# Anti-Money Laundering and Counter-Terrorist Finance

Pouyan Bohloul

Gabriela Chambi

Sandra Fadel

Nicole S. Healy

Eunjung Park

*See next page for additional authors*

# Anti-Money Laundering and Counter-Terrorist Finance


## Authors

Pouyan Bohloul, Gabriela Chambi, Sandra Fadel, Nicole S. Healy, Eunjung Park, and Cristina Robertson

# Anti-Money Laundering and Counter-Terrorist Finance

POUYAN BOHLOUL, GABRIELA CHAMBI, SANDRA FADEL, NICOLE S. HEALY, EUNJUNG PARK, AND CHRISTINA ROBERTSON*

## I. Introduction

This past year, anti-money laundering (AML) and counter-terrorist financing (CTF) regimes have been challenged to keep pace with technology and increasingly sophisticated global money laundering networks. Virtual currencies (VC) continue to evolve and authorities worldwide struggle with how to regulate and police these payment technologies. Efforts at VC legislation generally focus on protecting the integrity of the financial system, but regulators are also increasingly sensitive to the potential social benefits of the underlying technology.

### A. RECENT DEVELOPMENTS IN VIRTUAL CURRENCY

#### 1. *Virtual Currency Overview*

"Virtual currency (VC) is a digital representation of value" that can be traded online and functions as a medium of exchange, a unit of account, or a means to store value.[1] VC is global and operates outside traditional financial systems. VC "is not issued or guaranteed by any jurisdiction" but rather derives value from community members.

VC is a general term that represents a broad array of quickly evolving technologies that vary in degree of sophistication. Bitcoin is the most popular VC and represents a subclass of VC, cryptocurrency. There are currently over 700 different cryptocurrencies in operation; the market cap of

* Pouyan Bohloul, Esq., is a regular contributor to The World Bank Group's Doing Business Project. He received his J.D. from Florida State University College of Law and is licensed to practice law in Iran. Gabriela Chambi, JD candidate 2017, and Sandra Fadel, JD candidate 2017, attend American University Washington College of Law. Nicole S. Healy is a partner at Ropers Majeski Kohn & Bentley, P.C., in Redwood City, California, where her practice focuses on litigation including business disputes, securities violations, and shareholder litigation. Eunjung Park is an Associate in Anti Money Laundering Compliance at Societe Generale. Ms. Park received her law degree from American University, Washington College of Law in 2009, and previously worked for the African Development Bank Christina Robertson is a compliance attorney in Kansas City, Missouri.

1. *See* FIN. ACTION TASK FORCE, VIRTUAL CURRENCIES: KEY DEFINITIONS AND POTENTIAL AML/CFT RISKS 4 (2014), http://www.fatf-gafi.org/media/fatf/documents/reports/Virtual-currency-key-definitions-and-potential-aml-cft-risks.pdf.

the twenty-five largest cryptocurrencies exceeds twelve billion dollars.[2] Though cryptocurrencies have struggled to gain widespread acceptance as a daily payment method to purchase goods or services, adoption rates continue to rise.[3]

Cryptocurrencies allow anyone with computer access to efficiently obtain funding or make payments worldwide. The VCs pose considerable risk as potential vehicles for money laundering and terrorist financing because they are anonymous or pseudo-anonymous and mostly unregulated.

A flurry of ransomeware attacks this year brought attention to Bitcoin as a means to facilitate and mask criminal activity.[4] In a typical ransomeware attack, an individual or organization's computer or software is compromised by cybercriminals who then encrypt and hold that encrypted data hostage. Bitcoin is the preferred method of payment for ransomware attacks because funds can be sent or received from anywhere and are challenging to trace.[5]

The risk to AML and CTF efforts posed by VCs will continue to grow as the technology matures. The current blockchain technology that supports Bitcoin makes tracing a transaction challenging but not impossible.[6] But Zero-proof is a next generation technology that removes all identifying information from a payment, and thus renders the transaction untraceable.[7] Zcash, the first cryptocurrency to utilize this technology, promotes on its website "total payment confidentiality."[8]

### 2. *Criminal Prosecution*

Three U.S. cases from 2016 highlight the challenges of prosecuting AML cases that involve VC. The first case demonstrates that AML regulation of VC requires complex and multi-jurisdictional cooperation; seventeen countries and numerous domestic and foreign agencies and intelligence units

2. *See CryptoCurrency Market Capitalizations*, COINMARKETCAP, https://coinmarketcap.com (last updated Mar. 12, 2017, 6:20 PM).

3. *See* DONG HE ET AL., VIRTUAL CURRENCIES AND BEYOND: INITIAL CONSIDERATIONS 17 (2016), https://www.imf.org/external/pubs/ft/sdn/2016/sdn1603.pdf; *see also* RYAN FARELL, AN ANALYSIS OF THE CRYPTOCURRENCY INDUSTRY 14 (Univ. of Pa. ScholarlyCommons, 2015), http://repository.upenn.edu/wharton_research_scholars/130.

4. *See* Robert McMillan, *In the Bitcoin Era, Ransomeware Attacks Surge*, WALL ST. J., https://www.wsj.com/articles/in-the-bitcoin-era-ransomware-attacks-surge-1471616632?mg=id-wsj (last updated Aug. 19, 2016, 11:59 PM).

5. *Id.*

6. *See* Steven Norton, *CIO Explainer: What is Blockchain?*, WALL ST. J. (Feb. 2, 2016, 12:49 AM), http://blogs.wsj.com/cio/2016/02/02/cio-explainer-what-is-blockchain/.

7. *See* Joseph Mari, *When Blockchain, Cryptocurrencies, and AML Meet*, BANKING EXCHANGE (Nov. 7, 2016, 17:36), http://www.bankingexchange.com/news-feed/item/6547-when-blockchain-cryptocurrencies-and-aml-meet?Itemid=637.

8. *See* Press Release, Maureen Walsh, Zcash Launches at the First Open, Permmissionless Fin. Sys. Employing Zero-Knowledge Sec. (Oct. 28, 2016), https://z.cash/support/zcash-sprout-launch.html.

contributed to the *Liberty Reserve* investigation.[9] *State v. Espinoza* and *Coin.mx* illustrate the importance of modernizing AML statutes to include technology-based money laundering tools and the need for a coordinated approach to VC regulation.[10]

In May 2016, the U.S. District Court for the Southern District of New York sentenced Arthur Budovsky, the founder of Liberty Reserve, a digital currency company, to twenty years in prison for running an extensive VC-based money laundering operation.[11] Budovsky pled guilty to one count of conspiring to commit money laundering in January 2016.[12] Liberty Reserve laundered more than $250 million since its inception by converting criminal proceeds into its branded VC, Liberty Dollars (LR), processing the transactions, and then converting the VC into cash.[13] The Liberty Dollar was a predecessor to Bitcoin. Liberty Reserve employed insufficient and ineffective AML controls and failed to validate user identities.[14] Customers would make deposits and withdrawals through third-party currency exchangers located in various third-party countries, including Malaysia, Nigeria, and Russia.[15] As a result, account holders exchanged LR in nearly untraceable transactions. Assistant Attorney General Leslie R. Caldwell stated that Budovsky's twenty-year sentence demonstrates that "money laundering through the use of virtual currencies is still money laundering, and that online crime is still crime."[16]

---

9. *See Founder of Liberty Reserve Pleads Guilty to Laundering More Than $250 Million through His Digital Currency Business*, THE UNITED STATES DEPARTMENT OF JUSTICE (Jan. 29, 2016), https://www.justice.gov/opa/pr/founder-liberty-reserve-pleads-guilty-laundering-more-250-million-through-his-digital.

10. Jeffrey K. Berns, *Recent VC Ruling Emphasizes Why Congress Needs to Act Promptly to Pass VC Legislation*, BERSWEISS LLP (Sept. 21, 2016, 2:13 PM), https://www.law111.com/recent-vc-ruling-emphasizes-why-congress-needs-to-act-promptly-to-pass-vc-legislation.

11. *See id.*; *Liberty Reserve Founder Arthur Budovsky Sentenced in Manhattan Federal Court to 20 Years for Laundering Hundreds of Millions of Dollars Through His Global Digital Currency Business*, U.S. DEPARTMENT OF JUST. (May 6, 2016), https://www.justice.gov/usao-sdny/pr/liberty-reserve-founder-arthur-budovsky-sentenced-manhattan-federal-court-20-years.

12. *See Founder of Liberty Reserve Pleads Guilty to Laundering More Than $250 Million Through His Digital Currency Business*, *supra* note 9; *see also Liberty Reserve Founder Arthur Budovsky Sentenced in Manhattan Federal Court to 20 Years for Laundering Hundreds of Millions of Dollars Through His Global Digital Currency Business*, *supra* note 11.

13. *See Founder of Liberty Reserve Pleads Guilty to Laundering More Than $250 Million Through His Digital Currency Business*, *supra* note 9; *see also Liberty Reserve Founder Arthur Budovsky Sentenced in Manhattan Federal Court to 20 Years for Laundering Hundreds of Millions of Dollars Through His Global Digital Currency Business*, *supra* note 11.

14. *Liberty Reserve Founder Arthur Budovsky Sentenced in Manhattan Federal Court to 20 Years for Laundering Hundreds of Millions of Dollars Through His Global Digital Currency Business*, *supra* note 11.

15. Alan Brill & Lonnie Keene, *Cryptocurrencies: The Next Generation of Terrorist Financing?*, 6 DEF. AGAINST TERRORISM REV. 7, 7-30 (2014).

16. *Liberty Reserve Founder Arthur Budovsky Sentenced in Manhattan Federal Court to 20 Years for Laundering Hundreds of Millions of Dollars Through His Global Digital Currency Business*, *supra* note 11.

On the other hand, in *State v. Espinoza*, Miami-Dade County Circuit Court Judge Teresa Pooler dismissed felony anti-money laundering charges against a website developer stating that Bitcoins are not a "monetary instrument" or "payment instrument" as defined by statute and that "money transmission" does not include the sale of Bitcoin.[17] The judge further noted that "virtual currency" is not included as a category within the statutory definition of "monetary instrument" and that Bitcoin does not fall within any of the existing categories.[18]

The defendant sold Bitcoins to an undercover agent who claimed that he would use the bitcoins to buy stolen credit cards.[19] Judge Pooler stated that "[n]othing in our frame of reference allows us to accurately define or describe Bitcoin."[20] In her analysis, Judge Pooler referenced the Internal Revenue's classification of virtual currency as property before concluding that "Bitcoin has a long way to go before it is the equivalent of money."[21]

Shortly thereafter, a federal judge in New York ruled in Coin.mx that Bitcoins "function as pecuniary resources and . . . means of payment."[22] In July 2015, Anthony Murgio was arrested for operating an illegal online Bitcoin exchange called Coin.mx and charged with violating federal anti-money laundering laws.[23] Investigators believe Murgio knowingly facilitated payments for victims of the ransomware attacks, and thus, enabled the attacks. Murgio sought to dismiss charges against him by arguing that Bitcoins are not "funds" under the federal law prohibiting the operation of an unlicensed money transmitting business. In September 2016, Judge Alison Nathan of the U.S. District Court for the Southern District of New York rejected Murgio's argument ruling that "Bitcoins are funds within the plain meaning of that term."[24]

17. *See* David Ovalle, *Bitcoin Not Money, Miami Judge Rules in Dismissing Laundering Charges*, MIAMI HERALD (July 25, 2016, 10:22 AM), http://www.miamiherald.com/news/local/crime/article91682102.html; *see also* State v. Espinoza, No. F14-2923, slip op. (Fla. 11th Cir. 2016).

18. *See Espinoza*, No. F14-2923at 6-7. .

19. *See* Ovalle, *supra* note 13 at 2; *see also* Patricia Hurtado & Susannah Nesmith, *Florida State Judge Rules Bitcoin Doesn't Qualify as Money*, BLOOMBERG TECH. (July 25, 2016, 8:11 PM), https://www.bloomberg.com/news/articles/2016-07-25/florida-state-judge-rules-bitcoin-doesn-t-qualify-as-money.

20. *Id.*

21. *Id.* at 6.

22. Jonathan Stempel, *Bitcoin Is Money, U.S. Judge Says in Case Tied to JPMorgan Hack*, REUTERS (Sept. 19, 2016, 8:08 PM), http://www.reuters.com/article/us-jpmorgan-cyber-bitcoin-idUSKCN11P2DE.

23. *See id.*

24. *Id.*

3. *Regulatory Response*

a. Japan

Japan enacted a law in May 2016 to regulate VC.[25] The new law defines VC as "asset-like values" and will go into effect one year from its adoption. The law requires that exchanges register with the Financial Services Agency (FSA).[26] Exchanges will also be subject to AML and know your customer (KYC) obligations.[27] The FSA will conduct on-site inspections and issue administrative orders as needed to ensure compliance.[28]

b. China

Since 2013, The People's Bank of China has prohibited financial institutions and employees from dealing in Bitcoin.[29] The Cyberspace Administration of China acknowledged in October 2015 the innovation potential of Bitcoin's underlying technology, and in January 2016 the People's Bank of China hinted at plans to develop its own VC.[30]

c. Russia

In 2014, the Russian Ministry of Finance issued legislation that banned the use, creation, and distribution of VC. In August 2016, the Ministry proposed an amendment to the VC ban that would treat VC as "foreign currency" to be used by Russians outside of Russia.[31]

d. United Kingdom

Jersey, a self-governing dependency of the United Kingdom, recently amended its AML legislation to include virtual currency exchange services.[32] The Proceeds of Crime Regulations went into effect in September and requires that VC exchanges register with, and are supervised by, the Jersey

25. *See Diet Oks Bill to Regulate Virtual Currency Exchanges*, THE JAPAN TIMES, http://www.japantimes.co.jp/news/2016/05/25/business/diet-oks-bill-regulate-virtual-currency-exchanges/#.WMYgE7G-Ixe (last visited Mar. 13, 2017).

26. David Meyer, *Burned by Bitcoin Scandal, Japan is Introducing Controls*, FORTUNE (May 26, 2016), http://fortune.com/2016/05/26/japan-bitcoin-exchanges/.

27. Naoya Ariyoshi, Susumu Tanizawa, & Hideki Katagiri, *Japan: the Essential Points of the Amendments to the Regulation on Virtual Currency Exchange Services*, MONDAQ (Jan. 21, 2017), http://www.mondaq.com/x/554128/Financial+Services/The+Essential+Points+Of+The+Amendments+To+The+Regulation+On+Virtual+Currency+Exchange+Services.

28. *See Diet Oks Bill to Regulate Virtual Currency Exchanges*, *supra* note 25.

29. *See* Valentin Schmid, *What Is Going On with China and Bitcoins?*, EPOCH TIMES (June 1, 2016, 2:48 PM), http://www.theepochtimes.com/n3/2080774-what-is-going-on-with-china-and-bitcoin/.

30. *See id.*; Sophia Yan, *China Wants to Launch Its Own Digital Currency*, CNN (Jan. 22, 2016, 1:02 AM), http://money.cnn.com/2016/01/21/technology/china-digital-currency/.

31. *Russia to Allow Foreign Trading of Virtual Currency*, BITLEGAL (Aug. 11, 2016), http://bitlegal.io/2016/08/11/russia-to-allow-foreign-trading-of-virtual-currency/.

32. *Id.*

Financial Services Commission.[33] Jersey intends to establish itself as an international center for digital industries, and to this end, the regulation provides an exception for smaller exchanges, which are intended to create a "regulatory sandbox" to encourage innovation.[34]

## B. Recent Developments in Anti-Money Laundering and Counter-Terrorism

### 1. *Financing*

The Panama Papers incident in May revealed how effectively assets can be transferred and hidden offshore.[35] Though the creation of offshore legal entities is not evidence of illegal activity *per se*, the system is susceptible to abuse by tax evaders, terrorists, and money launderers.[36] Of note in the Panama Papers data leak, and of interest to AML and CTF professionals, is the sophisticated and robust global network of entities and intermediaries that mask the identity of beneficial owners, disguise transactions, and hide funds.[37] In response, AML and CTF programs are bolstering customer due diligence requirements in an effort to better expose and monitor beneficial ownership, and thus preserve the integrity of established financial systems.

### 2. *Regulatory Response in the United States*

In May 2016, the U.S. Treasury Department's Financial Crimes Enforcement Network (FinCEN) issued final rules under the Bank Secrecy Act (BSA) to clarify and enhance customer due diligence (CDD) requirements and focus on beneficial owner identification.[38] The new rules are effective July 1, 2016, but covered entities have until May 11, 2018, to

33. Proceeds of Crime (Supervisory Bodies) (Virtual Currency Exchange Business) (Exemption) (Jersey) Order 2016, *available at* https://www.jerseylaw.je/laws/enacted/Pages/RO-101-2016.aspx.

34. Sara Jones, *Virtual Currency Regulation in Jersey Takes Effect*, Ogier (Apr. 10, 2016), https://www.ogier.com/publications/virtual-currency-regulation-in-jersey-takes-effect; *see also Digital Jersey Welcomes Innovative Regulation for Virtual Currency*, Digital Jersey (Sept. 26, 2016), https://www.digital.je/news/regulation-for-virtual-currency.

35. The Panama Papers references a data leak of 11.5 million files from Mossack Fonseca, a Panama-based law firm in 2016. The leaked records disclosed the attorney-client records of more than 200,000 offshore entities. *See* Frederik Obermaier et al., *About the Panama Papers*, Suddeutsche Zeitung, http://panamapapers.sueddeutsche.de/articles/56febff0a1bb8d3c3495adf4/ (last visited Mar. 13, 2016); *Giant Leak of Offshore Financial Records Exposes Global Array of Crime and Corruption*, Int'l Consortium of Investigative Journalists (Apr. 3, 2016), https://panamapapers.icij.org/20160403-panama-papers-global-overview.html.

36. Obermaier et al., *supra* note 35.

37. *Giant Leak of Offshore Financial Records Exposes Global Array of Crime and Corruption*, *supra* note 35.

38. *See* Customer Due Diligence Requirements for Financial Institutions, 81 Fed. Reg. 29,398 (May 11, 2016) (to be codified at 31 C.F.R. pts. 1010, 1020, 1023, et al.), https://www.federalregister.gov/documents/2016/05/11/2016-10567/customer-due-diligence-requirements-for-financial-institutions.

comply. Covered entities include the following: "[b]anks; brokers or dealers in securities; mutual funds; and futures commission merchants and . . . brokers in commodities."[39] The BSA is the primary AML law in the United States and, as amended by the USA Patriot Act, incorporates CTF requirements as well.

The new rules outline the four core elements of an effective CDD program: customer identification and verification; beneficial ownership identification and verification; risk profiling based on an understanding of customer relationships; and ongoing transaction and risk-based customer monitoring.[40]

Beneficial ownership of all legal entities must be identified and verified at account opening.[41] FinCEN provides a form that provides the required beneficial ownership information. In the absence of any knowledge that would reasonably call into question the reliability of the information, covered entities may rely on ownership information provided by the customer.[42] FinCEN considers beneficial ownership to include not just those individuals with an equity interest in the legal entity but also those who exercise control over the entity. FinCEN believes if covered entities know the identity of the individuals that own or control their legal entity customers and comply with AML and CTF regulations, criminals will be denied access to the United States financial system. In addition, this insight into beneficial ownership will assist law enforcement in investigations, prevent financial sanction evasion, and advance U.S. compliance with international AML standards and commitments.[43]

### 3. *Enforcement Challenges in the United States*

FinCEN's suspicious activity reporting requirement informs the enforcement arm of the U.S. AML/CTF regulatory scheme. This year the United States faced a challenge to the application of AML enforcement measures that function to protect the U.S. financial system from exposure to high-risk activity. Section 311 of the USA PATRIOT Act authorizes the FinCEN to "impose a variety of special measures against institutions that it finds to be of primary money-laundering concern . . . ." The first four of these five special measures may be authorized by agency order; FinCEN "may impose the fifth special measure . . . only by rulemaking."[44] A list of the jurisdictions and institutions subject to these special measures, as well as links to FinCEN's findings and the special measures imposed on various

39. *Id.*

40. *Id.*

41. *Id.*

42. *Id.* at 29,298.

43. *Id.* at 29,431.

44. *See id.*; *see also* 31 U.S.C § 5318A(a)(2)(B)-(C) (stating the first through fourth special measures may be impose by "regulation, order, or otherwise as permitted by law," however, the fifth special measure may only be imposed by regulation, after providing for notice and comment).

institutions, is available at the agency's website.[45] FinCEN has only imposed such a final rule seven times since 2004. Financial institutions have sought judicial review of FinCEN's Section 311 designations even more rarely.[46]

In a recent case challenging a Section 311 designation, FBME Bank Ltd. (FBME), a Tanzanian bank, obtained a preliminary injunction barring implementation of FinCEN's final rule and fifth special measure, which would have frozen FBME out of the U.S. financial markets.[47] While the court would "not . . . second guess FinCEN's exercise of its broad discretion in finding that FBME poses a primary money laundering concern," it found that FinCEN had not complied with the notice provisions of the Administrative Procedures Act (APA) because it had failed to supply FBME with the unclassified and otherwise unprotected evidence on which it based its decision to bar the bank's access to the United States financial system and further failed to address adequately whether it had considered alternatives to barring the bank from the United States financial system.[48] The court found that FinCEN's failure to disclose non-classified and unprotected information during the final rule's notice and comment period was a procedural error that deprived FBME of an opportunity to review and comment on those materials.[49] Further, FinCEN had not adequately described whether it had considered alternatives to the Section 311 designation, such as imposing conditions on opening or maintaining correspondent accounts, rather than entirely prohibiting such accounts.[50]

Rather than appeal the ruling, FinCEN asked the district court to remand the matter to the agency so that it could have what the court termed a "do-over." That is, FinCEN requested "an opportunity to correct any mistakes it might have made the first time around and to promulgate—following proper procedures—the same rule, a new rule altogether, or perhaps even no rule at all."[51] The court agreed, stayed its ruling, and remanding the case to FinCEN.[52] In its order, the court noted that voluntary remand is favored where the agency has decided to re-consider its decisions and re-start the

45. *See 311 Special Measures*, FINCEN, https://www.fincen.gov/resources/statutes-and-regulations/311-special-measures (last visited Mar. 13, 2017).

46. *See FBME Bank Ltd.*, 2016 WL 5108018, at *4 (*citing* Section 311—Special Measures, FinCEN, https://www.fincen.gov/statutes_regs/patriot/section311.html).

47. *See* FBME Bank Ltd. v. Lew, 125 F. Supp. 3d 109 (D.D.C. 2015) (mem. op.) (giving opinion granting preliminary injunction); *see also* § 5318A(b)(5) (stating certain payable-through or correspondent accounts may be prohibited).

48. *See FBME Bank Ltd.*, 125 F. Supp. at 114. FinCEN had claimed that "FBME openly advertises the bank to its potential customer base as willing to facilitate the evasion of AML regulations. In addition, FBME solicits and is widely recognized by its high-risk customers for ease of use." *FinCEN Takes Action to Protect U.S. Financial System*, FINCEN (July 17, 2014), https://www.fincen.gov/news/news-releases/fincen-takes-action-protect-us-financial-system.

49. *See FMBE Bank Ltd* , 125 F. Supp. at 118.

50. *See id.*

51. *Id.*

52. *Id.*

rulemaking process.[53] Moreover, the court found that the remand would not unduly prejudice FBME.[54]

Thereafter, on March 31, 2016, FinCEN published a final rule under Section 311, designating FBME as a "financial institution of primary money laundering concern."[55] The order would have gone into effect 120 days from publication, but FMBE again challenged it.[56] On September 20, 2016, FBME won a second injunction against FinCEN's designation, including on the grounds that FinCEN's disclosures to FBME were insufficient.[57] While the FBME case is limited to its facts, it may encourage other financial institutions to challenge FinCEN's Section 311 rulemaking process.

The FBME case highlights the tension between FinCEN's use of data drawn from SARs, which have not been disclosed to the financial institution but from which the agency has drawn conclusions regarding purportedly suspicious transactions and the institution's AML controls and the imposition of sanctions on the institution.[58] In *FBME Bank Ltd. v. Lew*, the court concluded that the use of aggregate SAR information put the bank on

53. *Id.* at 73.

54. *Id.*

55. *See* Imposition of Special Measure Against FBME Bank Ltd., Formerly Known as the Federal Bank of the Middle East Ltd., as a Financial Institution of Primary Money Laundering Concern, 81 Fed. Reg. 18480 (Mar. 31, 2016) (to be codified at 31 C.F.R. pt. 1010), https://www.fincen.gov/sites/default/files/shared/FBME_FR_20160325.pdf; *FinCEN Issues Final Rule Imposing a Prohibition on the Opening or Maintaining of Correspondent Accounts for, or on Behalf of, FBME Bank Ltd.*, FINCEN, https://www.fincen.gov/sites/default/files/shared/20160325.pdf (last visited Mar. 13, 2017).

56. *See FinCEN Issues Final Rule Imposing a Prohibition on the Opening or Maintaining of Correspondent Accounts for, or on Behalf of, FBME Bank Ltd.*, *supra* note 55.

57. *See* FBME Bank Ltd. v. Lew, No. 15-CV-01270 (CRC), 2016 WL 5108018, at *30 (D.D.C Sept. 20, 2016) (mem. op.); *see also* Ben DiPietro, *FBME Bank Wins Second Injunction Against FinCEN Rule*, WALL ST. J. (Sept. 21, 2016, 4:33 PM), http://blogs.wsj.com/riskandcompliance/2016/09/21/fbme-bank-wins-second-injunction-against-fincen-rule/. Analyzing FinCEN's Section 311 final rulemaking pursuant to the APA, in particular, FBME's challenge to the final rule under 5 U.S.C. § 706(2) on the basis that FinCEN's rulemaking was arbitrary and capricious, the district court found that FinCEN failed to fully comply with two notice provisions but that the errors were harmless. *See FBME Bank Ltd.*, 2016 WL 5108018, at *5. More significantly, the court found that FinCEN had not adequately responded to certain comments from FBME. *See id.* at *30. On that basis, the court again stayed implementation of the final rule. *See id.*

58. *See FBME Bank Ltd.*, 2016 WL 5108018, at *7 (citing Notice of Finding That FBME Bank Ltd., Formerly Known as Federal Bank of the Middle East, Ltd., Is a Financial Institution of Primary Money Laundering Concern, 79 Fed. Reg. 42,639, 42,640 (July 22, 2014), https://www.fincen.gov/sites/default/files/special_measure/FBME_NOF.pdf). The court noted that, in its proposed final rule, FinCEN stated that between April 2013 and April 2014, "FBME conducted at least $387 million in wire transfers through the U.S. financial system that exhibited indicators of high-risk money laundering typologies, including widespread shell company activity, short-term 'surge' wire activity, structuring, and high-risk business customers" and that "FBME was involved in at least 4,500 suspicious wire transfers through U.S. correspondent accounts that totaled at least $875 million between November 2006 and March 2013." *FBME Bank Ltd.*, 2016 WL 5108018, at *7.

notice of FinCEN's concerns, and access to individual SARs would not have assisted the bank's efforts to push back against the Section 311 designation where FinCEN had discussed its concerns regarding AML controls at length with the bank.[59] These facts are unique to this case, however, and financial institutions' concerns regarding due process in like situations are not frivolous.

In another recent case, FinCEN first issued and then withdrew its Section 311 findings and notice of proposed rulemaking in which it designated Banca Privada d'Andorra (BPA) an institution of special money-laundering concern.[60]

FinCEN explained its decision by stating that "BPA no longer operates in a manner that poses a threat to the U.S. financial system."[61] That determination followed the bank's takeover by the Andorran banking authorities in which the Andorran government assumed control of the bank's "management and operations, arrested the chief executive officer on money laundering charges, and are in the final stages of implementing a resolution plan that is isolating the assets, liabilities, and clients of BPA that raise money laundering concerns."[62] As a result of the takeover, BPA's assets were placed into a new entity, Vall Bank, which was later sold.[63]

In both of these cases, the banks resisted FinCEN's Section 311 designation and sought more information regarding the basis for the agency's determination. Because each Section 311 determination is based on the specific facts and circumstances presented, however, and because so few Section 311 final rules have been sought or challenged, it is difficult to draw any general conclusions regarding the circumstances under which courts will affirm FinCEN's designations. It seems likely, however, that the more

59. *See id.*, at *8.

60. *See FinCEN Names Banca Privada d'Andorra a Foreign Financial Institution of Primary Money Laundering Concern*, FINCEN (Mar. 10, 2015), https://www.fincen.gov/news/news-releases/fincen-names-banca-privada-dandorra-foreign-financial-institution-primary-money; *Notice Regarding the Withdrawals of Findings and Proposed Rulemakings Under Section 311*, FINCEN (Feb. 19, 2016), https://www.fincen.gov/news/news-releases/notice-regarding-withdrawals-findings-and-proposed-rulemakings-under-section-311. In October 2015, the Cierco family, the majority shareholders of Banca Privada d'Andorra, filed suit in Washington, D.C., asking the court to rescind the Section 311 designation. *See Ramon and Higini Cierco File Lawsuit Against the U.S. Treasury and the Financial Crimes Enforcement Network, Claiming the Agency's Actions Against Banca Privada d'Andorra Are Wholly Unjustified and Unconstitutional*, PR NEWSWIRE (Oct. 17, 2015, 13:12), http://www.prnewswire.com/news-releases/ramon-and-higini-cierco-file-lawsuit-against-the-us-treasury-and-the-financial-crimes-enforcement-network-claiming-the-agencys-actions-against-banca-privada-dandorra-are-wholly-unjustified-and-unconsti tutional-300155903.html.

61. *Notice Regarding the Withdrawals of Findings and Proposed Rulemakings under Section 311*, *supra* note 60.

62. *See id.*

63. The Ciercos sued the Treasury Department over the Section 311 findings. The court dismissed the case as moot where the shareholders obtained the relief requested when FinCEN withdrew its findings. *See* Cierco v. Lew, 190 F. Supp. 3d 16, 18–19, 21 (D.D.C. 2016) (mem. op.) (dismissing complaint under Fed. R. Civ. P. 12(b)(1) for mootness).

generalized APA analysis followed by the court in FBME will provide guidance for future judicial review of Section 311 rulemaking.

### 4. *Regulatory Response in the European Union*

In May 2015, the European Union (EU) adopted the Fourth Anti-Money Laundering Directive (4AMLD) to improve the effectiveness of the EU's efforts to detect and prevent money laundering and terrorist financing.[64] On July 5, 2016, the European Commission approved a proposal (Proposal) to amend the 4AMLD.[65] The Proposal introduces new requirements, modifies current requirements, and promotes increased collaboration among Member States.

Each EU Member State must transpose, or adopt laws to implement, the directive. The Proposal accelerates the 4AMLD transposition deadline, of June 26, 2017; all EU Member States must now transpose and enter 4AMLD into force by January 1, 2017.[66]

The issues addressed by the Proposal include: terrorist financing risks posed by virtual currencies, risks linked to anonymous pre-paid instruments, the limited information powers of EU Financial Intelligence Units (FIUs), enhanced due diligence for high risk countries, and access to beneficial ownership information.

Obliged entities are defined by and subject to the requirements of the 4AMLD.[67] The Proposal broadens the scope of obliged entities to include VC platforms offering exchange services between virtual and fiat currencies and custodian wallet providers.[68]

Public authorities within the EU do not currently monitor VC transfers; no specific rules exist at the Union or Member State level that would establish a monitoring framework.[69] Recognizing that this gap in enforcement may be exploited by those engaged in money-laundering or terrorist financing, the Proposal requires that exchanges and virtual currency custodians implement preventive AML measures and report suspicious

64. Directive 2015/849, of the European Parliament and of the Council of 20 May 2015 on the Prevention of the Use of the Financial System for Purposes of Money Laundering or Terrorist Financing, amending Regulation No 648/2012 of the European Parliament and of the Council, and repealing Directive 2005/60/EC of the European Parliament and of the Council and Commission Directive 2006/70/EC, 2015 O.J. (L 141) 1 [hereinafter 4AMLD].

65. *Proposal for a Directive of the European Parliament and of the Council Amending Directive (EU) 2015/849 of the European Parliament and of the Council of 20 May 2015 on the Prevention of the Use of the Financial System for the Purposes of Money Laundering or Terrorist Financing and Amending Directive 2009/101/EC*, COM (2016) 450 final (July 5, 2016) [hereinafter *Proposal*].

66. *See id.* at 4.

67. *See* 4AMLD, *supra* note 64 at art. 2.

68. *See Proposal*, *supra* note 65 at 12.

69. See *id.*

transactions.[70] As obliged entities, they are also subject to online financial data and data privacy obligations.[71]

Acknowledging both the terrorist financing risks and legitimate social utility of pre-paid cards, 4AMLD Article 12 authorizes Member States to waive certain CDD requirements for obliged entities when the transaction falls below a certain threshold.[72] The Proposal lowers the CDD transaction threshold of 4AMLD from _250 to _150.[73] Additionally, the Proposal requires that Member States enact controls to ensure that anonymous prepaid cards used within the Union but issued outside the Union are subject to issuing requirements equivalent to those of the EU.[74]

The Proposal clarifies that closed loop cards are low risk for money laundering and terrorist financing and are therefore outside the scope of 4AMLD. Closed loop cards are prepaid cards that can only be used within a limited network or to acquire a limited range of goods and services.[75]

FIUs are public authorities within a Member State that collect, identify, and analyze information about suspicious transactions. FIUs in certain Member States can only request information from an obliged entity once a suspicious activity report (SAR) has been filed. As a result, these FIUs are prevented from gaining timely access to information held by those obliged entities on payment accounts and account holder identities. To accelerate the detection of terrorist financing and money laundering, and improve the cooperation across borders, FIUs must be able to obtain information from obliged entities and have timely access to relevant financial, administrative, and law enforcement information in the absence of an SAR.[76] The Proposal authorizes FIUs to request information from any obliged entity regardless of whether an SAR has been filed. The Proposal delegates to the Member States the task of defining the conditions under which FIUs can request information.[77] FIUs must still respect security and confidentiality requirements governing information access, handling, and dissemination.[78]

Currently there is no obligation at the EU level to implement banking registries or electronic data retrieval systems, which would provide FIUs with access to bank account information. The 4AMLD encourages but does not require these information systems; as a result, not all Member States have these systems in place.[79] Therefore, FIUs are challenged to detect criminal and terrorist financial movements at the national level. The

70. See *id.*

71. *See id.* at 13.

72. *See* 4AMLD, *supra* note 64 at art. 12. .

73. *See Proposal*, *supra* note 65 at 13.

74. The Proposal Directive specifies that "[t]he rule should be enacted in full compliance with Union obligations in respect of international trade, especially the provisions of the General Agreement on Trade in Services." *Id.* at 23.

75. *Id.*

76. *See id.* at 13 – 14.

77. *Proposal*, *supra* note 53, at 14.

78. *Id.*

79. *See* 4AMLD, *supra* note 52, at 57.

Proposal modifies 4AMLD to require Member States to set up automated centralized databases that enable FIUs to quickly identify bank account and payment information. These systems would allow FIUs and other AML authorities to identify all bank and payment accounts belonging to an individual through a centralized automated search query.[80] Access to these registries should be limited to a need-to-know basis and subject to maximum retention periods for personal data.[81]

Under 4AMLD Article 18, obliged entities are required to apply enhanced CDD to manage and mitigate risks when dealing with individuals or entities in countries identified by the EU as high risk.[82] Currently, each Member State independently determines the enhanced CDD measures that are appropriate for high-risk jurisdictions. This inconsistent and uncoordinated approach by Member States creates vulnerability in monitoring these high-risk countries. Accordingly, the Proposal harmonizes the monitoring of high-risk countries by requiring Member States to adopt a minimum standard of enhanced CDD measures that are compliant with FATF recommendations.[83]

Currently, companies, trusts, and other legal entities are required to maintain accurate information on their beneficial ownership.[84] Articles 30 and 31of the 4AMLD provide guidance on the collection, storing, and access to ultimate beneficial ownership information.[85] The Proposal seeks to synchronize these requirements across entities and Member States.

Stressing the importance of public access to information, the Proposal amends Directive 2009/101/EC to require that Member States make beneficial ownership of for-profit firms and legal entities publically available.[86] The Proposal asserts that public access to this information results in enhanced scrutiny by society, provides additional guarantees to potential business partners, and contributes to the integrity of business

80. *Id.*

81. *Id.* at 15

82. Article 9 of 4AMLD authorizes the Commission to identify high-risk third countries that have deficient anti-money laundering and counter terrorist financing controls. *See* 4AMLD, *supra* note 52 at arts. 9, 18. The list of high-risk third countries was adopted in July 2016. *See Commission Delegated Regulation (EU) 2016/1675 of 14 July 2016 Supplementing Directive (EU) 2015/849 of the European Parliament and of the Council by Identifying High-Risk Third Countries with Strategic Deficiencies*, COM (2016) (July. 14, 2016).

83. The minimum enhanced due diligence standards should require checks on the customer, identifying the purpose and nature of the business relationship as well as the source of funds, and transaction monitoring. The enhanced due diligence measures should be fully compliant with lists drafted by the Financial Action Task Force (FATF). In addition, the list of countermeasures set out by FATF should be adequately reflected in the EU legislation. *See Proposal*, *supra* note 53 at 15. The FATF is an intergovernmental body that sets standards and promotes measures to combat money laundering, terrorist financing, and other threats to the financial system. *See Who We Are*, FIN ACTION TASK FORCE, http://www.fatf-gafi.org/about/ (last visited Mar. 15, 2017).

84. *Proposal*, *supra* note 53, at 15.

85. *Id.*

86. *Id.* at 26.

transactions and the financial system.[87] The Proposal provides that trusts engaged in commercial or business-like activity should also make beneficial ownership information publically available.[88] But the privacy concerns of trusts created for charitable purposes or to hold family assets require that beneficial ownership information be shared only with those who have a legitimate interest.[89]

Finally, a beneficial owner according to Article 3(6)(a) of the 4AMLD is a legal person owning twenty-five percent plus one share or an ownership interest of more than twenty-five percent in a corporate entity.[90] The Proposal recommends lowering this threshold to ten percent for passive non-financial entities.[91] Passive non-financial entities do not create income on their own, but function primarily as an intermediary to channel income from other sources.[92] These entities may exist only to distance beneficial owners from their assets, and accordingly present a high risk for money laundering and tax evasion.[93]

### 5. *Iran's First Counter-Terrorism Finance Law*

On March 17, 2016, the Islamic Republic of Iran (Iran) enacted its first CTF law, known as The Law on Combating Terrorism Finance.[94] The brief law defines terrorist financing, outlines reporting obligations for banks and financial agencies, and permits international cooperation.[95] The Iranian Parliament approved the law on February 2, 2016, and the Guardian Council confirmed it on March 3, 2016.[96]

The promulgation of this law is an effort by the Iranian regime to adopt international banking and AML standards and thereby modernize its banking legislation in response to the Joint Comprehensive Plan of Action (JCPOA).[97] The JCPOA was signed between Iran and the five permanent members of the United Nations Security Council (China, France, Russia,

87. *Id.* at 16.

88. *Id.*

89. *See id.* at 17. "The legitimate interest with respect to money laundering, terrorist financing and the associated predicate offences should be justified by readily available means, such as statutes or mission statement of non-governmental organisations, or on the basis of demonstrated previous activities relevant to the fight against money laundering and terrorist financing or associated predicate offences, or a proven track record of surveys or actions in that field." *Id.* at 28.

90. *Proposal*, *supra* note 53, at 17.

91. *Id.*

92. *Id.*

93. *Id.*

94. *See* The Law on Combating Terrorism Finance (Iran), www.tejaratbank.ir/file_manager/1659577/download/1/CFT-law.html.

95. *Id.*

96. *See Ratification of the Law of Combating the Financing of Terrorism (CFT)*, CENTRAL BANK OF THE ISLAMIC REPUBLIC OF IRAN (Mar. 8, 2016), http://www.cbi.ir/showitem/14423.aspx.

97. Iranian officials have responded to these speculations by publishing a scanned picture of the 2009 proposed bill of the previous administration. *See*, *The Picture of the Bill of the Law on*

Germany, United States, and the United Kingdom) in July 2015 and provides Iran with a multiyear plan for phased economic sanctions relief upon the verification of Iran's implementation of certain nuclear commitments.[98] On January 16, 2016, the International Atomic Energy Agency (IAEA) verified that Iran had implemented the key nuclear-related measures required by the JCPOA.[99]

Iran's counter-terrorism finance law requires that authorities and law enforcement personnel under the direction of a judicial authority identify and block funds and assets procured and collected for terrorist activities.[100] Individuals and entities subject to the law are required to maintain records of suspicious transactions and customers for no less than five years.[101] Any suspicious activity must be reported to the High Commission of Anti-Money Laundering for further action.[102] Knowingly or intentionally failing to report suspicious activity can result in criminal liability.[103] If the failure to report suspicious activity is due to negligence, then some lesser punishment may be imposed.

## II. Conclusion

VC regulation continues to challenge regulators, legislators, and law enforcement. The anonymity and global reach of VC ensures that the threat it poses to successful AML and CTF initiatives is unlikely to diminish. Though there is little consensus on how to define, much less regulate VCs, the initial wave of regulation is directed at intermediaries like VC exchanges and virtual wallet providers.

Regulators focused this year on strengthening CDD programs and implementing controls to capture beneficial ownership information. This signals a distinct trend towards proactive information-driven monitoring as a tool to combat money laundering and terrorist financing. Authorities acknowledge that the global nature of the threat posed by money laundering and terrorism requires cooperation among financial partners and across

---

*Combating Terrorism Finance in Ahmadi Nejhad's Administration*, EGHTESAD ONLINE, (Sep. 5 2016).

98. *See Joint Comprehensive Plan of Action*, U.S. DEPARTMENT OF STATE, https://www.state.gov/e/eb/tfs/spi/iran/jcpoa/ (last visited Mar. 15, 2017) (containing full text of the Joint Comprehensive Plan of Action and its annexes) [hereinafter *JCPOA*]; *see also* U.S. DEPARTMENT OF THE TREASURY, FREQUENTLY ASKED QUESTIONS RELATING TO THE LIFTING OF CERTAIN U.S. SANCTIONS UNDER THE JOINT COMPREHENSIVE PLAN OF ACTION (JCPOA) ON IMPLEMENTATION DAY (2016), https://www.treasury.gov/resource-center/sanctions/Programs/Documents/jcpoa_faqs.pdf.

99. *See JCPOA Implementation*, U.S. DEPARTMENT OF THE TREASURY (Jan. 16, 2016), https://www.treasury.gov/resource-center/sanctions/OFAC-Enforcement/Pages/jcpoa_implementation.aspx.

100. *See* The Law on Combating Terrorism Finance, *supra* note 94 at art. 5.

101. *Id.* at art. 13.

102. *Id.* at art. 14.

103. *Id.* at Note 1.

jurisdictions. Criminals and terrorists engaged in financial crimes will continue to attempt to exploit opportunities that result from uncoordinated or incompatible regulatory schemes.