

OKLAHOMA CITY UNIVERSITY LAW REVIEW

VOLUME 49

FALL 2024

NUMBER 1

ESSAY

THE NEXUS BETWEEN FINANCIAL INSTITUTIONS, MONEY LAUNDERING, AND ORGANIZED CRIME: THE IMPORTANCE OF DUE DILIGENCE AND “KNOW YOUR CUSTOMER” IN THE GLOBAL FINANCIAL REALM

*Gavin Howell**

* Juris Doctor Candidate, Oklahoma City University School of Law, May 2025. First and foremost, I dedicate this work to my mother, Amber Howell. Without her positive attitude, perseverance, and desire to do anything in her power so I can reach the stars, I would be nowhere close to where I am today. I am deeply grateful for the constant support and kindness from my family and friends throughout my time in law school. I thank the legal practitioners and mentors who have allowed me to learn and instilled in me an even greater passion for the rule of law and helping people at vulnerable times in their lives. I also want to thank my professors and the faculty at OCU Law for their support and pushing me to be the best I can be. Lastly, I want to extend my sincere gratitude to the Board and members of the Oklahoma City University Law Review for their timeless hours spent editing this piece.

I. Introduction

A. What Is Money Laundering?

“Money laundering is the criminal’s way of . . . ensur[ing] that, in the end, crime pays.”¹ Criminal organizations launder money to disguise the origin of their “dirty” money to avoid detection.² Money laundering “provides the fuel” for criminals engaged in activities like trafficking, arms dealing, and terrorism “to operate and expand their criminal enterprises,” posing drastic “economic, security, and social consequences” for society.³ Launderers, in their movement of funds through multiple types of businesses, manipulate and erode a nation’s financial systems.⁴ Unfortunately, financial institutions are entangled in criminal organization account holders’ illicit activities through knowingly or unknowingly harboring their “dirty” money, in turn fostering their money laundering schemes.⁵ As evinced in a deferred prosecution agreement between HSBC Bank and the United States Department of Justice (DOJ), the DOJ asserts a strong intolerant stance against financial institutions that, through “stunning failures of oversight” and willful blindness, become a “conduit” to criminal organizations’ money laundering activities.⁶

1. See John McDowell & Gary Novis, *The Consequences of Money Laundering and Financial Crime*, 6 ECON. PERSPS.: AN ELEC. J. U.S. DEP’T STATE, no. 2, May 2001, at 6, 6 [hereinafter *The Consequences of Money Laundering*], <https://www.hsd.org/c/view?docid=3549> [<https://perma.cc/FR29-8HS5>]; see also *United States v. Medeles-Arguello*, 701 F. App’x 390, 390-91 (5th Cir. 2017) (per curiam) (“[T]he testimonies of numerous witnesses show[ed] that [the defendant] and [their] co-conspirators knowingly operated a brothel business which caused persons under the age of 18 to engage in commercial sex acts [The defendant] directed the management of the lucrative and extensive brothel business. . . .”); see also Press Release, U.S. Att’y’s Off., S.D. Tex., Federal Jury Convicts Sex Trafficking Ring Leader (Apr. 24, 2015), <https://www.justice.gov/usao-sdtx/pr/federal-jury-convicts-sex-trafficking-ring-leader> [<https://perma.cc/YYE9-STZG>] (ordering that assets of around \$2.5 million funded with sex trafficking proceeds be forfeited to the United States).

2. *The Consequences of Money Laundering*, *supra* note 1, at 6.

3. *Id.*

4. *Id.*

5. Joel Slawotsky, *Reining in Recidivist Financial Institutions*, 40 DEL. J. CORP. L. 280, 316-17 (2015) (footnote omitted) (explaining that financial institutions play a vital role “in providing services to a host of rogue actors . . . [and] have engaged in money laundering and banking services for terrorists and global drug dealers”).

6. Press Release, Off. of Pub. Affs., U.S. Dep’t of Just., HSBC Holdings Plc. and HSBC Bank USA N.A. Admit to Anti-Money Laundering and Sanctions Violations,

“Money laundering is one of the oldest, multi-faceted, and increasingly sophisticated white-collar crimes in the world.”⁷ The first stage of money laundering is the collection and placement of “dirty” money into the financial system.⁸ To avoid detection, launderers, through a process called “smurfing,” will deposit smaller amounts of their funds into multiple institutions since a smaller transaction is less likely to raise suspicion.⁹ After “placing” the dirty money into the financial system, launderers will “layer” their funds by “mov[ing] . . . [them] in a series of unnoticeable processes,” concealing the funds’ true source, but remaining in ultimate control.¹⁰ Launderers will mix illegitimate and legitimate funds together and execute wire transfers to offshore banks with lenient reporting requirements.¹¹ Here, a criminal organization certainly accomplishes its goal of masking its funds, as it is harder for law enforcement to trace funds spread across various jurisdictions.¹² Lastly, the funds are completely integrated in accounts across the world and are used to purchase property such as luxury homes, private jets, and yachts.¹³ Launderers create businesses by subsequently reselling luxury property they have purchased with their illicit funds.¹⁴

Forfeit \$1.256 Billion in Deferred Prosecution Agreement (Dec. 11, 2012) [hereinafter HSBC Deferred Prosecution Agreement], <https://www.justice.gov/opa/pr/hsbc-holdings-plc-and-hsbc-bank-usa-na-admit-anti-money-laundering-and-sanctions-violations> [https://perma.cc/GK2Y-AL9Y] (“HSBC is being held accountable for stunning failures of oversight – and worse – that led the bank to permit narcotics traffickers and others to launder hundreds of millions of dollars through HSBC subsidiaries, and to facilitate hundreds of millions more in transactions with sanctioned countries [Homeland Security Investigators] will continue to aggressively target financial institutions whose inactions are contributing in no small way to the devastation wrought by the international drug trade.”).

7. Maame Nyakoa Boateng, Comment, *Global Partnership Should Be the Way Forward to Combat Money Laundering*, 126 DICK. L. REV. 837, 838-39 (2022) [hereinafter *Global Partnership*] (footnote omitted).

8. *Id.* at 841.

9. *See id.* (“As financial institutions have begun to recognize small deposits as suspicious, ‘smurfers’ have reduced the amount of the deposits they make even further, making it even harder for the banks to detect them. . . . [T]he volume of business that banks handle on a daily basis makes it harder for them to track every single transaction and exposes them to significant money laundering risks.”) (footnotes omitted).

10. *See id.* at 843.

11. *See id.* (“With the click of a button, . . . money launderers can facilitate the movement of money between accounts and intermediaries in different nations.”) (footnote omitted).

12. *Id.*

13. *See id.* at 844-45.

14. *See id.* at 844.

B. Pertinent Statutes

Under the Money Laundering Control Act of 1986 (the Act), anyone who knowingly engages in a financial transaction¹⁵ of property that “represents the proceeds of some form of unlawful activity,” with the intent of promoting the continuance of an unlawful activity, knowing that the transaction is part of a scheme “to conceal or disguise the nature, the location, the source, the ownership, or the control of the proceeds of [an] unlawful activity,” is guilty of the federal offense of money laundering.¹⁶ Furthermore, persons who transport, or attempt to do so, “a monetary instrument or funds from a place in the United States to or through a” foreign country, or vice versa, with the objective “to promote the carrying on of specified unlawful activity” or “to conceal or disguise” the proceeds or source of a “specified unlawful activity,” are also guilty under the statute.¹⁷ Moreover, persons are criminally liable under the Act when, with the intent of promoting the continuance of an unlawful activity, they conceal or disguise the property or proceeds of an unlawful activity “to avoid a transaction reporting requirement under State or Federal law.”¹⁸ Under the Act, a person who “knowingly engages or attempts to engage in a monetary transaction in criminally derived property of a value greater than \$10,000 and is derived from specified unlawful activity” is guilty of a federal offense.¹⁹ Importantly, money laundering has broad “extraterritorial jurisdiction” against foreign nations as long as at least some of the acts took place in the United States and the “transaction[] involves funds or monetary instruments of a value exceeding \$10,000.”²⁰

Examples of predicate offenses under the Money Laundering Control Act include organized crime in general; arson; corruption; bribery;

15. 18 U.S.C. § 1956(c)(4) (“[T]he term ‘financial transaction’ means (A) a transaction which in any way or degree affects interstate or foreign commerce (i) involving the movement of funds by wire or other means or (ii) involving one or more monetary instruments, or (iii) involving the transfer of title to any real property, vehicle, vessel, or aircraft, or (B) a transaction involving the use of a financial institution which is engaged in, or the activities of which affect, interstate or foreign commerce in any way or degree.”).

16. 18 U.S.C. § 1956.

17. *Id.*

18. 18 U.S.C. § 1956(a)(3)(C).

19. 18 U.S.C. § 1957(a); *see also* 18 U.S.C. § 1957(f) (“‘[M]onetary transaction’ means the deposit, withdrawal, transfer, or exchange, in or affecting interstate or foreign commerce, of funds or a monetary instrument . . . by, through, or to a financial institution . . .”).

20. 18 U.S.C. § 1956(f).

counterfeiting currency and products; trafficking of drugs, humans, firearms, or stolen goods; cybercrime; extortion; forgery; fraud; kidnapping; robbery; sexual exploitation; terrorism and financing thereof; and murder.²¹ Moreover, certain offenses against a foreign nation qualify as predicate offenses under the Act: violations of foreign drug laws; violent crimes such as murder, kidnapping, extortion, or terrorism; fraud involving a foreign bank; bribery of a Government official; trafficking; sexual exploitation of children; and acts for which the United States would be obligated to extradite under a treaty with the nation in question.²²

Before the enactment of the Money Laundering Control Act of 1986, the Bank Secrecy Act (BSA) was “the principal tool against money laundering,” but nonetheless remains an ever-important statute for financial institutions to heed.²³ “The BSA authorizes the Department of the Treasury to impose reporting and other [similar] requirements on financial institutions . . . to . . . detect and prevent money laundering” through its Financial Crimes Enforcement Unit (FinCEN).²⁴ Hence, financial institutions are required to assist U.S. Government agencies in this manner by: (1) keeping records of cash purchases of negotiable instruments; (2) filing reports of cash transactions exceeding \$10,000 (within a single business day), also known as a currency transaction report (CTR); and (3) reporting suspicious activity that might be a signal of criminal activity.²⁵ Additionally, under the BSA, financial institutions must report their relationships with foreign banks.²⁶ Most importantly, the BSA requires financial institutions to establish Anti-Money Laundering (AML) Programs as a barrier between the institution and

21. 18 U.S.C. § 1956(c)(7) (explaining other predicate offenses include the destruction of aircraft, assassination of a political official, embezzlement by a bank officer or employee, fraudulent bank entries, and violations of the Foreign Corrupt Practices Act).

22. 18 U.S.C. § 1956(c)(7)(B).

23. Lynne D. Boylston, Note, *Attorneys’ Fees and the Money Laundering Control Act of 1986: Further Erosion of Criminal Defense Advocacy*, 21 GA. L. REV. 929, 940 (1987).

24. *The Bank Secrecy Act*, U.S. TREASURY, FIN. CRIMES ENF’T NETWORK, <https://www.fincen.gov/resources/statutes-and-regulations/bank-secrecy-act> [<https://perma.cc/V2H8-5HZD>]. FinCEN is the primary federal agency responsible for preventing money laundering and terrorist financing.

25. See 31 C.F.R. §§ 1010.311, 1020.320 (2011). A bank does not have to notify an account holder when they file a CTR, but if an account holder suddenly backs out of a transaction the bank will instead file a Suspicious Activity Report (SAR) which is worse for an account holder since an SAR signals possible criminal activity on their part.

26. 31 U.S.C. § 5314(a).

money laundering activity financing criminal organizations.²⁷

II. Foreign Entities and Due Diligence

A. The “Bare” Minimum

“Banks are the first layer of defense against money launderers and other criminal enterprises who choose to utilize our nation’s financial institutions to further their criminal activity”²⁸ The five pillars of an effective BSA/AML compliance program include: (1) customer due diligence; (2) independent review; (3) ongoing AML training; (4) written internal policies, procedures, and controls; and (5) a designated compliance officer.²⁹ In general, a bank’s due diligence assessment should seek to understand the anticipated activity of the account.³⁰

Customer due diligence, otherwise known as the “know your customer” rule, is the most important pillar of an institution’s AML compliance program.³¹ As part of conducting “due diligence” on customers, financial institutions are required to conduct a series of checks to verify their customers’ identities to assess the risk, if any, they present to the business.³² Financial institutions must:

27. See 31 U.S.C. § 5318(h); see also 31 U.S.C. § 5311 (“It is the purpose of this subchapter . . . to . . . prevent the laundering of money and the financing of terrorism through the establishment by financial institutions of reasonably designed risk-based programs to combat money laundering . . .”).

28. HSBC Deferred Prosecution Agreement, *supra* note 6 (“When a bank disregards the Bank Secrecy Act’s reporting requirements, it compromises that layer of defense, making it more difficult to identify, detect and deter criminal activity.”).

29. See 31 U.S.C. § 5318(h) (“In order to guard against money laundering and the financing of terrorism through financial institutions, each financial institution shall establish anti-money laundering . . . programs, including, at a minimum—(A) the development of internal policies, procedures, and controls; (B) the designation of a compliance officer; (C) an ongoing employee training program; and (D) an independent audit function to test programs.”).

30. See *Beneficial Ownership Requirements for Legal Entity Customers—Overview*, FED. FIN. INST. EXAMINATION COUNCIL 1 (May 5, 2018), <https://www.ffiec.gov/press/pdf/Beneficial%20Ownership%20Requirements%20for%20Legal%20Entity%20CustomersOverview-FINAL.pdf>.

31. 31 C.F.R. §§ 1010, 1020, 1023-24, 1026 (“Customer due diligence is universally recognized as fundamental to mitigating illicit financial risk . . .”).

32. See 31 C.F.R. 1010.100(t), (ff) (2012). Examples of financial institutions that are subject to the AML compliance requirement include banks, casinos, currency exchangers, securities dealers, operators of credit card systems, loan companies, and finance companies.

[E]stablish and maintain written policies and procedures that are reasonably designed to: 1. identify and verify the identity of customers[;] 2. identify and verify the identity of the beneficial owners of companies opening accounts [with the institution;] 3. understand the nature and purpose of customer relationships to develop customer risk profiles[;] [and] 4. conduct ongoing monitoring to identify and report suspicious transactions and, on a risk basis, to maintain and update customer information.³³

Financial institutions that fail to engage in appropriate due diligence of their account holders may have a “heavy price” to pay.³⁴

A “beneficial owner” of a company account holder is a person who has ultimate control over the funds in the company’s account.³⁵ Simply, beneficial ownership is determined under two prongs: (1) control and (2) ownership.³⁶ A beneficial owner has “significant responsibility to control, manage or direct a legal entity customer,” which “includes[] an executive officer or senior manager.”³⁷ One beneficial owner must be identified for each customer and own at least 25% in equity of the legal entity customer.³⁸ For high-risk account holders, this threshold percentage can be as low as 10%.³⁹ Along with their ownership interest, a beneficial owner receives substantial economic benefits from the assets of a

33. *Information on Complying with the Customer Due Diligence (CDD) Final Rule*, U.S. TREASURY, FIN. CRIMES ENF’T NETWORK, <https://www.fincen.gov/resources/statutes-and-regulations/cdd-final-rule#:~:text=The%20CDD%20Rule%20has%20four,owners%20of%20companies%20opening%20accounts> [https://perma.cc/PB4R-7YMB].

34. HSBC Deferred Prosecution Agreement, *supra* note 6 (“The record of dysfunction that prevailed at HSBC for many years [is] astonishing. Today, HSBC is paying a heavy price for its conduct . . .”).

35. A company account holder is also referred to as a “legal entity customer.” See 31 C.F.R. § 1010.230(e)(1) (2016) (stating for the purpose of the Beneficial Ownership Rule, a legal entity customer is defined as “a corporation, limited liability company, or other entity that is created by the filing of a public document with a Secretary of State . . . , a general partnership, and any similar entity formed under the laws of a foreign jurisdiction that opens an account”).

36. *Beneficial Ownership Requirements for Legal Entity Customers—Overview*, *supra* note 30, at 1, 1.

37. *Id.* at 1-2 (footnote omitted).

38. *Id.* at 2.

39. Dan Ryan, *FinCEN: Know Your Customer Requirements*, HARV. L. SCH. F. ON CORP. GOVERNANCE (Feb. 7, 2016), <https://corpgov.law.harvard.edu/2016/02/07/fincen-know-your-customer-requirements/> [https://perma.cc/5EEH-9HPG].

company.⁴⁰ When verifying the identity of a beneficial account holder, “[a] bank need not establish the accuracy of every [piece] of identifying information obtained, but must verify enough information to form a reasonable belief that it knows the true identity of [a] beneficial owner[] of [a] legal entity customer.”⁴¹ In the event that a bank cannot form a reasonable belief of the true identity of a beneficial owner, a bank should have procedures in place describing: (1) circumstances in which an account should not be opened; (2) “[t]he terms under which a customer [can] use an account while the bank [works] to verify the identity of [a] beneficial owner[]”; (3) when an account should be closed after the bank has failed to identify a beneficial owner; and (4) when the bank should file a suspicious activity report (SAR) pursuant to a transaction signaling criminal activity.⁴²

B. Correspondent Banking Relationships

“The global financial system, trade flows, and economic development rely on correspondent banking relationships.”⁴³ Correspondent bank accounts allow foreign banks to conduct business in the United States without having to expand their geographic footprint.⁴⁴ The function of a correspondent bank account resembles that of an agent conducting business on a principal’s behalf: the foreign bank’s U.S. correspondent conducts financial transactions on the foreign bank’s behalf in the U.S. and vice versa for a U.S. banks’ foreign correspondent. “[S]ervices [that]

40. 31 C.F.R. § 1010 (stating that an individual who reaps economic benefits from a “reporting company,” but exercises “substantial control” over the company under CFR 1010.380(d)(1)(i)(A) as a “senior officer,” does not fall within the exception to the definition of a “beneficial owner” under CFR 1010.380(d)(3)(iii)).

41. *Beneficial Ownership Requirements for Legal Entity Customers—Overview*, *supra* note 30, at 4.

42. *Id.*

43. Bd. of Governors of the Fed. Rsrv. Sys. et al., *U.S. Department of the Treasury and Federal Banking Agencies Joint Fact Sheet on Foreign Correspondent Banking: Approach to BSA/AML and OFAC Sanctions Supervision and Enforcement*, U.S. DEP’T OF THE TREAS. 1 (Aug. 30, 2016), <https://home.treasury.gov/system/files/136/archive-documents/Foreign-Correspondent-Banking-Fact-Sheet.pdf> [https://perma.cc/SP92-XG9T].

44. See Fernando L. Aenlle-Rocha, *Correspondent Banking After September 11: New Controls will Combat Money Laundering and Money Transfers that Aid Illegal Acts*, L.A. LAW. 27, 27 (emphasis omitted) [hereinafter *Correspondent Banking*] (“By virtue of . . . correspondent [banking] relationships, respondent banks, [those that conduct business on behalf of foreign banks], have avoided the financial costs and regulatory hurdles that are associated with licensing, staffing, and operating full-service banks in the United States.”).

correspondent bank[s] provide include wire transfers; check clearing and payment; trade finance; cash and treasury management; and securities, derivatives, or foreign exchange settlement”⁴⁵ Thus, correspondent banking plays a valuable role in the international financial system and is wholly popular across the world.⁴⁶ While the ability for an international bank to maintain its global services without having to actually “step into” another country may sound like paradise, financial institutions face several risks with correspondent banking, and when correspondent banking’s function is abused, criminal organizations flourish in their money laundering activities.⁴⁷

The fundamental objective of correspondent banking relationships is to make money through the execution of payments.⁴⁸ Categories of foreign banks that face a greater risk of entanglement in money laundering include: “(1) shell banks with no physical presence in any country for conducting business with their clients, (2) offshore banks with licenses limited to transacting business with persons outside the licensing jurisdiction, or (3) banks [in foreign jurisdictions] with weak anti-money laundering controls that invite banking abuses and criminal misconduct.”⁴⁹ A U.S. Senate Committee Report by the Permanent Subcommittee on Investigations titled *Correspondent Banking: A Gateway for Money Laundering* concluded that due to U.S. banks’ poor due diligence with their correspondent relationships and measly AML procedures, U.S. banks were unwilling channels for illicit funds, and with foreign correspondent banks’ access to the American banking and international wire transfer

45. Rena S. Miller, *Overview of Correspondent Banking and “De-Risking” Issues*, CONG. RSCH. SERV. 1 (2022) [hereinafter *De-Risking Issues*], <https://crsreports.congress.gov/product/pdf/IF/IF10873/3>.

46. *See id.* (“The value of global cross-border payments is estimated to increase from almost \$150 trillion in 2017 to over \$250 trillion by 2027, according to the Bank of England . . . [T]he European Central Bank reported roughly \$746 billion worth of daily transactions channeled through correspondent banking arrangements within Eurozone countries alone in 2019”); *see also Correspondent Banking*, *supra* note 44, at 27 (emphasis omitted) (“The worldwide demand for and popularity of U.S. dollars and the lucrative potential of correspondent banking have resulted in the development of thousands of correspondent banking relationships, which account for more than \$1 trillion in wire transfers per day.”) (emphasis omitted).

47. *See Correspondent Banking*, *supra* note 44.

48. *See De-Risking Issues*, *supra* note 45, at 2.

49. MINORITY STAFF OF THE U.S. S. PERMANENT SUBCOMM. ON INVESTIGATIONS, 107TH CONG., REP. ON CORRESPONDENT BANKING: A GATEWAY FOR MONEY LAUNDERING 1 (Comm. Print 2001) [hereinafter *Gateway for Money Laundering*].

systems, criminals were commingling and disguising illicit funds.⁵⁰ U.S. Senator Carl Levin (D-MI) best summed up the need for financial institutions to “step it up” in their due diligence and compliance areas: “We cannot condemn jurisdictions with weak [AML] controls, weak banking oversight, and unregulated offshore sectors, and then tolerate U.S. banks doing business with the very banks that those jurisdictions license and unleash on the world.”⁵¹

Some banks, fearful of the mere possibility that bearing liability will cause their reputation and profitability to plummet, may shed their correspondent banking relationships with banks as a whole in “high-risk” areas as opposed to “managing” their risks.⁵² This phenomenon, known as “de-risking,” introduces risk into the global financial system as a mass termination of correspondent relationships forces entities into channels that are either less regulated or unregulated altogether, making any implemented AML safeguards effectively moot.⁵³ While active correspondent banking relationships declined by about 20% between 2012 and 2019, the volume of payments did not drop off “indicating that banks in smaller countries might be seeking out intermediary banks to conduct correspondent banking for them,” otherwise “known as *lengthening the payment chain*.”⁵⁴

U.S. banks maintaining correspondent accounts for foreign account holders complain that the due diligence, recordkeeping, and certifications required for foreign account holders are simply too much to bear, especially for correspondent accounts from jurisdictions with high crime

50. See *id.* at 1-2, 13, 56; see also *Correspondent Banking*, *supra* note 44, at 27 (emphasis omitted) (“Poor due diligence by U.S. banks . . . enable[s] correspondent accounts to be opened for poorly regulated or managed banks[] . . . and . . . the owners and customers of corrupt banks. Correspondent accounts [give] foreign banks and their . . . customers access to the American banking system, which is known for its soundness. Correspondent accounts also [give] access to the international wire transfer system—the most important link in the money laundering chain . . .”).

51. *Role of U.S. Correspondent Banking in International Money Laundering: Hearings Before the U.S. S. Permanent Subcomm. on Investigations of The Comm. on Gov’t Affs.*, 107th Cong. 8 (2001) (opening statement of Sen. Carl Levin (D. Mich.)).

52. *De-Risking Issues*, *supra* note 45, at 1.

53. See *FATF Clarifies Risk-Based Approach: Case-by-Case, Not Wholesale De-Risking*, FIN. ACTION TASK FORCE (Oct. 23, 2014) [hereinafter *Wholesale De-Risking*], <https://www.fatf-gafi.org/en/publications/Fatfgeneral/Rba-and-de-risking.html> [<https://perma.cc/U486-J89E>]; see also *De-Risking Issues*, *supra* note 45, at 1-2 (noting an increase in “de-risking” instances could send entities into less regulated “shadow payments” that could have an adverse effect on global financial integrity).

54. *De-Risking Issues*, *supra* note 45, at 2.

levels.⁵⁵ However, “[d]e-risking’ should never be an excuse for a bank to avoid implementing a risk-based approach.”⁵⁶ Similar to a corporation’s risk management with their corporate compliance program to ensure compliance with the Foreign Corrupt Practices Act, financial institutions should identify and assess their laundering and criminal organization financing risks and take the appropriate steps to mitigate as opposed to completely eliminating the risks.⁵⁷ Furthermore, foreign correspondent accounts have been used to circumvent the law and facilitate illicit transactions; thus, “special scrutiny” must be paid to them.⁵⁸ “A business can never completely eliminate risk, unless it is willing to simply close up shop. Rather, the goal of most organizations is to bring the risk to manageable levels.”⁵⁹

HSBC Bank, through their entanglement with the Mexican drug cartel, clearly did not get the message of the importance of supervising their correspondent relationships.⁶⁰ HSBC violated the BSA by “ignor[ing] the money laundering risks associated with [carrying out] business with certain Mexican customers” and by failing to have an adequate AML/BSA compliance program.⁶¹ HSBC’s lackadaisical supervision over one of their customers, Grupo Financiero, whose own AML diligence fell way short of passing muster, resulted in “at least \$881 million in drug trafficking proceeds” by Mexican and Columbian drug cartels being laundered through HSBC Bank USA without fail.⁶² HSBC Bank USA failed to put due care and attention to its AML program, instead, prioritizing lower costs and higher profits, an all-too-common excuse for

55. *Id.*

56. *Wholesale De-Risking*, *supra* note 53.

57. *See id.* (“‘De-risking’ should never be an excuse for a [financial institution] to avoid implementing a risk-based approach The FATF Recommendations only require financial institutions to terminate customer relationships, on a case-by-case basis, where the money laundering and terrorist financing risks cannot be mitigated What is not in line with the FATF standards is the wholesale cutting loose of entire classes of customer, without taking into account, seriously and comprehensively, their level of risk or risk mitigation measures for individual customers within a particular sector.”) (emphasis omitted).

58. *De-Risking Issues*, *supra* note 45, at 2.

59. Philip J. Ruce, *Anti-Money Laundering: The Challenges of Know Your Customer Legislation for Private Bankers and the Hidden Benefits for Relationship Management* (“*The Bright Side of Knowing Your Customer*”), 128 *BANKING L.J.* 548, 549 (2011).

60. *See* Statement of Facts at 3, *United States v. HSBC*, No. 1:12-cr-00763-ILG (E.D.N.Y. Dec. 11, 2012) [hereinafter *HSBC Statement of Facts*].

61. *Id.*

62. *Id.*

businesses failing to maintain adequate safeguards against white-collar criminal risks despite blatant indicators of program deficiencies and their high-risk line of business.⁶³ Thus, “drug traffickers were depositing hundreds of thousands of dollars in bulk U.S. currency each day into HSBC Mexico accounts” and peso brokers wire transferred the U.S. currency to U.S. exporters, making “HSBC Mexico [] the preferred financial institution for drug cartels and money launderers.”⁶⁴ HSBC serves as a sheer example of the importance for financial institutions to understand the AML and supervisory regime of the foreign account holder’s licensing jurisdiction and the AML record of the foreign account holder.

C. Law Enforcement Difficulties in Intercepting Money Laundering Activity

Law enforcement faces great difficulty in intercepting and shutting down illegal money laundering enterprises. Indeed, with traffickers’ use of virtual currencies, an ever increasingly prevalent method of commencing transactions pursuant to technology’s pervasive role in our society today, law enforcement has a difficult time even knowing about suspicious transactions tracking to enterprises carrying out such sinister “business.”⁶⁵ “Drug and human traffickers use virtual currency and peer-to-peer mobile payments because transactions are somewhat anonymous [V]irtual currency ATMs—stand-alone machines that facilitate buying, selling, and exchange of virtual currencies—can be used for illegal activities such as laundering drug trafficking proceeds.”⁶⁶ Online marketplaces used for these purposes “are sometimes located on the ‘dark web,’ a hidden part of the internet where users access sites using specialized software . . . to connect to buyers and sellers” leaving law enforcement in the dark.⁶⁷

A financial institution cannot be established for the express purpose

63. *Id.* at 10.

64. *Id.* at 17.

65. See *As Virtual Currency Use in Human and Drug Trafficking Increases, So Do the Challenges for Federal Law Enforcement*, U.S. GOV’T ACCOUNTABILITY OFF. (Feb. 24, 2022) [hereinafter *Challenges for Federal Law Enforcement*], <https://www.gao.gov/blog/virtual-currency-use-human-and-drug-trafficking-increases-so-do-challenges-federal-law-enforcement> [<https://perma.cc/UHH3-7VH7>].

66. *Id.*

67. *Id.*

of laundering criminal proceeds.⁶⁸ In *United States v. Budovsky*, the defendant was charged “with creating and operating an unlicensed money transmitting business designed to facilitate illegal financial transactions and launder criminal proceeds.”⁶⁹ The Government alleged that the defendant’s digital currency outlet, Liberty Reserve, incorporated in Costa Rica, “provided access to ‘instant, real-time currency for international commerce’” and that the business “touted itself as the Internet’s ‘largest payment processor and money transfer system,’ serving ‘millions’ . . . around the world, including . . . the United States.”⁷⁰ More pertinently, the Government alleged that Liberty Reserve took steps to assist criminals by hiding their identities and that the defendant focused on concealing Liberty’s assets and operations by failing to properly register as a “money transmitting business” in the United States and Costa Rica.⁷¹ Through their blatant concealment steps, Liberty achieved notoriety as the “bank of choice for the criminal underworld.”⁷² For these reasons and others, the court denied the defendant’s motion to dismiss the indictment against him.⁷³

Samuel Bankman-Fried (SBF), recently “sentenced . . . to 25 years in prison for his orchestration of multiple fraudulent schemes” with his cryptocurrency exchange firm, FTX, and his cryptocurrency trading firm, Alameda Research, also engaged in money laundering and the operation

68. See *United States v. Budovsky*, No. 13cr368 (DLC), 2015 WL 5602853 (S.D.N.Y. Sept. 23, 2015).

69. See *id.* at *1, *3 (“The Indictment charges Budovsky in three counts with (1) conspiracy to commit money laundering . . . ; (2) conspiracy to operate an unlicensed money transmission business . . . ; and (3) operation of an unlicensed money transmission business . . .”).

70. See *id.* at *1, *5 (“Liberty Reserve had 200,000 users in the United States . . .”).

71. *Id.* at *1-*2 (“Budovsky and his co-defendants are alleged to have intentionally created, structured, and operated Liberty Reserve as a business venture designed to help criminals conduct illegal transactions and launder the proceeds of their crimes.”). Liberty Reserve did not require users to validate their identities, allowed users to hide their account numbers when conducting transactions, and users were prohibited from directly depositing or withdrawing funds; instead, they were required to utilize third-party exchangers, pre-approved by Liberty, who were unregulated and unlicensed.

72. See *id.* at *1-*2 (“[F]rom 2006 to 2013, Liberty Reserve processed an estimated 55 million separate financial transactions and laundered more than \$6 billion in criminal proceeds. . . . Budovsky and his associates were well aware of Liberty Reserve’s function as an unlawful money laundering enterprise and deliberate[] attract[ion of] a criminal customer base . . .”). Criminal users of Liberty Reserve included those of computer hackers, credit card and identity thieves, fraudsters, procurers of child pornography, and drug traffickers.

73. See *id.* at *1, *4, *15.

of unlicensed money transmitting businesses.⁷⁴ SBF was unable to open bank accounts for FTX due to U.S. banks' general resistance at the time of conducting business with cryptocurrency companies and FTX's noncompliance with institutions' due diligence and licensing requirements.⁷⁵ SBF chose to not have FTX or Alameda properly registered or comply with the regulatory requirements of licensure, instead choosing to use customers' Alameda trading accounts to process FTX customer deposits and withdrawals.⁷⁶ Furthermore, SBF defrauded FTX customers by misappropriating their deposits and using these deposits to pay Alameda expenses and debts and to make investments, later using Alameda funds to pay "an approximately \$45 million hole in [FTX] customer assets" resulting from the initial misappropriation of their assets.⁷⁷ Throughout SBF's ordeal, the Government and the court exhibited great intolerance to those who chose to engage in financial crime, regardless of who the person was, or the infancy of a new business outlet.⁷⁸

The Government is doing all that it can to combat the illicit use of virtual currencies. Federal agencies tasked with investigating and

74. See Press Release, U.S. Att'y's Off., S.D.N.Y., Samuel Bankman-Fried Sentenced to 25 Years In Prison (Mar. 28, 2024) [hereinafter *Bankman-Fried Sentencing*], <https://www.justice.gov/usao-sdny/pr/samuel-bankman-fried-sentenced-25-years-prison> [<https://perma.cc/K9FP-KR3M>] ("Bankman-Fried was previously found guilty on . . . one count of conspiracy to commit money laundering . . ."); see also Superseding Indictment, United States v. Bankman-Fried, No. S5 22 Cr. 673 (LAK), 2023 WL 3021304 (S.D.N.Y. Mar. 28, 2023) [hereinafter *Superseding Indictment*] (delineating that initially the Government indicted SBF for, among other things, conspiracy to operate an unlicensed money transmitting business and conspiracy to commit money laundering but the Government did not end up moving forward with the unlicensed money transmitting charge).

75. See *Superseding Indictment*, *supra* note 74, at ¶¶ 14, 16-17.

76. *Id.* at ¶17.

77. *Id.* at ¶¶ 7, 22, 67, 94 ("Alameda commingled FTX customer funds with Alameda assets in Alameda accounts[,] . . . took money from [FTX customer] accounts, . . . [and] spent billions of dollars of those FTX customer funds . . . to finance Alameda's trading and expenses, . . . venture investments[,] . . . and to bankroll tens of millions of dollars in campaign contributions made in the names of individuals but in fact funded from Alameda accounts.").

78. See *Bankman-Fried Sentencing*, *supra* note 74 ("Today's sentence . . . is an important message to others who might be tempted to engage in financial crimes that justice will be swift, and the consequences will be severe. . . . Anyone who believes they can hide their financial crimes behind wealth and power, or behind a shiny new thing they claim no one else is smart enough to understand, should think twice. . . . The FBI will remain relentless in [their] efforts to [pursue and hold accountable] perpetrators of fraud . . .").

prosecuting cases involving virtual currency include the Drug Enforcement Administration (DEA), the Federal Bureau of Investigation (FBI), the Department of Homeland Security (DHS), and the Department of the Treasury.⁷⁹ Furthermore, banking and securities regulators oversee financial institutions' compliance with AML and the BSA and law enforcement use these regulators' data to uncover criminal activity.⁸⁰

Since "many virtual currency transactions are permanently recorded on public blockchains," law enforcement has used blockchain analytics to investigate and uncover criminal activity.⁸¹ Unfortunately, this is not always effective due to privacy technology, nonetheless, allowing criminals to hide their movement of funds and the financial institutions that are not in compliance with AML and BSA safeguards.⁸²

The United States Government Accountability Office (GAO) recommended to FinCEN and the Internal Revenue Service (IRS) that they review the Money Services Business (MSB) registration requirements for virtual currency exchanges and administrators operating virtual currency ATM's and suggested a requirement that ATM operators submit the locations and physical addresses of their virtual currency ATM's upon MSB registration.⁸³ FinCEN has also issued guidance for financial institutions to proactively detect trafficking activity involving virtual currencies (and convertible virtual currencies (CVC)) through identifying

79. *Challenges for Federal Law Enforcement*, *supra* note 65 ("Federal data indicate that virtual currencies . . . are increasingly being used in illegal activities The use of virtual currencies has added to the challenges federal law enforcement face when trying to prevent and discover [illegal activity].").

80. *Id.* ("In 2016, DHS's Immigration and Customs Enforcement's Homeland Security Investigations [Unit] and the Secret Service identified and seized \$1.2 million from a trafficker's virtual currency wallet. In 2020, an investigation by [the Department of the] Treasury's Internal Revenue Service Cyber Crime Unit helped shut down Helix, a dark web platform that laundered money for drug traffickers.").

81. *Id.* (specifying that blockchain analytic "tools use machine-learning algorithms to analyze behavioral patterns, interpret information on public blockchain ledgers, and create large databases of transactions that help identify payments associated with specific virtual currency wallets").

82. *See id.*; *see also* U.S. GOV'T ACCOUNTABILITY OFF., GAO-22-105101, *TRAFFICKING: USE OF ONLINE MARKETPLACES AND VIRTUAL CURRENCIES IN DRUG AND HUMAN TRAFFICKING* (2022).

83. *See* U.S. GOV'T ACCOUNTABILITY OFF., GAO-22-105462, *VIRTUAL CURRENCIES: ADDITIONAL INFORMATION COULD IMPROVE FEDERAL AGENCY EFFORTS TO COUNTER HUMAN AND DRUG TRAFFICKING* (2022) (explaining that the IRS adopted and implemented the Recommendation and that FinCEN is implementing the Recommendation as part of a larger effort to implement the requirements of the Anti-Money Laundering Act of 2020 and addressing the registration process for virtual currency exchanges and ATMs).

virtual currency abuse typologies⁸⁴ and “red flags”⁸⁵ associated with the identified typologies that financial institutions should be on the lookout for.⁸⁶ With research, recommendations from federal agencies specializing in the financial realm, and learning over time, law enforcement can continue to effectively go to bat with dangerous criminal organizations laundering their proceeds.

III. Due Diligence in High-Risk Jurisdictions

A. Knowing What the Customer is “Really Up To” in Jurisdictions With Poor or No AML Safeguards

A common-sense premise in every line of business and life in general is that you should know who you are dealing with. For financial institutions, specifically banks that deal on an international scale in “high risk” jurisdictions, “know your customer” is paramount to protection from involvement in criminal organizations’ money laundering activities.⁸⁷

84. See generally *FIN-2019-A003, Advisory on Illicit Activity Involving Convertible Virtual Currency* U.S. TREASURY, FIN. CRIMES ENF’T NETWORK 1 (May 9, 2019), <https://www.fincen.gov/sites/default/files/advisory/2019-05-10/FinCEN%20Advisory%20CVC%20FINAL%20508.pdf#:~:text=The%20Financial%20Crimes%20Enforcement%20Network%20%28FinCEN%29%20is%20issuing,foreign-located%20Money%20Service%20Businesses%20%28MSBs%29%2C%20and%20CVC%20kiosks> [<https://perma.cc/GW8G-3FH6>] (identifying virtual currency abuse typologies to include darknet marketplaces selling illicit goods and services only purchasable by virtual currency, unregistered peer-to-peer exchangers of virtual currencies, unregistered foreign-located MSB’s, and crypto ATM’s)

85. *Id.* at 8-9 (noting that red flags indicating illicit activity with virtual currency include, among many others, transactions conducted with CVC addresses linked to darknet marketplaces, a customer’s contact information linked to a known CVC peer-to-peer virtual currency exchange platform, a customer utilizing an unregistered CVC exchanger or foreign located MSB in a high risk jurisdiction lacking basic AML safeguards, a customer operating CVC kiosks in locations with a high incidence of criminal activity, or multiple rapid transactions between virtual currencies with unrelated purposes, which could be “attempts to break the chain of custody” with funds that may be illicit).

86. Press Release, U.S. Treasury, Fin. Crimes Enf’t Network, New FinCEN Guidance Affirms Its Longstanding Regulatory Framework for Virtual Currencies and a New FinCEN Advisory Warns of Threats Posed by Virtual Currency Misuse (May 9, 2019), <https://www.fincen.gov/news/news-releases/new-fincen-guidance-affirms-its-longstanding-regulatory-framework-virtual> [<https://perma.cc/4QFV-A28X>].

87. Press Release, U.S. Treas., Fin. Crimes Enf’t Network, Financial Action Task Force Identifies Jurisdictions with Anti-Money Laundering and Combating the Financing of Terrorism and Counter-Proliferation Deficiencies (Nov. 3, 2023),

Ultimately, for an unlawful enterprise to remain afloat, “criminals must be able to hide, move, and access [their] illicit proceeds.”⁸⁸ Thus, the question begs: if a foreign financial institution does not adequately “know” its own customer, how can U.S. financial institutions that have correspondent relationships with foreign banks be expected to “know” whom they are really dealing with?

The Financial Action Task Force (FATF) is the global “watchdog” setting international standards to tackle the harm that violent criminal activities, fizzling from criminal organizations’ laundering of illicit proceeds, cause to society.⁸⁹ The FATF classifies high-risk jurisdictions as those with “significant strategic deficiencies” in their efforts to counter money laundering and financing of criminal organizations and calls on “high risk” identified countries “to apply enhanced due diligence, and in the most serious cases, . . . apply counter-measures to protect the international financial system from the ongoing money laundering, terrorist financing, and proliferation financing (ML/TF/PF) risks emanating from the country.”⁹⁰ The jurisdictions currently listed as “high-risk”⁹¹ by the FATF include the Democratic People’s Republic of

<https://www.fincen.gov/news/news-releases/financial-action-task-force-identifies-jurisdictions-anti-money-laundering-and-5#:~:text=As%20a%20general%20matter,%20FinCEN%20advises%20U.S.%20financial%20institutions%20to> [<https://perma.cc/H6U9-K3K8>] (stating generally, U.S. financial institutions should “apply enhanced due diligence when maintaining correspondent accounts for foreign banks operating under a banking license issued by a country designated by an intergovernmental group or organization of which the United States is a member, as noncooperative with respect to international anti-money laundering principles or procedures, and with which designation the U.S. representative to the group or organization concurs”).

88. *Combating Illicit Financing by Anonymous Shell Companies Through the Collection of Beneficial Ownership Information: Hearing Before the U.S. S. Comm. On Banking, Housing, and Urb. Affs.*, 116th Cong. (2019) (statement of Steven M. D’Antuono, Acting Deputy Assistant Dir.: Crim. Investigative Div., Fed. Bureau of Investigation, Dep’t of Just.).

89. *See Declaration of the Ministers of the Financial Action Task Force*, FIN. ACTION TASK FORCE, at para. 1 (Apr. 18, 2024), <https://www.fatf-gafi.org/en/the-fatf/ministerial-declarations.html> [<https://perma.cc/7PQQ-XMS2>]; *see also Global Partnership*, *supra* note 7, at 846.

90. *High-Risk Jurisdictions Subject to a Call for Action – 21 February 2020*, FIN. ACTION TASK FORCE (Feb. 21, 2020), <https://www.fatf-gafi.org/en/publications/high-risk-and-other-monitored-jurisdictions/documents/call-for-action-february-2020.html> [<https://perma.cc/36KC-QFY8>].

91. The FATF’s list of countries identified as “high-risk” is often externally referred to as the “black list.”

Korea, Iran, and Myanmar.⁹² The FATF does give grace to jurisdictions “actively working” with them in addressing “strategic deficiencies” within agreed timeframes, placing these jurisdictions under “increased monitoring.”⁹³

Financial institutions in “high-risk” areas do not truly “know” their customers. U.S. banks with corresponding accounts in jurisdictions lacking the AML safeguards on par with the U.S. face elevated risks of stepping into an area they want no part of: facilitating the money laundering activities of dangerous criminal organizations. Indeed, when a bank fails to assess AML risks associated with correspondent banks originating from jurisdictions with dismal safeguards addressing links to criminal financing, a precarious situation in this regard is bound to come to fruition exposing the U.S. financial system to major AML vulnerabilities.⁹⁴ Financial institutions must be proactive with AML precautions and in responding to “red flags,” instead of merely placing a potential issue to the side. A financial institution whose AML program fails to conduct due diligence on affiliates before opening correspondent accounts on their behalf; is backlogged with suspicious activity alerts; fails

92. *High-Risk Jurisdictions Subject to a Call for Action – February 2024*, FIN. ACTION TASK FORCE (Feb. 23, 2024), <https://www.fatf-gafi.org/en/publications/High-risk-and-other-monitored-jurisdictions/Call-for-action-february-2024.html> [https://perma.cc/94QN-ZF4L].

93. *Jurisdictions Under Increased Monitoring – 23 February 2024*, FIN. ACTION TASK FORCE (Feb. 23, 2024), <https://www.fatf-gafi.org/en/publications/High-risk-and-other-monitored-jurisdictions/Increased-monitoring-february-2024.html> [https://perma.cc/VKZ7-SWSE] (elaborating that the FATF’s list of countries under “increased monitoring” is “often externally referred to as the ‘grey list’”). Jurisdictions currently subjected to “increased monitoring” by the FATF include Bulgaria, Burkina Faso, Cameroon, Croatia, Democratic Republic of Congo, Haiti, Jamaica, Kenya, Mali, Mozambique, Namibia, Nigeria, Philippines, Senegal, South Africa, South Sudan, Syria, Tanzania, Turkey, Vietnam, and Yemen.

94. See STAFF OF THE PERMANENT S. SUBCOMM. ON INVESTIGATIONS, THE COMM. ON HOMELAND SEC. AND GOV’T AFF’S, 112 CONG., U.S. VULNERABILITIES TO MONEY LAUNDERING, DRUGS, AND TERRORIST FINANCING: HSBC CASE HISTORY 2, 10 (COMM. PRINT 2012), [https://www.hsgac.senate.gov/wp-content/uploads/imo/media/doc/PSI%20REPORT-HSBC%20CASE%20HISTORY%20\(9.6\).pdf](https://www.hsgac.senate.gov/wp-content/uploads/imo/media/doc/PSI%20REPORT-HSBC%20CASE%20HISTORY%20(9.6).pdf) (“Correspondent accounts continue to provide a gateway into the U.S. financial system, and wrongdoers continue to abuse that entryway. . . . HSBC is the quintessential global bank, operating hundreds of affiliates in 80 countries, with its U.S. affiliate acting as the gateway into the U.S. financial system for the entire network. The [Office of the Comptroller of the Currency] allowed AML problems at [HSBC USA] to build up until they represented major AML vulnerabilities for the United States.”).

to file SARs with the Government; and is poorly staffed, led, and monitored does not pass muster for an effective AML program and surely will not keep the institution from falling into the criminal underworld.⁹⁵

B. Recent Improvements of AML Enforcement

The Anti-Money Laundering Act of 2020 (AML 2020) entailed sweeping expansion of AML regulations and revisions to the BSA. In the process, AML 2020 streamlined and modernized AML and BSA requirements and improved the “coordination and cooperation” among federal and state AML law enforcement agencies.⁹⁶ Furthermore, AML 2020 granted the Secretary of the Treasury authority to require financial institutions to “maintain appropriate procedures” in their AML compliance programs to not only guard against money laundering but also the “financing of terrorism, or other forms of illicit finance.”⁹⁷ Financial institutions can also enter into “collaborative arrangements” to pool their AML resources to better comply with BSA’s compliance requirements.⁹⁸

AML 2020 shows how the law must “roll with the times” to prevent criminals from skirting past accountability with their new methods

95. See *id.* at 3 (detailing problems identified by the Office of the Comptroller of the Currency with HSBC USA’s AML program).

96. See *The Anti-Money Laundering Act of 2020 – Key Takeaways*, DAVIS POLK & WARDWELL LLP 1, 2 (Jan. 4, 2021) [hereinafter *Davis Polk*], https://www.davispolk.com/sites/default/files/2021-06/2021-01-04_the_anti_money_laundering_act_of_2020_key_takeaways.pdf [https://perma.cc/5CPP-FRN8]; see also Anti-Money Laundering Act of 2020, Pub. L. No. 116-283, div. F, title LXI, § 6112(a), 134 Stat. 4564 (2021) (“The Secretary . . . shall work with foreign counterparts . . . to promote stronger anti-money laundering frameworks and enforcement of anti-money laundering laws.”); see also Anti-Money Laundering Act of 2020 § 6103 (establishing the “FinCEN Exchange” to facilitate a “voluntary public-private information sharing partnership among law enforcement agencies, . . . financial institutions, and FinCEN to . . . effectively and efficiently combat money laundering, terrorism financing, organized crime, and other financial crimes, including by promoting innovation and technical advances in reporting . . . [and to] protect the financial system from illicit use”); see also 31 U.S.C. § 310(d) (incorporating the “FinCEN Exchange” provisions of AML 2020).

97. 31 U.S.C. § 5318(a)(2) (incorporating the “financing of terrorism” and “other forms of illicit finance” provisions of AML 2020); see also Anti-Money Laundering Act of 2020 § 6102(c)(2); see also 31 U.S.C. § 5318(a)(2) (incorporating the “financing of terrorism” and “other forms of illicit finance” provisions of AML 2020).

98. 31 U.S.C. § 5318(p)(1) (“Sharing of Compliance Resources” as called for by AML 2020); see also Anti-Money Laundering Act of 2020 § 6213(a).

pursuant to increased technology.⁹⁹ The Act expanded the BSA's definition of "financial institution" to include persons and businesses that exchange and transmit "currency, funds, or value that substitutes for currency."¹⁰⁰ The Act also increased law enforcement's ability to protect the U.S. financial system from corrupt international financial institutions, granting federal law enforcement agencies the power to subpoena international financial institutions that maintain a correspondent account in the U.S. and request records relating to either the correspondent account or the foreign institution's accounts outside of the U.S.¹⁰¹ Furthermore, if a foreign bank fails to comply with a subpoena issued by the U.S. Government, the Government may petition the district court to compel the foreign bank's compliance and the court may hold the foreign bank in contempt.¹⁰² Moreover, the Government may require the termination of the correspondent account relationship and impose severe financial penalties for the bank's noncompliance, and the Government can pull funds from the correspondent account to fulfill the bank's penalties.¹⁰³ AML 2020, while assisting law enforcement in their pursuit of stopping foreign bad actors from pervading the U.S. financial system, makes institutions, foreign and domestic, think twice before exhibiting negligence with AML safeguards allowing criminal organizations to thrive on the institution's dime.

99. *Anti-Money Laundering and Countering the Financing of Terrorism National Priorities*, U.S. TREASURY, FIN. CRIMES ENFT NETWORK, 1, 4-5 (June 30, 2021), [https://www.fincen.gov/sites/default/files/shared/AML_CFT%20Priorities%20\(June%2030%2C%202021\).pdf](https://www.fincen.gov/sites/default/files/shared/AML_CFT%20Priorities%20(June%2030%2C%202021).pdf) ("Cybercrime is a significant illicit finance threat: the size, reach, speed, and accessibility of the U.S. financial system make covered institutions attractive targets to criminals FinCEN [also] notes that . . . convertible virtual currencies . . . have grown as the currency of [choice] in a wide variety of online illicit activity.").

100. *See* Anti-Money Laundering Act of 2020 § 6102(d)(1)(B); *see also* 31 U.S.C. § 5312(a)(2) (revised definition of "financial institution" in the BSA in accord with AML 2020).

101. *See* Anti-Money Laundering Act of 2020 § 6308(a)(3)(A); *see also* 31 U.S.C. § 5318(k)(3)(A) (incorporating the expanded U.S. law enforcement subpoena powers of AML 2020).

102. *See* Anti-Money Laundering Act of 2020 § 6308(a)(3)(D); *see also* 31 U.S.C. § 5318(k)(3)(D) (Government authority to petition the district court upon non-compliance in the BSA as outlined in AML 2020).

103. *See* Anti-Money Laundering Act of 2020 § 6308(a)(3)(E)-(F); *see also* 31 U.S.C. § 5318(k)(3)(E)-(F) (Government authority to terminate correspondent relationship and impose financial penalties upon non-compliance with a subpoena in the BSA as outlined in AML 2020).

The Corporate Transparency Act (CTA),¹⁰⁴ enacted as part of AML 2020, “is intended to discourage the use of shell companies to disguise and move illicit funds” by requiring certain U.S. entities and foreign entities conducting “business in the U.S. to report beneficial ownership information to FinCEN.”¹⁰⁵ The Act requires reporting companies to provide the name, date of birth, current residential or business address, and the “unique identifying number” of an “acceptable identification document,” such as a passport or a driver’s license, of all beneficial owners and applicants of the reporting company.¹⁰⁶ FinCEN maintains this disclosed information, which remains confidential unless a court order grants law enforcement agencies the right to the information or a financial institution requests access to facilitate their cooperation with customer due diligence requirements.¹⁰⁷ Reporting companies that fail to entirely provide or accurately provide the requisite information are subject to prison time and hefty fines.¹⁰⁸

104. It is important to note that on March 1, 2024, the U.S. District Court for the Northern District of Alabama held the CTA to be unconstitutional, reasoning that it exceeded the limits of Congress’s foreign affairs, Commerce Clause, and taxing powers, while unfairly burdening small businesses by requiring them to divulge “highly sensitive information.” Although the district court’s holding places a substantial wrinkle in the validity of the CTA, the judgment does not extend beyond the plaintiffs in the case and does not tarnish the reporting regime as a whole. Thus, while things could change in the future with the CTA following the appeals process, for the time being, the CTA, as is, is still in effect. *See Nat’l Small Bus. Ass’n v. Yellen*, Case No. 5:22-cv-1448-LCB, 2024 WL 899372 (N.D. Ala. Mar. 1, 2024); *see also* Aseel Rabie et al., *Corporate Transparency Act Ruled Unconstitutional, but Scope of Judgement Is Limited*, HARV. L. SCH. F. ON CORP. GOVERNANCE (Apr. 2, 2024), <https://corpgov.law.harvard.edu/2024/04/02/corporate-transparency-act-ruled-unconstitutional-but-scope-of-judgment-is-limited/> [<https://perma.cc/VT4M-P6U6>]; *see also* Mark Friedlich, *Corporate Transparency Act Ruled Unconstitutional: What it Means for Beneficial Ownership Reporting*, WOLTERS KLUWER (Mar. 5, 2024), <https://www.wolterskluwer.com/en/expert-insights/corporate-transparency-act-ruled-unconstitutional-what-it-means-for-beneficial-ownership-reporting> [<https://perma.cc/HQ54-5M5F>].

105. *Davis Polk*, *supra* note 96, at 4; *see also* Corporate Transparency Act, Pub. L. No. 116-283, §§ 6401–6403, 134 Stat. 3388 (2021).

106. Corporate Transparency Act, Pub. L. No. 116-283, § 6403(a), 134 Stat. 3388 (2021); *see also* 31 U.S.C. § 5336(b)(2) (“Beneficial Ownership Information Reporting Requirements”).

107. Corporate Transparency Act, Pub. L. No. 116-283, § 6403(a), 134 Stat. 3388 (2021); *see also* 31 U.S.C. § 5336(c)(2)(B) (“Retention and Disclosure of Beneficial Ownership Information by FinCEN”).

108. *See also* 31 U.S.C. § 5336(h)(1), (3) (“Penalties”).

III. Conclusion

“[M]oney laundering is not a victimless crime.”¹⁰⁹ “A single fraud scheme can pose security threats to nations, cost a government or company billions of dollars, devastate families, and fuel the criminal activities of illegal arms dealers, corrupt public officials, and sex [and drug] trafficking offenders.”¹¹⁰ It is reprehensible that some financial institutions, through sheer negligence, willful blindness, and overall lack of attention to pervasive money laundering risks, have allowed criminal organizations promoting vile activities to thrive financially.¹¹¹ “Corporate citizens, no matter how big or powerful, must be held accountable for their actions.”¹¹² It’s time for financial institutions to take responsibility and step up to the AML plate.

Unfortunately, with the global world that we live in today, any quality and advancement of AML safeguards in the U.S. could turn out to be useless since the effects of other jurisdictions’ AML regulations, if any, that are not up to par with the U.S. nonetheless seep inside our borders.¹¹³ Thus, a global partnership should exist between countries, whether “high” or “low” risk, in order to understand how illegal monies are transferred across borders, improve jurisdictions’ AML safeguards to increase safety and financial integrity across the world, allow jurisdictions to gain new resources and ideas to fight against money laundering and corruption, and

109. *Global Partnership*, *supra* note 7, at 839.

110. *Id.* at 839-40 (footnotes omitted).

111. *See generally HSBC Statement of Facts*, *supra* note 60; *see also* Press Release, U.S. Att’y’s Off., S.D. Fla., Wachovia Enters into Deferred Prosecution Agreement (Mar. 17, 2010) [hereinafter *Wachovia*], <https://www.justice.gov/archive/usao/fls/PressReleases/2010/100317-02.html> [https://perma.cc/8ERW-FZQY] (elaborating, in executing a deferred prosecution agreement with Wachovia Bank, that the Bank “willfully” failed to establish an AML program and identify and report suspicious transactions, allowing more than \$420 billion in laundered financial transactions).

112. *Wachovia*, *supra* note 111.

113. Rena S. Miller, Liana W. Rosen, *U.S. Efforts to Combat Money Laundering, Terrorist Financing, and Other Illicit Financial Threats: An Overview*, CONG. RSCH. SERV. 1 (2022) <https://crsreports.congress.gov/product/pdf/IF/IF11064#:~:text=The%20United%20States%20maintains%20a%20multifaceted%20policy%20regime%20for%20tackling> (“Given the global nature of the international financial system and the transnational criminal activity that attempts to exploit it, the United States and other countries have engaged in a variety of international efforts designed to improve global AML responses and build international cooperation and information sharing on AML issues . . .”).

to prevent criminal organizations from *jurisdiction shopping*.¹¹⁴

A financial institution who turns the other way to piping hot red flags in transactions gives criminal organizations “a virtual carte blanche to finance their operations” and acts as a “conduit” for money laundering.¹¹⁵

The party is over; there is no pride in a financial institution serving as the “go to” for violent and heartless criminal organizations to launder their muddled proceeds and continue to wreak havoc on society.

114. See *Global Partnership*, *supra* note 7, at 840, 853-55; see also *International Standards On Combating Money Laundering And The Financing Of Terrorism & Proliferation, The FATF Recommendations*, FIN. ACTION TASK FORCE 1, 25 (2023) <https://www.fatf-gafi.org/content/dam/fatf-gafi/recommendations/FATF%20Recommendations%202012.pdf.coredownload.inline.pdf> [<https://perma.cc/84N8-ERQX>] (“Countries should ensure that, when necessary, cooperative investigations with appropriate competent authorities in other countries take place. . . . Countries should ensure that competent authorities conducting investigations [of money laundering] are able to use a wide range of investigative techniques . . . [and] that competent authorities have timely access to a wide range of information . . .”).

115. *Wachovia*, *supra* note 111 (“Wachovia’s blatant disregard for [U.S.] banking laws gave international cocaine cartels a virtual carte blanche to finance their operations Wachovia disregarded numerous financial transactions that should have raised ‘red flags’ and caused their bank to act as a conduit to launder money.”).