

Virtual Currencies and Money Laundering: Legal Background, Enforcement Actions, and Legislative Proposals

Jay B. Sykes Legislative Attorney

Nicole VanatkoLegislative Attorney

April 3, 2019

Congressional Research Service

7-.... www.crs.gov R45664

SUMMARY

R45664

April 3, 2019

Jay B. Sykes

Legislative Attorney -re-acte--@crs.loc.gov

Nicole Vanatko

Legislative Attorney -re-acte--@crs.loc.gov

For a copy of the full report, please call 7-.... or visit www.crs.gov.

Virtual Currencies and Money Laundering: Legal Background, Enforcement Actions, and Legislative Proposals

Law enforcement officials have described money laundering—the process of making illegally obtained proceeds appear legitimate—as the "lifeblood" of organized crime. Recently, money launderers have increasingly turned to a new technology to conceal the origins of illegally obtained proceeds: virtual currency. Virtual currencies like Bitcoin, Ether, and Ripple are digital representations of value that, like ordinary currency, function as media of exchange, units of account, and stores of value. However, unlike ordinary currencies, virtual currencies are not legal tender, meaning they cannot be used to pay taxes and creditors need not accept them as payments for debt. While virtual currency enthusiasts tout their technological promise, a number of

commentators have contended that the anonymity offered by these new financial instruments makes them an attractive vehicle for money laundering. Law enforcement officials, regulators, and courts have accordingly grappled with how virtual currencies fit into a federal anti-money laundering (AML) regime designed principally for traditional financial institutions.

The federal AML regime consists of two general categories of laws and regulations. First, federal law requires a range of "financial institutions" to abide by a variety of AML program, reporting, and recordkeeping requirements. Second, federal law criminalizes money laundering and various forms of related conduct.

Over the past decade, federal prosecutors and regulators have pursued a number of cases involving the application of these laws to virtual currencies. Specifically, federal prosecutors have brought money laundering charges against the creators of online marketplaces that allowed their users to exchange virtual currency for illicit goods and services. In one of these prosecutions, a federal district court held that transactions involving Bitcoin can serve as the predicate for money laundering charges. Federal prosecutors have also pursued charges against the developers of certain virtual currency payment systems allegedly designed to facilitate illicit transactions and launder the proceeds of criminal activity. Specifically, prosecutors charged these developers with conspiring to commit money laundering and operating unlicensed money transmitting businesses. In adjudicating the second category of charges, courts have concluded that the relevant virtual currency payment systems were "unlicensed money transmitting businesses," rejecting the argument that the relevant criminal prohibition applies only to money transmitters that facilitate cash transactions. Finally, the Financial Crimes Enforcement Network (FinCEN)—the bureau within the Treasury Department responsible for administering the principal federal AML statute—has pursued a number of administrative enforcement actions against virtual currency exchangers, assessing civil penalties for failure to implement sufficient AML programs and report suspicious transactions.

As these prosecutions and enforcement actions demonstrate, virtual currencies have a number of features that make them attractive to criminals. Specifically, commentators have noted that money launderers are attracted to the anonymity, ease of cross-border transfer, lack of clear regulations, and settlement finality that accompanies virtual currency transactions. Several bills introduced in the 116th Congress are aimed at addressing these challenges. These bills would, among other things, commission agency analyses of the use of virtual currencies for illicit activities and clarify FinCEN's statutory powers and duties. Commentators have also identified legal uncertainty as an additional challenge facing prosecutors, regulators, and participants in virtual currency transactions. Moreover, a number of observers have argued that existing AML regulations are likely to stifle innovation by virtual currency developers. In response to these concerns about legal clarity and burdensome regulation, at least one legislative proposal contemplates exempting certain blockchain developers from various AML requirements.

Contents

Legal Background	2
Requirements for "Financial Institutions"	2
Criminal AML Provisions	
FinCEN Guidance	4
Prosecutions and Enforcement Actions	5
Online Marketplaces for Illicit Goods	6
AlphaBay	
Virtual Currency Payment Systems Used for Illicit Purposese-Gold	7
Liberty Reserve	
FinCEN Enforcement Actions Against Virtual Currency Exchangers	
RippleBTC-e	
Issues for Congress and Proposed Legislation	11
Regulatory Challenges Posed by Virtual Currencies	
Bills in the 116th Congress	12
Legislation Commissioning Agency Analyses	12
H.R. 1414, FinCEN Improvement Act of 2019	
H.R. 528, Blockchain Regulatory Certainty Act	13
Contacts	
Author Contact Information	14

aw enforcement officials have described money laundering—the process of making illegally obtained proceeds appear legitimate—as the "lifeblood" of organized crime. According to one estimate, criminals launder roughly \$1 trillion to \$2 trillion annually worldwide, a sum that represents between 2% and 5% of global gross domestic product. Without the ability to conceal and spend these large sums of "dirty" money, criminal organizations "could operate only at a small fraction of current levels, and with far less flexibility."

Over the past decade, money launderers have turned to a new technology to conceal the origins of illegally obtained proceeds: virtual currency. Virtual currencies like Bitcoin, Ether, and Ripple are digital representations of value that, like ordinary currency, function as media of exchange, units of account, and stores of value.⁴ However, unlike ordinary currency, virtual currencies are not legal tender, meaning they cannot be used to pay taxes and creditors need not accept them as payments for debt.⁵ According to their proponents, virtual currencies (1) have the potential to offer cheaper and faster transactions than traditional bank-centric payment networks,⁶ (2) provide inflation-resistant alternatives to traditional fiat currencies,⁷ and (3) often involve promising new technologies (such as blockchain technology) that will spur innovation across a variety of fields.⁸ However, other commentators have argued that the anonymity offered by certain decentralized virtual currencies—that is, virtual currencies that are not issued or maintained by a central organization—makes them an attractive vehicle for money laundering.⁹ These observers have contended that criminals often use such virtual currencies not only to buy and sell illicit goods and services, but also to launder illegally obtained fiat currencies.¹⁰

⁶ See Jerry Brito & Andrea Castillo, Bitcoin: A Primer for Policymakers 13-14 (2016).

=

¹ William R. Schroeder, *Money Laundering: A Global Threat and the International Community's Response*, FBI L. ENFORCEMENT BULLETIN at 2 (May 2001).

 $^{^2\} PwC, PwC\ Global\ Economic\ Crime\ Survey\ 2016\ (2016), \ https://www.pwc.com/gx/en/economic-crime-survey/pdf/Global\ Ec$

³ Andrew J. Camelio & Benjamin Pergament, *Money Laundering*, 35 Am. CRIM. L. REV. 965, 966 (1998).

⁴ See Virtual Currencies: Key Definitions and Potential AML/CFT Risks, FIN. ACTION TASK FORCE at 4 (June 2014), https://www.fatf-gafi.org/media/fatf/documents/reports/Virtual-currency-key-definitions-and-potential-aml-cft-risks.pdf [hereinafter "2014 FATF Report"].

⁵ See id

⁷ See Maximilian Heath, Cryptocurrency ATMs Coming to Argentina to Exploit Peso Volatility, Reuters (Oct. 3, 2018), https://www.reuters.com/article/us-crypto-currencies-argentina/cryptocurrency-atms-coming-to-argentina-to-exploit-peso-volatility-idUSKCN1MD2FK; PAUL VIGNA & MICHAEL J. CASEY, THE AGE OF CRYPTOCURRENCY: How BITCOIN AND DIGITAL MONEY ARE CHALLENGING THE GLOBAL ECONOMIC ORDER 295 (2015); Alan Feuer, The Bitcoin Ideology, N.Y. TIMES (Dec. 14, 2013), https://www.nytimes.com/2013/12/15/sunday-review/the-bitcoin-ideology.html.

⁸ See Brito & Castillo, supra note 6, at 21-29.

⁹ See Illicit Use of Virtual Currency and the Law Enforcement Response: Hearing Before the Subcomm. On Terrorism and Illicit Finance, 115th Cong. at 3 (June 20, 2018) (Statement of Thomas P. Ott, Assoc. Dir., Enforcement Div., Fin. Crimes Enforcement Network) ("Virtual currency payments pose money laundering, sanctions evasion, and other illicit financing risks that necessitate careful assessment and mitigation.") [hereinafter "Ott Testimony"]; Brett Nigh & C. Alden Pelker, Virtual Currency: Investigative Challenges and Opportunities, FBI L. ENFORCEMENT BULLETIN (Sept. 8, 2015), https://leb.fbi.gov/articles/featured-articles/virtual-currency-investigative-challenges-and-opportunities (noting that virtual currencies "can be exploited by criminals to further their illegal activities," and that law enforcement "will investigate criminals who use virtual currency to move or hide money derived from criminal or terrorist acts"); 2014 FATF Report, supra note 4, at 9 (explaining that decentralized virtual currencies "are potentially vulnerable to money laundering and terrorist financing abuse" because of the anonymity they afford their users and the inability of law enforcement to "target one central location or entity... for investigative or asset seizure purposes").

¹⁰ See Joshua Fruth, 'Crypto-cleansing': Strategies to Fight Digital Currency Money Laundering and Sanctions Evasion, REUTERS (Feb. 13, 2018), https://www.reuters.com/article/bc-finreg-aml-cryptocurrency/crypto-cleansing-

While it is difficult to definitively assess the volume of money laundered through virtual currencies, the virtual currency security firm CipherTrace has estimated that criminals laundered roughly \$2.5 billion of Bitcoin on major exchanges between January 9, 2009, and September 20, 2018.¹¹ An official from the Treasury Department's Financial Crimes Enforcement Network (FinCEN) has similarly indicated that virtual currencies have been "exploited to support billions of dollars of . . . suspicious activity." While such figures represent only a fraction of both global money laundering and virtual currency transaction volume, government officials have identified virtual currencies as a growth industry for money launderers that presents regulators and law enforcement with unique challenges.¹³

This report provides a general overview of the application of federal anti-money laundering (AML) law to virtual currencies. First, the report outlines the basic architecture of federal AML law. Second, the report discusses administrative guidance concerning the application of federal AML law to virtual currencies. Third, the report reviews a number of prominent criminal prosecutions and administrative enforcement actions involving federal AML law and virtual currencies. Finally, the report discusses a number of legislative proposals to reform certain elements of the federal AML regime surrounding virtual currencies and further investigate the use of virtual currencies in criminal activities.

Legal Background

The federal AML regime consists of two general categories of laws and regulations. First, federal law requires a range of "financial institutions" to abide by a variety of AML compliance program, reporting, and recordkeeping requirements. Second, federal law criminalizes money laundering and various forms of related conduct.

Requirements for "Financial Institutions"

The Bank Secrecy Act (BSA) and its various amendments¹⁴ represent the centerpiece of the federal AML regime for "financial institutions"—a category that includes federally insured banks, securities brokers and dealers, currency exchanges, and money services businesses. 15 Under the BSA and associated regulations, covered "financial institutions" must, among other things,

strategies-to-fight-digital-currency-money-laundering-and-sanctions-evasion-idUSKCN1FX29I.

¹¹ See CipherTrace, Cryptocurrency Anti-Money Laundering Report, 2018 03, 3 (2018), https://ciphertrace.com/wp-content/uploads/2018/10/crypto_aml_report_2018q3.pdf.

¹² See Ott Testimony, supra note 9, at 3.

¹³ See id. (indicating that suspicious transaction reports involving virtual currencies increased 90 percent from 2016 to 2017); Illicit Use of Virtual Currency and the Law Enforcement Response: Hearing Before the Subcomm. On Terrorism and Illicit Finance, 115th Cong. at 5-6 (June 20, 2018) (Statement of Robert Novy, Deputy Dir., Office of Investigations, U.S. Secret Serv.) (noting that "[t]he growing illicit use of digital currencies risks undermining the effectiveness of existing U.S. laws and regulations, especially those intended to limit the ability of criminals to profit from their illicit activities") [hereinafter "Novy Testimony"]; Illicit Use of Virtual Currency and the Law Enforcement Response: Hearing Before the Subcomm. On Terrorism and Illicit Finance, 115th Cong. at 6-7 (June 20, 2018) (Statement of Gregory C. Nevano, Deputy Assistant Dir., Illicit Trade, Travel, and Fin. Div., Homeland Sec. Investigations, Dep't of Homeland Sec.) (observing that anonymity-enhanced virtual currencies present new challenges to law enforcement).

¹⁴ Pub. L. No. 91-508, 84 Stat. 1114-2 (1970).

¹⁵ 31 U.S.C. § 5312(a)(2); 31 C.F.R. § 1010.100. See also John Madinger, Money Laundering: A Guide for CRIMINAL INVESTIGATORS 57 (3d ed. 2012) ("The network of statutes that combine . . . to create a comprehensive antimoney laundering package is centered on the Bank Secrecy Act.").

establish AML programs that meet certain minimum standards, ¹⁶ report certain types of transactions to the Treasury Department, ¹⁷ and maintain certain financial records. ¹⁸

Specifically, the BSA requires "financial institutions" to establish AML programs that include, at a minimum, (1) the development of internal policies, procedures, and controls, (2) the designation of a compliance officer, (3) an ongoing employee training program, and (4) an independent audit function to test the program. "Financial institutions" must also report certain large currency transactions and suspicious activities to FinCEN—the bureau within the Treasury Department responsible for administering the BSA. Finally, the BSA and associated regulations require "financial institutions" to maintain certain types of records. FinCEN regulations require banks, for example, to retain records related to certain large transactions involving foreign banks and the taxpayer identification numbers associated with certain accounts.

Money services businesses (MSBs) represent one category of "financial institution" that must register with FinCEN and, like other "financial institutions," abide by AML program, reporting, and recordkeeping requirements. ²² Under FinCEN's regulations, MSBs include a variety of specific categories of businesses, including "money transmitters"—that is, (1) persons who accept "currency, funds, or other value that substitutes for currency from one person" and transmit those items "to another location or person by any means," and (2) "[a]ny other person engaged in the transfer or funds." ²³ In addition to imposing regulatory requirements on MSBs, federal law makes it a crime to knowingly operate an "unlicensed money transmitting business." ²⁴ An entity qualifies as an "unlicensed money transmitting business" under this provision (Section 1960 of Title 18) if it

- 1. is "operated without an appropriate money transmitting license in a State where such operation is punishable as a misdemeanor or a felony";
- 2. fails to comply with the BSA's federal registration requirement for "money transmitting businesses"; or
- 3. "otherwise involves the transportation or transmission of funds that are known to the defendant to have been derived from a criminal offense or are intended to be used to promote or support unlawful activity."²⁵

Criminal AML Provisions

In addition to imposing various AML requirements on "financial institutions," federal law also criminalizes money laundering and certain related conduct. Specifically, 18 U.S.C. § 1956(a)(1) (Section 1956) makes it unlawful for a person who "know[s] that the property involved in a

²³ Id. § 1010.100(ff)(5)(i).

¹⁶ See 31 U.S.C. § 5318(h); 31 C.F.R. ch. X (setting forth AML program requirements for various categories of "financial institutions").

¹⁷ See 31 U.S.C. §§ 5313-16, 5318(g).

¹⁸ See 31 C.F.R. ch. X (setting forth recordkeeping requirements for various categories of "financial institutions").

¹⁹ See 31 U.S.C. § 5318(h).

²⁰ See 31 U.S.C. §§ 5313, 5318(g). Reports on large currency transactions and suspicious activities are commonly referred to as currency transaction reports (CTRs) and suspicious activity reports (SARs), respectively.

²¹ See 31 C.F.R. § 103.34.

²² See id. part 1022.

²⁴ See 18 U.S.C. § 1960.

²⁵ *Id.* § 1960(b)(1).

financial transaction represents the proceeds of some form of unlawful activity" to "conduct[] or attempt[] to conduct such a financial transaction which in fact involves the proceeds of specified unlawful activity"26—

- (A) (i) with the intent to promote the carrying on of specified unlawful activity; or
 - (ii) with intent to engage in conduct constituting [tax evasion or tax fraud]; or
- (B) knowing that the transaction is designed in whole or in part—
 - (i) to conceal or disguise the nature, the location, the source, the ownership, or the control of the proceeds of specified unlawful activity; or
 - (ii) to avoid a transaction reporting requirement under State or Federal law.²⁷

For purposes of this prohibition, the term "financial transaction" includes transactions "involving the movement of funds" and transactions "involving one or more monetary instruments." 28

Similarly, 18 U.S.C. § 1957(a) (the so-called "Spending Statute") prohibits monetary transactions in criminally derived property. Specifically, Section 1957(a) makes it unlawful to "knowingly engage[] or attempt[] to engage in a monetary transaction in criminally derived property of a value greater than \$10,000 and is derived from specified unlawful activity."²⁹ In other words, unlike Section 1956, Section 1957 makes it a crime to knowingly spend the proceeds of specified unlawful activity, even if such spending does not promote such activity and is not designed to conceal the origins of the proceeds.

FinCEN Guidance

Because neither Congress nor FinCEN has formally amended the BSA regulatory regime in response to the advent of virtual currencies, prosecutors and regulators have been required to analyze whether virtual currency transactions and business models fall within some of the preexisting legal categories discussed above. In 2013, FinCEN attempted to clarify certain aspects of this analysis by issuing administrative guidance addressing the circumstances in which participants in virtual currency transactions qualify as MSBs.³⁰

In its 2013 guidance, FinCEN took the position that "users" of virtual currencies do not qualify as MSBs subject to federal registration requirements, while "administrators" and "exchangers" of virtual currencies may qualify as MSBs.31 Specifically, the guidance explained that users of virtual currencies—that is, persons who obtain virtual currencies to purchase goods or services—

²⁶ The relevant "specified unlawful activities" are enumerated at 18 U.S.C. § 1956(c)(7).

²⁷ 18 U.S.C. § 1956(a)(1). Similarly, 18 U.S.C. § 1956(a)(2) prohibits "international transportation money laundering," while 18 U.S.C. § 1956(a)(3), which is most relevant in law enforcement "sting operations," prohibits conducting financial transactions with property that is represented to be the proceeds of specified unlawful activity. For a more detailed overview of these statutory provisions, see CRS Report RL33315, Money Laundering: An Overview of 18 U.S.C. § 1956 and Related Federal Criminal Law, by Charles Doyle.

²⁸ 18 U.S.C. § 1956(c)(4).

²⁹ Id. § 1957(a).

³⁰ Application of FinCEN's Regulations to Persons Administering, Exchanging, or Using Virtual Currencies, Fin. CRIMES ENFORCEMENT NETWORK (Mar. 18, 2013), https://www.fincen.gov/sites/default/files/shared/FIN-2013-G001.pdf.

³¹ See id. at 2-3.

are not MSBs because they are not involved in money transmission. ³² By contrast, FinCEN indicated that virtual currency *administrators* (persons "engaged as a business" in putting a virtual currency into circulation and who have the authority to withdraw such currency from circulation) and *exchangers* (persons "engaged as a business in the exchange of virtual currency for real currency, funds, or other virtual currency") may be "money transmitters" and, by extension, MSBs. ³³ Specifically, FinCEN explained that virtual currency administrators and exchangers qualify as MSBs (unless they fall within a specific exemption) when they (1) "accept[] or transmit[] a convertible virtual currency," or (2) "buy[] or sell[] convertible virtual currency for any reason." ³⁴ Accordingly, under FinCEN's guidance, virtual currency issuers and exchangers will generally qualify as MSBs unless they fall within a specific statutory or regulatory exemption. ³⁵

Prosecutions and Enforcement Actions

Over the past decade, federal prosecutors and regulators have pursued a number of cases involving the application of federal AML law to virtual currencies. In a number of criminal cases, federal prosecutors have brought money-laundering and certain related charges against the operators of online marketplaces and virtual currency payment systems used to disguise the proceeds of illicit activities.³⁶ FinCEN has also brought civil enforcement actions against virtual currency exchangers for failure to comply with the BSA's AML program, reporting, and recordkeeping requirements.³⁷

While FinCEN's 2013 guidance identified the circumstances in which certain participants in virtual currency transactions qualify as MSBs, it did not indicate whether the relevant categories—that is, users, administrators, and exchangers—exhaust the range of actors who may qualify as MSBs. However, FinCEN has subsequently issued several administrative rulings clarifying the application of its regulations to a number of specific virtual currency business models. *See* Application of FinCEN's Regulations to Persons Issuing Physical or Digital Negotiable Certificates of Ownership of Precious Metals, Fin. CRIMES ENFORCEMENT NETWORK (Aug. 14, 2015),

https://www.fincen.gov/sites/default/files/administrative_ruling/FIN-2015-R001.pdf; Request for Administrative Ruling on the Application of FinCEN's Regulations to a Virtual Currency Payment System, Fin. CRIMES ENFORCEMENT NETWORK (Oct. 27, 2014), https://www.fincen.gov/sites/default/files/administrative_ruling/FIN-2014-R012.pdf; Request for Administrative Ruling on the Application of FinCEN's Regulations to a Virtual Currency Trading Platform, Fin. CRIMES ENFORCEMENT NETWORK (Oct. 27, 2014),

https://www.fincen.gov/sites/default/files/administrative_ruling/FIN-2014-R011.pdf; Application of Money Services Business Regulations to the Rental of Computer Systems for Mining Virtual Currency, Fin. Crimes Enforcement Network (April 29, 2014), https://www.fincen.gov/sites/default/files/administrative_ruling/FIN-2014-R007.pdf; Application of FinCEN's Regulations to Virtual Currency Software Development and Certain Investment Activity, Fin. Crimes Enforcement Network (Jan. 30, 2014), https://www.fincen.gov/sites/default/files/shared/FIN-2014-R002.pdf; Application of FinCEN's Regulations to Virtual Currency Mining Operations, Fin. Crimes Enforcement Network (Jan. 30, 2014), https://www.fincen.gov/sites/default/files/shared/FIN-2014-R001.pdf.

3

³² *Id*. at 2.

³³ *Id*. at 3.

³⁴ *Id.* A "convertible" virtual currency is a virtual currency that either has an equivalent value in real currency or acts as a substitute for real currency. *Id.* at 1.

³⁵ See Peter Van Valkenburgh, The Bank Secrecy Act, Cryptocurrencies, and New Tokens: What is Known and What Remains Ambiguous, COIN CENTER at 8 (May 2017), https://coincenter.org/files/2017-05/report-bsa-crypto-token1.pdf.

³⁶ See "Silk Road," "AlphaBay," "e-Gold," "Liberty Reserve" infra.

³⁷ See "Ripple," "BTC-e" infra.

Online Marketplaces for Illicit Goods

Federal prosecutors have brought money-laundering charges against the creators of online marketplaces that allowed their users to exchange virtual currency for a range of illicit goods and services. In one of these prosecutions, a federal district court held that transactions involving Bitcoin can serve as the predicate for money-laundering charges.

Silk Road

In 2013, federal authorities shut down Silk Road, which they alleged was "the most sophisticated and extensive criminal marketplace on the Internet," enabling tens of thousands of users to anonymously buy and sell illegal drugs, malicious software, and other illicit goods and services.³⁸ Federal prosecutors charged the site's creator with, among other things, conspiracy to commit money laundering under Section 1956.³⁹ The prosecutors alleged that the site's creator conspired to conduct "financial transactions" involving the proceeds of unlawful activity—namely, narcotics trafficking and computer hacking—with the intent to promote the carrying on of such activity. 40 In defending this charge, Silk Road's creator argued that his alleged conduct facilitating the exchange of Bitcoin for illegal goods and services—did not involve "financial transactions" within the meaning of Section 1956, which defines that term to include (among other things) transactions "involving one or more monetary instruments." Specifically, the site's creator contended that because Bitcoin does not qualify as a "monetary instrument"—which Section 1956 defines to mean the currency of a country, personal checks, bank checks, money orders, investment securities, or negotiable instruments—transactions involving Bitcoin do not represent "financial transactions" under Section 1956.42

The U.S. District Court for the Southern District of New York rejected this argument, holding that transactions involving Bitcoin can qualify as "financial transactions" under Section 1956 because they fall under a separate category of transactions identified by the relevant statutory definition: transactions involving "the movement of funds." Specifically, the court reasoned that Bitcoin transactions involve "the movement of funds" because the term "funds" includes "money," which in turn refers to "an object used to buy things." Because Bitcoin can be used to buy things, the court reasoned that Bitcoin transactions involve "the movement of funds" and therefore qualify as "financial transactions" under Section 1956. 45 As a result, the court explained, "[o]ne can money launder using Bitcoin."46

Congressional Research Service

³⁸ United States v. Ulbricht, 31 F. Supp. 3d 540, 549-50 (S.D.N.Y. 2014). See also David Adler, Silk Road: The Dark Side of Cryptocurrency, FORDHAM J. OF CORP. & FIN. L. BLOG (Feb. 21, 2018), https://news.law.fordham.edu/jcfl/2018/02/21/silk-road-the-dark-side-of-cryptocurrency/.

³⁹ *Ulbricht*, 31 F. Supp. 3d at 568-69.

⁴⁰ *Id.* at 569.

⁴¹ See id.; 18 U.S.C. § 1956(c)(4).

⁴² *Ulbricht*, 31 F. Supp. 3d at 569; 18 U.S.C. § 1956(c)(5).

⁴³ *Ulbricht*, 31 F. Supp. 3d at 570; 18 U.S.C. § 1956(c)(4) (emphasis added).

⁴⁴ *Ulbricht*, 31 F. Supp. 3d at 570.

⁴⁵ Id.

⁴⁶ Id. The defendant's conviction was ultimately affirmed by the U.S. Court of Appeals for the Second Circuit, which did not address this interpretive issue with Section 1956. See United States v. Ulbricht, 858 F.3d 71 (2d Cir. 2017).

AlphaBay

Similarly, in 2017, federal prosecutors brought money-laundering conspiracy charges against the creator of AlphaBay, another online marketplace that allowed its users to exchange virtual currency for illicit goods and services.⁴⁷ The prosecutors alleged that by facilitating the exchange of virtual currencies (including Bitcoin, Monero, and Ether) for illegal narcotics and other illicit goods and services, the site's creator had conspired to conduct "financial transactions" involving the proceeds of unlawful activities.⁴⁸ However, the federal government dismissed these charges after AlphaBay's creator died in July 2017.⁴⁹

Virtual Currency Payment Systems Used for Illicit Purposes

Federal prosecutors have also pursued charges against the developers of certain virtual currency payment systems allegedly designed to facilitate illicit transactions and launder the proceeds of criminal activity. 50 Specifically, prosecutors have charged these developers with conspiring to commit money laundering and operating unlicensed money transmitting businesses under Sections 1956 and 1960, respectively. In adjudicating the second category of charges, courts have concluded that the relevant virtual currency payment systems were "unlicensed money transmitting businesses" under Section 1960, rejecting the argument that the provision applies only to money transmitters that facilitate cash transactions.

e-Gold

In 2007, federal prosecutors charged e-Gold—an "alternative payment system" and virtual currency purportedly backed by stored physical gold—and its founders and director with money laundering and operating an unlicensed money transmitting business.⁵¹ The prosecutors alleged that e-Gold "was widely accepted as a payment mechanism for transactions involving credit card and identification fraud, high yield investment programs and other investment scams, and child exploitation" because of the anonymity it offered its users.⁵²

In charging the defendants for failing to register their business, prosecutors alleged that e-Gold operated as an "unlicensed money transmitting business" in each of the three ways identified by Section 1960—the provision criminalizing the operation of "unlicensed money transmitting businesses." Specifically, the prosecutors alleged that e-Gold (1) lacked a required state money transmitter license, (2) failed to comply with the BSA's federal registration requirements for "money transmitting businesses" (requirements set forth in Section 5330 of Title 31), and (3) was involved in the transmission of funds that were "known to have been derived from a criminal offense" or that were "intended to be used to promote and support unlawful activity."53

In defending these charges, the defendants presented an intricate argument for the proposition that Section 1960 applies only to businesses that facilitate *cash* (as opposed to virtual currency)

⁴⁷ Indictment, United States, v. Cazes, No. 1:17-cr-00144 ¶ 57 (E.D. Cal. Jun. 1, 2017).

⁴⁹ See United States v. 2013 Lamborghini Aventador LP700-4, No. 1:17-cv-00967, 2018 WL 3752131 at *4 (E.D. Cal. Aug. 8, 2018).

⁵⁰ See "e-Gold," "Liberty Reserve" infra.

⁵¹ Indictment, United States v. e-Gold, Ltd., No. 07-109 ¶¶ 1-6 (D.D.C. Apr. 24, 2007).

⁵² *Id*. ¶ 2.

⁵³ *Id*. ¶ 76.

transactions. Specifically, the defendants argued that because Section 1960 does not define the term "money transmitting business," it must "borrow" the definition of that term in Section 5330—the BSA provision establishing federal registration requirements for "money transmitting businesses." The defendants further reasoned that (1) Section 5330 provides that an entity is a "money transmitting business" only if it must file currency transaction reports (CTRs), and (2) businesses that do not facilitate cash transactions need not file CTRs. Accordingly, under the defendants' theory, a business like e-Gold that does not facilitate *cash* transactions does not qualify as a "money transmitting business" under Section 5330 and (by extension) Section 1960. Section 1960.

The U.S. District Court for the District of Columbia rejected this argument, holding that e-Gold was indeed a "money transmitting business" under Section 1960 for two reasons. First, the court rejected the defendants' contention that Section 1960 must "borrow" Section 5330's definition of "money transmitting business." The court rejected this argument on the grounds that Section 1960 contains its own definition of the term "money transmitting" and does not reflect an intent to "borrow" the definition of "money transmitting business" from Section 5330. The court further explained that because e-Gold was a business engaged in "money transmitting" as defined by Section 1960—that is, "transferring funds on behalf of the public"—it was a "money transmitting business" under Section 1960.

Second, the court evaluated whether e-Gold also qualified as a "money transmitting business" under Section 5330—an issue that remained relevant because of the federal government's charge that the defendants violated Section 1960 by violating Section 5330's registration requirements. The court concluded that e-Gold was indeed a "money transmitting business" under Section 5330, rejecting the defendants' argument that e-Gold did not fall within that category because it was not required to file CTRs. 60 Specifically, the court rejected the argument that a business is required to file CTRs only if it facilitates cash transactions, Instead, the court explained that because the statute imposing CTR obligations imposes such obligations when money transmitting businesses facilitate cash transactions (as opposed to if they facilitate such transactions), all money transmitting businesses have a continuing obligation to file CTRs "in the eventuality that they ever are involved" in a reportable cash transaction. 61 The court accordingly concluded that because e-Gold was required to file CTRs and satisfied the other elements of the relevant statutory definition, e-Gold was a "money transmitting business" under Section 5330 even though it did not process cash transactions. 62 After the court denied the defendants' motion to dismiss the charges for operating an unlicensed money transmitting business, the defendants pleaded guilty to those charges and money laundering.⁶³

⁵⁸ *Id.* at 89-93.

⁵⁴ United States v. E-Gold, Ltd., 550 F. Supp. 2d 82, 87-88 (D.D.C. 2008).

⁵⁵ 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. *See* 31 C.F.R. § 1010.311. 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. *See id.*; 31 U.S.C. § 5313(a).

⁵⁶ See United States v. E-Gold, Ltd., 550 F. Supp. 2d 82, 87-88 (D.D.C. 2008).

⁵⁷ *Id*. at 89.

⁵⁹ *Id*. at 93.

⁶⁰ Id. at 93-97.

⁶¹ Id. at 94-95.

⁶² Id. at 97.

⁶³ Digital Currency Business E-Gold Pleads Guilty to Money Laundering and Illegal Money Transmitting Charges,

Liberty Reserve

Similarly, in May 2013, federal prosecutors charged the founder of Liberty Reserve—a Costa Rica-based virtual currency service—with conspiracy to commit money laundering, conspiracy to commit international money laundering, and operating an unlicensed money transmitting business. Liberty Reserve administered a virtual currency known as "LR" and described itself as a "payment processor and money transfer system. Sa According to prosecutors, Liberty Reserve's founder "intentionally created, structured, and operated" the service "as a business venture designed to help criminals conduct illegal transactions and launder the proceeds of their crimes, facilitating a broad range of criminal activity that included identity theft, credit card fraud, computer hacking, child pornography, and narcotics trafficking. Specifically, Liberty Reserve allegedly facilitated such activity by allowing its users to set up accounts using fake names and, for an additional fee, hide their account numbers when sending funds within the system. Recause of this anonymity, prosecutors alleged, Liberty Reserve became the "bank of choice for the criminal underworld," laundering over \$6 billion between 2006 and 2013.

In defending the charge for operating an unlicensed money transmitting business, Liberty Reserve's founder argued that Liberty Reserve was not an "unlicensed money transmitting business" under Section 1960 because it did not transfer "funds" within the meaning of that provision. ⁶⁹ However, the U.S. District Court for the Southern District of New York rejected this argument, relying on an earlier case from the same district to conclude 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." Liberty Reserve's founder was ultimately convicted of operating an unlicensed money transmitting business and pleaded guilty to conspiring to commit money laundering. ⁷¹

DEP'T OF JUSTICE (July 21, 2008), https://www.justice.gov/archive/opa/pr/2008/July/08-crm-635.html.

⁶⁷ *Id.* at *1.

⁶⁴ Sealed Indictment, United States v. Liberty Reserve, S.A., 13-crim-368 (S.D.N.Y. 2013).

⁶⁵ United States v. Budovsky, No. 13-cr-368, 2015 WL 5602853 at *1 (S.D.N.Y. Sept. 23, 2015).

⁶⁶ Id.

⁶⁸ *Id.* at *1.

⁶⁹ *Id.* at *14.

⁷⁰ *Id.* (quoting United States v. Faiella, 39 F. Supp. 3d 544, 545-47 (S.D.N.Y. 2014)). In September 2016, another judge in the Southern District of New York agreed with the conclusion that virtual currencies qualify as "funds" under Section 1960. *See* United States v. Murgio, 209 F. Supp. 698, 707-08 (S.D.N.Y. 2016).

In May 2013, FinCEN identified Liberty Reserve as a "financial institution of primary money laundering concern" under Section 311 of the PATRIOT Act, marking the first time FinCEN exercised that authority against a virtual currency business. *See* Treasury Identifies Virtual Currency Provider Liberty Reserve as a Financial Institution of Primary Money Laundering Concern under USA Patriot Act Section 311, DEP'T OF THE TREASURY (May 28, 2013), https://www.treasury.gov/press-center/press-releases/pages/jl1956.aspx. By designating Liberty Reserve, FinCEN prohibited U.S. financial institutions from maintaining correspondent relationships with foreign banks that do business with Liberty Reserve, effectively cutting the company off from the U.S. financial system. *Id*.

⁷¹ See Founder of Liberty Reserve Pleads Guilty to Laundering More Than \$250 Million Through His Digital Currency Business, DEP'T OF JUSTICE (Jan. 29, 2016), https://www.justice.gov/opa/pr/founder-liberty-reserve-pleads-guilty-laundering-more-250-million-through-his-digital.

FinCEN Enforcement Actions Against Virtual Currency Exchangers

Consistent with its 2013 guidance, FinCEN has pursued a number of administrative enforcement actions against virtual currency exchangers, assessing civil penalties for failure to implement sufficient AML programs and report suspicious transactions.

Ripple

In 2015, FinCEN brought an enforcement action against California-based virtual currency developer and exchanger Ripple Labs, Inc. (Ripple), assessing a \$700,000 civil penalty for failure to register as a MSB and failure to implement and maintain an effective AML program. 72 At the time of the enforcement action, Ripple's virtual currency (XRP) was the second-largest virtual currency by market capitalization, trailing only Bitcoin.⁷³ Ripple sold XRP in exchange for fiat currency⁷⁴ without registering as a MSB until 2013, when it incorporated a subsidiary to engage in the relevant sales and transfers.⁷⁵ While Ripple's subsidiary ultimately registered with FinCEN, it allegedly failed to fulfill its AML obligations under the BSA. 76 Specifically, FinCEN alleged that Ripple's subsidiary failed to timely establish an AML program that met the BSA's requirements and lacked sufficient controls for implementing the program.⁷⁷ Because of this absence of necessary controls, Ripple's subsidiary negotiated an approximately \$250,000 transaction with a felon without adhering to its know-your-customer requirements and rejected a number of suspicious transactions without filing suspicious activity reports (SARs) with FinCEN. 78 In response to FinCEN's allegations, Ripple and its subsidiary entered into a settlement agreement, committing to undertake a series of remedial measures and pay a \$700,000 civil penalty.⁷⁹

BTC-e

In 2017, FinCEN brought another major enforcement action against BTC-e, one of the largest virtual currency exchanges in the world. 80 FinCEN alleged that BTC-e facilitated transactions involving ransomware, computer hacking, identity theft, tax refund fraud schemes, public corruption, and drug trafficking. 81 FinCEN further contended that BTC-e willfully violated MSB registration requirements, failed to maintain an effective AML program, and failed to file required

⁷⁴ A "fiat currency" is a currency designated as legal tender that is not backed by a commodity. *See* FATF Report, *supra* note 4, at 4.

⁷² See FinCEN Fines Ripple Labs Inc. in First Civil Enforcement Action Against a Virtual Currency Exchanger, Fin. CRIMES ENFORCEMENT NETWORK (May 5, 2015), https://www.fincen.gov/news/news-releases/fincen-fines-ripple-labs-inc-first-civil-enforcement-action-against-virtual. FinCEN assessed this penalty in coordination with the U.S. Attorney's Office for the Northern District of California. See id.

⁷³ *Id*.

⁷⁵ Attachment A, Settlement Agreement, DEP'T OF JUSTICE (May 5, 2015), https://www.justice.gov/sites/default/files/opa/press-releases/attachments/2015/05/05/settlement_agreement.pdf.

⁷⁶ *Id*. ⁷⁷ *Id*.

⁷⁸ *Id*.

⁷⁹ Id.

⁸⁰ FinCEN Fines BTC-e Virtual Currency Exchange \$110 Million for Facilitating Ransomware, Dark Net Drug Sales, Fin. Crimes Enforcement Network (July 26, 2017), https://www.fincen.gov/news/news-releases/fincen-fines-btc-e-virtual-currency-exchange-110-million-facilitating-ransomware.

⁸¹ *Id*.

SARs.⁸² Specifically, FinCEN alleged that BTC-e did not verify basic information about its customers and failed to file SARs on thousands of suspicious transactions, including transactions involving Liberty Reserve and other entities that were widely known to be violating U.S. law.⁸³ Because of this conduct, FinCEN assessed a \$110 million civil money penalty against BTC-e and its founder.⁸⁴

Issues for Congress and Proposed Legislation

Regulatory Challenges Posed by Virtual Currencies

As these prosecutions and enforcement actions demonstrate, virtual currencies have a number of features that make them attractive to criminals. Specifically, commentators have noted that money launderers have been attracted by the anonymity, lack of clear regulations, and settlement finality that accompanies virtual currency transactions. The ease of transferring virtual currencies across international borders further complicates AML efforts, as AML regulations are not widely applied internationally to virtual currency despite increasing evidence of misuse. The Treasury Department's 2018 Money Laundering Risk Assessment accordingly identified virtual currencies as a vulnerability in U.S. AML efforts. Seeveral bills introduced in the 116th Congress aim to address to these challenges. These bills would, among other things, commission agency analyses of the use of virtual currencies for illicit activities and clarify that FinCEN's statutory powers and duties include international coordination on issues related to virtual currencies.

Commentators have also identified legal uncertainty as an additional challenge facing prosecutors, regulators, and participants in virtual currency transactions. ⁹¹ Specifically, these observers have noted that applying the BSA's regulatory regime to virtual currencies requires analyzing novel business models using legal categories developed primarily for traditional financial institutions. ⁹² While the weight of legal authority supports the application of some of these categories to certain virtual currency business models, ⁹³ at least one anomalous decision

84 See id. at 9.

⁸² See Assessment of Civil Money Penalty, In the Matter of BTC-E a/k/a Canton Bus. Corp. and Alexander Vinnik, No. 2017-03, Fin. Crimes Enforcement Network at 3 (July 26, 2017), https://www.fincen.gov/sites/default/files/enforcement_action/2017-07-

^{26/}Assessment%20for%20BTCeVinnik%20FINAL%20SignDate%2007.26.17.pdf.

⁸³ Id. at 5-8.

⁸⁵ See Novy Testimony, supra note 13, at 3-4.

⁸⁶ Adler, supra note 38.

 $^{^{87}}$ Dep't of the Treasury, National Strategy for Combatting Terrorist and Other Illicit Finance 37, 39 (2018).

⁸⁸ Dep't of the Treasury, National Money Laundering Risk Assessment 3 (2018).

⁸⁹ See "Legislation Commissioning Agency Analyses" infra.

⁹⁰ See "H.R. 1414, FinCEN Improvement Act of 2019" infra.

⁹¹ See Alma Angotti & Anne Marie Minogue, Risks and Rewards: Blockchain, Cryptocurrency and Vulnerability to Money Laundering, Terrorist Financing and Tax Evasion, Thomson Reuters (Nov. 26, 2018), https://www.navigant.com/insights/global-investigations-and-compliance/2018/thomson-reuters-westlaw-blockchain-cryptocurrency.

⁹² See id. (noting that it is "difficult" to "seamlessly" apply existing laws and regulations to virtual currencies).

⁹³ See "Prosecutions and Enforcement Actions" supra.

indicates that some judges demand more explicit indicia of congressional intent to apply existing law in this relatively new field. Moreover, a number of commentators have argued that providing greater legal certainty to legitimate virtual currency activities is necessary to preserve the United States' position as a "global leader" in encouraging technological innovation. This interest in legal clarity—in addition to a desire to shield certain virtual currency innovators from "expensive and onerous" AML requirements energies—has generated a legislative proposal to exempt certain blockchain developers from various money transmitter requirements.

Bills in the 116th Congress

Legislation Commissioning Agency Analyses

In January 2019, the House passed three bills that would commission studies concerning the use of virtual currencies for illicit purposes. H.R. 56, the Financial Technology Protection Act, would establish an Independent Financial Technology Task Force to Combat Terrorism and Illicit Financing (Task Force) led by the Treasury Secretary. The bill would direct the Task Force to (1) "conduct independent research on terrorist and illicit use of new financial technologies, including digital currencies," and (2) "develop legislative and regulatory proposals to improve counter-terrorist and counter-illicit financing efforts." H.R. 56 would further require the Task Force to annually report its findings to Congress. The bill would also establish two programs to incentivize members of the public to assist the federal government's efforts to combat the illicit use of virtual currencies. First, the bill would direct the Treasury Secretary to establish a reward of up to \$450,000 for persons who "provide[] information leading to the conviction of an individual involved with terrorist use of digital currencies." Second, the bill would direct the Treasury Secretary to create a grant program "for the development of tools and programs to detect terrorist and illicit use of digital currencies." After passing the House in January 2019, H.R. 56 was referred to the Senate Committee on Banking, Housing, and Urban Affairs.

A second bill, H.R. 428, the Homeland Security Assessment of Terrorists' Use of Virtual Currencies Act, would similarly commission an analysis of the use of virtual currencies by terrorists. ¹⁰³ Specifically, H.R. 428 would direct the Under Secretary of Homeland Security for Intelligence and Analysis to conduct a "threat assessment" analyzing "the actual and potential threat posed by individuals using virtual currency to carry out activities in furtherance of an act of terrorism, including the provision of material support or resources to a foreign terrorist

¹⁰⁰ *Id.* § 3(c).

¹⁰² Id. § 5(b).

⁹⁴ See United States v. Petix, No. 15-CR-227A, 2016 WL 7017919, at *7 (W.D.N.Y. Dec. 1, 2016) (concluding that Bitcoin does not qualify as "money" or "funds" under Section 1960).

⁹⁵ See Beyond Silk Road: Potential Risks, Threats, and Promises of Virtual Currencies: Hearing Before the U.S. Senate Committee on Homeland Security & Governmental Affairs, 113th Cong. at 1 (Nov. 18, 2013) (Statement of Patrick Murck, General Counsel, The Bitcoin Foundation, Inc.).

⁹⁶ Jeffrey Alberts & Leighton Dellinger, *Criminalizing Free Enterprise: The Bank Secrecy Act and the Cryptocurrency Revolution*, 21 No. 6 Westlaw J. Bank & Lender Liability 2, at *1 (Aug. 10, 2015).

⁹⁷ See "H.R. 528, Blockchain Regulatory Certainty Act" infra.

⁹⁸ H.R. 56, 116th Cong. § 3(a)-(b) (2019).

⁹⁹ Id.

¹⁰¹ Id. § 4.

¹⁰³ H.R. 428, 116th Cong. (2019).

organization."104 After passing the House in January 2019, H.R. 428 was referred to the Senate Committee on Homeland Security and Governmental Affairs.

Finally, H.R. 502, the Fight Illicit Networks and Detect Trafficking Act (the FIND Trafficking Act), would direct the Government Accountability Office (GAO) to conduct a study "on how virtual currencies and online marketplaces are used to facilitate sex and drug trafficking." The bill would require GAO to provide Congress with a report summarizing the results of the study, together with any recommendations for legislative or regulatory action that would assist the federal government in combatting the use of virtual currencies to facilitate sex and drug trafficking. 106 After passing the House in January 2019, H.R. 56 was referred to the Senate Committee on Banking, Housing, and Urban Affairs.

H.R. 1414, FinCEN Improvement Act of 2019

In March 2019, the House passed H.R. 1414, the FinCEN Improvement Act of 2019. 107 The bill would, among other things, clarify that FinCEN's statutory power to coordinate with foreign financial intelligence units on antiterrorism and AML initiatives "includ[es] matters involving emerging technologies or value that substitutes for currency."109 After passing the House in March 2019, H.R. 1414 was referred to the Senate Committee on Banking, Housing, and Urban Affairs.

H.R. 528, Blockchain Regulatory Certainty Act

In January 2019, H.R. 528, the Blockchain Regulatory Certainty Act, was introduced in the House of Representatives. 110 The bill would create a safe harbor from federal and state money transmitter licensing and registration requirements for certain blockchain developers. Specifically, the bill would provide that noncontrolling "blockchain developers" and providers of a "blockchain service" shall not be treated as "money transmitters," MSBs, "or any other State or Federal legal designation[s] requiring licensing or registration as a condition to acting as a blockchain developer or provider of a blockchain service." A blockchain developer or provider of a blockchain service would qualify as a noncontrolling developer or provider as long as it does not have control over users' digital currency in the regular course of business. 112 Some commentators have argued that such a safe harbor is necessary to provide legal certainty to actors in the virtual currency space, including persons who contribute code to virtual currency platforms or develop blockchain-related software but do not take custody of others' virtual currency. 113 However, another commentator has noted that it is "debat[able]" whether federal registration

¹⁰⁵ H.R. 502, 116th Cong. § 3 (2019).

¹¹² *Id*.

¹⁰⁴ Id. § 2(a).

¹⁰⁶ *Id.* § 3(c).

¹⁰⁷ H.R. 1414, 116th Cong. (2019).

¹⁰⁸ See 31 U.S.C. § 310(b)(2)(H).

¹⁰⁹ H.R. 1414, 116th Cong. § 3 (2019).

¹¹⁰ H.R. 528, 116th Cong. (2019).

¹¹¹ Id. § 2(a).

¹¹³ Peter Van Valkenburgh, Bitcoin Innovators Need Legal Safe Harbors, COIN CENTER (Jan. 24, 2017), https://coincenter.org/entry/bitcoin-innovators-need-legal-safe-harbors.

requirements apply to such persons.¹¹⁴ H.R. 528 was referred to the House Committee on Financial Services and the House Committee on the Judiciary in January 2019.

Author Contact Information

Jay B. Sykes Legislative Attorney fedacted@crs.loc.go√-.... Nicole Vanatko Legislative Attorney fedacted@crs.loc.gov, 7-....

¹¹⁴ Tim Prentiss, *Congressman Introduces Three Blockchain Bills*, ETHNEWS (Jan. 18, 2019), https://www.ethnews.com/congressman-introduces-three-blockchain-bills.

EveryCRSReport.com

The Congressional Research Service (CRS) is a federal legislative branch agency, housed inside the Library of Congress, charged with providing the United States Congress non-partisan advice on issues that may come before Congress.

EveryCRSReport.com republishes CRS reports that are available to all Congressional staff. The reports are not classified, and Members of Congress routinely make individual reports available to the public.

Prior to our republication, we redacted phone numbers and email addresses of analysts who produced the reports. We also added this page to the report. We have not intentionally made any other changes to any report published on EveryCRSReport.com.

CRS reports, as a work of the United States government, are not subject to copyright protection in the United States. Any CRS report may be reproduced and distributed in its entirety without permission from CRS. However, as a CRS report may include copyrighted images or material from a third party, you may need to obtain permission of the copyright holder if you wish to copy or otherwise use copyrighted material.

Information in a CRS report should not be relied upon for purposes other than public understanding of information that has been provided by CRS to members of Congress in connection with CRS' institutional role.

EveryCRSReport.com is not a government website and is not affiliated with CRS. We do not claim copyright on any CRS report we have republished.