

August 2020

Do We Need KYC/AML: The Bank Secrecy Act and Virtual Currency Exchanges

Stan Sater

Founders Legal Bekiares Eliezer

Follow this and additional works at: <https://scholarworks.uark.edu/alr>



Part of the [Antitrust and Trade Regulation Commons](#), [Banking and Finance Law Commons](#), and the [E-Commerce Commons](#)

Recommended Citation

Stan Sater, *Do We Need KYC/AML: The Bank Secrecy Act and Virtual Currency Exchanges*, 73 Ark. L. Rev. 397 (2020).

Available at: <https://scholarworks.uark.edu/alr/vol73/iss2/5>

This Article is brought to you for free and open access by ScholarWorks@UARK. It has been accepted for inclusion in Arkansas Law Review by an authorized editor of ScholarWorks@UARK. For more information, please contact ccmiddle@uark.edu.

DO WE NEED KYC/AML: THE BANK SECRECY ACT AND VIRTUAL CURRENCY EXCHANGES

Stan Sater*

Technology is moving faster than government or law can keep up. It's moving faster than you can keep up: you should be asking the question of what are your rights and who owns your data.

– Gus Hunt,
2013 CIA Chief Technology Officer¹

I. INTRODUCTION

The Currency and Foreign Transactions Reporting Act, commonly referred to as the Bank Secrecy Act (the BSA), is the U.S. government's 800-pound gorilla when it comes to regulating virtual currency.² It has been expanded, transformed, and updated since its initial passage in 1970 to keep pace with new developments in global terrorism and money laundering, all the while only being challenged twice on its constitutional merits.³ The BSA, as notably amended by the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (USA PATRIOT Act), imposes financial recordkeeping and reporting requirements, know your customer (KYC) requirements, and requirements to

* Associate, Founders Legal | Bekiares Eliezer, LLP; J.D. 2019 Tulane University Law School.

1. EDWARD SNOWDEN, PERMANENT RECORD 248 (2019) (quoting Ira “Gus” Hunt) (quotation marks omitted and alteration adopted).

2. Currency and Foreign Transactions Reporting Act, Pub. L. No. 91-508, 84 Stat. 1118 (1970).

3. United States v. Miller, 425 U.S. 435, 441, 443 (1976); Cal. Bankers Ass'n v. Shultz, 416 U.S. 21, 54 (1974); see PETER VAN VALKENBURGH, ELECTRONIC CASH, DECENTRALIZED EXCHANGE, AND THE CONSTITUTION 7 (2019), [https://perma.cc/LG8E-NSM8]; BSA Timeline, FIN. CRIMES ENFORCEMENT NETWORK, [https://perma.cc/N5NJ-AMP7] (last visited Nov. 28, 2019). Most recently, the U.S. Supreme Court declined to overrule Miller in its Carpenter decision. Carpenter v. United States, 138 S. Ct. 2206, 2220 (2018) (“We do not disturb the application of Smith and Miller . . .”).

implement and maintain an anti-money laundering (AML) program.⁴ Noncompliance can lead to both civil money penalties of varying amounts and criminal penalties of up to twenty-years imprisonment.⁵

The BSA imposes these recordkeeping and reporting requirements not on suspected criminals but on the financial institutions. In this way, every financial institution, as that term is broadly defined in the BSA, has been deputized as a law enforcement agent constantly surveilling its customers and reporting information to the government that is determined to “have a high degree of usefulness in criminal, tax, or regulatory investigations or proceedings, or in the conduct of intelligence or counterintelligence activities, including analysis, to protect against international terrorism.”⁶ At the center of this mass financial data gathering dragnet is the Financial Crimes Enforcement Network (FinCEN). FinCEN administers the BSA rules and implements regulations (BSA Regulations) through its delegated authority by the Department of Treasury.⁷

The emergence of bitcoin and other virtual currencies raised an important question as to the scope of the BSA and FinCEN’s authority. The question is whether the BSA and FinCEN’s authority governing legacy financial institutions could be imputed onto a new financial system that seeks the removal of the very intermediaries that previously acquiesced to FinCEN’s authority. In 2013, FinCEN published guidance titled *Application of FinCEN’s Regulations to Persons Administering, Exchanging, or Using Virtual Currencies (2013 Guidance)*.⁸ The 2013 Guidance

4. Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT ACT) Act of 2001, Pub. L. No. 107-56, 115 Stat. 272 (codified in scattered sections in numerous titles of U.S.C.).

5. 18 U.S.C. § 1956 (2018); 31 C.F.R. §§ 1010.820, .840 (2019).

6. 31 U.S.C. §§ 5311, 5312(a)(2) (2012).

7. *What We Do*, FIN. CRIMES ENFORCEMENT NETWORK, [<https://perma.cc/JFV3-RDT2>] (last visited Mar. 20, 2020). The Office of Comptroller of the Currency (OCC), the Federal Deposit Insurance Corporation (FDIC), the Federal Reserve, and the National Credit Union Administration also have authority to enforce the BSA against their respective regulated institutions. See 12 U.S.C. §§ 1786, 1818(i)(2) (2018); 15 U.S.C. § 78u (2012); 31 C.F.R. § 1023.220 (2019).

8. FIN. CRIMES ENF’T NETWORK, U.S. DEP’T OF THE TREASURY, FIN-2013-G001, APPLICATION OF FINCEN’S REGULATIONS TO PERSONS ADMINISTERING, EXCHANGING, OR

interpreted the BSA Regulations and contextualized them to the virtual currency ecosystem while also inventing new terms such as “user,” “exchanger,” “administrator,” “virtual currency,” and “convertible virtual currency.”⁹ In subsequent guidance and administrative rulings, FinCEN regularly uses these terms as well as defining new terms to continually apply the BSA Regulations to different business models that are of note in the virtual currency ecosystem.¹⁰

Along with putting forth continual regulatory guidance, FinCEN has issued three enforcement actions. Two of the three enforcement actions directly relate to virtual currency exchange activities. Based on the resulting civil money penalties from the enforcement actions as well as criminal prosecutions citing violations of the BSA since 2013, it is evident that virtual currency businesses and individuals are being subject to the full spectrum of the BSA. While FinCEN issues new guidance and publishes public remarks, its goal of fostering a “culture of compliance” rather amounts to a culture of coerced compliance that necessitates a further inspection into whether the potential benefits from the financial information gleaned from the BSA requirements outweigh the privacy infractions of individuals and businesses.¹¹

The structure of this Article is in three parts. Parts II discusses the history of FinCEN and how it became the lead enforcer of the BSA, the most influential financial law in the United States. Part III consolidates and explains FinCEN’s regulations, previous administrative rulings, and guidance involving the regulation of money transmission under the BSA as applied to virtual currency exchanges. This Part further weaves in criminal prosecutions

USING VIRTUAL CURRENCIES 1 (Mar. 18, 2013), [<https://perma.cc/XQ8Y-G6A4>] [hereinafter 2013 GUIDANCE].

9. *Id.* at 1-3.

10. See Kenneth A. Blanco, Director, Fin. Crimes Enf’t Network, Prepared Remarks Delivered at the 2018 Chicago-Kent Block (Legal) Tech Conference (Aug. 09, 2018), [<https://perma.cc/2FWS-ZS67>].

11. *Id.* In the six months following FinCEN’s May 2019 Guidance, FinCEN received over 10,000 Suspicious Activity Reports (“SARs”) related to convertible virtual currency. More than 1,900 unique filers, most of whom never filed SARs prior to May 2019, directly referenced certain key terms found in the 2019 Guidance. Kenneth A. Blanco, Director, Fin. Crimes Enf’t Network, Prepared Remarks Delivered at Chainalysis Blockchain Symposium (Nov. 15, 2019), [<https://perma.cc/V8TW-RP4D>] [hereinafter New York City-Blanco Remarks].

concerning virtual currency exchanges and how virtual currency exchanges have evolved based on such criminal prosecutions. Part IV highlights how the industry has proactively responded to public guidance, statements, and actions from FinCEN and other financial KYC/AML regulators. Through the industry's response to mainly FinCEN, the industry has splintered into custodial products and services that mirror the legacy financial system and non-custodial products and services. The non-custodial products and services being built for the future of virtual currency do not exhibit the same information risks and characteristics as their custodial, command and control financial institution counterparts as the users allows remain in control of their funds and information. As this burgeoning ecosystem is seeking to remove the very financial institutions that have been bent into submission, there are other means for FinCEN to protect the integrity of the financial systems rather than foisting BSA compliance on projects building software protocols that facilitate value exchange in the truest of peer-to-peer fashions. Therefore, this Article takes the position that FinCEN should articulate an express exemption for non-custodial services that build software that cannot be altered to serve as deputized intermediaries to surveil its users on behalf of the government through notice and comment rulemaking as it did in 2011 to accommodate the Internet's impact on the BSA.¹²

II. FINCEN AS THE LEAD ENFORCER OF THE BSA

As it applies to virtual currency, FinCEN is probably the most enigmatic financial regulator to the mainstream user. Most virtual currency discussions center around the Securities and Exchange Commission's enforcement of the U.S. securities laws and its interpretation of the oft cited *Howey* test as applied to the issuance of new virtual currencies.¹³ However, little attention is

12. Formal rulemaking is required by the BSA to alter the definition "financial institution." See 31 U.S.C. § 5312(a)(2)(Y) (2012).

13. In *SEC v. W.J. Howey Co.*, the Supreme Court stated that a financial instrument is an "investment contract", a catch-all term listed as a "security", if the instrument "involves [(1)] an investment of money; (2)] in a common enterprise"; (3) with a reasonable expectation of profits to be (4) derived from the entrepreneurial or managerial "efforts of others." *SEC v. W.J. Howey Co.*, 328 U.S. 293, 301 (1946); see also *United Hous. Found., Inc., v. Forman*, 421 U.S. 837, 852 (1975); *United States v. Namer*, 680 F.2d 1088, 1096 (5th Cir. 1982) (referring to an "investment contract" as a "catch-all statutory phrase"). Any issuance

focused on understanding an albeit quieter, more powerful financial regulator—FinCEN—that serves two significant roles within the U.S. financial system: (1) “regulator of all financial institutions and the [a]dministrator of the [BSA]”; and (2) the “Financial Intelligence Unit, or FIU, of the United States.”¹⁴ This Part outlines the creation of FinCEN, its mandate from Congress, and how it uses its two roles to oversee certain activities within the virtual currency ecosystem.

A. History of FinCEN

The BSA was passed in the beginning of the first financial technology wave with the introduction of ATMs, credit cards and debit cards, the Automatic Clearinghouse (ACH) system, and the Society for Worldwide Interbank Financial Telecommunication (SWIFT). When Congress passed the BSA, it had two goals in mind: (1) “create a paper trail to inform law enforcement of potentially suspicious activity” and (2) “use the BSA as a weapon to prosecute money launderers” based upon that paper trail.¹⁵ Other than two BSA cases related to privacy and the U.S. Constitution, the BSA was of little concern until 1985 when the First National Bank of Boston pleaded guilty to knowingly violating and willfully failing to comply with the BSA by failing to report over \$1.2 billion in cash transactions.¹⁶ With the Money Laundering Control Act following in 1986 and subsequent regulatory changes requiring financial institutions to maintain procedures to monitor BSA compliance, including Suspicious Activity Reports (SARs) in 1992, the modern BSA compliance program was born. Soon thereafter, it became clear that monitoring and enforcing

of an “investment contract” is considered to be a securities offering requiring registration with the SEC under Section 5 of the Securities Act of 1933. See SEC. & EXCH. COMM’N, RELEASE NO. 81207, REPORT OF INVESTIGATION PURSUANT TO SECTION 21(A) OF THE SECURITIES EXCHANGE ACT OF 1934: THE DAO 10-11 (July 25, 2017), [<https://perma.cc/KAV8-ALU6>].

14. Kenneth A. Blanco, Director, Fin. Crimes Enf’t Network, Prepared Remarks Delivered at the Federal Identity (FedID) Forum and Exposition (Sept. 24, 2019), [<https://perma.cc/MKN2-7BC2>] [hereinafter Tampa-Blanco Remarks].

15. Scott Sultzer, *Money Laundering: The Scope of the Problem and Attempts to Combat It*, 63 TENN. L. REV. 143, 153-54 (1995).

16. *Id.* at 158; *United States v. First Nat’l Bank of Boston*, CR 85 52-MA (D. Mass. filed Feb. 7, 1985).

each financial institution's BSA compliance program necessitated a single administrative agency.¹⁷

FinCEN was created within the Department of Treasury by Executive Order in 1990 with the express mission "to provide governmentwide, multi-source intelligence and analytical network in support of the detection, investigation, and prosecution of domestic and international money laundering and other financial crimes by Federal, State, local, and foreign law enforcement agencies."¹⁸ In 1994, FinCEN's mission was broadened to include regulatory responsibilities, and the Treasury's Office of Financial Enforcement (FinCEN's predecessor) was merged with FinCEN.¹⁹ In 2002, following the enactment of the USA PATRIOT Act²⁰, FinCEN became an official Bureau within the Treasury Department "to support law enforcement efforts and foster interagency and global cooperation against domestic and international financial crimes, and to provide U.S. policy makers with strategic analyses of domestic and worldwide trends and patterns."²¹ On March 8, 2004, FinCEN joined with the Department of the Treasury's Office of Terrorism and Financial Intelligence, which leads "fighting the financial war on terror, combating financial crime, and enforcing economic sanctions against rogue nations."²² In 2012, FinCEN launched FinCEN Query, allowing authorized federal, state, and local law enforcement "to easily access, query, and analyze eleven (11) years of FinCEN data; apply filters and narrow search results; utilize enhanced data; and import lists of data (e.g., names, identification numbers, and

17. See Annunzio-Wylie Anti-Money Laundering Act, Pub. L. No. 102-550, tit. XV, sec. 1517, 106 Stat. 4044 (1992) (codified at 31 U.S.C. § 5318(g) (2014)); see generally Money Laundering Control Act of 1986, Pub. L. No. 99-570, 100 Stat. 3207-18 (1986) (codified as amended in scattered sections of 18 and 31 U.S.C.).

18. Treas. Order 105-08 (Apr. 25, 1990), [<https://perma.cc/BH7E-LFGC>].

19. Financial Crimes Enforcement Network, 74 Fed. Reg. 59,096, 59,096 n.5 (Nov. 17, 2009).

20. See Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT ACT) Act of 2001, Pub. L. No. 107-56, tit. III, Subtitle B, sec. 361(a)(2), § 310(a), 115 Stat. 272, 329.

21. Treas. Order 180-01 (Sept. 26, 2002).

22. FIN. CRIMES ENF'T NETWORK, ANN. REP. FISCAL YEAR 2004 3 (Jan. 2005), [<https://perma.cc/M8C3-PLQ3>].

addresses).”²³ FinCEN Query captures four BSA report types: SARs, Currency Transaction Reports (CTRs),²⁴ the Designation of Exempt Person (DOEP), and Registered Money Service Business (RMSB).²⁵

B. FinCEN’s Reach

The BSA is a series of statutory provisions designed to prevent money-laundering and terrorist financing. The BSA places an affirmative duty on all financial institutions operating in the United States to disclose those who conduct transactions in excess of \$10,000 through CTRs and to file other information regarding suspected illegal or suspicious transactions through SARs.²⁶ As previously mentioned, such oversight of the financial institutions subject to the BSA was delegated to FinCEN, which is

23. Press Release, Fin. Crimes Enf’t Network, FinCEN Query Now Available for Authorized Users: IT Modernization Program is on Schedule and Within Cost (Sept. 10, 2012), [<https://perma.cc/B72W-ZR5Q>].

24. A CTR is a report on a “deposit, withdrawal, exchange of currency[,] or other payment or transfer” through a financial institution that involves more than \$10,000 in currency. Filing Obligations for Reports of Transactions in Currency, 31 C.F.R. § 1010.311 (2011). A “domestic financial institution” is required to file CTRs with the Treasury Department when it “is involved in a transaction for the payment, receipt, or transfer of United States coins or currency” exceeding \$10,000. 31 U.S.C. § 5313(a) (1994); 31 C.F.R. § 1010.311.

25. Bank Secrecy Act, FinCEN Query (FCQ), IRM 4.26.4 (Jan. 6, 2016), [<https://perma.cc/KWG9-7YLT>].

26. An MSB must report transactions that the MSB “knows, suspects, or has reason to suspect” are suspicious, if the transaction is conducted or attempted by, at, or through the MSB, and the transaction involves or aggregates to at least \$2,000.00 in funds or other assets. Reports by Money Services Businesses of Suspicious Transactions, 31 C.F.R. § 1022.320(a)(2) (2016). A transaction is “suspicious” if the transaction: (i) “involves funds derived from illegal activity”; (ii) “is intended or conducted in order to hide or disguise funds or assets derived from illegal activity,” or to disguise “the ownership, nature, source, location, or control of such funds or assets” derived from illegal activity; (iii) “[i]s designed, whether through structuring or other means, to evade any requirements” in the Bank Secrecy Act or its implementing regulations; (iv) “[s]erves no business or apparent lawful purpose, and the [MSB] knows of no reasonable explanation for the transaction after examining the available facts, including the background and possible purpose of the transaction;” or (v) “[i]nvolves use of the [MSB] to facilitate criminal activity.” 31 C.F.R. § 1022.320(a)(2). Since the enactment of the BSA in 1970, the monetary thresholds have never been adjusted for inflation. A \$10,000 transaction in 1970 is approximately a \$68,000 transaction in 2020 when taking inflation into account. In effect, the scope of transactions that trigger the BSA has continually expanded over the last fifty years simply through inflation. Of note, the civil money penalties for violating the BSA were adjusted upward to account for inflation in 2015. J.P. Koning, *Why Aren’t Anti-Money-Laundering Regulations Adjusted for Inflation?*, AIER.ORG (Jan. 23, 2020), [<https://perma.cc/L58X-QQZF>].

responsible for shaping how financial institutions comply with the BSA Regulations. Using the BSA Regulations, FinCEN has deputized financial institutions as law enforcement agents to help carry out its mission to “safeguard the financial system from illicit use and combat money laundering and promote national security through the collection, analysis, and dissemination of financial intelligence and strategic use of financial authorities.”²⁷ FinCEN does this by issuing regulations, interpretive guidance, community outreach and training, collecting and analyzing reports, and engaging in civil enforcement actions. Regardless of the financial activity, all BSA obligations that apply to a particular financial institution ultimately flow from FinCEN’s regulations.²⁸

Failure to comply with the BSA Regulations can result in the imposition of civil money penalties and criminal penalties. As a regulatory agency lacking independent litigating authority, FinCEN is only authorized to impose civil money penalties.²⁹ Civil money penalties can range from \$500 for each negligent violation to \$50,000 for patterns of negligent violations.³⁰ Willful violations can amount to \$25,000 or the amount of the transaction, whichever is greater.³¹ Failure to establish an adequate AML program can result in a \$25,000 penalty per day.³² Civil money penalties may be imposed regardless of any imposition of criminal penalties.³³

FinCEN’s authority to levy civil money penalties is very broad and, unlike other regulators, FinCEN has not publicly published a list of factors or procedures that it uses before imposing

27. *What We Do*, FIN. CRIMES ENFORCEMENT NETWORK, [<https://perma.cc/V684-YKLT>] (last visited Jan. 5, 2020).

28. FinCEN regulations for brokers or dealers in securities are covered under 31 C.F.R. § 1023. *See generally* Rules for Brokers or Dealers in Securities, 31 C.F.R. § 1023 (2011). Futures commission merchants are covered under 31 C.F.R. § 1026. *See generally* Rules for Futures Commission Merchants and Introducing Brokers in Commodities, 31 C.F.R. § 1026 (2011). Introducing brokers in commodities are covered under 31 C.F.R. § 1026. *See generally* 31 C.F.R. § 1026. Mutual funds are covered under 31 C.F.R. § 1024. *See generally* Rules for Mutual Funds, 31 C.F.R. § 1024 (2011).

29. *See* 31 C.F.R. § 1010.810 (2014).

30. 31 U.S.C. § 5321(a)(6)(A)-(B) (2004).

31. 31 U.S.C. § 5321(a)(1).

32. *See* 31 U.S.C. § 5321(a)(1).

33. 31 U.S.C. § 5321(d).

civil money penalties.³⁴ Its broad authority appears to allow it to impose a civil money penalty unilaterally and without a fact-finding hearing before an administrative law judge.³⁵ Once a civil money penalty is imposed, the financial institution may only seek a lengthy and expensive review from a federal district court.³⁶ The enforcement proceedings seemingly therefore promote forced settlement under duress and a market response to submit extraneous reports to FinCEN.³⁷

As a result, FinCEN's BSA database houses nearly 300 million records servicing on average some 30,000 searches of this data each day and 7.4 million queries per year from more than "12,000 agents, analysts, and investigative personnel from over 350 unique federal, state, and local agencies across the United States with direct access to this critical reporting by financial institutions."³⁸ While the majority of these reports come from financial institutions via CTRs and SARs, FinCEN also collects information from cash crossing the U.S. border upon exit and entry, from retail stores receiving cash payments in excess of \$10,000, and "from individuals with foreign bank accounts."³⁹ FinCEN further works with over 164 foreign countries sharing its financial intelligence information with them "when appropriate."⁴⁰ With access to a variety of databases, FinCEN is at the center of one of the largest repositories of financial information in the world in a position to readily provide any FIU in the world with information and provide foreign governments with policy recommendations, analytical training, advice, and staff support.⁴¹

34. Robert B. Serino, *FinCEN's Lack of Policies and Procedures for Assessing Civil Money Penalties in Need of Reform*, BUS. L. TODAY, July 2016, at 1, 4.

35. *Id.*

36. *See id.* at 2.

37. *Id.* at 2-3; *see* 31 U.S.C. §5318(g)(3)(A) (2014) (providing immunity to any financial institution that, in good faith, "makes a voluntary disclosure of any possible violation of law or regulation to a government agency").

38. New York City-Blanco Remarks, *supra* note 11.

39. Tampa-Blanco Remarks, *supra* note 14.

40. *Id.*

41. *International Programs*, FIN. CRIMES ENFORCEMENT NETWORK, [<https://perma.cc/ATM7-7P4S>] (last visited Dec. 26, 2019).

III. FINCEN ENTERS VIRTUAL CURRENCY

This Part outlines FinCEN's key definitions and interpretive opinions of how the BSA Regulations apply to various virtual currency business models. This Part also incorporates criminal prosecutions that relied in part on FinCEN's interpretations of the BSA and places these decisions in a chronological order in parallel with FinCEN's public guidance to display how the understanding of the BSA as applied to virtual currency has evolved since 2013.

A. Definitions

In 2011, FinCEN adopted a set of final rules (the 2011 Final Rules) amending the definition of "money services business" recognizing that the Internet and other technological advancements were changing how businesses were offering money services business (MSB) services.⁴² One such MSB service is a money transmitter.⁴³ A "money transmitter" is "[a] person that provides money transmission services" or "[a]ny other person engaged in the transfer of funds" whereby "money transmission services" means the acceptance of currency, funds, or other value that substitutes for currency from one person and the transmission of currency, funds, or other value that substitutes for currency to another location or person by any means."⁴⁴ In sum, FinCEN's rules apply to all transactions involving money transmission including fiat to fiat transactions, fiat to value that substitutes for currency transactions, and value that substitutes for currency to value that substitutes for currency transactions.

This expansive view of what it means to be a money transmitter made it relatively easy for FinCEN in 2013 to affirmatively bring virtual currency within its regulatory jurisdiction via interpretive guidance. FinCEN began the 2013 Guidance by clearly defining "real" currency and "virtual" currency.⁴⁵ FinCEN defined real currency as (1) a jurisdiction's coin and paper money

42. Definitions and Other Regulations Relating to Money Services Businesses, 76 Fed. Reg. 43585 (July 21, 2011).

43. 31 C.F.R. § 1010.100(ff) (2014).

44. 31 C.F.R. § 1010.100(ff)(5)(i)(A).

45. 2013 GUIDANCE, *supra* note 8, at 1.

that is (2) “designated as legal tender” for that jurisdiction and (3) “is customarily used and accepted as a medium of exchange in the” jurisdiction.⁴⁶ Virtual currency is defined as “a medium of exchange that operates like a currency in some environments, but does not have all the attributes of real currency.”⁴⁷ Convertible virtual currency (CVC) is a virtual currency that “has an equivalent value in real currency, or acts as a substitute for real currency.”⁴⁸ Virtual currencies and CVCs are not legal tender in any jurisdiction; however, both are value that substitutes for currency.

Within the CVC ecosystem, there are three participants: (1) users, (2) administrators, and (3) exchangers. “A user is a person that obtains virtual currency to purchase goods or services.”⁴⁹ Users who use virtual currency to purchase goods or services on their own behalf are not money transmitters.⁵⁰ “An administrator is a person engaged as a business in issuing (putting into circulation) a virtual currency, and who has the authority to redeem (to withdraw from circulation) such virtual currency.”⁵¹ “An exchanger is a person engaged as a business in the exchange of virtual currency for real currency, funds, or other virtual currency.”⁵² Unless an exemption exists, FinCEN classifies both an administrator and an exchanger as money transmitters if it accepts and transmits CVC in exchange for real currency or another CVC for any reason.⁵³ Therefore, administrators and exchangers, as money transmitters, must (1) register with FinCEN as an MSB⁵⁴; (2) develop,

46. *Id.*

47. *Id.*

48. *Id.*

49. *Id.* at 2 (emphasis omitted).

50. 2013 GUIDANCE, *supra* note 8, at 2.

51. *Id.* (emphasis omitted).

52. *Id.* (emphasis omitted).

53. *Id.* at 3. The BSA Regulations identify six circumstances that fall outside the scope of the definition of “money transmitter.” 31 C.F.R. § 1010.100(ff)(5)(ii) (2019). The most notable of the six include: a person who merely “[p]rovides the delivery, communication, or network” instruments for transmission; a payment processor who facilitates payment for goods or services “by agreement with the creditor or seller”; and accepting or transmitting funds “integral to the sale of goods or . . . services . . . by the person . . . accepting and transmitting the funds.” 31 C.F.R. § 1010.100(ff)(5)(ii)(A)-(B), (F).

54. 31 U.S.C. § 5330(a)(1) (2012); 31 C.F.R. § 1022.380(a)(1), (b)(1)(i), (b)(2) (2019). MSB registration with FinCEN must be renewed every two years. 31 C.F.R. § 1022.380(b)(2).

implement, and maintain an AML program⁵⁵; (3) establish record-keeping and reporting measures, including filing SARs and CTRs; and (4) comply with the Funds Transfer Rule and the Funds Travel Rule.⁵⁶

B. Application of BSA Regulations to Virtual Currency Exchanges

Since before Bitcoin, the government has pursued a number of criminal cases asserting BSA violations by virtual currency businesses. In 2007, e-Gold, its founders, and its directors were charged with money laundering and operating an unlicensed money transmitting business.⁵⁷ e-Gold was an alternative payment system with a virtual currency backed by physical gold.⁵⁸ Arguing that e-Gold was not a “money transmitting business”

55. 31 U.S.C. § 5318(h) (2012). The AML program must: (i) “[i]ncorporate [written] policies, procedures, and internal controls reasonably designed to assure [ongoing] compliance”; (ii) designate an individual compliance officer responsible for assuring “day to day compliance with the program and” Bank Secrecy Act requirements; (iii) provide training for appropriate personnel, which specifically includes “training in the detection of suspicious transactions”; and (iv) “[p]rovide for independent review to monitor and maintain an adequate program.” 31 C.F.R. § 1022.210(d) (2019); accord 31 U.S.C. § 5318(a)(2), (h).

56. 31 C.F.R. §§ 1010.311, 1010.410(e)-(f), 1022.320(a)(1) (2019). Subsection (e) is the Funds Transfer Rule and only applies to nonbank entities. 31 C.F.R. § 1010.410(e); FIN. CRIMES ENF’T NETWORK, U.S. DEP’T OF TREASURY, FIN-2014-R011, REQUEST FOR ADMINISTRATIVE RULING ON THE APPLICATION OF FINCEN’S REGULATIONS TO A VIRTUAL CURRENCY TRADING PLATFORM 7 (2014), [<https://perma.cc/9B7A-H96T>] [hereinafter OCTOBER 2014 ADMINISTRATIVE RULING]. Although this subsection expressly excludes banks from its requirements (31 C.F.R. § 1020.410(a) is the Funds Transfer Rule applying to banks), it uses broad language that is nonspecific to banks. 31 C.F.R. § 1010.410(e); see STEVEN MARK LEVY, FEDERAL MONEY LAUNDERING REGULATION: BANKING, CORPORATE, & SECURITIES COMPLIANCE 3-36 (Supp. 2012). Additionally, subsection (f), the Funds Travel Rule, applies to any institution acting as an intermediary in the transmitting of funds. See 31 C.F.R. 1010.410(f); OCTOBER 2014 ADMINISTRATIVE RULING, *supra*, at 7. This subsection also uses broad language non-specific to banks, which allows it to encompass any financial institution. See 31 C.F.R. 1010.410(f); *Funds Transfers Record-keeping—Overview, Funds Transfer Recordkeeping, Regulatory Requirements, BSA/AML Manual*, FFIEC BSA/AML INFOBASE, [<https://perma.cc/BE7V-V7SB>] (last visited Mar. 29, 2020). A financial institution must pass on all the information it receives from a previous financial institution when it is processing a transmittal of funds of \$3,000 or more. 31 C.F.R. 1010.410(f)(2). For virtual currency businesses, the Funds Travel Rule “is the most commonly cited violation” of the BSA. Gertrude Chavez-Dreyfuss, *U.S. to Strictly Enforce Anti-Money Laundering Rules in Cryptocurrencies – FinCEN Chief*, CNBC (Nov. 15, 2019), [<https://perma.cc/HE66-NK7K>].

57. Indictment at 6, 9, 18, *United States v. e-Gold, Ltd.*, 550 F. Supp. 2d 82 (D.D.C. 2008) (No. 07-109), 2007 WL 2988241.

58. *Id.* at 6.

because it did not process cash transactions, e-Gold never registered as a “money transmitting business” nor did it file CTRs.⁵⁹ The U.S. District Court for the District of Columbia rejected all of e-Gold’s arguments, ruling that e-Gold was engaged in “money transmitting” by “transferring funds on behalf of the public,” which required it to comply with Section 5330’s registration requirements and file CTRs.⁶⁰ Thus, the e-Gold decision combined with the 2011 Rule was enough for FinCEN to bridge the gap between the new era of virtual currencies and the BSA.

In the post-2013 Guidance era, the criminal prosecution of Charlie Shrem, the former CEO of BitInstant, the most popular virtual currency exchange in the United States at the time, set the scene for the government’s willingness to rely on its imprisonment trump card provided by the BSA.⁶¹ On August 19, 2014, relying in part on FinCEN’s 2013 Guidance, the Southern District of New York denied Charlie Shrem’s motion to dismiss the indictment of violating Section 1960⁶²; Shrem later pleaded guilty for selling approximately \$1 million to an unlicensed money transmitting business that operated on the Silk Road and was sentenced to two years in prison.⁶³ The arrest and ultimate sentencing of Shrem sent a shock throughout the Bitcoin world, putting on full display the government’s willingness to prosecute rather than settle with those engaged in allegedly illicit transactions

59. *United States v. e-Gold, Ltd.*, 550 F. Supp. 2d 82, 87-88 (D.D.C. 2008).

60. *Id.* at 88, 93, 97.

61. See Carla L. Reyes, *Moving Beyond Bitcoin to an Endogenous Theory of Decentralized Ledger Technology Regulation: An Initial Proposal*, 61 VILL. L. REV. 191, 206 & n. 93 (2016). Shortly following the Shrem case, federal prosecutors charged the founder of Liberty Reserve with conspiracy to commit money laundering, conspiracy to commit international money laundering, and operating an unlicensed money transmitting business. *United States v. Budovsky*, No. 13cr368 (DLC), 2015 WL 5602853, at *1-3, *11 (S.D.N.Y. Sept. 23, 2015). Relying in part on *United States v. Faiella*, the U.S. District Court for the Southern District of New York held that virtual currencies are “funds” under Section 1960 because they can “be easily purchased in exchange for ordinary currency, act as a denominator of value, and [are] used to conduct financial transactions.” See *id.* at *14 (quoting *United States v. Faiella*, 39 F. Supp. 3d 544, 545 (S.D.N.Y. 2014)) (quotation marks omitted). Thus, Liberty Reserve was operating as an unlicensed, foreign-based money transmitter in violation of Section 1960. See *id.*; *Founder of Liberty Reserve Pleads Guilty to Laundering More Than \$250 Million Through His Digital Currency Business*, U.S. DEP’T OF JUSTICE (Jan. 29, 2016), [<https://perma.cc/RC46-9U47>] [hereinafter *Liberty Reserve*].

62. *United States v. Faiella*, 39 F. Supp. 3d 544, 546-47 (S.D.N.Y. 2014).

63. See Tanya Macheel, *Charlie Shrem Saga Ends with Two-Year Sentence in New York Court*, COINDESK (Jan. 21, 2015), [<https://perma.cc/NA6S-YZAX>].

denominated in virtual currency.⁶⁴ Following the 2013 Guidance and the prosecution of Charlie Shrem, it was generally understood that custodial virtual currency exchanges operating within the United States were required to register with FinCEN as money transmitters.

As criminal prosecutions were occurring in parallel, FinCEN continued to clarify the BSA's application on subsequent business models through a series of administrative rulings, two of which were issued in January 2014.⁶⁵ In its second administrative ruling in January 2014, FinCEN expressly stated that "[t]he production and distribution of software, in and of itself, does not constitute acceptance and transmission of value, even if the purpose of the software is to facilitate the sale of virtual currency."⁶⁶ Therefore, the development of software alone, despite the purpose, does not amount to the developer being a money transmitter.

In FinCEN's October 2014 Administrative Ruling on the Application of FinCEN's Regulations to a Virtual Currency Trading Platform, it ruled that:

[a]n exchanger will be subject to . . . FinCEN regulations regardless of whether the exchanger [is] . . . attempting to match two (mostly) simultaneous and offsetting transactions involving the acceptance of one type of currency and the transmission of another[] or . . . transacting from its own reserve in either convertible virtual currency or real currency

. . .⁶⁷

64. Kashmir Hill, *Winklevosses, Bitcoin Community Shocked by Arrest of BitInstant CEO Charlie Shrem*, FORBES (Jan. 27, 2014), [<https://perma.cc/YY5Y-7KPP>].

65. GIBSON DUNN & CRUTCHER LLP, *U.S. Developments in Virtual Currencies: FinCEN Administrative Rulings and New York Department of Financial Services Hearings* (Feb. 12, 2014), [<https://perma.cc/J3PP-7WB2>]. Other than the actions discussed in this section, federal prosecutors have brought criminal prosecutions against online marketplaces for illicit goods such as Silk Road and AlphaBay that used virtual currency as a payment method. *United States v. Ulbricht*, 31 F. Supp. 3d 540, 549-50 (S.D.N.Y. 2014); *Indictment at 21, United States v. Cazes*, No. 1:17-CR-00144 (E.D. Cal. June 1, 2017), dismissed, No. 1:17-CR-00144-LJO-SKO (E.D. Cal. Apr. 27, 2018); *see United States v. 2013 Lamborghini Aventador LP700-4*, No. 1:17-cv-00967-ljo-sko, 2018 WL 3752131, at *4 (E.D. Cal. Aug. 8, 2018).

66. FIN. CRIMES ENF'T NETWORK, DEP'T OF THE TREASURY, FIN-2014-R002, APPLICATION OF FINCEN'S REGULATIONS TO VIRTUAL CURRENCY SOFTWARE DEVELOPMENT AND CERTAIN INVESTMENT ACTIVITY 2 (2014), [<https://perma.cc/ZCF4-788A>] [hereinafter JANUARY 2014 RULING].

67. OCTOBER 2014 ADMINISTRATIVE RULING, *supra* note 55, at 6.

Neither the method of funding the transaction nor the fact that the parties transacting are never identified has any bearing on the analysis. The fact that the company sits in the middle of the exchange between parties conducting each trade and the inapplicability of the integral exemption qualifies the exchange as a money transmitter.⁶⁸

Almost two years after the last FinCEN administrative ruling, the Southern District of New York, which had previously presided over the *Shrem* case, denied Anthony Murgio's motion to dismiss two counts charging him with "operating, and conspiring to operate" his business, Coin.mx, "as an unlicensed money transmitting business."⁶⁹ Murgio was subsequently sentenced to five years in prison for processing "more than \$10 million in illegal Bitcoin transactions" through his cryptocurrency exchange Coin.mx between 2013 and 2015.⁷⁰

One year later, FinCEN issued its second supervisory enforcement action against BTC-e, a foreign-located money services business acting as an exchanger of convertible virtual currencies.⁷¹ FinCEN determined that BTC-e, a virtual currency exchange, and Alexander Vinnik, one of BTC-e's operators, willfully violated U.S. AML laws and assessed a \$110 million civil

68. *Id.* at 3. In order for the integral exemption to apply, three conditions must exist: (1) "[t]he money transmission component must be part of the provision of goods or services distinct from money transmission itself"; (2) "[t]he exemption can only be claimed by the person that is engaged in the provision of goods or services distinct from money transmission"; and (3) "[t]he money transmission component must be integral (that is, necessary) for the provision of the goods or services." *Id.* at 4.

69. *United States v. Murgio*, 209 F. Supp. 3d 698, 704-05, 715 (S.D.N.Y. 2016).

70. *Operator of Unlawful Bitcoin Exchange Sentenced to More Than 5 Years in Prison for Leading Multimillion-Dollar Money Laundering and Fraud Scheme*, DEP'T OF JUST. (June 27, 2017), [<https://perma.cc/G9Q8-D2CN>].

71. *See* BTC-e, No. 2017-03, at *2 (U.S. Dep't of Treasury July 26, 2017), [<https://perma.cc/2ZYN-Z9WU>] [hereinafter *BTC-e Action*]. The first digital asset related supervisory enforcement action was issued in May 2015 against Ripple Labs. Ripple Labs agreed to pay a \$700,000 civil money penalty for willfully violating the BSA requirements by operating as an MSB and selling its digital asset, XRP, without registering and "failing to implement and maintain an adequate [AML] program," and failing to file SARs for several transactions. Ripple also entered into a settlement agreement to defer criminal prosecution. *FinCEN Fines Ripple Labs Inc. in First Civil Enforcement Action Against a Virtual Currency Exchanger*, FIN. CRIMES ENF'T NETWORK (May 5, 2015), [<https://perma.cc/SKG9-E8YD>]. FinCEN assessed this penalty in coordination with the U.S. Attorney's Office for the Northern District of California. *See Settlement Agreement: Attachment B*, U.S. DEP'T OF JUSTICE 1 (May 5, 2015), [<https://perma.cc/5U6U-FGGL>].

money penalty on BTC-e.⁷² From November 5, 2011 to the date of the action, BTC-e and Vinnik failed to verify basic customer information, failed to maintain an AML compliance program, allowed over \$40 million in transfers from bitcoin mixers,⁷³ “processed transactions involving funds stolen from the Mt. Gox exchange,” “processed thousands of suspicious transactions without ever filing a single SAR,” failed to maintain records from transmittals in excess of \$3,000, and “lacked basic [internal] controls” to prevent users using the exchange for illicit purposes.⁷⁴ Yet, BTC-e never filed any reports with FinCEN.⁷⁵ Thus, BTC-e and Vinnik were found to have clearly willfully violated their reporting requirements and obligations as exchangers and administrators of digital assets.

As FinCEN has shown on previous occasions, foreign operating financial institutions are well within its authority as promulgated under the BSA and the USA PATRIOT Act.⁷⁶ Jamal El-Hindi, Acting Director for FinCEN at the time noted,

We will hold accountable foreign-located money transmitters, including virtual currency exchangers, that do business in the United States when they willfully violate U.S. anti-money laundering laws . . . Treasury’s FinCEN team and our law enforcement partners will work with foreign counterparts across the globe to appropriately oversee virtual

72. *BTC-e Action*, *supra* note 69, at *3, *9. In order to show willfulness, “[t]he government need not show that the entity or individual had knowledge that the conduct violated the Bank Secrecy Act, or that the entity or individual otherwise acted with an improper motive or bad purpose.” *Id.* at 3 n.10; *see* 31 U.S.C. § 5321(a)(1) (2012).

73. “Mixers anonymize bitcoin addresses and obscure bitcoin transactions by weaving together inflows and outflows from many different users. Instead of directly transmitting bitcoin between two bitcoin addresses, the mixer disassociates connections. Mixers create layers of temporary bitcoin addresses operated by the mixer itself to further complicate any attempt to analyze the flow of bitcoin.” *BTC-e Action*, *supra* note 69, at *5-6.

74. *Id.* at *3-7, *9. In 2014, Mt. Gox was hacked, losing approximately 850,000 bitcoins “worth \$473 million at the time and reflecting 7% of the total supply of bitcoin.” Nathaniel Whittemore & Clay Collins, *A History of Crypto Exchanges: A Look at Our Industry’s Most Powerful Institutions*, NOMICS (Nov. 14, 2019), [<https://perma.cc/336P-VUKY>]. At the time of the hack, Mt. Gox was responsible for approximately 70%-80% of all bitcoin transactions. *Id.*

75. *See BTC-e Action*, *supra* note 69, at *5, *7.

76. *See generally* United States v. Budovsky, No. 13cr368 (DLC), 2015 WL 5602853, at *7 & n.5 (S.D.N.Y. Sept. 23, 2015); *Liberty Reserve*, *supra* note 60.

currency exchangers and administrators who attempt to subvert U.S. law and avoid complying with U.S. AML safeguards.⁷⁷

Almost two years after the BTC-e action, on April 18, 2019, FinCEN issued its third digital assets related supervisory enforcement action against Eric Powers, an individual operator of a P2P convertible virtual currency exchange.⁷⁸ Powers advertised his services to buy and sell bitcoin from others on web forums and various websites with some transactions taking place in person, through mail, through wire, or directly on an exchange on behalf of others.⁷⁹ During the time period, Powers never registered as an MSB, filed a CTR or SAR, or implemented an AML program or internal controls as per the BSA and its implementing regulations.⁸⁰ The action reiterated the requirement that MSBs must report suspicious transactions that “involve or aggregate to at least \$2,000 in funds or other assets.”⁸¹

Unlike the prior enforcement actions, the Powers action merits a deeper analysis for four reasons. First, Powers was an individual selling on his own account and transacting directly with his counterparties.⁸² A first pass reading of the action implies that mere two-party exchange is money transmission, which goes against the common interpretation that “money transmission” requires three parties. Further, it contradicts FinCEN’s January 2014 Administrative Ruling on the Application of FinCEN’s Regulations to Virtual Currency Software Development and Certain Investment Activity.⁸³ The January 2014 Ruling stated that a company is operating as a user if it is trading CVC on its own account and not making transfers at the behest of third parties.⁸⁴ The Powers action fails to state the determinative factors and time

77. *FinCEN Fines BTC-e Virtual Currency Exchange \$110 Million for Facilitating Ransomware, Dark Net Drug Sales*, FIN. CRIMES ENFORCEMENT NETWORK (July 27, 2017), [<https://perma.cc/MJX6-JUY5>] (quotation marks omitted).

78. In the Matter of: Eric Powers, No. 2019-01, at *2-3 (U.S. Dep’t of Treasury Apr. 18, 2019), [<https://perma.cc/Z6XG-DPG5>] [hereinafter *Powers Action*].

79. *Id.* at *3.

80. *Id.* at *2, *4, *7, *8.

81. *Id.* at *5; see 31 U.S.C. § 5318(g)(1) (2012); 31 C.F.R. § 1022.320(a)(2) (2019).

82. See *Powers Action*, *supra* note 76, at *3.

83. *Id.*; JANUARY 2014 RULING, *supra* note 64, at 3.

84. JANUARY 2014 RULING, *supra* note 64, at 3.

at which he was no longer trading on his account and began trading at the behest of others.

Second, despite this ambiguity in interpretation, FinCEN conveniently introduced a new term—peer-to-peer exchanger (P2P Exchanger)—to gloss over the need for deeper analysis. P2P Exchangers are “natural persons engaged in the business of buying and selling CVCs[,] . . . [who] generally advertise and market their services through classified advertisements, specifically designed web platform websites, online forums, other social media, and word of mouth.”⁸⁵ This definition fails to define “engaged in the business of” or establish a definitive frequency-of-exchange threshold to be considered engaged in any business activity.⁸⁶ Perhaps, a P2P exchanger could be engaged in money transmission simply because they accept and transmit money or CVC to another location, like an exchange or wallet, on a frequent basis and for gain or profit.⁸⁷ FinCEN clearly demonstrates from the facts that Powers engaged in these transactions frequently, but fails to state whether Powers profited or gained from his services or explain the new P2P exchanger definition and, in a conclusory manner, states that Powers was a money transmitter at all relevant times. While this P2P Exchanger term is not law, nor sets any binding legal precedent, it is now part of the key terms that FinCEN has been shown to use in its enforcement actions and subsequent guidance reports.

Third, the relevant period of activity was December 6, 2012 to September 24, 2014.⁸⁸ The relevant period began before FinCEN issued its first guidance in 2013 but after the 2011 MSB Rule, thereby putting Powers on notice that his activity fell within FinCEN’s jurisdiction. As well, the end of the relevant period to

85. See FIN. CRIMES ENF’T NETWORK, DEP’T OF THE TREASURY, FIN-2019-G001, APPLICATION OF FINCEN’S REGULATIONS TO CERTAIN BUSINESS MODELS INVOLVING CONVERTIBLE VIRTUAL CURRENCIES 14 (2019), [<https://perma.cc/3FRS-SK87>] [hereinafter 2019 GUIDANCE].

86. The term “frequently” was last interpreted by FinCEN via public guidance in 2002 and defined in a way that is situationally dependent on the business. DEP’T OF THE TREASURY, FIN. CRIMES ENF’T NETWORK, GUIDANCE ON INTERPRETING “FREQUENTLY” FOUND IN THE CRITERIA FOR EXEMPTING A “NON-LISTED BUSINESS” UNDER 31 C.F.R. §103.22(D)(2)(VI)(B), [<https://perma.cc/XKY5-YUPD>].

87. See 31 C.F.R. § 1010.100(ff)(5)(i), (8) (2019); 2019 GUIDANCE, *supra* note 85, at 5.

88. *Powers Action*, *supra* note 76, at *2.

the date of the enforcement action, April 18, 2019, is four and a half years. The statute of limitations for BSA violations is five years for criminal violations and six years for civil penalties.⁸⁹ Arguably, FinCEN made a point to get this action filed and efficiently settled before it lost its criminal prosecution leverage due to the statute of limitations lapsing.

Fourth, FinCEN seemingly goes out of its way to put in the body of the enforcement action that Powers conducted fifty-three transactions with customers with “@tormail.org” email addresses.⁹⁰ FinCEN notes that while the use of The Onion Router (TOR) “in and of itself is not suspicious, transactions through a torrent service may be a *strong indicator* of potential illicit activity when no additional due diligence is conducted to determine customer identity and whether or not funds are not derived from illegal activity.”⁹¹ Rather than provide further explanation, FinCEN notes that using TOR is simply suspicious on its face. The broader message behind the Powers enforcement action is that individuals, depending on their activities, can be subject to the BSA Regulations.

FinCEN followed its Powers enforcement action one month later with a new guidance report and an advisory report on illicit activities that involve convertible virtual currencies that should serve as “red flags” for MSBs, along with the “information that would be most valuable to law enforcement” if an MSB were to file a related SAR.⁹² The 2019 Guidance did not present any new expectations or requirements.⁹³ Rather, the Guidance comprehensively reiterated FinCEN’s regulations, related administrative rulings, and guidance since 2011.⁹⁴ The 2019 Guidance then applied these rules and interpretations to common business models and activities in the industry, clarifying its regulatory approach to this

89. 31 U.S.C. § 5321(b)(1) (2012); 18 U.S.C. § 3282(a) (2018).

90. *Powers Action*, *supra* note 76, at *5.

91. *Id.* at *6 (emphasis added).

92. See FIN. CRIMES ENF’T NETWORK, DEP’T OF THE TREASURY, FIN-2019-A003, ADVISORY ON ILLICIT ACTIVITY INVOLVING CONVERTIBLE VIRTUAL CURRENCY 1 (2019), [<https://perma.cc/6SE3-K2BR>]; see also 2019 GUIDANCE, *supra* note 83, at 12, 15.

93. Kenneth A. Blanco, Director, Fin. Crimes Enf’t Network, Prepared Remarks at the 12th Annual Las Vegas Anti-Money Laundering Conference (Aug. 13, 2019), [<https://perma.cc/9CWT-7KWL>].

94. *Id.*

evolving industry and expressly reminding the industry that “a person that chooses to set up a transaction system that makes it difficult to comply with existing regulations may not invoke such difficulty as a justification for non-compliance or as a reason for preferential treatment.”⁹⁵

Expressly stated multiple times within the 2019 Guidance is that persons who provide “the delivery, communication, or network access services used by a money transmitter to support money transmission services” are exempt from the definition of money transmitter.⁹⁶ Applying to services that provide means of storing and transacting in virtual currencies, FinCEN articulated four factors to determine if the service crosses from simply tools to engaged in money transmission services: “(a) who owns the value; (b) where the value is stored; (c) whether the owner interacts directly with the payment system where the CVC runs; and, (d) whether the person acting as intermediary has total independent control over the value.”⁹⁷ Therefore, hosted, or custodial, wallets are money transmitters because the user deposits value into an account with the service provider, whereby the service provider maintains the private keys and control over the user’s virtual currencies, rather than the user transacting directly on the underlying virtual currency blockchain. Similar to other money transmitters like Venmo, the user directs the service provider to transfer the value on their behalf. In contrast, unhosted, or non-custodial, services are not money transmitters because these services are merely downloadable software that allows the user to store and conduct transactions without losing independent control over their virtual currencies.⁹⁸ The conclusion reached in the 2019 Guidance for this use case is logical because these service providers are providing tools for trade and are not directly engaging in money transmission services.⁹⁹

Applying the delivery, communication, or network access services exemption to trading platforms, the focus is not only on the custodial issue, but also on how it provides a platform for

95. 2019 GUIDANCE, *supra* note 83, at 11 n.38.

96. *Id.* at 24; 31 C.F.R. § 1010.100(ff)(5)(ii)(A) (2019).

97. 2019 GUIDANCE, *supra* note 83, at 15.

98. *Id.* at 16.

99. *Id.* at 20.

users to engage in trade. If the platform only provides an interface for users to post bids and offers and trades are settled through non-custodial wallets, then the platform is not a money transmitter.¹⁰⁰ However, if the platform matches the buyer and seller and purchases the virtual currency from the seller to then transmit to the buyer directly within its platform, then the platform is a money transmitter.¹⁰¹ Thus, a virtual currency exchange that is exempt from FinCEN's regulations seems to be a non-custodial platform which solely provides a means for buyers and sellers to find each other and transact directly between their non-custodial wallets without advertising or marketing their services and not for profit or gain from trading fees.¹⁰²

IV. GOING FORWARD

The previous Parts have discussed the origins of FinCEN and how it enforces the BSA Regulations, including against virtual currency businesses. This Part shows how virtual currency businesses have responded to these regulatory measures and why the BSA recordkeeping and reporting requirements are not necessary once inside the virtual currency universe. With an understanding of how the government can obtain the same information through chain analysis, this Part suggests that FinCEN, not Congress, should adopt new rules as it did in 2011 to solidify this understanding and promote the creation of software that promotes financial inclusion and privacy.

A. The Market Responds

FinCEN's actions and those that stem from the BSA more generally have clear effects on the market. Following the FinCEN enforcement action against BTC-e, popular trading platforms Bitfinex and BitMEX started geo-blocking U.S. persons in late 2017.¹⁰³ On September 4, 2018, Shapeshift, a non-custodial virtual currency trading platform, announced that the platform

100. *Id.* at 24.

101. *Id.*

102. 2019 GUIDANCE, *supra* note 83, at 24; 31 C.F.R. § 1010.100(ff)(8)(iii) (2019).

103. Larry Cermak, *U.S. Customers to Be Blocked from Trading on Binance.com*, THE BLOCK (June 14, 2019), [<https://perma.cc/5Y7Y-RXZB>].

would require mandatory KYC on users.¹⁰⁴ Shapeshift had previously prided itself on allowing users to trade without accounts or collecting their personal information.¹⁰⁵ In a Twitter response to the announcement, Shapeshift CEO Erik Voorhees stated, “KYC is something we’re building under duress.”¹⁰⁶ Voorhees further explained,

[W]e basically spent literally millions of dollars and a very long time . . . navigating every nuance of international KYC regulation. The conclusion we came to was that there is still a lot of grey area...The likelihood of those succeeding seemed to be too low given the stake of the company.¹⁰⁷

Voorhees continued, “KYC was not added as a result of any enforcement action, but rather as a proactive step we took to de-risk the company amid uncertain and changing global regulations.”¹⁰⁸

In June 2019, Binance, which is headquartered in Malta, announced that it would geo-block and suspend the trading activities of U.S. persons.¹⁰⁹ At the same time, Binance announced a partnership with BAM Trading Services, a FinCEN registered MSB, to launch Binance.US, which serves as a separate corporate entity from Binance to service U.S. persons and licenses its technology and brand from Binance.¹¹⁰ In December 2019, Binance again showed the effect of being regulated by governments when it suspended the ability for a user to withdraw his bitcoin to a Wasabi wallet due to risk management concerns and anti-money laundering/counter financing terrorism (AML/CFT) controls in place.¹¹¹

104. Totle, *Trade Voors: ShapeShift Shifts to KYC*, MEDIUM (Sep. 9, 2018), [<https://perma.cc/J9C2-3D8D>].

105. Stan Higgins, *Inside ShapeShift’s Cryptocurrency Exchange, No Login Required*, COINDESK (Mar. 19, 2015), [<https://perma.cc/367X-3Z3J>].

106. Erik Voorhees (@ErikVoorhees), TWITTER (Sep. 5, 2018), [<https://perma.cc/S59G-3E3T>].

107. Erik Voorhees on *Maximalism, KYC & Shoddy Reporting*, WHAT BITCOIN DID (Mar. 22, 2019) [<https://perma.cc/3TZ3-4UA2>].

108. Marc Hochstein, *Crypto Exchange ShapeShift’s CEO Says Move to Collect IDs Was ‘Proactive,’* COINDESK (Sept. 25, 2018), [<https://perma.cc/W29H-ESS2>].

109. Jon Russell, *Binance Begins to Restrict US Users Ahead of Regulatory-Complaint Exchange Launch*, TECHCRUNCH (Jun. 14, 2019), [<https://perma.cc/7ANB-FWYX>].

110. *Id.*

111. *CZ on Regulations, Exchanges & Privacy*, BINANCE BLOG (Dec. 20, 2019), [<https://perma.cc/S3WD-2S3P>].

A Binance Singapore user's account withdrawal function was frozen due to risk management concerns.¹¹² The user was attempting to send his bitcoin from his KYC Binance account to his Wasabi wallet.¹¹³ Wasabi is a software wallet that uses CoinJoin, which allows users to mix and anonymize their bitcoins.¹¹⁴ Because the user had a history of sending his bitcoin from Binance to a Wasabi wallet, Binance saw this as a "red flag" and suspended his account until he contacted them to answer further questions.¹¹⁵ This instance on Binance's platform highlights how AML/KYC procedures required by financial regulators are implemented in ways that over censor transactions without specific and articulable facts to suspect criminal activity.

This withdrawal controversy further illustrates the issue that KYC/AML policies, no matter the location, are effectively pre-crimes investigations, as they are all mostly predicated or influenced by the BSA. Meanwhile, the incident brings forward important questions that have yet to be answered. Should users have access to and be able to employ privacy measures upon purchasing virtual currencies from regulated exchanges? Will exchanges censor deposits of bitcoins that can be traced to CoinJoins? What is the difference between using downstream privacy enhancing services and purchasing privacy virtual currencies on an exchange and then moving the virtual currencies off-exchange? Is buying a privacy virtual currency in and of itself suspicious activity? Is using privacy enhancing software and practicing good privacy hygiene suspicious activity? Will exchanges develop their own blacklist of virtual currency addresses to censor user deposits and withdrawals in the name of regulatory compliance? Without answers to these questions or the government being forced to publicly announce facts and circumstances that validate its reasonable articulable suspicions, the government collects, analyzes, filters, and stores everything until it later becomes useful, all the while promising not to use it for a bad purpose unless you are a criminal.

112. @bittlecat, TWITTER (Dec. 19, 2019), [<https://perma.cc/H7NQ-A94U>].

113. *Id.*

114. *See FAQ*, WASABI WALLET, [<https://perma.cc/9TTJ-72S7>] (last visited Mar. 15, 2020).

115. @bittlecat, TWITTER (Dec. 19, 2019), [<https://perma.cc/H7NQ-A94U>].

B. Promoting Financial Privacy over BSA Compliance

The biggest issue in virtual currency right now is:

the tech isn't getting built as fast and well as it could be because everyone is engaging in "decentralization theater" to keep the regulators off their backs; . . . regulators are 2–3 years behind the tech curve, are easily duped, are confused, and are terrified of losing cases, so they only go after the easy targets that don't require rethinking the laws[; and] legislators are primarily influenced by D.C. insider lobbyists, who in turn are funded by corporate-style blockchain projects, and are proposing truly terribly drafted and ill-considered laws[.]¹¹⁶

Specific to FinCEN, the current BSA system "is geared towards compliance expectations that bear little relationship to the actual goal of preventing or detecting financial crime, and fail to consider collateral consequences for national security, global development[,] and financial inclusion."¹¹⁷ Laws are meant to promote the general welfare, uphold social norms, and protect individuals against abuses of governmental power. In this way, certain laws are designed to make law enforcement's job more difficult in gathering information that can later be used against individuals. The structure of the BSA sacrifices personal privacy to the government to help identify financial criminals and terrorists, yet there is no prohibition from this information being used for other forms of surveillance. Rather than making it easier to identify these nefarious users, the mass amount of information reported to the government makes it easier for users to be lost in the crowd and creates more systems susceptible to data leaks, breaches, and attacks.¹¹⁸

116. *_g4brielShapir0, Size Does Matter — Part 1: A Philosophy of Securities Laws for Tokenized Networks*, MEDIUM (Dec. 25, 2019), [<https://perma.cc/5WUH-422B>].

117. *Combating Money Laundering and Other Forms of Illicit Finance: Opportunities to Reform and Strengthen BSA Enforcement, Before the S. Comm. on Banking, Hous., and Urban Affairs* (Jan. 9, 2018) (testimony of Greg Baer, President, The Clearing House Association), [<https://perma.cc/L9Y5-A2DC>].

118. In 2015, the U.S. government revealed a data breach from its Office of Personnel Management exposing the personal information of "4 million current and former federal employees." Robert Hackett, *A Product Demo May Have Revealed What Could Be the Biggest Ever Government Data Breach*, FORTUNE (June 12, 2015), [<https://perma.cc/HR2B-4698>]. Related to virtual currency, popular trading venues BitMEX and Binance were victims of data leaks and KYC data breaches. Marie Huillet, *BitMEX Investigating 'Extent of*

Despite mainstream media reports and false narratives from public officials, money laundering and other violations of the BSA are not the predominant use cases for virtual currencies. In fact, the public nature of the Bitcoin blockchain, in particular, makes performing signal intelligence by FinCEN much easier than traditional, closed financial institutions subject to the BSA Regulations. Rather than forcing institutions to collect personal information and transaction details, leaving these systems highly susceptible to attack, FinCEN can simply perform blockchain analysis and engage in traditional police work to target financial criminals rather than monitoring systems that are daily infringements on people's privacy.

Using just one example, in 2013, the government, through old-fashioned police work, was able to arrest and subsequently prosecute Ross Ulbricht for his involvement as the leader of Silk Road.¹¹⁹ Silk Road was shut down, and Ulbricht was prosecuted for a multiplicity of crimes including violating Section 1960 of the BSA, ultimately receiving a controversial life-in-prison sentence for his convictions.¹²⁰ Ulbricht made a handful of uncorrelated mistakes in preserving his identity that led to him being tracked.¹²¹ The Ulbricht case shows that even for those who are digitally mindful, they still leave behind enough of a digital fingerprint through, among other means, IP addresses, VPN server logs, and reusable virtual currency addresses to be found. Since the Ulbricht case, there have been countless criminal prosecutions and civil class action lawsuits that utilize chain analysis to bring wrongdoers to justice. The government has access to numerous other investigatory means and technological capabilities such as transaction clustering and heuristics that enable it to track

Impact' After Mass Email Leak, COIN TELEGRAPH (Nov. 2, 2019), [<https://perma.cc/TG56-UHDQ>]; *Update & Action Response: Third-Party Vendor KYC Matter*, BINANCE BLOG (Aug. 23, 2019), [<https://perma.cc/6RAX-KAE3>].

119. *United States v. Ulbricht*, 31 F. Supp. 3d 540, 546-47 (S.D.N.Y. 2014); *see also* David Segal, *Eagle Scout. Idealist. Drug Trafficker?*, N.Y. TIMES (Jan. 18, 2014), [<https://perma.cc/CD55-ZMWT>].

120. *Ulbricht*, 31 F. Supp. 3d at 549-50; *see also* David Adler, *Silk Road: The Dark Side of Cryptocurrency*, FORDHAM J. CORP. & FIN. L. BLOG (Feb. 21, 2018), [<https://perma.cc/2L8X-WNDJ>]; Andy Greenberg, *Silk Road Creator Ross Ulbricht Loses His Life Sentence Appeal*, WIRED (May 31, 2017), [<https://perma.cc/MM4Y-45FC>].

121. Tim Hume, *How FBI Caught Ross Ulbricht, Alleged Creator of Criminal Marketplace Silk Road*, CNN, [<https://perma.cc/B5H3-F846>] (last updated Oct. 5, 2013).

criminals that do not necessitate the collective violations of an entire country's financial privacy.

What is needed is both a cultural change from the population and a rule change from FinCEN. It is understood that if a user is using the legacy financial institutions to purchase virtual currency with fiat currency, the BSA Regulations apply.¹²² However, once moving your virtual currency to other virtual currency native products and services, the government should not be allowed to use KYC information to inextricably link all future transactions from that address and, through statistical clustering, trace it back to real world persons not engaging with the fiat world without weighing the person's right to privacy. The only way to break this link currently is for users to regain their financial privacy and proactively use downloadable tools such as CoinJoin and other anonymity enhancing services, which FinCEN believes are money transmission services subject to its oversight.¹²³ Whether these services register with FinCEN is another matter as is whether users using these services from KYC accounts could be forced to comply with the regulations as well.

With approximately seven years of intricate study of virtual currencies, FinCEN, rather than Congress, should now take the time to adopt formal rules through a notice and comment process as it did in 2011, solidifying a new system of oversight that appeases their concerns about money laundering and illicit financial transactions without restricting the benefits that virtual currencies provide to legitimate users. Based on FinCEN's rhetoric, it is clear that exerting any form of control over a user—either through account sign ups or control over a user's private keys—means regulatory liability. Therefore, regardless of a service's or software's profit scheme, non-controlling developers and software providers should be expressly exempt from complying with the BSA Regulations as money transmitters. These services, if truly decentralized, are configured in such ways that it is not a matter of “won't comply” but rather a matter of “can't comply.”

122. SEC. OF THE U.S. DEP'T OF THE TREASURY, A REPORT TO THE CONGRESS IN ACCORDANCE WITH SECTION 359 OF THE UNITING AND STRENGTHENING AMERICA BY PROVIDING APPROPRIATE TOOLS REQUIRED TO INTERCEPT AND OBSTRUCT TERRORISM ACT OF 2001 3, 6-7 (Nov. 2002), [<https://perma.cc/XM5M-YQKR>].

123. See 2019 Guidance, *supra* note 92, at 19-20.

V. CONCLUSION

Ultimately, “[w]hat is basically at issue here is whether the type of partnership between government and private enterprise . . . can operate effectively to insure the maintenance of [ethical] standards in the long run.”¹²⁴ The BSA, while technologically neutral, did not envision a technology like bitcoin that mimics certain qualities of cash but is based on free, open source software built for international, open, technical standards rather than proprietary software built for national, highly guarded, closed, technical standards existing solely for highly regulated financial institutions. Bitcoin and other virtual currencies are shoved into the value that substitutes for currency category, but the truly decentralized projects building products and services that enable virtual currency transactions are not like other financial institutions. While custodial services like those mentioned in Section IV.A closely resemble the “one-to-one” intermediation model of finance that simply replace banks and other traditional financial institutions outlined in the BSA, non-custodial services are placed in a legal gray area. While FinCEN is trying to figure out how to overlay the rule of law onto these services, the BSA system in place incentivizes over-reporting of financial information on unsuspecting users and forces projects to alter their development paths.¹²⁵ Without an updated rule making that prevents overregulation, maintains the openness principles of virtual currency, and expressly limits FinCEN’s ability to gather information from any non-custodial service built using open source software or coerce individuals into compliance, legitimate businesses and users will be prevented from benefiting from this new technology.

124. *Silver v. N.Y. Stock Exch.*, 373 U.S. 341, 366 (1963).

125. See Alex Wearn, *Pragmatic Decentralization: How IDEX Will Approach Industry Regulations*, MEDIUM (Nov. 1, 2018), [<https://perma.cc/WP3G-KGS9>].