contributions.[71] However, because the transaction records needed to corroborate a donor's identity may in part be located in a foreign jurisdiction with a weak anti-money laundering regime or a limited record of cooperating with the United States, investigators may have difficulty gathering the financial records necessary to corroborate the information provided by the contributor.

Likewise, donations by foreign nationals are difficult to detect. Campaigns and political committees may not knowingly accept contributions from foreign nationals, but they are required only to take "minimally intrusive" steps to verify a contributor's true nationality.[72] As long as a contributor provides a donor attestation and uses a U.S. address, the contribution would appear legitimate and not prompt any additional due diligence requirements on the part of the recipient.[73]

Foreign-source donations are particularly difficult to detect when a non-intermediated payment method such as a virtual currency is used. In contrast, when donors use financial intermediaries such as banks to execute donations, the location of the financial intermediary is a data point that campaigns can use to identify foreign donors, with donations originating at foreign financial institutions carrying a higher risk of being from foreign donors.

Recommendations

As alarming as the idea of a foreign adversary launching a cyberattack on our election systems is, foreign intervention in political campaigns ahead of election day is more

likely. Foreign adversaries need not alter the outcome of an election to advance their objectives. Rather, they can weaken the United States simply by amplifying wedge issues and sowing perpetual discord, probably with less risk of blowback. Our system of free speech, combined with dramatic shifts during the past 20 years in the ways that Americans discover and consume information, leaves us extremely vulnerable to foreign interference. Enhancing the transparency of campaign finance requires urgent attention from lawmakers.

In national security matters, the primary objective of the United States should be intercepting threats before they can harm our citizens or our institutions. As much as successful prosecutions can satisfy our sense of justice, convictions are a poor remedy for national security harms. Thus, we should ensure that our law enforcement and intelligence agencies have the financial information needed to detect, monitor, and disrupt threats at the earliest possible stage.

Specifically, we should equip our law enforcement and intelligence agencies with reliable information about the ownership of companies formed in the United States, ensure that financial institutions are adequately monitoring their customer relationships, and require financial institutions to report cross-border financial transactions. Together, these three measures will enhance the transparency of campaign finance, and financial transparency as a whole.

Ban Anonymous Companies

First, as discussed earlier, anonymous companies are the most critical threat to financial transparency. The House Financial Services Committee released a draft bill in November 2017 that, if implemented, would effectively ban anonymous companies from being formed in the United States by requiring the names of beneficial owners of companies formed in the United States to be reported to FinCEN at the time of formation.[74] The bipartisan bill has been endorsed by transparency advocates,[75] the Delaware Secretary of State,[76] and the financial services industry.[77] The November proposal is the most direct remedy to the use of anonymous U.S. companies to circumvent campaign finance laws and other illicit finance threats, because there will no longer be anonymous U.S. companies once the bill becomes law and is implemented.

To be sure, this would be an additional regulatory burden for companies formed in the United States. But currently, determining the true, beneficial owner of a company is a burden that is spread across our economy. Banks face challenges in determining beneficial ownership when they establish accounts for businesses or when they investigate suspicious transactions, and businesses are currently on their own when they need to vet counterparties in commercial transactions. These costs, along

with the costs of fraud that anonymous companies conceal, are borne by every American, repeatedly.

Do Not Delay Enforcement of the CDD Rule

Second, the CDD rule that FinCEN issued in 2016 and went into effect last month should be enforced immediately. CDD is the core of an effective BSA compliance regime. Enforcement of the rule should not be delayed, as a House bill suggests.[78] Delaying enforcement of the rule would send a confusing message, particularly to banks, which were being held to account for the rule's substance even before it was proposed, according to the FFIEC.[79]

Effective CDD animates the suspicious activity reporting regime by ensuring that financial institutions have the ability to detect and report unusual transactions. Effective CDD, when paired with a strong suspicious activity monitoring program, makes it difficult for criminals to maintain accounts that were created with stolen identities or to use straw account holders to hide their identities. When effective CDD measures are in place, criminals must establish a plausible purpose for the account relationship and the nature of the transactions that they will conduct through the account.[80] This makes money laundering more difficult by requiring a new account holder to provide not only a valid identification but also a reasonable explanation for the expected account activity. If the actual account activity does not match the expected account activity, effective suspicious activity monitoring programs will generate alerts that provide early warning that illicit activity may be afoot.

Require Cross-Border Funds Transfers to be Reported

Third, FinCEN should require cross-border funds transfers to be reported by financial institutions. The Intelligence Reform and Terrorism Prevention Act of 2004 obligated FinCEN to require such reports, subject to a feasibility study and consultations with the Bank Secrecy Act Advisory Group.[81] In 2007, FinCEN determined that implementing the rule would be feasible,[82] and in 2009, FinCEN published an additional study of cross-border funds transfer reporting that examined implications and benefits.[83] In 2010, FinCEN proposed requiring money transmitters to report cross-border funds transfers worth $1,000 or more and requiring banks to report all cross-border funds transfers, but the proposal was never finalized.[84]

Because of technological advances,[85] this data would be more valuable today than it was in 2004 when Congress required the Treasury Secretary to collect it. The analysis of this data would be invaluable in determining how our adversaries are

exploiting the U.S. financial system and intercepting threats. Banks monitor these transfers today, but they do so without all of the information available to the U.S. government, and without knowledge of all the other wire transfers a person or entity is conducting through the United States. As a result, only a patchwork of cross-border wire transfer information is available for analysis through information currently filed by banks.

Combining comprehensive cross-border funds transfer records with information held only by the U.S. government could enable the rapid detection of illegal spending by foreign adversaries. Canada and Australia already have reporting requirements in place and have found that the data are valuable in combating transnational organized crime and terrorist financing.[86]

Alone, each of these recommendations would help protect our elections from interference. If implemented together, each would strengthen the others. Creating a reliable beneficial ownership registry would help banks conduct CDD. In turn, strong CDD programs would play a role in validating information in the registry and in identifying fraudulent registrations. Cross-border funds transfers records would become even more valuable if transfers by companies are matched with their true owners, so that analysts could attribute transactions to individuals with a high degree of certainty.

Endnotes

1 The Federalist No. 68, "Alexander Hamilton."

2 18 U.S.C. 2386.

3 18 U.S.C. 219.

4 52 U.S.C. 30101 et seq.

5 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.

6 Customer Due Diligence Requirements for Financial Institutions, 82 Fed. Reg. 91, May 11, 2016 (Final Rule).

7 Customer Due Diligence Requirements for Financial Institutions, 82 Fed. Reg. 91, May 11, 2016 (Final Rule).

8 H.R.6068, 115th Cong., June 12, 2018 (Referred to House Financial Services Committee), available at https://www.congress.gov/bill/115th-congress/house-bill/6068/text.

9 Cross-Border Electronic Transmittals of Funds, 75 Fed. Reg. 189, Sept. 30, 2010 (Proposed Rule).

10 31 U.S.C. 5136.

11 Dov Levin, "Sure, the U.S. and Russia often meddle in foreign elections. Does it matter?," The Washington Post, Sept. 7, 2016, available at https://www.washingtonpost.com/news/monkey-cage/wp/2016/09/07/sure-the-u-s-and-russia-often-meddle-in-foreign-elections-does-it-matter/?utm_term=.91324cbb9867.

12 Dov Levin, "Sure, the U.S. and Russia often meddle in foreign elections. Does it matter?," The Washington Post, Sept. 7, 2016, available at https://www.washingtonpost.com/news/monkey-cage/wp/2016/09/07/sure-the-u-s-and-russia-often-meddle-in-foreign-elections-does-it-matter/?utm_term=.91324cbb9867.

13 Dov Levin, "Sure, the U.S. and Russia often meddle in foreign elections. Does it matter?," The Washington Post, Sept. 7, 2016, available at https://www.washingtonpost.com/news/monkey-cage/wp/2016/09/07/sure-the-u-s-and-russia-often-meddle-in-foreign-elections-does-it-matter/?utm_term=.91324cbb9867.

14 Director of Central Intelligence, "The USSR and the Third World," Sept. 19, 1984 (sanitized copy approved for release June 28, 2010), available at https://www.cia.gov/library/readingroom/docs/CIA-RDP87T00126R000600630005-0.pdf.

15 Director of Central Intelligence, "The USSR and the Third World," Sept. 19, 1984 (sanitized copy approved for release June 28, 2010), available at https://www.cia.gov/library/readingroom/docs/CIA-RDP87T00126R000600630005-0.pdf.

16 Congressional Record, E4722, Statement of the Honorable C.W. "Bill" Young of Florida in the House of Representatives, Dec. 9, 1987, available at https://www.cia.gov/library/readingroom/docs/CIA-RDP11M01338R000400470089-2.pdf.

17 Office of the Director of National Intelligence, "Assessing Russian Activities and Intentions in Recent US Elections," Jan. 17, 2017, declassified version, available at https://www.dni.gov/files/documents/ICA_2017_01.pdf.

18 Office of the Director of National Intelligence, "Assessing Russian Activities and Intentions in Recent US Elections," Jan. 17, 2017, declassified version, available at https://www.dni.gov/files/documents/ICA_2017_01.pdf.

19 United States v. Internet Research Agency LLC et al, 1:18-cr-00032, U.S. District Court for the District of Columbia, Feb. 16, 2018.

20 United States v. Internet Research Agency LLC et al, 1:18-cr-00032, U.S. District Court for the District of Columbia, Feb. 16, 2018.

21 United States v. Internet Research Agency LLC et al, 1:18-cr-00032, U.S. District Court for the District of Columbia, Feb. 16, 2018.

22 United States v. Internet Research Agency LLC et al, 1:18-cr-00032, U.S. District Court for the District of Columbia, Feb. 16, 2018.

23 United States v. Internet Research Agency LLC et al, 1:18-cr-00032, U.S. District Court for the District of Columbia, Feb. 16, 2018.

24 United States v. Internet Research Agency LLC et al, 1:18-cr-00032, U.S. District Court for the District of Columbia, Feb. 16, 2018.

25 Marwa Eltagouri, "The rise of 'Putin's chef,' the Russian oligarch accused of manipulating the U.S. election," Feb. 17, 2018, available at https://www.washingtonpost.com/news/worldviews/wp/2018/02/16/the-rise-of-putins-chef-yevgeniy-prigozhin-the-russian-accused-of-manipulating-the-u-s-election/?utm_term=.b2f200346fff.

26 United States v. Internet Research Agency LLC et al, 1:18-cr-00032, U.S. District Court for the District of Columbia, Feb. 16, 2018.

27 United States v. Internet Research Agency LLC et al, 1:18-cr-00032, U.S. District Court for the District of Columbia, Feb. 16, 2018.

28 United States v. Internet Research Agency LLC et al, 1:18-cr-00032, U.S. District Court for the District of Columbia, Feb. 16, 2018.

29 Olag Tanas, "Russia Sticks to Conservative $40 Oil Forecast for 2018 Budget," Bloomberg, June 29, 2017, available at https://www.bloomberg.com/news/articles/2017-06-29/russia-sticks-to-conservative-40-oil-forecast-for-2018-budget.

30 United States v. Internet Research Agency LLC et al, 1:18-cr-00032, U.S. District Court for the District of Columbia, Feb. 16, 2018.

31 United States v. Internet Research Agency LLC et al, 1:18-cr-00032, U.S. District Court for the District of Columbia, Feb. 16, 2018.

32 "Transcript of Mark Zuckerberg's Senate hearing," April 10, 2018, available at https://www.washingtonpost.com/news/the-switch/wp/2018/04/10/transcript-of-mark-zuckerbergs-senate-hearing/?utm_term=.f68a3437af7a.

33 The Clearing House, Letter to Chairman and Ranking Member of the Senate Judiciary Committee, Aug. 8, 2016, available at https://www.theclearinghouse.org/-/media/tch/documents/research/articles/2016/08/20160808_tch_letter_incorporation_transparency_and_law_enforcement_assistance_act_support.pdf.

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

35 United States v. Ravneet Singh et al, 14MJ0201, U.S. District Court for the Southern District of California, Jan. 21, 2014.

36 United States v. Ravneet Singh et al, 14MJ0201, U.S. District Court for the Southern District of California, Jan. 21, 2014.

37 United States v. Ravneet Singh et al, 14MJ0201, U.S. District Court for the Southern District of California, Jan. 21, 2014.

38 United States v. Ravneet Singh et al, 14MJ0201, U.S. District Court for the Southern District of California, Jan. 21, 2014.

39 Justice Department, "Mexican Businessman Indicted in Broadening Campaign Finance Investigation," Feb. 20, 2014, available at https://www.justice.gov/sites/default/files/usao-sdca/legacy/2015/04/30/cas14-0220-AzanoIndict.pdf.

40 Justice Department, "Mexican Businessman Jose Susumo Azano Matsura Sentenced for Trying to Buy Himself a Mayor," Oct. 27, 2017, available at https://www.justice.gov/usao-sdca/pr/mexican-businessman-jose-susumo-azano-matsura-sentenced-trying-buy-himself-mayor.

41 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.

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

43 Financial Action Task Force, "Transparency And Beneficial Ownership," October 2014, available at http://www.fatf-gafi.org/media/fatf/documents/reports/Guidance-transparency-beneficial-ownership.pdf.

44 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.

45 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.

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 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.

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

49 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.

50 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.

51 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.

52 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.

53 International Consortium of Investigative Journalists, "The Panama Papers," undated, available at https://www.icij.org/investigations/panama-papers/.

54 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.

55 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.

56 Financial Action Task Force, "United States Mutual Evaluation Report," December 2016, available at http://www.fatf-gafi.org/media/fatf/documents/reports/mer4/MER-United-States-2016.pdf.

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

58 Director of National Intelligence, 2017 Public-Private Analytic Exchange Program, "Risks and Vulnerabilities of Virtual Currency," 2017, https://www.dni.gov/files/PE/Documents/9---2017-AEP_Risks-and-Vulnerabilities-of-Virtual-Currency.pdf.

59 Director of National Intelligence, 2017 Public-Private Analytic Exchange Program, "Risks and Vulnerabilities of Virtual Currency," 2017, https://www.dni.gov/files/PE/Documents/9---2017-AEP_Risks-and-Vulnerabilities-of-Virtual-Currency.pdf.

60 Director of National Intelligence, 2017 Public-Private Analytic Exchange Program, "Risks and Vulnerabilities of Virtual Currency," 2017, https://www.dni.gov/files/PE/Documents/9---2017-AEP_Risks-and-Vulnerabilities-of-Virtual-Currency.pdf.

61 Michael Bernardo, "Virtual Currencies: Bitcoin, Blockchains and Beyond," FDIC, Oct. 25, 2016, available at https://www.fdic.gov/conference/presentations/virtual_currencies_benardo.pdf.

62 Michael Bernardo, "Virtual Currencies: Bitcoin, Blockchains and Beyond," FDIC, Oct. 25, 2016, available at https://www.fdic.gov/conference/presentations/virtual_currencies_benardo.pdf.

63 FinCEN, "Application of FinCEN's Regulations to Persons Administering, Exchanging, or Using Virtual Currencies," March 18, 2013, available at https://www.fincen.gov/sites/default/files/shared/FIN-2013-G001.pdf.

64 FinCEN, in the matter of Ripple Labs Inc., May 5, 2015, available at https://www.fincen.gov/sites/default/files/shared/Ripple_Assessment.pdf.

65 FinCEN, in the matter of BTC-E a/k/a Canton Business Corporation and Alexander Vinnik, July 26, 2017, available at https://www.fincen.gov/sites/default/files/enforcement_action/2017-07-26/Assessment%20for%20BTCeVinnik%20FINAL%20SignDate%2007.26.17.pdf.

66 FinCEN, in the matter of BTC-E a/k/a Canton Business Corporation and Alexander Vinnik, July 26, 2017, available at https://www.fincen.gov/sites/default/files/enforcement_action/2017-07-26/Assessment%20for%20BTCeVinnik%20FINAL%20SignDate%2007.26.17.pdf.

67 FinCEN, in the matter of BTC-E a/k/a Canton Business Corporation and Alexander Vinnik, July 26, 2017, available at https://www.fincen.gov/sites/default/files/enforcement_action/2017-07-26/Assessment%20for%20BTCeVinnik%20FINAL%20SignDate%2007.26.17.pdf.

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

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

70 Federal Election Commission, Advisory Opinion 2014-02, May 8, 2014, available at https://www.fec.gov/files/legal/aos/2014-02/2014-02.pdf.

71 Federal Election Commission, Advisory Opinion 2014-02, May 8, 2014, available at https://www.fec.gov/files/legal/aos/2014-02/2014-02.pdf.

72 11 CFR 103.3(b)(1); Federal Election Commission, Advisory Opinion 1998-14, August 13, 1998, available at https://www.fec.gov/files/legal/aos/1998-14/1998-14.pdf.

73 11 CFR 103.3(b)(1); Federal Election Commission, Advisory Opinion 1998-14, August 13, 1998, available at https://www.fec.gov/files/legal/aos/1998-14/1998-14.pdf.

74 H.R. _____, "Counter Terrorism and Illicit Finance Act," Nov. 14, 2017, available at https://financialservices.house.gov/uploadedfiles/bills-115hr-pih-ctifa.pdf.

75 FACT Coalition, "Delaware Endorses Bill to Tackle Anonymous Companies," June 12, 2018, available at https://thefactcoalition.org/delaware-endorses-bill-to-tackle-anonymous-companies?utm_medium=press/news-releases.

76 Secretary Jeffrey W. Bullock, Letter to House Financial Services Committee Chairman and Ranking Member, June 8, 2018, available at https://thefactcoalition.org/wp-content/uploads/2018/06/DE-June-2018-Letter-to-HFSC-on-BOT.pdf.

77 Letter to the Honorable Steve Pearce and the Honorable Blaine Luetkemeyer, Jan. 4, 2018, available at https://www.sifma.org/wp-content/uploads/2018/02/Counter-Terrorism-and-Illicit-Finance-Act.pdf.

78 H.R.6068, 115th Cong., June 12, 2018 (Referred to House Financial Services Committee). Available at https://www.congress.gov/bill/115th-congress/house-bill/6068/text.

79 Federal Financial Institutions Examination Council, "Customer Due Diligence — Overview," May 5, 2018, available at https://www.ffiec.gov/press/pdf/Customer%20Due%20Diligence%20-%20Overview%20and%20Exam%20Procedures-FINAL.pdf.

80 Customer Due Diligence Requirements for Financial Institutions, 82 Fed. Reg. 91, May 11, 2016 (Final Rule).

81 31 U.S.C. 5318(n).

82 Cross-Border Electronic Transmittals of Funds, 75 Fed. Reg. 189, Sept. 30, 2010 (Proposed Rule).

83 Financial Crimes Enforcement Network, "Implications and Benefits of Cross- Border Funds Transmittal Reporting," January 2009, available at https://www.fincen.gov/sites/default/files/shared/ImplicationsAndBenefitsOfCBFTR.pdf.

84 Cross-Border Electronic Transmittals of Funds, 75 Fed. Reg. 189, Sept. 30, 2010 (Proposed Rule).

85 Juan C. Zarate and Chip Poncy, "Designing a New AML System," The Clearing House, Q3 2016, available at https://www.theclearinghouse.org/banking-perspectives/2016/2016-q3-banking-perspectives/articles/a-new-aml-system.

86 Financial Crimes Enforcement Network, "Implications and Benefits of Cross- Border Funds Transmittal Reporting," January 2009, available at https://www.fincen.gov/sites/default/files/shared/ImplicationsAndBenefitsOfCBFTR.pdf.