International Lawyer

Volume 50
Number 0 *International Legal Developments Year in Review: 2015*
Article 30

2016

Anti-Money Laundering and Counter-Terrorist Finance: Year-in-Review 2015

Nicole S. Healy

Emily N. Christiansen

THE YEAR IN REVIEW
AN ANNUAL PUBLICATION OF THE ABA/SECTION OF INTERNATIONAL LAW

Anti-Money Laundering and Counter-Terrorist Finance: Year-in-Review 2015

NICOLE S. HEALY AND EMILY N. CHRISTIANSEN*

I. Introduction

This past year has seen continued activity in money laundering ("ML") regulation and enforcement involving "cryptocurrency," terrorist finance ("TF"), and forfeiture law.

Money launderers and others engaged in criminal activity were early adopters of virtual or cryptocurrencies such as Bitcoin, which permits them to avoid the formal financial system, and thus, detection mechanisms. When cryptocurrencies have been used for illicit activity, some perpetrators have been successfully prosecuted. But the relative anonymity that is a key feature of many cryptocurrencies makes investigation and prosecution difficult. Further, as discussed below, the United States and other countries have taken various approaches to regulating cryptocurrencies, with some countries encouraging their use, others substantially forbidding them, and still others taking a middle path.

Recent terrorist activity has focused the spotlight on terrorist finance. As law enforcement and regulators continue to respond to new threats, individuals and organizations involved in financing terrorism are responding by utilizing new technologies such as cryptocurrency, crowdfunding, and online payment systems. Terrorist organizations are highly diversified and opportunistic; in addition to adopting sophisticated funding mechanisms, they continue to use low-tech, informal currency transfer systems. Further, as the group calling itself the Islamic State has shown, terrorists are exploiting natural resources and antiquities to fund their operations. Finally, terrorist groups engage in criminal activity such as drug trafficking, extortion, and kidnapping for ransom to raise funds.

The United States has long prohibited the financing of terrorism. United States law permits private civil suits against those who finance acts that injure or kill United States citizens or residents abroad — as primary, or as of 2015, secondary violators. Because of the difficulties involved in suing and collecting judgments from terrorists or terrorist

* 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. Emily N. Christiansen is an Associate Attorney at Kessler Topaz Meltzer & Check, LLP in Radnor, Pennsylvania. The authors are co-chairs of the ABA Section of International Law Anti-Money Laundering Committee.

PUBLISHED IN COOPERATION WITH
SMU DEDMAN SCHOOL OF LAW

organizations, however, individuals injured by terrorism have pursued cases against other entities, including financial institutions. Although a number of cases involving allegations of terrorist finance have been filed against major financial institutions, few have been tried. One such case has led to a large settlement in 2015, however, following a jury's finding of liability.

Finally, for the second year in a row, the United States Supreme Court has taken up the pretrial restraint of allegedly forfeitable assets, which the defendant sought to use for legal fees. In 2014, the Court held that there was no Fifth or Sixth Amendment violation when tainted assets were restrained without a pretrial hearing as to the grand jury's determination that probable cause existed that the defendant committed the offense for which forfeiture was authorized. In 2015, the Court considered whether substitute assets may be restrained when the defendant allegedly dissipated purportedly tainted assets. In March 2016, a plurality decided that the government could not restrain untainted assets pretrial.

A. Recent Developments

1. *Cryptocurrencies*

Cryptocurrencies, such as Bitcoin, were certainly not new in 2015, but with the first Bitcoin debit card set to debut,[1] and companies and governments investigating new applications for the technology behind Bitcoin,[2] regulators, legal authorities, and courts around the world are addressing complex issues surrounding these currency substitutes.

Cryptocurrencies are digital or virtual currencies that have no intrinsic value; no physical form; often no supply controlled by a central bank (although some early versions had a central controller); and are not backed by a government or other legal entity.[3] Instead, these currencies are privately created, and both the currency and transactions between users are conducted and verified via secure cryptographic communications.[4]

There are currently over six hundred cryptocurrencies in existence, but only six of those have market capitalization of more than ten million dollars.[5] Altogether, cryptocurrencies have a market capitalization of about $5.3 billion,[6] approximately $4.8 billion[7] of which is attributable to Bitcoin, the best-known cryptocurrency. Despite this, the volume of Bitcoin transactions is modest. Approximately 80% of users appear to treat it as a commodity, speculating in Bitcoin and hoping to turn a profit when its value increases,

1. *See* Cade Metz, *Coinbase Just Debuted the First Bitcoin Debit Card in the US*, Wired (Nov. 20, 2015, 9:00 AM), http://www.wired.com/2015/11/coinbase-unveils-countrys-first-Bitcoin-debit-card/?mbid=social_twitter.

2. *See The Great Chain of Being Sure About Things*, The Economist (Oct. 31, 2015), http://www.economist.com/news/briefing/21677228-technology-behind-Bitcoin-lets-people-who-do-not-know-or-trust-each-other-build-dependable.

3. Edward V. Murphy, M. Maureen Murphy & Michael V. Seitzinger, *Bitcoin: Questions, Answers, and Analysis of Legal Issues*, Cong. Res. Serv. 1 (Oct. 13, 2015), fas.org/sgp/crs/misc/R43339.pdf.

4. *Id.*

5. *See Crypto-Currency Market Capitalizations*, https://coinmarketcap.com/.

6. *Id.*

7. *Id.*

rather than using it as a currency substitute to pay for goods and services.[8] By contrast, nearly $1.36 *trillion* in physical United States dollars are in circulation.[9]

While some have questioned whether the growth of non-currency transactions will lead to the development of the surveillance state,[10] many countries are increasingly moving to cashless transactions, that is, transactions by debit or credit card, or other currency substitute, instead of physical currency.[11] Along with currency substitutes such as credit or debit cards, cryptocurrencies[12] may soon provide a viable alternative to cash transactions. As the United States Treasury Department noted in its 2015 National Money Laundering Risk Assessment, "[t]he development of virtual currencies is an attempt to meet a legitimate market demand."[13]

Unlike credit cards, wire transfers, electronic funds transfers, and other similar non-currency methods of transferring value, cryptocurrencies are pseudonymous, written under a false name. The most widely used and best known cryptocurrency, Bitcoin, is very transparent as to completed transactions, but pseudonymous as to the participants.

Bitcoin transactions are viewable on a publicly distributed ledger or "blockchain,"[14] which contains a complete record of all transactions ever processed using Bitcoins, and permits any user's computer to verify the validity of any completed transaction.[15] The blockchain does not record personally identifying information; instead transactions are authenticated by "digital signatures corresponding to the sending addresses."[16] The system is highly secure and transactions are irreversible.[17]

Because this system is pseudonymous by design, criminals or would-be criminals cannot steal a user's identity and access their Bitcoin wallet without permission.[18] At the same

8. *See* Cade Metz, *Coinbase Just Debuted the First Bitcoin Debit Card in the US*, WIRED (Nov. 20, 2015, 9:00 AM), http://www.wired.com/2015/11/coinbase-unveils-countrys-first-Bitcoin-debit-card/?mbid=social_twitter.

9. *See* Alex Kroeger, *Essays on Bitcoin* 33, http://economics.nd.edu/assets/165129/alex_kroeger_essays_on_Bitcoin.pdf.

10. *See* Brett Scott, *£1984: Does a Cashless Economy Make for a Surveillance State?*, THE GUARDIAN (Sept. 30, 2015, 10:52 AM), http://www.theguardian.com/sustainable-business/2015/sep/30/1984-does-a-cashless-economy-make-for-a-surveillance-state.

11. Sweden is on track to becoming a cashless society, with cash transactions accounting for only 3% of the economy (compared with 9% in the Eurozone and 7% in the U.S.). *See* Camilla Lindskog, *Sweden Moving Towards Cashless Economy*, CBS NEWS (Mar. 18, 2012, 7:24 PM), http://www.cbsnews.com/news/sweden-moving-towards-cashless-economy/.

12. This article uses the term "cryptocurrency" to refer to currencies which exist only in digital, virtual, or electronic form.

13. *See* U.S. DEP'T OF THE TREASURY, NATIONAL MONEY LAUNDERING RISK ASSESSMENT 58 (2015), https://www.treasury.gov/resource-center/terrorist-illicit-finance/Documents/National%20Money%20Laundering%20Risk%20Assessment%20%E2%80%93%2006-12-2015.pdf.

14. *See Frequently Asked Questions*, BITCOIN, https://Bitcoin.org/en/faq#how-does-Bitcoin-work.

15. *See id.*

16. *Id.*; *see also* Edward V. Murphy, M. Maureen Murphy & Michael V. Seitzinger, *Bitcoin: Questions, Answers, and Analysis of Legal Issues*, CONG. RES. SERV. 1 (Oct. 13, 2015), fas.org/sgp/crs/misc/R43339.pdf.

17. Bitcoin transactions are unique messages secured by mathematically linked public-private cryptographic keys. The public key identifies the sender or recipient; the private key creates a unique and unforgeable signature that completes the transaction. *See Private Key*, BITCOIN WIKI (Feb. 10, 2015), https://en.Bitcoin.it/wiki/Private_key; *see also Six Things Bitcoin Users Should Know About Private Keys* BITZUMA (Apr. 23, 2014), bitzuma.com/posts/six-things-Bitcoin-users-should-know-about-private-keys/.

18. *See* sources cited *supra* note 17. However, while criminals and terrorists have enthusiastically adopted cryptocurrencies to mask their illegal activities, researchers believe that by utilizing sophisticated computer

time, because users can buy and sell goods or Bitcoins without revealing their true identities, cryptocurrencies may be used to conceal or facilitate illicit activity. "Criminals like the digital currency because it can be held in a digital wallet that does not have to be registered with any government or financial authority—and because it can be easily exchanged for real money."[19]

Bitcoin and other cryptocurrencies have been used to perpetrate and facilitate criminal activity, including black market transactions, drug trafficking, murder for hire, and buying and selling stolen credit card information. These currencies are also increasingly enabling new forms of criminal activity including crowd-funding child exploitation material, buying and selling lethal toxins over the Internet, and engaging in online extortion.[20] Indeed, hackers who seize control of computers for ransom, including those belonging to financial firms and police departments, often demand Bitcoins in lieu of currency in exchange for returning control of the computer to the user.[21]

Bitcoin is also becoming a preferred mechanism for terrorists looking to fund their operations. The United States Treasury Department has reported that terrorist financiers are increasingly turning to cryptocurrencies as authorities stem the flow of illicit funds through banks and financial institutions.[22]

2. *Criminal Prosecutions*

Authorities in the United States have already successfully prosecuted cases in which cryptocurrencies were used to facilitate criminal activity. The guilty verdict following the three week trial of Ross Ulbricht, aka "Dread Pirate Roberts," the kingpin behind the Silk Road online black market bazaar, demonstrated that Bitcoins can be traced—at least once investigators have access to the computer from which the transactions were made.[23] In the case against Ulbricht, FBI agents were able to examine the Silk Road's computer servers in Iceland as well as Ulbricht's confiscated laptop and matched the Bitcoin wallet addresses found in each to the Bitcoin public ledger blockchain. The FBI, therefore, determined that Ulbricht's laptop received 3,760 transactions from the Silk Road—the equivalent of $18 million.[24] Ulbricht was convicted on all seven charges for which he was

analysis, transactions involving large quantities of cryptocurrency can be tracked, and if paired with other information from law enforcement, may provide insight concerning the perpetrators. Sarah Meiklejohn et al., *A Fist Full of Bitcoins: Characterizing Payments Among Men with No Name*, 38 ; LOGIN: 6, 10-14 (Dec. 2013), http://cseweb.ucsd.edu/~smeiklejohn/files/login13.pdf.

19. Nathaniel Popper, *For Ransom, Bitcoin Replaces the Bag of Bills*, SEATTLE TIMES (July 25, 2015, 5:17 PM), http://www.seattletimes.com/nation-world/for-ransom-Bitcoin-replaces-the-bag-of-bills/.

20. *See* U.S. DEP'T OF JUSTICE, ASSISTANT ATTORNEY GENERAL LESLIE R. CALDWELL DELIVERS REMARKS AT THE ABA'S NATIONAL INSTITUTE ON BITCOIN AND OTHER DIGITAL CURRENCIES (June 26, 2015), http://www.justice.gov/opa/speech/assistant-attorney-general-leslie-r-caldwell-delivers-remarks-aba-s-national-institute.

21. *See* Popper, *supra* note 19.

22. *See* U.S. DEP'T OF THE TREASURY, NATIONAL TERRORIST FINANCING RISK ASSESSMENT 3 (2015), https://www.treasury.gov/resource-center/terrorist-illicit-finance/Documents/National%20Terrorist%20Financing%20Risk%20Assessment%20%E2%80%93%2006-12-2015.pdf.

23. *See* Nicky Woolf, *Silk Road's 'Dread Pirate Roberts' Convicted of Running Online Drug Marketplace*, THE GUARDIAN (Feb. 4, 2015), http://www.theguardian.com/technology/2015/feb/04/silk-road-ross-ulbricht-convicted-drug-charges.

24. *See* Jose Paliery, *Bitcoin Fallacy Led to Silk Road Founder's Conviction*, CNN MONEY (Feb. 5, 2015), http://money.cnn.com/2015/02/05/technology/security/Bitcoin-silk-road/.

indicted, including drug trafficking, continuing criminal enterprise, aiding and abetting the distribution of drugs online, computer hacking, and money laundering.[25] He was sentenced to life imprisonment in May 2015 and has appealed his conviction and sentence.[26]

In a bizarre twist, two former federal agents, Carl M. Force, IV and Shaun W. Bridges, who had been members of the Baltimore Silk Road Task Force were charged with money laundering, wire fraud, and related offenses for stealing Bitcoins during their investigation into the Silk Road and Ulbricht. Force, a former DEA agent, developed a number of unauthorized online personas and engaged in numerous illegal activities for personal financial gain. Specifically, he solicited and received Bitcoins as part of the investigation, failed to report receipt of the funds, and transferred them to his personal account. Force pled guilty to extortion, money laundering, and obstruction of justice and admitted that he offered to sell Ulbricht fake drivers' licenses and inside information about the Silk Road investigation.[27] Force was sentenced to 78 months in prison.[28] Bridges, a former U.S. Secret Service agent, diverted over $800,000 in Bitcoin to a personal account at Mt. Gox, the now-defunct Bitcoin exchange that was based in Japan, and then days before seeking a seizure warrant for Mt. Gox's accounts as part of the Silk Road investigation, wired the money into a personal investment account in the United States. Bridges pled guilty and admitted that he stole $820,000 worth of Bitcoins through a series of complex transactions.[29] In December 2015, he was sentenced to serve 71 months imprisonment. In yet another twist, in January 2016, Bridges was re-arrested at his home in Maryland, the day before he was scheduled to report to prison, allegedly while planning to flee the United States. Law enforcement agents reportedly seized passports, "corporate records for 'offshore entities' in Belize, Nevis and Mauritius (including one that had been created after his guilty plea)," and stolen bulletproof vests, at least one of which apparently came from the Secret Service.[30]

---

25. Verdict Form, United States v. Ulbricht, 31 F. Supp. 3d 540 (S.D.N.Y. 2014) (No. 1:14-CR-00068-KBF).

26. *See* U.S. DEP'T OF JUSTICE, ROSS ULBRICHT, A/K/A "DREAD PIRATE ROBERTS," SENTENCED IN MANHATTAN FEDERAL COURT TO LIFE IN PRISON (May 29, 2015), http://www.justice.gov/usao-sdny/pr/ross-ulbricht-aka-dread-pirate-roberts-sentenced-manhattan-federal-court-life-prison.

27. *See* U.S. DEP'T OF JUSTICE, FORMER SILK ROAD TASK FORCE AGENT PLEADS GUILTY TO EXTORTION, MONEY LAUNDERING AND OBSTRUCTION 1 (July 1, 2015), https://oig.justice.gov/press/2015/2015-07-01.pdf.

28. *See* U.S. DEP'T OF JUSTICE, FORMER SILK ROAD TASK FORCE AGENT SENTENCED TO 78 MONTHS IN PRISON FOR EXTORTION, MONEY LAUNDERING, AND OBSTRUCTION (Oct. 19, 2015), http://www.justice.gov/usao-ndca/pr/former-silk-road-task-force-agent-sentenced-78-months-prison-extortion-money-laundering.

29. *See* U.S. DEP'T OF JUSTICE, FORMER SILK ROAD TASK FORCE AGENT PLEADS GUILTY TO MONEY LAUNDERING AND OBSTRUCTION 1 (Aug. 31, 2015), https://oig.justice.gov/press/2015/2015-08-31.pdf.

30. *See* Joe Mullin, *Secret Service Agent Pleads Guilty to Stealing Money from Silk Road Dealers*, ARS TECHNICA (Aug. 31, 2015, 6:50 PM), http://arstechnica.com/tech-policy/2015/08/secret-service-agent-pleads-guilty-to-stealing-money-from-silk-road-dealers/.; Andy Greenberg, *Corrupt Silk Road Investigator Re-Arrested for Allegedly Trying to Flee the US*, WIRED *(Feb. 1, 2016, 3:11 PM)*, http://www.wired.com/2016/02/corrupt-silk-road-investigator-re-arrested-trying-to-flee-the-us/.

3. *Regulatory Responses to Cryptocurrency Risks*

Even though it may be possible for government authorities to track Bitcoins and other cryptocurrencies and identify those behind illicit transactions, in light of their potential for misuse, the debate about regulating cryptocurrencies continues. The Financial Action Task Force ("FATF"), an inter-governmental organization whose mission is to "set standards and promote effective implementation of legal, regulatory and operational measures for combating money laundering, terrorist financing and other related threats to the integrity of the international financial system," issued its "Guidance for a Risk-Based Approach to Virtual Currencies."[31] FATF's Guidance proposes applying a risk-based approach to "anti-money laundering" and "counter-terrorism finance" ("AML/CFT") risks relating to virtual currencies.[32]

The recent November 2015 terrorist attacks in Paris, France, led to a heightened focus on potential terrorist financing including the use of cryptocurrency. In response to the attacks, G7 finance officials reportedly announced plans to tighten the regulation of cryptocurrencies at the November 2015 G-20 summit in Antalya, Turkey.[33]

At the same time, the treatment and regulation of cryptocurrencies, and of the technology that powers cryptocurrency transactions, have become even more important as mainstream banks, financial institutions, securities markets, and other registries investigate other uses for blockchains and public ledgers.[34] Because they provide a secure, inexpensive, and transparent way to record transactions, various organizations are considering using blockchains to register ownership and title transfer of securities, real estate, and other property, in addition to cryptocurrencies.

4. *Cryptocurrency Regulation: a Global Survey*

How cryptocurrencies are treated largely depends on what they are used for and where the activities are taking place. What follows is a brief worldwide survey of the proposed and recently enacted AML/CFT laws and regulations pertaining to cryptocurrencies.[35]

a. Argentina

In May 2014, Argentina's central bank issued warnings about the use of cryptocurrencies.[36] On August 1, 2014, new regulations imposed by the Unidad de Informacion Financiera, the agency of the Argentine government with AML/CFT

31. *Who We Are*, FATF, http://www.fatf-gafi.org/about/.

32. *Guidance for a Risk-Based Approach to Virtual Currencies*, FATF 3 (June 26, 2015), http://www.fatf-gafi.org/media/fatf/documents/reports/Guidance-RBA-Virtual-Currencies.pdf.

33. *See* Tina Bellon, *G7 Plan to Get Tough on Virtual Currencies After Paris Attacks - Spiegel*, REUTERS (Nov. 18, 2015), http://www.reuters.com/article/2015/11/18/france-shooting-g7-finance-idUSL8N13D32220151118#GVKJSmUrskhDdJ4Z.97.

34. *See The Great Chain of Being Sure About Things*, THE ECONOMIST (Oct. 31, 2015), http://www.economist.com/news/briefing/21677228-technology-behind-Bitcoin-lets-people-who-do-not-know-or-trust-each-other-build-dependable.

35. The Library of Congress maintains a very useful blog addressing global regulation of cryptocurrencies, *see generally Regulation of Bitcoin in Selected Jurisdictions*, LIBR. OF CONGRESS, http://www.loc.gov/law/help/bitcoin-survey/index.php (last updated July 7, 2015).

36. *See* J.M.P., *Bitcoin in Argentina: If it can't make it there*, ECONOMIST (June 12, 2014, 1:36 PM), http://www.economist.com/blogs/schumpeter/2014/06/Bitcoin-argentina.

authority, required all financial services companies in Argentina to report transactions involving Bitcoin and digital currencies.[37] The government was primarily concerned about the ability of criminals to use cryptocurrencies for money laundering and terrorist finance.[38]

b. Australia

In September 2015, two of Australia's largest banks, Westpac and Commonwealth Bank of Australia, closed the accounts of at least seventeen Bitcoin and cryptocurrency-related exchanges and businesses, citing concerns over risks, policies, and compliance with AML/CFT regulations.[39] The acting chief of the Australian Bankers Association stated that the banks were obligated to close the accounts in order to comply with Australian AML/CFT laws if the banks could not view the full chain of transactions, and that new regulations and guidance specifically applicable to Bitcoins and cryptocurrencies would be necessary.[40] Despite that, there was also news that the Commonwealth Bank of Australia was investigating ways to introduce cryptocurrency technology into international money transfers.[41]

In October 2015, the Australian government announced that it would review the regulatory powers of the Reserve Bank of Australia and the Australian Securities and Investments Commission in order to create a graduated regulatory response to Bitcoin and other digital currencies.[42]

c. Brazil

In November 2015, Brazil's House of Representatives held a hearing to discuss proposed legislation that would give Brazil's central bank oversight of all digital currency activity.[43]

---

37. Tanaya Macheel, *Argentinian Bitcoin Exchange Loses its Bank Accounts*, COINDESK (Aug. 5, 2014, 7:00 PM BST), http://www.coindesk.com/argentina-Bitcoin-exchange-loses-bank-accounts/.

38. Carlo Caraluzzo, *Mandatory Bitcoin Reporting Ordered in Argentina*, COINTELEGRAPH (July 12, 2014, 5:50 PM), http://cointelegraph.com/news/mandatory-bitcoin-reporting-ordered-in-argentina.

39. Paul Smith, *Big Australian banks stun bitcoin companies by closing their accounts*, AUSTL. FIN. REV. (Sept. 21, 2015, 6:30 PM), http://www.afr.com/technology/big-banks-cut-off-accounts-of-bitcoin-companies-in-battle-for-the-future-of-payments-20150921-gjr7hu.

40. *Id.*

41. Jessica Sier & James Eyers, *CBA joins global banks in project to explore bitcoin model*, AUSTL. FIN. REV. (Sept. 16, 2015, 6:15 PM), http://www.afr.com/technology/cba-joins-global-banks-in-Bitcoin-research-20150916-gjo40b.

42. Australian Government, Improving Australia's financial system: Government response to the Financial System Inquiry, at 15 (2015), http://www.treasury.gov.au/~/media/Treasury/Publications%20and%20Media/Publications/2015/Government%20response%20to%20the%20Financial%20System%20Inquiry/Downloads/PDF/Government_response_to_FSI_2015.ashx.

43. Stan Higgins, *Brazil Holds Hearing on Bitcoin Regulation Bill Amid Oversight Push*, COINDESK (Nov. 20, 2015, 6:20 PM BST), http://www.coindesk.com/brazil-holds-hearing-on-Bitcoin-regulation-bill-amid-oversight-push/.

d. Canada

In 2014, Canada amended its AML/CFT laws in order to subject digital currencies to the same reporting requirements as money-services businesses.[44] Companies in Canada that deal in cryptocurrencies, as well as cryptocurrency companies targeting Canadian customers, must now register with the Financial Transactions and Reports Analysis Centre of Canada (FINTRAC), implement compliance programs, keep and retain prescribed records, report suspicious terrorist-related property transactions, and determine if any of their customers are "politically exposed persons" and, if so, confirm the source of funds.[45]

e. China

Since December 2013, according to the Notice on Precautions Against the Risks of Bitcoins issued by the Central Bank of China and four other Chinese government agencies and commissions, Bitcoins and other cryptocurrencies are considered a "virtual commodity" and cannot be circulated and used as currency.[46] Banks and other financial institutions in China are prohibited from dealing in Bitcoins, and the government also warned about the risks of using Bitcoins for money laundering.[47] In April 2014, China's central bank ordered all Chinese commercial banks and financial service companies to close any accounts trading in Bitcoins.[48]

f. European Union

In May 2015, the European Union adopted an anti-money laundering package designed to improve the cooperation between the member states' Financial Intelligence Units, bring about coordinated policies for EU states dealing with non-member states with deficient AML controls, and combat the financing of terrorism.[49] Building on that new AML framework, the European Commission began working on an assessment of the ML/TF risks facing the EU.[50] The European Commission's full analysis and recommendations will be available by June 2017 and, based upon a January 26, 2015 request by the European Council, the European Commission will pay particular attention to cryptocurrencies as one of the sectors for assessment.[51]

---

44. Samuel Rubenfield, *Canada Enacts Bitcoin Regulations*, WALL ST. J. (June 23, 2014, 6:41 PM ET), http://blogs.wsj.com/riskandcompliance/2014/06/23/canada-enacts-Bitcoin-regulations/.

45. Christine Duhaime, *Canada implements world's first national digital currency law; regulates new financial technology transactions*, DUHAIME L. (June 22, 2014), http://www.duhaimelaw.com/2014/06/22/canada-implements-worlds-first-national-Bitcoin-law/.

46. *Regulation of Bitcoin in Selected Jurisdictions*, *supra* note 35, at *China*.

47. *Id.*

48. Chao Deng & Lingling Wei, *China Cracks Down on Bitcoin: PBOC Orders Big Banks to Close Trading Accounts in Virtual Currency*, WALL ST. J., http://www.wsj.com/articles/SB10001424052702304157204579475233879506454 (last updated Apr. 1, 2014, 10:15 AM ET).

49. Press release, Eur. Comm'n, European Agenda on Security - State of Play, MEMO/15/6115 (Nov. 17, 2015), http://europa.eu/rapid/press-release_MEMO-15-6115_en.htm.

50. *Id.*

51. *Id.*

g. Russia

Bitcoin and other virtual currencies appear to be banned in Russia.[52] On January 27, 2014, the Central Bank of the Russian Federation recommended that "Russian individuals and legal entities refrain from transactions involving bitcoin" because, in its view, many of the services dealing in Bitcoin exchange were engaged in "dubious activity."[53] The Central Bank was specifically concerned about Bitcoin's potential for use in "money laundering or terrorist activities."[54] In February 2014, Russia's Prosecutor General's Office came out in strong opposition to virtual currencies, explaining that, "Russia's official currency is the ruble. The introduction of other types of currencies and the issue of money surrogates are banned."[55] On October 8, 2014, the Russian Ministry of Finance proposed legislation that would make transactions in Bitcoin a misdemeanor and impose a fine on those dealing in cybercurrencies.[56] As part of the proposal, individuals would be allowed to play with cryptocurrencies, but would not be able to exchange those currencies for real money.[57] But Russia's Ministry of Economic Development strongly criticized the proposed legislation, arguing that the legislation lacked precision and could harm Russia's economy.[58] In January 2015, Russia's media regulator, Roskomnadzor, blacklisted five websites related to cryptocurrencies.[59]

h. Sweden

The Swedish Financial Supervisory Authority publicly recognized cryptocurrencies as a means of payment.[60] In Sweden, cryptocurrencies are treated like regular currencies and Bitcoin exchanges must register with the regulator and follow its rules and regulations, including AML/CFT regulations applicable to other financial institutions.[61]

i. United Kingdom

In March 2015, the government of the United Kingdom announced that it intends to apply AML regulation "to digital currency exchanges in the UK, to support innovation and prevent criminal use and will formally consult on the proposed" regulations with the next Parliament.[62]

---

52. *See Russian media watchdog blocks Bitcoin sites*, RT TV (Jan. 13, 2015, 3:56 PM), https://www.rt.com/news/222215-russia-bans-Bitcoin-sites/.

53. *Regulation of Bitcoin in Selected Jurisdictions*, *supra* note 35, at *Russia*.

54. *See Russian media watchdog blocks Bitcoin sites*, *supra* note 52.

55. *Id.*

56. *Regulation of Bitcoin in Selected Jurisdictions*, *supra* note 35.

57. *See 'You can play with you bitcoins, but you can't pay with them': Russia may ban cryptocurrencies by 2015*, RT TV (Sept. 12, 2014, 11:00 PM), https://www.rt.com/business/187440-bitcoin-ban-russia-cryptocurrency/.

58. *Yes to bitcoin! Russian ministry says quasi-money ban may endanger banks, retailers*, RT TV (Dec. 27, 2015, 10:35 AM), https://www.rt.com/news/218019-bill-ban-Bitcoin-russia/.

59. *Russian media watchdog blocks Bitcoin sites*, *supra* note 52.

60. *See Regulation of Bitcoin in Selected Jurisdictions*, *supra* note 35, at *Sweden*.

61. *See id.*

62. HM Treasury, Digital currencies: response to the call for information, at 4 (Mar. 2015), https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/414040/digital_currencies_response_to_call_for_information_final_changes.pdf (U.K.).

j. United States of America

In March 2013, the United States Treasury Department's Financial Crimes Enforcement Network (FinCEN) issued interpretive guidance entitled the Application of FinCEN's Regulations to Persons Administering, Exchanging, or Using Virtual Currencies.[63] FinCEN clarified that a user of virtual currencies is not a "money services business" (MSB) and is therefore "not subject to MSB registration, reporting, and record-keeping regulations," but that an administrator or service that exchanges Bitcoin for other currencies is an MSB and, more specifically, a money transmitter subject to FinCEN's regulations.[64]

FinCEN has subsequently released two administrative rulings concerning the application of the regulations to two companies involved in virtual currency activities.[65] One related to a business proposing to facilitate payments between credit card holders and businesses that deal only in cryptocurrencies;[66] the other proposed to set up a virtual currency trading platform.[67] In both instances, FinCEN denied the companies' applications for exemption from the MSB regulations.[68]

On May 5, 2015, in conjunction with the United States Attorney for the Northern District of California,[69] FinCEN brought its first cryptocurrency enforcement action against Ripple Labs Inc., a virtual currency exchange, for failing to register as an MSB and failing to implement and maintain an AML program.[70] Ripple ultimately settled with FinCEN and the Department of Justice (DOJ) and paid a total penalty of $700,000 ($450,000 to the DOJ and $250,000 to the Treasury),[71] agreed to cooperate with FinCEN and DOJ, to register as an MSB, and to implement a compliance program.[72]

63. *See generally* Application of FinCEN's Regulations to Persons Administering, Exchanging, or Using Virtual Currencies, FIN-2013-G001 (Mar. 18, 2013), http://www.fincen.gov/statutes_regs/guidance/html/FIN-2013-G001.html.

64. *Id.* at 1-2.

65. *See generally* Request for Administrative Ruling on the Application of FinCEN's Regulations to a Virtual Currency Trading Platform, FIN-2014-R011 (Oct. 27, 2014), https://www.fincen.gov/news_room/rp/rulings/pdf/FIN-2014-R011.pdf; Request for Administrative Ruling on the Application of FinCEN's Regulations to a Virtual Currency Payment System, FIN-2014-R012 (Oct. 27, 2014), https://www.fincen.gov/news_room/rp/rulings/pdf/FIN-2014-R012.pdf.

66. *See* Request for Administrative Ruling on the Application of FinCEN's Regulations to a Virtual Currency Trading Platform, *supra* note 65, at 1.

67. *Id.*

68. *Id.* at 4, 6.

69. Press release, FinCEN, FinCEN Fines Ripple Labs Inc. in First Civil Enforcement Action Against a Virtual Currency Exchanger: Company Agrees to $700,000 Penalty and Remedial Actions, at 1 (May 5, 2015), https://www.fincen.gov/news_room/nr/pdf/20150505.pdf.

70. *Id.*

71. *See* Press release, U.S. Dep't of Justice, Ripple Labs Inc. Resolves Criminal Investigation (May 5, 2015), https://www.justice.gov/opa/pr/ripple-labs-inc-resolves-criminal-investigation.

72. *See* Press release, FinCEN Fines Ripple Labs Inc. in First Civil Enforcement Action Against a Virtual Currency Exchanger, *supra* note 69, at 1-2.

B. Terrorist Finance

1. *2015 ATA Amendments: Secondary Liability for Terrorist Funding*

Following the murder by Palestinian hijackers of Leon Klinghoffer, a wheelchair-bound American tourist, aboard the cruise ship *Achille Lauro*, Congress passed the Anti-Terrorism Act of 1990 ("ATA").[73] When United States citizens or residents are injured or killed outside the United States, the ATA permits victims and their survivors to sue funders of terrorists and terrorist organizations for damages.[74]

On September 26, 2015, the ATA was amended to include an express cause of action for aiding and abetting or conspiring to fund terrorism.[75] The Act's stated purpose is

> to provide civil litigants with the broadest possible basis, consistent with the Constitution of the United States, to seek relief against persons, entities, and foreign countries, wherever acting and wherever they may be found, that have provided material support, directly or indirectly, to foreign organizations or persons that engage in terrorist activities against the United States.[76]

Previously, the Second and Seventh Circuits, and district courts in the Fifth and Eleventh Circuits, held that the ATA did not provide for secondary liability.[77] The 2015 amendments to section 2333 have now explicitly broadened the scope of liability to include secondary actors.[78]

---

73. The ATA "initially was apparently enacted in error in 1990, repealed in 1991, and reenacted in 1992." In re Terrorist Attacks on Sept. 11, 2001, 714 F.3d 118, 122 n.2 (2d. Cir. 2013), *citing* S. Rep. No. 102-342, at 22 (1992). The hijackers were members of the Palestinian Liberation Front, and affiliate of the Palestinian Liberation Organization or "PLO," which Congress had previously found was a terrorist organization. *See* 22 U.S.C. § 5201(b), *et seq*.

74. *See* 18 U.S.C. § 2333(a) (added Pub.L. 102-572, Title X, § 1003(a)(4), Oct. 29, 1992, 106 Stat. 4522; amended Pub. L. 103-429, § 2(1), Oct. 31, 1994, 108 Stat. 4377).

75. *See* Justice Against Sponsors of Terrorism Act, S. 2040, 114th Cong., § 2(a)5 (2015). *See also* § 4(d) which provides that: "In an action under subsection (a) for an injury arising from an act of international terrorism committed, planned, or authorized by an organization that had been designated as a foreign terrorist organization . . . liability may be asserted as to any person who aided, abetted, or conspired with the person who committed such an act of international terrorism." 18 U.S.C. § 2333(d). Section 2334 has been amended to provide that: "The district courts shall have personal jurisdiction, to the maximum extent permissible under the 5th Amendment to the Constitution of the United States, over any person who commits or aids and abets an act of international terrorism or otherwise sponsors such act or the person who committed such act, for acts of international terrorism in which any national of the United States suffers injury in his or her person, property, or business by reason of such an act in violation of section 2333." 18 U.S.C. § 2334(e).

76. *See id*. § 2(b).

77. *See* Rothstein v. UBS AG, 708 F.3d 82, 82 (2d. Cir 2013); In re Terrorist Attacks on Sept. 11, 2001, 714 F.3d 118, 125 (2d. Cir. 2013), *cert. denied*, 134 S. Ct. 2870 (2014); Abecassis v. Wyatt, 7 F. Supp. 3d 668, 676–77 (S.D. Tex. 2014) (affirming that ATA did not prohibit aiding and abetting but finding that the complaint stated a claim for *respondeat superior* liability); In re Chiquita Brands Int'l, Inc., Alien Tort Statute & S'holder Derivative Litig., No. 08-01916-MD, 2015 WL 71562, at *7 (S.D. Fla. Jan. 6, 2015) (although the ATA did not provide for secondary liability, plaintiffs stated a claim against Chiquita as a primary violator). *Id.*

78. Where not expressly precluded, a defendant need not be the primary actor but may be found secondarily liable. *See* Halberstam v. Welch, 705 F.2d 472, 484–85 (D.C. Cir. 1985). Congress cited *Halberstam* in its findings in connection with the Justice against Sponsors of Terrorism Act.

a. Civil Suits Against Financial Institutions

While a number of plaintiffs have brought suits alleging that financial institutions have been complicit in financing terrorism and terrorist support organizations, few cases have gone to trial. Although each case is different, these lawsuits generally involve complicated legal, evidentiary, and other issues, and may implicate international relations. Among other things, evidence may be outside the United States; the parties may engage in extensive motion practice; and evidence concerning terrorist organizations may be subject to national security restrictions in the United States and other countries.

On September 22, 2014, a jury in Brooklyn, New York, which heard evidence concerning approximately 300 plaintiffs injured or killed in 24 separate attacks during the second Palestinian Intifada, found Arab Bank liable for providing material support to Hamas.[79] The court had bifurcated the case and scheduled a second trial to determine damages for the plaintiffs who claimed that they or their relatives had been injured or killed in Hamas attacks in Israel and the Palestinian Territories years earlier.[80] Three days before the damages trial was set to begin in August 2015, Arab Bank, a Jordanian-headquartered entity that is one of the largest financial institutions in the Middle East,[81] settled the lawsuits.[82] The settlement reportedly resolves all of the cases filed by approximately 500 plaintiffs, however, the details are confidential and Arab Bank has contested reports valuing the settlement at just over $1 billion.[83]

Other ATA suits have been filed including against Bank of China Ltd. (see *Wultz v. Bank of China Ltd.*), which was accused of providing services to the Palestine Islamic Jihad ("PIJ"),[84] and Crédit Lyonnais, S.A., which was accused of aiding Hamas (*Strauss v. Crédit*

79. *See* Nate Raymond & Joseph Ax, *Arab Bank Settles U.S. Litigation Over Attacks by Militants*, REUTERS, (Aug. 14, 2015, 6:32 PM), http://www.reuters.com/article/us-arab-bank-jo-settlement-hamas-idUSKCN0QJ21120150814.

80. *See also* Gill v. Arab Bank, PLC, 893 F. Supp. 2d 542, 573 (E.D.N.Y. 2012) (granting bank's summary judgment motion).

81. Arab Bank reported a net income after tax of $ 442.1 million for 2015. *See* Arab Bank Fact Sheet, *available at* http://www.arabbank.com/en/investfactsheet.aspx.

82. *See* Stephanie Clifford, *Arab Bank Reaches Settlement in Suit Accusing it of Financing Terrorism*, N.Y. TIMES, Aug. 14, 2015, http://www.nytimes.com/2015/08/15/nyregion/arab-bank-reaches-settlement-in-suit-accusing-it-of-financing-terrorism.html?hp&action=click&pgtype=Homepage&module=second-column-region&region=top-news&WT.nav=top-news&_r=1.

83. *See* Raymond & Ax, *supra* note 79; *Report of $1 Billion Settlement "Inaccurate," says Arab Bank*, JERUSALEM POST, (Aug, 22, 2015, 9:23AM), http://www.jpost.com/Arab-Israeli-Conflict/Report-of-1-billion-settlement-inaccurate-says-Arab-Bank-412907.

84. *See* Wultz v. Bank of China Ltd., 811 F. Supp. 2d. 841 (S.D.N.Y. 2011) *opinion withdrawn on reconsideration*, 865 F. Supp. 2d 425 (S.D.N.Y. 2012) (between 2003 and 2006, defendants allegedly facilitated wire transfers totaling millions of U.S. dollars to the PIJ, which planned and executed terrorist attacks, including a 2006 suicide bombing in Israel that injured a U.S. citizen and killed his teenaged son). The *Wultz* case reportedly stirred up tensions between China and Israel. Published reports have indicated that, in 2005, Israeli intelligence officials notified Bank of China ("BoC"), a state-backed institution, that terrorists had funded operations in Gaza and the West Bank through accounts at BoC. The plaintiffs' efforts to obtain testimony on this point by a former Israeli intelligence official, with Israel's assistance, angered Beijing, straining the relationship between the two countries, and embroiling the U.S., not only because of the venue but also because Rep. Eric Cantor, a cousin of the Wultzes, had brokered the arrangement with the Israeli government. *See* James Loeffler & Moira Paz, *Uncivil Damages, American Victims of Palestinian Terrorism are suing a Chinese Bank. Israel is trying to stop them*, SLATE, (Feb. 13, 2014, 12:49 PM), http://www.slate.com/

Lyonnais, S.A.). The *Wultz* case has since been voluntarily dismissed, although plaintiffs filed a notice of appeal relating to a sealed document. The *Strauss* case remains pending.[85]

b. Financial Action Task Force Report—Terrorist Finance Mechanisms

In October 2015, FATF issued a report titled "Emerging Terrorist Finance Risks" ("TF Report").[86] The TF Report makes for chilling reading—it discusses the means used by terrorists to raise funds to be used for operations, to provide material support for fighters and their families, and to meet their other financial requirements.

The TF Report explains that while lone terrorists or terrorist recruits may be self-funded, large-scale terrorist organizations are sophisticated modern businesses with accounting and finance staff, spreadsheets and financial reports, social media fundraising platforms, and complex financial networks.[87] Moreover, large-scale terrorist organizations are not squeamish about their revenue sources. While it is unlikely that each organization uses every one of these money raising schemes, the TF Report describes the fund raising mechanisms as including the following: bank robbery; fraudulent loan applications; insurance fraud; direct social media requests (some of which are video or image based to avoid detection); crowdfunded donations, sometimes based on misleading representations about the funding requests; kidnapping for ransom; extortion; and the exploitation of antiquities or natural resources.[88] The funds may be laundered or moved by means of informal transfer systems, prepaid debit cards, as cash, in cryptocurrency, or through complex structuring and layering transactions.[89]

Given the use of the formal financial system for at least some of these transactions, it is incumbent on financial institutions to examine and if necessary recalibrate their due diligence and internal controls to detect and interrupt the misuse of the financial sector, and to report any suspicious activity.

Informal financial transactions are obviously harder to spot, and the use of social media for messaging and fundraising requires ongoing monitoring. FATF repeatedly noted in the TF Report that social media providers have not been complicit in terrorist finance and have in fact reported suspicious activity. However, such companies must continue to maintain and enhance their controls in order to continue to identify and disrupt the misuse of their platforms. Although the authors of this year-in- review report are not aware of any ATA suits against social media companies or crowdfunding platforms, there is no reason to believe that, if evidence that such an entity had actual knowledge of or was

---

articles/news_and_politics/jurisprudence/2014/02/wultz_vs_bank_of_china_daniel_wultz_parents_attempt_to_use_domestic_courts.html.

85. Strauss v. Crédit Lyonnais, S.A., No. CV-06-0702 (CPS), 2006 WL 2862704 (E.D.N.Y. Oct. 5, 2006); Strauss v. Crédit Lyonnais, S.A., 925 F. Supp. 2d 414, 425 (E.D.N.Y. 2013). The cases were consolidated on October 7, 2011. Both lawsuits pled claims under 18 U.S.C. § 2333(a) and allege that the bank violated 18 U.S.C. §§ 2339B, 2339C, by maintaining accounts for a non-profit organization linked to Hamas. The court heard oral argument on defendant's motion to dismiss the complaint for lack of personal jurisdiction or, alternatively, for summary judgment, on October 8, 2015. The court has not yet ruled on the motions.

86. *See* FATF, EMERGING TERRORIST FINANCING RISKS (2015), http://www.fatf-gafi.org/publications/methodsandtrends/documents/emerging-terrorist-financing-risks.html.

87. *See id.*, at 11

88. *See id.*, at 12–20.

89. *See id.*, at 20–23.

extremely reckless as to the use of its technology to fund terrorism, a plaintiff would not bring an ATA suit.

C. Recent United States Supreme Court Forfeiture Cases

Under federal law, property may be forfeited either civilly or criminally where it represents the proceeds of certain criminal activity, or can be traced to such proceeds. In addition, when the proceeds have been dissipated and cannot be traced, federal law provides for the criminal forfeiture of substitute assets.[90]

Civil forfeiture proceedings are *in rem*; that is, the government proceeds against the property to establish its superior title. A criminal forfeiture is imposed upon conviction, as part of a defendant's sentence. For both civil and criminal forfeitures, under the relation-back principle, the tainted assets belong to the government from the time of the violation.[91]

The government may restrain forfeitable assets prior to trial. That is, the government may obtain a seizure warrant if the court finds that "there is probable cause to believe that the property to be seized would, in the event of conviction, be subject to forfeiture," and that an order imposing a bond or other security or conditions may not be sufficient to ensure that the property will be available if the defendant is convicted.[92]

In its past two terms, the United States Supreme Court has addressed the collision between a criminal defendant's Fifth and Sixth Amendment right to retain chosen counsel and the government's right to restrain assets pretrial. In *Kaley v. United States*, decided in 2014, the Supreme Court held that allegedly tainted assets may be restrained pretrial, even when the defendant requires those assets to retain counsel.[93]

In *Kaley*, the defendant had not challenged the nexus between the alleged offense and the restrained property. This term, the Court considered whether the government may

---

90. Substitute property may be criminally forfeited where the forfeitable property: "(A) cannot be located upon the exercise of due diligence; (B) has been transferred or sold to, or deposited with, a third party; (C) has been placed beyond the jurisdiction of the court; (D) has been substantially diminished in value; or (E) has been commingled with other property which cannot be divided without difficulty." 21 U.S.C. § 853(p).

91. The relation back principle has always applied to civil forfeitures. *See* United States v. Nichols, 841 F.2d 1485, 1499 (10th Cir. 1985); *see also* United States v. Stowell, 133 U.S. 1, 16-17 (1890) (it is settled doctrine that whenever Congress enacts a forfeiture statute, "the forfeiture takes effect immediately upon the commission of the act; the right to the property then vests in the United States, although their title is not perfected until judicial condemnation; . . . and the condemnation, when obtained, relates back to that time, and avoids all intermediate sales and alienations, even to purchasers in good faith."); United States v. 1960 Bags of Coffee, 12 U.S. 398, 408(1814); Caldwell v. United States, 49 U.S. 366, 382 (1850). By statute, the relation back principle has also been applied to criminal forfeitures. *See* 21 U.S.C. § 853(c); *see also Nichols*, 841 F.2d at 1488-89 & n.2 ("Section 853(c) was enacted in response to decisions holding that the relation back concept did not apply in criminal forfeiture proceedings.")

92. *See* 21 U.S.C. § 853(f). Section 853(f) states that: "[t]he Government may request the issuance of a warrant authorizing the seizure of property subject to forfeiture under this section in the same manner as provided for a search warrant. If the court determines that there is probable cause to believe that the property to be seized would, in the event of conviction, be subject to forfeiture and that an order under subsection (e) of this section may not be sufficient to assure the availability of the property for forfeiture, the court shall issue a warrant authorizing the seizure of such property." 21 U.S.C. § 853(f).

93. *See* Kaley v. United States, __ U.S. __, 134 S. Ct. 1090, 1105 (2014); *see also* United States v. Monsanto, 491 U.S. 600, 616 (1989); Caplin & Drysdale, Chtd. v. United States, 491 U.S. 617, 631 (1989) (both holding that attorneys' fees are not exempt from forfeiture).

obtain a pretrial order restraining substitute assets, which necessarily have no nexus to the offense, where the defendant contends she needs those assets to retain chosen counsel.[94]

A year later, in *Luis v. United States*, the Supreme Court again took up the issue of the government's pretrial restraint of assets. This time, however, the court considered whether the government could restrain untainted assets before trial where the defendant required those assets to retain counsel.[95] Luis was argued on November 10, 2015 and the Court issued its opinion on March 30, 2016, following the death of Justice Scalia.

Luis had been charged with "paying kickbacks, conspiring to commit fraud, and engaging in other crimes all related to health care" under 18 U.S.C. § 1349; §371; 42 U. S. C. § 1320a-7b(b)(2)(A).[96] Luis's alleged schemes purportedly netted her almost $45 million, nearly all of which she had spent. Attempting to preserve the $2 million remaining in her possession for forfeitures and criminal penalties — including, potentially, the forfeiture of untainted substitute assets, the government obtained a freeze order under 18 U.S.C. § 1345(a)(2) from the District Court for the Southern District of Florida, which the Eleventh Circuit affirmed *per curiam*.[97]

The Supreme Court reversed. In a plurality opinion written by Justice Breyer, the Court affirmed that the right to counsel is "fundamental" and held that the "pretrial restraint of legitimate, untainted assets needed to retain counsel of choice violates the Sixth Amendment."[98] Although this issue has been resolved, other issues remain for future courts to decide. For example, in *Kaley*, the Court held that it was unnecessary for the trial court to conduct a pretrial hearing to determine whether there was probable cause to believe that the seized assets would be forfeitable because that evidence would be considered at trial.[99] In *Luis*, the Court assumed that the government could distinguish tainted from untainted assets. What if it cannot? Will trial courts develop a presumption in favor of defendants regarding assets that cannot be readily identified as untainted? As the dissent noted in *Luis*, however, the tainted assets were unavailable because the defendant had spent or given them away, placing them beyond the government's reach. Arguably, she was rewarded for being either a spendthrift or a clever money launderer.

---

94. *See* United States v. Luis, 564 F. App'x 493, 494 (11th Cir. 2014) *cert. granted*, 135 S. Ct. 2798, 192 L. Ed. 2d 846 (2015) and *vacated and remanded*, No. 14-419, 2016 WL 1228690 (U.S. Mar. 30, 2016). The petitioner identified the issue to be decided on certiorari as follows: "Whether the pretrial restraint of a criminal defendant's legitimate, untainted assets (those not traceable to a criminal offense) needed to retain counsel of choice violates the Fifth and Sixth Amendments." Luis v. United States, 14-419, *Question Presented*, *available at* http://www.supremecourt.gov/qp/14-00419qp.pdf.

95. The government sought to freeze Luis's assets under 18 U. S. C. §1345, which permits the government to freeze (1) property "obtained as a result of" the crime, (2) property "traceable" to the crime, and (3) other "property of equivalent value." *Id.* § 1345(a)(2). *Luis*, 578 U.S. at ___, slip op. at 1 (Breyer, J.).

96. *Luis*, 578 U.S. at —, slip op. at 1 (Breyer, J.).

97. *Id.* at 1-2.

98. *Luis*, 578 U.S. at —, slip op. at 3 (Breyer, J.).

99. Ignoring that the defendant had argued that she required access to her assets to retain counsel, the *Kaley* majority stated that because a person could be restrained in custody pretrial, there was no reason not to permit the government to restrain her assets until the conclusion of the trial. *See Kaley*, 134 S.Ct. at 1098-99. While recognizing that criminal defendants "have a vital interest at stake: the constitutional right to retain counsel of their own choosing," *id.* at 1102, the Court found that this right was impaired "only when the grand jury should never have issued the indictment." *Id.* at 1103. Of course, by the time that question is resolved at trial, the defendant has been deprived of assets, counsel of her choice, and quite possibly her liberty.

THE YEAR IN REVIEW
AN ANNUAL PUBLICATION OF THE ABA/SECTION OF INTERNATIONAL LAW

Later cases will inevitably present different facts, and perhaps lead to a different conclusion as to whether any seized assets were in fact untainted.

Although *Luis* signals the outer limits of this trend, *Kaley* is one of a long line of decisions in which courts have chipped away at the Fifth and Sixth Amendment rights of criminal defendants to retain counsel of their choice and pay with funds that the government contends are the proceeds of criminal activity. It is facile to claim that an acquitted defendant will have access to her restrained funds after a trial given that effective representation of criminal defendants is at risk when funding for appointed defense attorneys and public defenders in jurisdictions across the country have been whittled away. While some white collar defendants may have third-party funding from their employers or insurers, defendants who are forced to rely on their own assets to secure counsel may find their resources unavailable.

II. Conclusion

Regulatory and law enforcement authorities in the United States and elsewhere continue to grapple with understanding, classifying, and regulating new technologies, such as cryptocurrencies, which are designed to transfer value more or less anonymously. Because many cryptocurrencies, such as Bitcoin, are decentralized, they have been enthusiastically adopted by criminals and terrorists. The creation of a shadow economy based on cryptocurrency, which is the logical outgrowth of their design, is worrisome given the difficulty in tracing the participants to cryptocurrency transactions. Regulatory and law enforcement agencies are likely to continue their efforts to monitor and control these transactions; whether they can is a function not only of developing legal mechanisms, but also of technological constraints.

Terrorist finance continues to be an area of great concern. In particular, terrorists and their financiers are using every possible means to fund their operations. This is likely to be an area in which enforcement agencies, regulators, the intelligence community, and others, will place substantial emphasis and resources for some time.

Finally, the Supreme Court has now twice addressed pretrial asset seizures when the defendant sought to use the assets to pay for counsel. It remains for the lower courts to continue to define the circumstances under which assets may be restrained in advance of trial.

VOL. 50

PUBLISHED IN COOPERATION WITH
SMU DEDMAN SCHOOL OF LAW