HARVARD LAW SCHOOL | The Case Studies

CSP023
MAY 2020

Anti-Money Laundering and Blockchain Technology

CHUNG-CHIA HUANG AND ASHER TRANGLE

Memorandum

FROM: Director of FinCEN
TO: Junior FinCEN Lawyer
RE: Recommendations Regarding Reforming BSA/AML Compliance
DATE: January 26, 2020

Welcome to your new position as a junior attorney at FinCEN. FinCEN plays a critical role in monitoring and enforcing financial crimes involving banks and other financial institutions. The organization takes this role very seriously, and we are proactively seeking more effective ways of detecting illegal activity and fighting financial crime. Over the past year, I have been monitoring articles and suggestions regarding how to improve or reform anti-money laundering laws. As new technologies develop, a number of startups are using blockchain technology with the goal of helping financial institutions comply with U.S. anti-money laundering (AML) laws. Financial institutions are eager to test whether blockchain technology products can simultaneously improve or increase their compliance with AML laws while reducing the enormous costs associated with the current AML framework.

I want you to look into what types of reforms, if any, FinCEN should seriously consider adopting. In particular, please research the viability of new technologies, such as blockchain and/or machine learning, for changing our regulatory approach and make a recommendation as to whether FinCEN should support the adoption of such technologies for AML compliance.

Please note that there may be other data sharing systems or technologies (e.g. permissioned ledgers) that have also been mentioned with respect to increasing the efficiency of AML compliance. Include the pros and cons of adopting your recommendations. I am certain that you understand the importance of FinCEN's role in the enforcement community; we are on the front lines of fighting financial crimes and cutting off funding for terrorist organizations and terrorist attacks. Adopting new technology to help combat these crimes may be very helpful—if not imperative—in the future. However, FinCEN cannot

Written by Chung-Chia Huang and Asher Trangle under the supervision of Howell E. Jackson, James S. Reid, Jr., Professor of Law at Harvard Law School. Case development at Harvard Law School is partially funded by a grant from Dechert LLP. Cases are developed solely as the basis for class discussion. They are not intended to serve as endorsements, sources of primary data, legal advice, or illustrations of effective or ineffective management.

support the use of new technology by financial institutions if it means less-effective monitoring or enforcement.

I would like your recommendation on my desk as soon as possible. I have had our analysts compile the following primer to help bring you up to speed on these issues.

Origins of the Bank Secrecy Act and Subsequent Legislation

FinCEN is a bureau of the U.S. Department of the Treasury and is tasked with safeguarding the financial system from illicit use and combating domestic and international financial crimes, including money laundering and terrorist financing.[1] As a feature of its enforcement powers, FinCEN is the designated administrator of the Bank Secrecy Act of 1970 (BSA) and the subsequent laws enhancing and amending the BSA.[2]

The goal of the BSA compliance scheme is to encourage financial institutions to help identify the source, volume, and movement of currency flowing through those financial institutions.[3] As initially conceived, the BSA was implemented as a way to fight the drug trade in the 1970s, as drug dealers were using the financial system to divert profits from illegal operations to legitimate sources.[4] To combat this money laundering, authorities sought to "follow the money" and establish a paper trail of all customer transactions in an effort to make it far more difficult for drug dealers to launder profits.[5] To accomplish this, the BSA established recordkeeping and reporting requirements like the Consumer Transaction Report (CTR) for all deposits, withdrawals, exchanges, or transfer of funds over $5,000 (since increased to $10,000).[6]

Since 1970, numerous other laws have been enacted by Congress enhancing and amending the BSA to provide FinCEN and other regulatory agencies with the most effective tools to detect and prevent money laundering and other financial crimes.[7] The Money Laundering Control Act of 1986 (MLCA) directed financial institutions to establish and maintain procedures designed to reasonably monitor and ensure compliance with the reporting and recordkeeping requirements of the BSA while imposing sanctions on financial institutions that assisted customers in laundering money.[8] Later, the Annunzio-Wylie Anti-Money Laundering Act of 1992 expanded the concept of the CTR and required financial institutions to file reports whenever they detected suspicious activity.[9] The Annunzio-Wylie Act also granted the U.S. Treasury broad authority to create AML regulations and demand reports for any violation of law or regulation.[10]

In the wake of the September 11, 2001 terrorist attacks, Congress passed the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (Patriot

1 *Mission*, FINCEN, www.fincen.gov/about/mission [perma.cc/LJX2-ARFE] (last visited Oct. 30, 2016).
2 FinCen, *History of Anti-Money Laundering Laws*, FINCEN, www.fincen.gov/history-anti-money-laundering-laws [perma.cc/Q9QL-R9FB] (last visited Oct. 30, 2016).
3 FFIEC, *Bank Secrecy Act Anti-Money Laundering Examination Manual: Introduction*, FED. FIN. INSTITUTIONS EXAMINATIONS COUNCIL, www.ffiec.gov/bsa_aml_infobase/pages_manual/OLM_002.htm [perma.cc/D99L-QUQE] (last visited Oct. 30, 2016); [hereinafter Fed. Fin. Institutions Examinations Council will be referred to as FFIEC).
4 Stavros Gadinis and Colby Mangels, *Collaborative Gatekeepers*, 73 WASH. & LEE L. REV. 797, 859 (2016) (citing Peter E. Meltzer, *Keeping Drug Money From Reaching the Wash Cycle: A Guide to the Bank Secrecy Act*, 108 BANKING L.J. 230, 231 (1991)).
5 *Id.*
6 *See* FFIEC, *supra* note 3; Gadinis & Mangels, *supra* note 4, at 859-60.
7 FinCEN, *supra* note 2.
8 *See* Money Laundering Control Act, Pub. L. No. 99-570, 100 Stat. 3207, § 1359; FFIEC, *supra* note 4; Gadinis & Mangels, *supra* note 4, at 861.
9 31 U.S.C. § 5318(g) (2012) (the Annuzio-Wiley Act's "Reporting of Suspicious Transactions" provision); Gadinis & Mangels, *supra* note 4, at 869-70.
10 Gadinis, *supra* note 4, at 869-70.

Act), which imposed striking new requirements on financial institutions as part of the broader goal to combat terrorism.[11] The Patriot Act included provisions to expand AML requirements to all financial institutions subject to U.S. regulatory jurisdiction, provide the Secretary of Treasury with the authority to impose "special measures" on financial institutions that are of "primary money-laundering concern," augment the existing BSA framework by strengthening customer identification procedures, impose a 120 hour period in which financial institutions must respond to regulatory requests for information, and improve information-sharing between financial institutions and the U.S. government.[12]

Aside from FinCEN, other federal agencies also shoulder responsibility for enforcing aspects of overall U.S. AML policy. For example, the Department of Justice (DOJ), focuses on the criminal aspect of the AML laws, investigates and brings charges against those laundering money. The DOJ not only targets natural persons who commit crimes, but also has power to investigate and prosecute financial institutions and their officers, directors, and employees.[13] Their investigations mostly lead to non-prosecution agreements or deferred-prosecution agreements. Bank regulators are also a crucial component of AML compliance schemes. Bank regulators execute examinations, whether on-site or off-site, to ensure the regulated banks are in compliance with prudential standards. On top of that, examinations would also include some AML aspects, such as whether the bank follows certain process or standards.[14]

The Current AML Compliance Regime

The current AML compliance regime has several important requirements that impose obligations on financial institutions. The key features of AML compliance include requirements that financial institutions file currency reports with the U.S. Department of the Treasury,[15] report suspicious transactions through Suspicious Activity Reports (SAR),[16] properly identify persons conducting transactions and opening bank accounts through customer identification programs (CIP—this compliance technique is commonly referred to as "know your customer" or "KYC"),[17] and maintain a paper trail by keeping appropriate records of financial transactions.[18] These features are designed to enable law enforcement and regulatory agencies to pursue investigations of criminal, tax, and regulatory violations, if warranted, and provide evidence useful in prosecuting money laundering and other financial crimes.[19]

Two of the most robust compliance mechanisms are SARs requirements (banks must detect and report any suspicious activity) and KYC requirements (banks must obtain and verify detailed information about customers when processing transactions and opening new accounts). According to Treasury regulations, the range of suspicious activities that a bank must report is broad. It first encompasses transactions involving funds that come from illegal activities or that are designed to mask illegal activities. In addition, it includes transactions that are designed to evade the BSA and its reporting requirements (such as the $10,000 CTR threshold). Finally, any other unusual activity or transactions which have no business or

[11] USA PATRIOT Act, Pub. L. No. 107-56, 115 Stat. 272 (2001), www.sec.gov/about/offices/ocie/aml/patriotact2001.pdf [perma.cc/XQR4-FYLV]; FFIEC, *supra* note 4.
[12] FFIEC, *supra* note 3.
[13] https://www.justice.gov/jm/jm-9-105000-money-laundering
[14] Interesting but not formal information. A job post of OCC hiring BSA examiner. https://careers.occ.gov/careers/explore/bank-supervision/bsa-aml/index-bsa-aml-supervision.html
[15] 31 C.F.R. §§ 1010.311 (requirements for financial institutions to report currency transactions in excess of $10,000); 1010.340 (requirements for filing a Report of International Transportation of Currency or Monetary Instruments (CMIR)); 1010.350 (requirements of reporting foreign financial accounts for each entity having a financial interest in a foreign account).
[16] *Id.* at §§ 1010.320 (SAR requirement for banks); 1025.320 (SAR requirement for insurance companies).
[17] *Id.* at §§ 1010.312 (requirement that financial institutions verify the identity of persons conducting currency transactions in excess of $10,000); 1020.320 (requirement for financial institutions to have a written Customer Identification Program).
[18] *Id.* at §§ 1010.306 (requirements that financial institutions maintain records relating to purchases of monetary instruments with currency in amounts between $3,000 and $10,000); 1010.415; 1010.420; 1010.430; 1020.410; *see also* FFIEC, *supra* note 4.
[19] FFIEC, *supra* note 3.

lawful purpose must also be reported.[20] This scheme imposes on a bank a duty to both use its judgment when it comes to detecting suspicious activity and also to explain its suspicions to the government in the SAR it files.[21]

KYC programs require that a bank verify "the identity of individuals and businesses that are account holders" and the bank must also "be familiar enough with their banking practices so that transactions that are outside the norm can be readily identified."[22] Thus, a bank must have a system installed to collect relevant information about a client's background, business purposes, and anticipated activities to make such a determination.[23]

In many ways, the AML scheme imposes greater burdens on financial institutions than the compliance regimes of other financial laws. Outside of the AML context, many other financial regulatory schemes, such as the U.S. securities laws, require financial institutions to identify problematic clients or transactions, yet only impose heavy liability if the financial institution *knowingly* or *negligently* allowed such transactions to occur.[24] Conversely, when it comes to AML, financial institutions must report customers and activities based merely on *suspicions* of misconduct.[25] Thus, financial institutions cannot be "willfully blind" when it comes to their customers or the transactions that they process.[26]

The BSA also places a heavy emphasis on the requirement that financial institutions create internal mechanisms to comply with these regimes. U.S. law sets out the "four pillars" of a BSA program that financial institutions must establish for its anti-money laundering programs, which must at a minimum include 1) development of internal policies, procedures, and controls, 2) a designated compliance officer, 3) ongoing employee training, and 4) an independent audit function to test programs.[27] A "fifth pillar" was added by the Treasury Department in May 2016 requiring banks to identify beneficial owners of legal entities which have accounts at the bank and to add risk-based customer due diligence procedures to its monitoring program.[28] Due to regulators' reliance on banks to discover and report problematic customers and transactions, any failure to comply with the AML regime results in harsh sanctions being imposed on financial institutions, with both civil and criminal penalties available to enforcement agencies.[29] In fact, a number of financial institutions have faced stiff fines not for processing suspicious transactions but because their compliance scheme or detection mechanisms were deemed insufficient.[30]

Beyond the mandatory compliance programs, there are a number of non-compulsory steps that financial institutions are encouraged to take to help the government reach its AML objectives. FinCEN has stressed to banks the importance of sharing information not only internally (within components or departments of the same institution) but also with entirely distinct financial institutions.[31] This inter-

[20] *See* 12 C.F.R. § 21.11(c); 31 C.F.R. § 1010.311; Gadinis, *supra* note 4, at 870-71; *see also* U.S. GOV'T ACCOUNTABILITY OFFICE, GAO-95-156, REPORT TO THE RANKING MINORITY MEMBER PERMANENT SUBCOMMITTEE ON INVESTIGATIONS, COMMITTEE ON GOVERNMENTAL AFFAIRS, U.S. SENATE 12 (1995), gao.gov/assets/160/155076.pdf [perma.cc/K4VN-YPLL] (listing other suspicious transactions such as customers changing the dollar amount of or cancelling transactions when informed of reporting requirements, unusually large purchases of money orders or cashier's checks, unusually large deposits, and international wire transfers).

[21] *See* Gadinis & Mangels, *supra* note 4, at 871.

[22] U.S. Gov't Accountability Office, *supra* note 18, at 12.

[23] See Bank Secrecy Act Anti-Money Laundering Examination Manual: Appendix F: Money Laundering and Terrorist Financing "Red Flags", FFIEC, www.ffiec.gov/bsa_aml_infobase/pages_manual/olm_106.htm [perma.cc/TUR6-PJVT] (last visited Oct. 30, 2016); Gadinis & Mangels, *supra* note 4, at 871 (citing 31 U.S.C. § 5318 (2012)).

[24] Gadinis & Mangels, *supra* note 4, at 801-02.

[25] *Id.* at 802.

[26] *See U.S. v. St. Michael's Credit Union*, 880 F.2d 579, 584-86 (1st Cir. 1989); *see* Gadninis & Mangels, *supra* note 35, at 873.

[27] *See* 31 U.S.C. § 5318(h) (2012).

[28] *See* 81 Fed. Reg. 29397 (May 11, 2016) (codified at 31 C.F.R. §§ 1010, 1020, 1023, 1024, 1026 (2016)) (established in the wake of the 2016 "Panama Papers" scandal).

[29] *See* 31 U.S.C. §§ 5321-22 (2012).

[30] *See* Samee Zafar, *Can Blockchain Prevent Money Laundering?*, Edgar, Dunn & Co. Mgmt. Consultants (Sept. 30, 2016), edgardunn.com/2016/09/can-blockchain-prevent-money-laundering [perma.cc/ZC4Q-WMJC] (noting the case of Standard Chartered Bank where the bank was fined $300 million because the bank had below-par AML systems and controls).

[31] FINCEN, FIN-2014-A007, ADVISORY TO U.S. FINANCIAL INSTITUTIONS ON CREATING A CULTURE OF COMPLIANCE 3, note 2 (2014), www.fincen.gov/sites/default/files/shared/FIN-2014-A007.pdf [perma.cc/EFG8-CAY6].

bank sharing mechanism was established by a Patriot Act safe-harbor provision contained in Section 314(b) that allows for financial institutions to voluntarily share information with each other to better identify and report potential money laundering or terrorist activities.[32] Voluntarily engaging in information exchange under Section 314(b) to help identify AML violations is strongly encouraged by FinCEN.[33]

Relevant Government Players

As noted above, given the iterative development of a comprehensive BSA / AML scheme over time, different federal entities have been entrusted responsibility for differing components of the overall system. Established in 1990, FinCEN has, in recent years, come to focus heavily on BSA/ AML from a lens centered on national security and antiterrorism.[34] Its stated mission is to "follow the money" and partner with law enforcement to support "the nation's foreign policy and national security objectives."[35] FinCEN could be seen as an "information conduit between financial institutions and government agencies" by collecting and storing troves of financial information provided by financial institutions for access by law enforcement agencies.[36] Given FinCEN's heavy focus on antiterrorism, it could be argued that FinCEN could be more reticent to develop or accept reformist arguments aimed at curbing compliance costs if it would result in decreased efficacy of BSA / AML outcomes. As noted later, other financial regulators (perhaps foreign analogues or other domestic entities charged with other aspects of AML / BSA) may be more attuned to potential inefficiencies in the overall scheme. Direct enforcement arising out of the information collected by FinCEN would likely be carried out by federal prosecuting agencies such as the Department of Justice. These actors may utilize the FinCEN in the course of developing their investigations or prosecuting bad actors who have violated the substance of AML laws (rather than simply being noncompliant). These actors may be less likely to interface with financial institutions or have a close working relationship such that they understand the staggering nature of compliance costs incurred under BSA / AML requirements.

Modern AML Outcomes: Mixed Results

As for the overall efficacy of AML, a 2015 article found that the current and comprehensive set of AML compliance requirements *were* effective in detecting and preventing money laundering operations and illegal financial activity.[37] Furthermore, according to Daniel Benjamin, the former National Security Council Director for Transnational Threats, some argue that the effort to disrupt terrorists' access to financial resources has been "the most successful part" of the fight against terrorism since 9/11.[38] However, some critics argue that insufficient empirical data has been collected and that no tests have been conducted to adequately examine the effectiveness of the current scheme. Therefore, the current system may not actually be the most effective.[39]

[32] USA PATRIOT Act, Pub. L. No. 107-56, 115 Stat. 307 § 314(b) (2001); 31 C.F.R. § 1010.540.
[33] FinCEN, INFORMATION SHARING BETWEEN FINANCIAL INSTITUTIONS: SECTION 314(b) FACT SHEET (2013), www.fincen.gov/sites/default/files/shared/314bfactsheet.pdf [perma.cc/32MD-8SL2].
[34] https://www.fincen.gov/what-we-do/
[35] *Id.*
[36] Jeffrey R. Boles, Financial Sector Executives As Targets for Money Laundering Liability, 52 Am. Bus. L.J. 365, 382 (2015)
[37] *See* Jimmy Yicheng Huang, *Effectiveness of US anti-money laundering regulations and HSBC case study*, 18 J. Money Laundering Control 525, 532 (2015) (using HSBC as a case study).
[38] *See* Anne L. Clunan, *The Fight against Terrorist Financing*, 121 POL. SCI. Q. 569, 569 (2006).
[39] *See generally* Lanier Saperstein, Geoffrey Sant & Michelle Ng, *The Failure of Anti–Money Laundering Regulation: Where Is The Cost-Benefit Analysis?*, 91 NOTRE DAME L. REV. 1 (2015); *see also* Zafar, *supra* note 28.

AML enforcement has become especially robust in the wake of the financial crisis. Four out of the eight largest fines against financial institutions since the Great Recession have involved AML violations.[40] Many of the most prominent global banks have faced AML sanctions since the financial crisis, including J.P. Morgan Chase, BNP Paribas, HSBC, TD Bank, Credit Suisse, and UBS.[41] Goldman Sachs is currently being investigated for allegedly aiding a fraud committed on Malaysia's 1MDB development fund and whether the investment bank violated U.S. AML laws.[42] Marking a dramatic increase in AML enforcement since 2009, financial institutions have been assessed over $12 billion in fines, penalties, and forfeitures for failure to report suspicious transactions as required by the AML regime.[43] From 2011-2015 the number of AML enforcement actions has risen 75%, and the dollar amount of penalties has increased by 431%.[44] In short, the U.S. AML regime has become a critical detection and enforcement mechanism that regulators use to hold banks accountable and to combat financial crimes.[45] However, critics of the current system posit that "regulators have been punishing the banks not because of any actual money laundering, but rather because the banks did not meet the regulators' own subjective vision of the ideal anti–money laundering or counter–terrorist financing program."[46]

The Growing Costs of AML Compliance

As noted above, the current U.S. AML regime enlists private financial institutions as gatekeepers and places monitoring and reporting requirements on banks.[47] Beyond the $12 billion fines levied on financial institutions for AML violations over the past decade, banks are facing increasing costs to meet AML compliance requirements. Banks have increased spending to adopt complex compliance systems that attempt to integrate new technologies while also dedicating entire staff members purely to compliance work.[48] For example, J.P. Morgan CEO Jamie Dimon revealed in his 2014 annual letter to shareholders that the bank had hired 8,000 new employees in 2013 to focus primarily on AML compliance and that J.P. Morgan employees had undergone 800,000 hours of compliance training.[49]

According to FinCEN's outreach report, a single large financial institution could have over 80 lines of business where each product employs its own AML compliance officer.[50] Because of this complexity, certain banks have faced added compliance costs totaling more than $4 billion annually as compared to pre-financial crisis levels.[51] These developments have led to concomitant increase in SAR reports from

---

40 Stephen Grocer, *A List of the Biggest Bank Settlements*, Moneybeat (Blog), Wall St. J. (June 23, 2014), blogs.wsj.com/moneybeat/2014/06/23/a-list-of-the-biggest-bank-settlements/s.wsj.com/moneybeat/2014/06/23/a-list-of-the-biggest- bank-settlements/; *see* Gadinis, *supra* note 4, at 801.

41 *See* Grocer, *supra* note 35; Gadinis, *supra* note 4, 801.

42 Justin Baer, Tom Wright & Bradley Hope, *Goldman Probed Over Malaysia Fund 1MDB*, WALL ST. J. (June 7, 2016).

43 U.S. Gov't Accountability Office, GAO-16-297, Financial Institutions: Fines, Penalties, and Forfeitures for Violations of Financial Crimes and Sanctions Requirements 11 (2016), gao.gov/assets/680/675987.pdf [perma.cc/36U3-GKYJ].

44 Stephen Heifetz & Evan Abrams, *Dramatic Rise in FinCEN Enforcement*, STEPTOE INTERNATIONAL COMPLIANCE (BLOG), STEPTOE & JOHNSON LLP (Oct. 11, 2016), www.steptoeinternationalcomplianceblog.com/2016/10/dramatic-rise-in-fincen-enforcement [perma.cc/3EVT-UM7U].

45 *See* Gadinis, *supra* note 4, at 801.

46 Saperstein, *supra* note 34, at 1.

47 *See generally* Gadinis, *supra* note 4.

48 *See* Gadinis, *supra* note 4, at 874-75.

49 Jamie Dimon, *Dear Fellow Shareholders*, J.P. MORGAN CHASE 21, 23 (Apr. 8, 2015), www.jpmorganchase.com/corporate/investor-relations/document/JPMC-AR2014-LetterToShareholders.pdf [perma.cc/BR6T-7Y83]; Anthony Effinger, *The Rise of the Compliance Guru—and Banker Ire*, BLOOMBERG (June 25, 2015), www.bloomberg.com/news/features/2015-06-25/compliance-is-now-calling-the-shots-and-bankers-are-bristling [perma.cc/D8RC-6GLM]; *see also* Monica Langley & Dan Fitzpatrick, *Embattled J.P. Morgan Bulks Up Oversight*, WALL ST. J., (Sep. 12, 2013).

50 FINCEN, FINANCIAL INSTITUTIONS OUTREACH INITIATIVE: REPORT ON OUTREACH TO LARGE DEPOSITORY INSTITUTIONS 5 (2009), www.fincen.gov/sites/default/files/shared/Bank_Report.pdf [perma.cc/L3M6-KVJE]; *see also* Gadinis, *supra* note 4, at 883.

51 Laura Noonan, *Banks Face Pushback Over Surging Compliance and Regulatory Costs*, FIN. TIMES (May 28, 2015), www.ft.com/content/e1323e18-0478-11e5-95ad-00144feabdc0.

approximately 50,000 in 1996 to roughly 1,800,000 in 2015.[52] It is estimated that the total spending on AML compliance alone has grown from $3.6 billion in 2008 to an estimated $10 billion annually in recent years.[53] Factoring in sanctions, financial institutions pay nearly $18 billion in AML costs annually.[54] Thus, banks are constantly looking for innovative ways to lower compliance costs without increasing their liability. However, executives are aware that regulators remain focused on compliance and any cutbacks or lapses in compliance procedures would likely be met with disapproval.[55] Beyond fines, banking executives have expressed concerns over being placed into a regulatory "penalty box" whereby *other* business activities must be curtailed or the business's ability to expand is explicitly constrained. As part of the consequences imposed on Wells Fargo for their recent fraudulent account scandal, the Fed imposed just such growth restrictions.[56] These growth restrictions could be a much greater source of concern or worry for financial institutions than the imposition of financial penalties for AML compliance breakdowns.

Sanctions Violations Penalties

In addition to AML obligations, banking entities face a number of regulatory and compliance burdens stemming from U.S. governmental sanctions imposed on foreign entities. The Treasury Department's Office of Foreign Asset control (OFAC) holds primary responsibility for implementing U.S. sanction policies. As some scholars note, "OFAC has become one of the most feared regulators of the global financial sector."[57] Recent sanctions against large multinational banks have accounted for some of the largest fines these entities have suffered.[58] In 2014, BNP Paribas paid $963 million as part of a settlement agreement with OFAC for alleged violations of U.S. sanctions laws.[59] In addition, OFAC has fined ING $619 million, HSBC $375 million and Credit Suisse nearly $500 million for sanctions violations.[60] Pressure from these types of sanctions violations fines have forced financial institutions to reexamine their relationships with correspondent banking.[61] Some of the largest fines paid by financial institutions actually stem from *sanctions* violations as opposed to AML compliance violations.

"De-risking": An Unintended Consequence of AML Compliance

A 2017 article in *The Economist* noted that the primary goal of AML laws (removing the ability of bad actors to cleanse their illicit money) could come into conflict with promoting financial inclusion as a means

---

52 *See* FinCEN, THE SAR ACTIVITY REVIEW: BY THE NUMBERS 1 (2004), www.fincen.gov/news_room/rp/files/sar_by_numb_03.pdf; [https://perma.cc/S2QL-F6HG] ; *Suspicious Activity Report Statistics*, FINCEN https://www.fincen.gov/reports/sar-stats; [https://perma.cc/GA39-48M5]; (last visited Oct. 30, 2016) (evaluating 2015 statistics).

53 WealthInsight, 2020 Foresight: The Impact of Anti-Money Laundering Regulations on Wealth Management 6 (2013), www.marketresearch.com/product/sample-7717318.pdf; [https://perma.cc/4MDV-9J83]; GOLDMAN SACHS, PROFILES IN INNOVATION: BLOCKCHAIN 71 (2016), www.the-blockchain.com/docs/Goldman-Sachs-report-Blockchain-Putting-Theory-into-Practice.pdf [perma.cc/YZ8U-2AKP].

54 Goldman Sachs, *supra* note 49, at 71.

55 *See* Noonan, *supra* note 47.

56 *See, e.g.,* Federal Reserve Board Cease-and-Desist Order in the matter of Wells Fargo & Company, Docket No. 18-007-B-HC (Feb. 2, 2018) (imposing restrictions on growth and limitations on the activities of Wells Fargo in response to widespread consumer abuses and other compliance breakdowns).

57 Wesley Laine, *OFAC, the dollar and US sanctions* (Fall 2016), (unpublished) at 11.

58 *Id.*

59 U.S. Department of the Treasury. "Treasury Reaches Largest Ever Sanctions-Related Saribas SA for $963 Million." *Treasury Reaches Largest Ever Sanctions-Related Settlement with BNP Paribas SA for $963 Million*. N.p., 30 June 2014. Web. <https://www.treasury.gov/press-center/press-releases/Pages/jl2447.aspx>

60 Laine, *supra* note 53.

61 A correspondent banking account is one used by a domestic financial institution to receive funds or make transactions from foreign banking entities.

to promote economic development.[62] So-called "de-risking" lies at the root of the problem. To decrease the chance of being fined, banks engage in de-risking—the process under which financial institutions refuse to provide services to customers labeled as a high-risk for money laundering, as computed by using the customer's personal information and geographic location.[63] *The Economist* also noted that such "de-risking" did not actually reduce the risk of financial crimes. Instead, it may actually increase the risk of those individuals becoming involved in illegal transactions by forcing them to engage in cash-based transactions and or to use unregulated financial networks (shadow banking).[64]

De-risking became a banking industry strategy primarily as a response to the heavy fines imposed by OFAC for violation of U.S. sanctions. Banking entities would stop providing their financial services "not so much as a legal decision, but rather as a risk management decision."[65] Because banks are unable to identify individual risky actors with accuracy on an efficient basis, these institutions will cut off services "on a wholesale basis" to entire countries, regions, or customers.[66] Preliminary studies show that "smaller emerging markets and developing economies in Africa, the Caribbean, Central Asia…may be the most affected."[67]

Aware of this criticism, one international consortium of regulators, the FATF, issued a supplemental guidance on how to perform KYC or customer due diligence while reducing the problem of "de-risking." The supplement proposed an initiative to support access to basic financial services and products for those who are either underserved or completely unserved. Individuals within those categories (and their transactions) would instead be subject to a less-stringent due diligence regime that could (1) exempt them from AML controls by a showing of their low-risk status; (2) subject them to a simplified due diligence program; or (3) make use of new forms of identify documentation and digital solutions.[68]

Alternative Benefits of AML Compliance

Despite AML / BSA's principal aim – countering funding for terrorism and eliminating bad actors who skirt economic sanctions – there may be other benefits that arise out of the mandatory information disclosures incumbent on financial institutions. Law enforcement officials may be alerted to otherwise unknown instances of criminal behavior through SARs. For example, the criminal investigation into Eliot Spitzer (which culminated in criminal prosecutions for some individuals for sex work) began as a result of North Fork Bank flagging activity on Spitzer's account and filing an SAR.[69] Beyond this dramatic example, law enforcement officials have noted that there may be "soft information" or other details contained in SARs that can assist with law enforcement efforts. This type of information would likely not be contained in know-your-customer or transaction-level data. Given that some criminal investigations rely on building or augmenting a case through iterative reports, it is possible that purely algorithmic ways of dealing with SARs would not be able to utilize this information optimally.

---

62 *The Economist, The unintended effects of rules aimed at stopping financial crimes (Aug. 3, 2017)*, https://www.economist.com/the-economist-explains/2017/08/03/the-unintended-effects-of-rules-aimed-at-stopping-financial-crimes.

63 *Id.*

64 *Id.*

65 Laine, *supra* note 53.

66 *Id.*

67 *Id.*

68 Financial Action Task Force, *Anti-Money Laundering and Terrorist Financing Measures and Financial Inclusion with a Supplement on Customer Due Diligence* (Nov. 2017), 2, http://www.fatf-gafi.org/media/fatf/content/images/Updated-2017-FATF-2013-Guidance.pdf.

69 *FBI Watched Spitzer Before February Incident*, THE WASHINGTON POST (Mar. 12, 2008), https://www.washingtonpost.com/wp-dyn/content/article/2008/03/11/AR2008031100380_2.html?sid=ST2008031102183

Understanding Blockchain Technology

Given high compliance costs, financial institutions are exploring the possibility of utilizing blockchain technology (specifically an online ledger) as one possible alternative to traditional compliance.[70] Blockchain technology first appeared in 2009 as the public ledger that recorded Bitcoin transactions.[71] Bitcoins are digital currency traded directly from one user to another (peer-to-peer) which means that there must be some way to verify transactions between two Bitcoin accounts so that the same Bitcoin would not be "spent" twice by the same person.[72] Because Bitcoin was conceived as a way to exchange currency outside of the traditional financial system and without use of a trusted third-party such as a bank to process the transactions, a new technology was created to solve the problems of verification and double spending.[73] This technological breakthrough was the blockchain ledger. The blockchain would replace the trusted third-party and serve as the ledger recording each transaction. It would be able to verify payment history and provide proof of the number of Bitcoins associated with each Bitcoin owner's account at any given moment.[74]

This technology functions as a distributed ledger displaying all transactions to ever occur. For Bitcoin, this blockchain ledger simultaneously exists identically on thousands of computers spread around the world ("nodes") and is made publicly available.[75] Each new Bitcoin transaction is recorded by adding another "block" to the "chain" and is then reflected on the public ledger shared by every node.[76] Despite being open and publicly available, the blockchain is counterintuitively extremely trustworthy and secure because every single node reflects the same ledger at the same time—producing a "consensus mechanism" whereby each of the nodes must be in agreement on how to update the blockchain for each transaction.[77] In this sense, it is the sheer force of thousands of computers being in agreement that makes the blockchain virtually incorruptible and a trusted, public source capable of verifying each transaction.[78] The Economist provides a helpful example:

> Let us say that Alice wants to pay Bob for services rendered. Both have Bitcoin "wallets"—software which accesses the blockchain rather as a browser accesses the web, but does not identify the user to the system. The transaction starts with Alice's wallet proposing that the blockchain be changed so as to show Alice's wallet a little emptier and Bob's a little fuller.
>
> The network goes through a number of steps to confirm this change. As the proposal propagates over the network the various nodes check, by inspecting the ledger, whether Alice actually has the Bitcoin she now wants to spend. If everything looks kosher, specialized nodes called miners will bundle Alice's proposal with other similarly reputable transactions to create a new block for the blockchain.[79]

But to make the blockchain incorruptible, each block in the chain contains a unique "hash" (a string of digits) which serves as the link between the blocks. Each block connects to the previous block on the chain

[70] *See* Yassi Bello Perez, *8 Banking Giants Embracing Bitcoin and Blockchain Tech*, COINDESK (July 27, 2015), www.coindesk.com/8-banking-giants-Bitcoin-blockchain/ [perma.cc/VX6S-F45N].
[71] *The Great Chain of Being Sure About Things*, ECONOMIST (Oct. 31, 2015), www.economist.com/news/briefing/21677228-technology-behind-Bitcoin-lets-people-who-do-not-know-or-trust-each-other-build-dependable [perma.cc/KC8S-RZ9N].
[72] *Id.*
[73] *Id.*
[74] *Id.*
[75] *Id.*
[76] *Id.*
[77] *Id.*
[78] *Id.*
[79] *Id.*

by including a copy of the previous block's hash. This is replicated all the way back to the initial block on the blockchain.[80] If any single digit is changed, it will result in a different hash for every single block—even in the earliest blocks. Thus, any tampering will necessarily cause a change to the entire chain and will be rejected.[81] As previously mentioned, the blockchain ledger's incorruptibility comes from the fact that it works from consensus—any single node that could be hacked to try to change the ledger would be rejected because it would not be in consensus with the thousands of other ledgers hosted on nodes around the world that are constantly checking for uniformity. Therefore, the only way to fraudulently alter the ledger would be to hack 51% of the nodes at the exact same time using the exact same change in a single block's hash. This is known as the "51% attack" and is thought to be virtually impossible:[82]

> Imagine that Alice changes her mind about paying Bob and tries to rewrite history so that her Bitcoin stays in her wallet. If she were a competent miner she could solve the requisite puzzle and produce a new version of the blockchain. But in the time it took her to do so, the rest of the network would have lengthened the original blockchain. And nodes always work on the longest version of the blockchain there is . . . To force the system to accept her new version Alice would need to lengthen it faster than the rest of the system was lengthening the original. Short of controlling more than half the computers—known in the jargon as a "51% attack"—that should not be possible.[83]

Thus, the true value of the blockchain lies in its use as a verified and trusted ledger.[84] Beyond Bitcoin, blockchain has a number of other potential uses because "the immutability, immediacy and transparency of information captured within a blockchain means that all necessary data can be recorded in shared ledgers and made available in near real time."[85]

Blockchain Technology and AML Compliance Costs

Because of blockchain technology's ability to present the "truth" of a transaction to all parties with access, there have been many proposals about how to best adopt blockchain to other uses. According to Julio Faura, the head of innovation at Santander Bank, "[blockchain's] distributed ledger is [a] very elegant way to solve financial problems" in the financial services industry.[86] Goldman Sachs estimates that blockchain technology for AML compliance mechanisms can save financial institutions an estimated of $3-5 billion.[87]

However, many banks remain skittish about allowing customer information to be stored in such an accessible database. This is where a closed or permissioned blockchain would be useful. While the blockchain technology underlying Bitcoin is a public ledger, the technology can also be adapted to become semi-private or "permissioned." This would allow for a policymaker to theoretically take advantage of a distributed ledger while mitigating privacy concerns by limiting access to certain designated parties.[88] A permissioned blockchain behaves in the same way as a public distributed ledger except that any entity seeking access must be validated or pre-approved.[89] Permissioned blockchains work where there is

---

80 *Id.*
81 *Id.*
82 *Id.*
83 *Id.*
84 Cliff Moyce, *How Blockchain Can Revolutionize Regulatory Compliance*, CORP. COMPLIANCE INSIGHTS (Aug. 10, 2016), corporatecomplianceinsights.com/blockchain-regulatory-compliance/ [perma.cc/D9KA-RENB].
85 *Id.*
86 Matthew Finnegan, *Why Banks Are Betting On the Blockchain - Not Bitcoin - To Transform The Financial Sector*, TECHWORLD (Aug. 4, 2016), www.techworld.com/e-commerce/why-banks-are-betting-on-blockchain-transform-financial-sector-3621840/[perma.cc/4JDK-XWRX].
87 *See* Goldman Sachs, *supra* note 49, at 71.
88 *See id.* at 10.
89 *See id*.

already an element of trust established between the participants—for instance, financial institutions that already have well-developed relationships.[90] A recent study published by Barclays Bank posited that a permissioned blockchain would be a groundbreaking innovation in the AML space by having a centralized version of the consensus-based "truth" accessible to all relevant parties.[91] Barclays believes this would create a system starkly different from the current AML regime where "every bank, government department and law firm has their own paper copy of the truth."[92] Thus, the centralized ledger could eliminate much of the duplicative work and back-and-forth processes between these entities that cause massive inefficiencies in the AML system.[93] These efficiencies are described below.

When a bank gains a new customer, a litany of due diligence requirements is triggered to ensure the customer is opening the bank account or conducting a transaction for a legitimate purpose. If information about the customer existed in a tamper-proof blockchain ledger that each financial institution could access, many costs incurred to "get to know" the customer could be avoided. [94] As an alternative to the current system, banks could access verified information about a client that is new to *that* bank based on the information pertaining to that customer produced by other financial institutions and stored on the blockchain ledger.[95] In essence, the diligence procedures performed by one bank can be piggy-backed and enhanced by other banks to comply with that bank's own internal procedures.[96] The blockchain would essentially create and store a customer's digital identity for use only by other financial institutions and regulators after the customer's identity and information has been verified once—creating for a client a "digital passport for transacting in financial services."[97] Banks could then amend existing data or upload new information about the customer to the blockchain after each new transaction or when the customer's information has been changed.[98] The blockchain's role would be to provide each institution with "proof-of-process, so all that steps are easily traceable and regulators can be confident about the veracity of the information."[99] Conversely, in the current system, it is estimated that KYC requests can take 30 to 50 days to complete satisfactorily[100] and involve duplicative work by multiple institutions. These banks have to obtain and verify copious amounts of documentation each time the same customer opens up an account with a new financial institution. Furthermore, using a blockchain for customer-related compliance processes may benefit bank customers as well. A recent study by Bain concluded that bank customers are also frustrated by the current KYC system whereby they have to provide the same documentation to different banks and wait weeks for access to a new account.[101]

Beyond reducing client on-boarding costs, blockchain technology can also assist with other AML compliance demands on a transaction-by-transaction basis. Those critical of the current AML scheme argue that the present approach encourages banks to hire excess employees and invest too much money in AML compliance despite a lack of certainty on the current regime's efficacy.[102] The current system

---

90 *See id*.
91 SIMON TAYLOR, BARCLAYS BANK PLC, BLOCKCHAIN: UNDERSTANDING THE POTENTIAL 3 (2015), www.barclayscorporate.com/content/dam/corppublic/corporate/Documents/insight/blockchain_understanding_the_potential.pdf [perma.cc/BBF7-QE58]
92 *Id.*
93 *See id.*
94 *See* Moyce, *supra* note 79.
95 *See id.*; Matthew Britton, *Could Blockchain Solve the KYC/AML Challenge?*, BCS Consulting (Sept. 29, 2016), www.bcsconsulting.com/blog/new-technology-can-enable-human-bank/ [perma.cc/FC74-7AE6].
96 *See* Moyce, *supra* note 79.
97 Britton, *supra* note 90.
98 *See id*.
99 Moyce, *supra* note 79; *see also* Britton, *supra* note 90.
100 JEREON VAN OERLE & PATRICK LEMMENS, ROBECO, DISTRIBUTED LEDGER TECHNOLOGY FOR THE FINANCIAL INDUSTRY 13 (2016), www.robeco.com/images/201605-distributed-ledger-technology-for-the-financial-industry.pdf.[perma.cc/74ND-ZJTA]
101 *See* Matthias Memminger, Mike Baxter & Edmun Lin, *You've Heard of Fintech, Get Ready for 'Regtech'*, AM. BANKER (Sept. 7, 2016), www.americanbanker.com/bankthink/youve-heard-of-fintech-get-ready-for-regtech-1091148-1.html [perma.cc/CA3W-PVZ8](noting also that "Half to three-quarters of onboarding requests never reach the final stage of account opening" wasting customers' time and effort).
102 *See* Zafar, *supra* note 28.

forces employees to comb through a financial institution's records to check whether the transactions were suspicious—with much of this process duplicated on both sides of a single transaction.[103] These critics posit that blockchain technology would allow banks on both ends of a transaction to quickly verify the credentials of all parties to a transaction.[104] Furthermore, with all of the transaction data stored and verified on the distributed ledger, it may be easier for banks and regulators to use algorithms to analyze and detect suspicious patterns and payments at an aggregate level.[105] This permissioned blockchain would not only hinder the ability of criminals to use financial institutions for illegal transactions, but also allow banks to fully take advantage of a Section 314(b) sharing program to immediately alert fellow institutions about suspicious activity.[106] If a bank discovers a suspicious transaction, then each bank where the customer has an account could be immediately alerted to prevent future suspicious transactions.[107] Using such a system, stakeholders would no longer receive post-hoc reports about isolated or individual transactions but would instead be able to monitor entire sets of aggregate transaction data in real time.[108]

Proponents of adopting blockchain note that regulators would also stand to benefit greatly from this technology.[109] Regulators would also be able to view each transaction posted on the blockchain as it occurs.[110] Proponents argue the blockchain would allow regulators to take a more proactive approach to analyzing suspicious transactions or patterns alongside or in tandem with banks.[111] By having more eyes on the system at any given time, the probability of detecting illegal activities likely increases, too. Thus, proponents conclude that this technology could dramatically reduce the time and effort currently spent on compliance, and, therefore, halt the growth of compliance costs while also "improving the quality, accuracy and confidence of and in the process."[112]

Financial Institutions and Start Ups Exploring Blockchain Use for KYC/AML

A number of startup companies have begun to harness the technology underlying Blockchain to build tools that could be used by banks and regulators to make compliance more efficient.[113] Some firms, such as Elliptic and Coinfirm, are using blockchain technology with an eye towards solving AML problems at financial institutions.[114] Another startup, Gem, is focused on digital identities and believes that it has potential applicability for AML compliance use in financial institutions.[115]

In addition, many established financial institutions, including Barclays, UBS, Deutsche Bank, Santander, and Bank of America,[116] are exploring ways to utilize blockchain technology either by developing their own technology or partnering with blockchain-based firms.[117] Bank of America has already applied for 15

---

103 *See id*.
104 *See id*.
105 *Id*.
106 *See id*.
107 Britton, *supra* note 90.
108 *See* Moyce, *supra* note 79; Zafar, *supra* note 28.
109 *See* Moyce, *supra* note 79.
110 *See id*.
111 *See id*.
112 *Id*.
113 *See* ACCENTURE, DISTRIBUTED CONSENSUS LEDGERS FOR PAYMENT (2015), www.accenture.com/t20151002T010405__w__/us-en/_acnmedia/Accenture/Conversion-Assets/DotCom/Documents/Global/PDF/Dualpub_22/Accenture-Banking-Distributed-consensus-ledgers-payment.pdf [perma.cc/B9EH-KSBD].
114 *See id.*; Richard Kastelein, *Coinfirm and Billon Team Up to Better Blockchain AML and Compliance*, BLOCKCHAIN NEWS (Sept. 3, 2016), www.the-blockchain.com/2016/09/03/coinfirm-billon-team-better-blockchain-aml-compliance/ [perma.cc/5JUP-UG5Y].
115 *See* Bryan Yurcan, *How Blockchain Fits into the Future of Digital Identity*, AM. BANKER (Apr. 8, 2016), www.americanbanker.com/news/bank-technology/how-blockchain-fits-into-the-future-of-digital-identity-1080345-1.html [perma.cc/U858-5EBF].
116 *See id.*; Alice Woodhouse, *Blockchain Technology Can Help Banks Beat Money-Laundering, Hong Kong Regulator Says*, S. CHINA MORNING POST (June 8, 2016), www.scmp.com/business/banking-finance/article/1969769/blockchain-technology-can-help-banks-beat-money-laundering [perma.cc/RB7L-K366].
117 *See* Finnegan, *supra* note 81.

blockchain-based patents.[118] Even IBM has entered into the KYC blockchain world by successfully testing blockchain-based KYC technology with the French banking and insurance group Crédit Mutuel Arkéa.[119]

Blockchain Technology: Enabling Money-Laundering?

Despite promising applications of blockchain technologies, certain aspects of cryptocurrencies specifically may also hinder anti-money laundering efforts. For example, to open an account with a traditional bank, a customer must provide a government-issued photo ID or other identity-verifying documents. In contrast, to create a Venmo account, a customer merely signs up using a phone number and email address.[120] In this example, this new technology may lower the barriers to accessing financial services for certain "risky" individuals and actually contribute to financial inclusion.[121] However, the anonymous nature of many of these new financial technologies could make it more difficult to detect, trace or enforce penalties for illegal transactions utilizing such technology. One other worry that some financial institutions could raise is the possibility that they could be exposed for past failures highlighted by successful newer technologies.

Regulatory Reaction

Former Comptroller of the Currency Thomas J. Curry responded positively and stated these new technologies afford ways to reduce costs and increase efficiency of AML compliance.[122] The Office of the Comptroller of the Currency is one of the U.S. financial regulatory agencies in charge of monitoring and enforcing BSA compliance for national banks. However, other financial regulators have reacted more mildly and noted some concerns. The Consumer Financial Protection Bureau has raised general concerns that vendors providing compliance-related services are too slow to adopt their technology to meet regulatory requirements.[123]

Some foreign regulators have taken a more accommodating stance regarding adopting blockchain to solve financial services compliance problems. The U.K. Financial Conduct Authority (FCA) is actively exploring potential uses of blockchain technology for financial services companies to meet U.K. AML obligations. Christopher Woolard, an executive member of the FCA Board, recently stated that the FCA is "particularly interested in exploring whether block chain technology can help firms meet know your customer or anti-money laundering requirements more efficiently and effectively," and that "we are engaged in discussions with government and industry on this issue."[124] Similarly, Benedicte Nolens, a former Senior Director at the Hong Kong Securities and Futures Commission, recently stated that blockchain has a real opportunity to address a "pretty significant inefficiency" with the current AML system by removing duplicative efforts and creating a record of all checks carried out for each client.[125] However, some foreign regulators echoed the CFTC and similarly urged caution. Nolens qualified her statements by directing financial institutions to ensure that any technology they are using is compliant with the rules as regulations can be slow to catch

[118] Woodhouse, *supra* note 111.
[119] Avi Mizrahi, *IBM Successfully Tests Blockchain KYC with France's Crédit Mutuel Arkéa*, FIN. MAGNATES (June 30, 2016, 2:53 PM), www.financemagnates.com/cryptocurrency/innovation/ibm-successfully-tests-blockchain-kyc-with-frances-credit-mutuel-arkea/ [perma.cc/FJ6E-9E4V].
[120] Venmo, How to Sign Up, https://help.venmo.com/hc/en-us/articles/209690068-How-to-Sign-Up
[121] World Bank, FinTech and Financial Inclusion, http://pubdocs.worldbank.org/en/877721478111918039/breakout-DigiFinance-McConaghy-Fintech.pdf
[122] *See* Katie Wechsler & Zachary Luck, *The Federal FinTech Promised Land*, 19 Fintech L. Rep. 2 (August 2016).
[123] *See id*.
[124] Christopher Woolard, Fin. Conduct Authority Dir. of Strategy and Competition, Speech at the FCA UK FinTech: Regulating for Innovation Conference (Feb. 22, 2016), www.fca.org.uk/news/speeches/uk-fintech-regulating-innovation [perma.cc/AN5B-ZCD9].
[125] Woodhouse, *supra* note 111.

up to innovative technology.[126] The Bank of England, England's central bank, noted with respect to blockchain technology that "[f]urther research would also be required into how digital identity management could be achieved while balancing privacy considerations."[127]

Most U.S. regulators are thus far taking a somewhat measured approach when it comes to blockchain technology, which has led some commentators to state that regulatory acceptance faces an "uphill battle."[128] At a recent conference, David Mills, Assistant Director of Operations and Payment Systems at the Federal Reserve, noted that there were a number of risks associated with the use of such technology. He cautioned that we need to "understand the limits of rich information and the tradeoff over the privacy of individuals . . . [w]e need to strike a balance between the two."[129] Mills also sympathized with the notion that there appears to be a lack of consensus among the regulators with respect to blockchain technology but said regulators are eager to learn more about it.[130]

Finally, while FinCEN has not officially weighed in on using blockchain for AML compliance, a 2015 FinCEN enforcement case against a blockchain company may provide insight into the thinking at one point in the past. Ripple Labs was a startup that used blockchain technology to process and settle transactions between financial institutions. According to the company, "Ripple solutions lower[ed] the total cost of settlement by enabling banks to transact directly, instantly and with certainty of settlement."[131] However, FinCEN stated Ripple violated AML requirements.[132] Ripple was given a $700,000 fine—a significant blow for a startup company—and ordered to enhance its AML compliance across its platform.[133] Many industry observers opined that FinCEN's enforcement action had the potential to create a chilling effect on bank partnerships with blockchain-based companies.[134] While Ripple's use of blockchain was not intended as an AML compliance tool, this enforcement action still illustrates the difficulties that banks face when adopting new and uncertain technology.[135]

Conclusion and Instructions

The director of FinCEN would, above all, like to hear your recommendation about (1) potential reforms that could improve the current AML compliance scheme; and (2) specifically, whether blockchain (or other technologies) should be seriously considered as one possible solution to AML compliance costs. Please also note that financial institutions will be hesitant to adopt the technology without it first being approved by regulatory bodies.[136] Please also consider how your proposed reform fits into the current liability regime. In addition, please acknowledge how issues over privacy, security, or financial inclusion issues may affect your answers.

Please consider the following questions when creating your presentation:

---

126 *Id*.
127 BANK OF ENG., OPEN BANK RESEARCH AGENDA 31 (2015), www.bankofengland.co.uk/research/Documents/onebank/discussion.pdf [perma.cc/N2BE-S5ZG].
128 Henry Engler, *Blockchain Faces Maze of Regulatory Complexities, Questions and Challenges*, Thomson Reuters (Feb. 23, 2016), blogs.thomsonreuters.com/answerson/blockchain-faces-maze-of-u-s-regulatory-complexities-questions-and-challenges/ [perma.cc/F6EN-8GM2].
129 *Id*.
130 *Id*.
131 *Company*, RIPPLE (last visited Oct. 30, 2016), ripple.com/company [perma.cc/76ZW-FV64].
132 *See* Sarah Todd & Ian McKendry, *What Ripple's FinCEN Fine Means for the Digital Currency Industry*, AM. BANKER (May 6, 2015), www.americanbanker.com/news/bank-technology/what-ripples-fincen-fine-means-for-the-digital-currency-industry-1074195-1.html [perma.cc/YQP9-AXE3].
133 *See id*.
134 *See id*.
135 *See* Goldman Sachs, *supra* note 49, at 77.
136 *See id*.

- Does the Academic Proposal (specifically, Sections 3 and 5) in Appendix I provide a satisfactory solution to fix the problems of the current regime?
    - Concretely, would you recommend that FinCEN or some governmental agency create a centralized CDD agency? If so, should it be controlled or run by (a) the government; (b) an industry group; (c) financial institutions themselves; or (d) some other "gatekeeper" or regulator?
    - Should legislative or administrative actors modify the current liability regime?
    - Should the standards for due diligence be changed in any way?

- If a centralized shared database is adopted, what would be the scope of the information shared and how would this new system apportion liability amongst responsible actors (which could potentially include FinCEN itself)?
    - Relatedly, what sets of information that financial institutions hold ought to be shared (or put into a centralized database)? What are the merits or drawbacks of more or less information being stored in such a system?

- How might other current technological developments apart from Blockchain affect your judgment on the proposed reform? Are those other technologies or modifications to a pure blockchain approach (e.g., permissioned ledgers, machine learning, etc.) that could serve either as complements to or substitutes for the proposed reforms contained in the Appendix materials?

Appendix I

ACADEMIC PROPOSALS

1. EXECUTIVE SUMMARY

(1) The current AML regime forces regulated entities to incur huge compliance costs, yet seemingly generates unsatisfactory results.

(2) Two potential reasons that the regime may generate low quality of information could be (a) that the system incentivizes defensive filing, and (b) pushes customers outside the legal banking sector due to "de-risking."

(3) This proposal suggests that policymakers adopt an act-based liability regime for violations of Customer Due Diligence ("CDD") requirements.

(4) Entities that fail to file Suspicious Activity Reports ("SARs") should be held strictly liable for these errors to prevent inefficient outcomes.

(5) Blockchain technology both enables money-laundering schemes via cryptocurrencies but may also provide tools, such as a distributed-ledger system, which could strengthen AML programs by increasing information sharing.

(6) Relatedly, this proposal suggests that CDD should be conducted centrally to reduce costs stemming from redundancies, either by a formal governmental agency or by a distributed blockchain ledger.

(7) A private cause of action holding banks liable to customers for SAR-related delays should be introduced to decrease defensive filing of SARs.

2. BACKGROUND

2.1. Theoretical Foundations of AML Law

Economics are one possible framework that can be used (and is used in this proposal) to analyze motivations leading to criminal behavior. According to famous economist Gary S. Becker, criminals commit crimes when the expected return of committing a crime outweighs its expected sanction (probability of imposition of penalties multiplied by the magnitude of actual sanctions).[137] As a result, it is intuitive to combat crime by diminishing potential or proceeds from committing a crime and/or by imposing sufficient penalties on people.

In microeconomic terms, laundering money provides criminals with a means to convert their illegal funds into legal funds that increase their purchasing power by virtue of its higher purchasing power.[138] Because illegal funds cannot directly be used for investment or consumption, they only store "potential" purchasing power, whereas funds that have been laundered and are now legal *can* be spent directly, and

[137] *See* Gary Becker, *Crime and Punishment: An Economic Approach*, 76 J. POL. ECON. 169, 183 (1968).
[138] Donato Masciandaro, *Economics of Money Laundering: A Primer*, 2 (Paolo Baffi Ctr. Bocconi Univ. Working Paper No. 171), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=970184, [reader may require academic or account access].

now contains "actual" purchasing power. Even absent anti-money laundering laws, criminals may still have difficulties publicly spending their cash. In addition, criminal organizations need to wash their illicit income to escape potential detection and confiscation.

Two separate events that affect the ultimate end result for the criminal must be analyzed. First, the criminal must decide whether to launder their money. If they decide to engage in money laundering, a second event determines the outcome–whether law enforcement will detect the laundering.[139] Laundering money provides a potential benefit to the criminal who can now reinvest illicit profits into lawful, profitable activities. The cost to the criminal of the laundering is the increased probability of detection as well as an additional sanction for the laundering activity itself. This model predicts that money laundering is positively associated with the amount of illicit gain, together with the relative profitability of money that is reinvested in other profitable activities, as compared to the lesser profitability of dirty money. Money laundering is negatively associated with the risk of detection of the crime, the severity of sanctions, and costs incurred at the first money laundering stage.[140] To combat money laundering, governments should increase the probability of detection, impose higher sanctions, and increase costs faced by money launderers. Anti-money laundering is necessary to prevent criminal activity from flourishing because of the increased value of newly cleansed money.

In most circumstances, however, money laundering is not performed by the same criminals who committed the underlying crime, but instead is performed by "professional money launderers." The separation of the role of money-laundering from the role of committing an underlying criminal act effectively professionalizes the business of money-laundering. The model must account for the interaction between criminals and money launderers.[141] Thus, the model ought to be expanded into a three-stage model by adding a "bargain process" between criminals and money launderers.[142] Now, the model contains three important stages that all affect the outcome for the criminal actor: (1) the decision to launder (or not); (2) how the proceeds will be allocated between the criminal and the launderer; and (3) whether law enforcement catches the illegal laundering. The expansion of the model also introduces two new variables that must be considered: (1) actions that deter *money launderers*, separate and apart from the criminal who committed the initial crime, and (2) the probability of detection of money laundering processes. Both deterrents have a negative effect on money laundering.[143] However, the latter has a weaker effect than the former because it has more of an impact on distribution of gains between criminals and money launderers, rather than the total amount of money laundering gains.[144]

This microeconomic model also has macroeconomic implications. From a macroeconomic perspective, all illicit gains can be spent in three ways: (1) consumption, (2) investment in the illegal sector, or (3) investment in the legal sector. Unless the actor who received illicit gains chooses to consume those gains, the wealth accumulated must be laundered at least once. The model predicts, therefore, that without some other actor stopping money laundering, criminals can continually accumulate wealth by laundering and reinvesting. This model indicates that the only way to stop such a cycle is to enact laws that increases the cost of money-laundering to the criminals or money launderers.

139 Masciandaro, *infra* note 18, at 9.
140 *Id.* at16.
141 Killian J. McCarthy et al., *Modeling the money launderer: Microtheoretical Arguments on Anti-Money Laundering Policy*, 43 INT'L REVIEW L. & ECON., 148, 149-150 (2011), [reader may require academic or account access].
142 *Id.* at 151-152.
143 *Id.* at 151.
144 *Id.* at 154.

The models introduced above have rationalized the current anti-money laundering law regime. On top of criminal deterrence, which is shouldered by traditional criminal law, there are two prongs of anti-money laundering laws—criminalization and regulation. On one hand, the government criminalizes money laundering, which is devoted to deterring professional money launderers as well as increasing the severity of sanctions. On the other hand, the government sets rules for financial institutions and delegates reporting obligations to them for detecting suspicious transactions. The regulation of financial institutions increases the cost of money laundering and enhances the probability of detection.

2.2. The Functioning of AML Laws

As introduced above, it may pay to impose sanctions only on financial institutions which have facilitated the money laundering process. These sanctions would increase the cost of laundering money for the individual customers that launder money. However, it would require financial institutions to report too many suspicious transactions.

According to Becker's theory, a rational, risk-neutral wrongdoer with unlimited-assets is indifferent to any combination of detection probability and expected sanction so long as the multiple of those factors remains the same. However, the cost of any given combination has different outcomes for a law enforcement agency. This is because the financial costs incurred by law enforcement to slightly increase the chances of detection (e.g., investment in more employees reviewing transactions) is higher than a marginal increase in fines or penalties that would be imposed on criminals for laundering money. This disparity between the costs of two methods of reducing the amount of money laundering implies that the state should maximize financial penalties that launderers would suffer in order to save on costs of having to invest in alternative and burdensome methods that increase the probability of detection.[145] Essentially, it is a better payoff for the government to simply increase the fines for money laundering as opposed to increase its spending on detection mechanisms, given that these are both ways that the government can reduce the amount of money laundering that a rational actor would undertake. However, in the real world, a rational actor can have limited assets and may be quite risk-averse. The former feature introduces the judgment-proof problem and the cost of imprisonment, and the latter generates unwanted overdeterrence.[146] Both features, combined with the concern of marginal deterrence,[147] make the high-sanction-low-probability combination less appealing. Hence, this model suggests that policymakers must (and inevitably will) focus on enhancing the chances of detection rather than simply increasing penalties.

Because the investment in enhancing the probability of detection is necessary, the state should shift its focus on how to increase detection at the lowest cost. One solution is to introduce a gatekeeper into the regulatory regime in an effort to improve the likelihood of detection at a lower cost. This would be successful if the gatekeeper has more information or ability than the State. In order for the information-sharing performed by the gatekeeper to be economically efficient, that gatekeeper must satisfy four conditions (as outlined by Professor Kraakman): (1) efficacy, (2) cost, (3) comparative advantage, and (4) private enforcement incentives.[148] Today, private-sector gatekeepers are common in our legal system,

[145] *Id.*
[146] *See generally,* STEVEN SHAVELL, FOUNDATIONS OF ECONOMIC ANALYSIS OF LAW (2004).
[147] *Id.*
[148] Reinier H. Kraakman, *The Anatomy of a Third-Party Enforcement Strategy*, 2 J. L. ECON. & ORG. 53, 57 (1986).

such as corporations in the context of corporate crime[149] or professionals in the context of initial public offerings.[150]

Banks and other reporting entities not only fit the aforementioned requirements of efficient gatekeepers, but may be better gatekeepers. The first two advantages arise out of the fact that banks must report transactions merely based on suspicion, rather than based on some higher standard such as negligence or knowledge. Given that banks are unlikely to have invested much into any particular transaction at the time at which they analyze a transaction for being "suspicious," they may have less of an incentive to finalize that transaction. In addition, if banks must have a high level of information and subjective intent in order to be liable for a failure to report suspicious activity, that could create a perverse incentive whereby banks may refuse to examine transactions in order to avoid ever obtaining the amount of information that could make them liable for failures to report illegal transactions. Instead, having a very low reporting threshold based on mere suspicion, instead of knowledge or negligence, can mitigate perverse effects that prevent banks from knowing details of transactions to escape from their liability.[151] Finally, the immunity granted to institutions that simply report suspicious activity provides certain ex-ante incentives that encourage banks to share and collaborate on information.[152] In sum, banks as gatekeepers are not only efficient in generating information at a lower cost for the law enforcement, but are "collaborative" ones who may have superior incentives to share information as compared to other potential gatekeepers.

2.3. International Actions and Recent Development

The rigorous development of international trade and the resulting capital liquidity around the world has called for global collaboration on enacting and enforcing AML laws. As a response, the G-7 countries formed the Financial Action Task Force (FATF)[153] which issued 40 Recommendations which comprise a framework of measures which countries should implement to combat money laundering and other ills. Some Recommendations imposed the gatekeeper liability on banks and other financial institutions for failing to conduct CDD or file SARs to combat laundering.[154]

The FATF and similar regional bodies such as the Asia/Pacific Group (APG) regularly conduct mutual evaluations of member state financial institutions which include on-site visits. If a member state is found to have incomplete or unsatisfactory compliance with certain international standards, then that member state will be put on a watchlist and risks negative consequences. Even though member states try to achieve full compliance, the cost-effectiveness of programs said to meet the full compliance level is unknown. The compliance program has incurred glaring social costs, the burden of has fallen on banks and society.[155] Fearing harsh penalties,[156] banks either withdraw their business from high-risk areas

[149] *See generally* Jennifer Arlen & Reinier Kraakman, *Controlling Corporate Misconduct: An Analysis of Corporate Liability Regimes*, 72 N.Y.U. L. REV. 687 (1997); A. Mitchell Polinsky & Steven Shavell, *Should Employees be Subject to Fines and Imprisonment Given the Existence of Corporate Liability?*, 13 INT'L REV. L. & ECON. 239 (1993); Alan O. Sykes, *The Economics of Vicarious Liability*, 93 YALE L. REV. 1231 (1984); Lewis Kornhauser, *An Economic Analysis of the Choice Between Enterprise and Personal Liability for Accident,* 70 CAL. L. REV., 1345 (1982).

[150] *See e.g.*, John C. Coffee, Jr., *Gatekeeper Failure and Reform: The Challenge of Fashioning Relevant Reforms*, 84 B.U. L. REV. 301, 301-364 (2004).

[151] *Id.* at 802-803.

[152] *Id.* at 841-843.

[153] Fin. Action Task Force (FATF), *Who We Are*, http://www.fatf-gafi.org/about/ (last visited:03/31/2019).

[154] Fin. Action Task Force (FATF), *The 40 Recommendations*, 2004, http://www.fatf-gafi.org/media/fatf/documents/FATF%20Standards%20-%2040%20Recommendations%20rc.pdf (last visited:03/31/2019).

[155] Martin Gill & Geoff Taylor, *Preventing Money Laundering or Obstructing Business? Financial Companies' perspectives on 'Know Your Customer' Procedures*, 44 BRIT. J. CRIM. 582, 582-594 (2004) (showing the banking industry's reaction to know-your-customer program).

[156] n 2018, an aggregate of $771.26 million in BSA/AML monetary penalties were assessed against 13 financial institutions. *See* BankersOnline*, BSA-AML Civil Money Penalties*, https://www.bankersonline.com/penalty/penalty-type/bsa-aml-civil-money-

(called "de-risking") or invest more in compliance.[157] De-risking leaves those unbanked to suffer from less access to banking service and forces them to use the shadow banking system.[158] The limited access to legitimate banking service, together with the proliferation of shadow banking, burdens society with high social costs. Alternatively to de-risking, banks are forced to invest an unprecedentedly high amount of money in AML compliance.[159]

These costs appear unjustifiable given studies which show the limited effectiveness of the current AML regime. First, the estimated amount of laundered dirty money has remained 2-5% of global GDP per year since 1998,[160] which suggests that AML efforts have had minimal impact. Second, more than half of the FATF member states receive low evaluation scores on the tests of CDD (Recommendation 10) and SARs (Recommendation 20).[161] The low scores likely indicate the standard is unachievable because banks have already invested heavily in compliance efforts. Both unsatisfactory outcomes call for a thorough investigation of the current AML regime.

3. PROBLEMS

Banks have far more knowledge and information than governmental regulators regarding bank customers and their money flows. This advantage should put banks in a better position to detect suspicious activities. According to the model above, the current regime is inefficient because of a number of problems, including but not limited to high compliance costs and expenses, the low quality of available information, draconian penalties for non-compliance, and decreased financial inclusion of unbanked or under-banked populations.

3.1. High Compliance Costs

To comply with AML standards, banks must conduct both customer due diligence (CDD) and process and file suspicious activity reports (SARs), both very costly requirements. For example, to conduct CDD, banks must hire and train more front-line staff to collect documents provided by customers as well as verify their accuracy. Moreover, the AML regimes not only require basic *first-time* due diligence but an *ongoing* CDD process for all customers. In addition, enhanced CDD processes must be created for specific customers who present a higher risk of potential money-laundering activities, such as politicians and their relatives.

SAR filing imposes another significant cost on banks. There are far more transactions that occur than the number of customers a bank serves. Moreover, the information regarding transactions is more monotonic

penalties (last visited:03/31/2019).

[157] Fin. Action Task Force (FATF), *FATF Clarifies Risk-Based Approach: Case-By-Case, Not Wholesale De-Risking* (23/12/2014), http://www.fatf-gafi.org/documents/news/rba-and-de-risking.html (last visited: 03/31/2019); Fin. Action Task Force (FATF), *Anti-Money Laundering and Terrorist Financing Measures and Financial Inclusion* (11/2017), http://www.fatf-gafi.org/media/fatf/content/images/Updated-2017-FATF-2013-Guidance.pdf (last visited: 03/31/2019).

[158] Fin. Action Task Force (FATF), *FATF Clarifies Risk-Based Approach: Case-By-Case, Not Wholesale De-Risking* (23/12/2014), http://www.fatf-gafi.org/documents/news/rba-and-de-risking.html.

[159] KYC360, *Anti-Money Laundering Compliance Costs Hit $25 Billion Annually–Study* (10/16/2018), https://kyc360.com/news/anti-money-laundering-compliance-costs-u-s-financial-services-firms-25-billion-annually-study/; LexisNexis, *The True Cost of Anti-Money Laundering Compliance–European Edition* (09/2017), https://risk.lexisnexis.com/global/-/media/files/corporations-and-non-profits/research/true-cost-of-aml-compliance-europe-survey-report-pdf.pdf (last visited: 03/31/2019). (estimating the U.S. banks have invested more than $25 billion and the European banks are investing more than $83.2 billion in AML compliance), [reader may require academic or account access].

[160] U.N. OFF. DRUGS & CRIME, MONEY LAUNDERING AND GLOBALIZATION, https://www.unodc.org/unodc/en/money-laundering/globalization.html (last visited: 03/31/2019); Michael Camdessus, *Money Laundering: the Importance of International Countermeasures* (02/10/1998), https://www.imf.org/en/News/Articles/2015/09/28/04/53/sp021098 (last visited: 03/31/2019); *See* also Ali Alkaabi, George Mohay, Adrian McCullagh & Nicholas Chantler, *A Comparative Analysis of the Extent of Money Laundering in Australia, UAE, UK and the USA*, SSRN 3 (2010) (summarizing and tabulating previous estimations from 1995 to 2009), https://ssrn.com/abstract=1539843, [reader may require academic or account access].

[161] Fin. Action Task Force (FATF), *Consolidated Table of Assessment Ratings*, FATF (03/01/2019), http://www.fatf-gafi.org/media/fatf/documents/4th-Round-Ratings.pdf (last visited: 03/31/2019).

and computerized. Hence, it is less practical to analyze this kind of information by human effort. Modern technologies and algorithms can perform these analyses, but the required technology is expensive and specialized. Banks either purchase software from outside vendors or develop their own systems; both approaches require considerable investment and constitute large financial burdens for small depository institutions, such as saving and loan companies or local credit unions. These smaller institutions may not even fully exploit the advantage of "big data" while paying a similar price.

3.2. Low Quality Information

Banks, when collecting information on behalf of law enforcement, generate information that is of minimal value. This occurs for two reasons. First, it is objectively true that the current AML compliance regime cannot possibly completely identify all money launderers or identify (and prosecute) all illegal transactions. Facing considerable amounts of information, it is neither practical nor cost-effective for banks to catch all money launderers. Moreover, money launderers are sophisticated actors constantly attempting to circumvent banks' practice and secure their illegal proceeds. Banks may be able to ascertain some patterns which money launderers are likely to follow, and use those to identify customers or transactions that match such patterns. However, those patterns may not adequately characterize all money laundering methods and sometimes mistakenly capture legal transactions. Such obstacles are external limits on the quality of information generated by banks.

The combination of a legal standard of "suspicion" coupled with immunity for banks subjectively disincentivizes financial institutions to improve information quality. The suspicion standard is a double-edged sword. On one hand, it permits banks to report transactions, without certainty of their illegality which results in the transmission of more information to law enforcement.[162] On the other hand, it may reduce the value of information within SARs. The financial regulator has a limited capacity to review all reports and now receives even more information from banks, which may dilute the value of information received. Banks may even be incentivized to file defensive reports, not only to evade liability stemming from alleged failures to report,[163] but also to lower the probability of being detected by law enforcement.

3.3. Draconian Penalties

High penalties may also lead to inefficient AML outcomes. Generally, to achieve optimal deterrence, the law enforcement agency sanction or penalty should be adjusted for the probability of law enforcement detection and imposition of the sanction, such that the expected sanction is equal to the amount of social harm created. In the context of AML, the penalties that could be imposed on banks to induce them to collaborate on AML should match the social harm this collaborative effort would have been able to deter. In an ideal world, simply setting penalties at an extremely high level because rational players always behave optimally when the *expected* sanction is set equal to the harm created.

In the real world, however, federal agencies have imperfect information. They may miscalculate the amount of harm or the probability of detection by law enforcement. This could cause them to set the sanction at a level that is above the optimal sanction amount. In a fault-based regime, such a scenario could lead to either over- or under-enforcement when a law enforcement agency fails to observe real behavior (or receive perfect information) and erroneously finds a bank negligent. This failure to observe real behavior forces banks to take rational, but socially undesirable, actions to hedge against this

[162] Gadinis, *supra* note 4, 802.
[163] Előd Takáts, *A Theory of "Crying Wolf": The Economics of Money Laundering Enforcement*, 27 J. L. ECON. & ORG. 32, 59-60 (2011).

overenforcement. Banks would likely go through a heightened scrutiny process that might be inefficient or even useless only to persuade law enforcement of bank compliance. They would also file more reports to be immune from uncertain liability. The inefficiency associated with the law enforcement agency's error is exacerbated by harsh penalties. Consider the following example:

Example 1. *Let us assume that the economically efficient, or optimal investment, in CDD compliance for a bank is $10 million. The penalty imposed on noncompliant banks is $150 million with a probability of 10% that law enforcement detects the noncompliance and imposes the penalty. Thus, from the perspective of the bank, the expected cost of noncompliance (financial sanction of $150 million multiplied by the 10% probability of its imposition) is $15 million. However, the law enforcement agency is unable to perfectly estimate the bank's expenditures on compliance. Rather, they might overestimate (50% chance) or underestimate (50% chance) this figure because they do not know exactly how much money the bank will invest in its anti-money laundering procedures. The misperception is symmetric, and we will assume that their error in estimation comes out to be 30% of the actual investment in compliance. That is, when a bank actually invests $10 million in CDD compliance, it is equally probable that the government perceives their investment as $7 or $13 million.*

In the above case, if law enforcement overestimates the amount of money banks have invested in compliance, that does not lead to an inefficient outcome because law enforcement's error will not result in a sanction and will not increase the expected costs that the bank will incur. However, if law enforcement *underestimates* this figure, the bank would expect to suffer a $15 million fine. Now, the actual cost for banks is $17.5 million. The actual cost is calculated by adding the original investment of $10 million plus the potential expected sanction. The expected sanction is equal to the amount of the sanction ($150 million) multiplied by the probability of detection by law enforcement (10%) multiplied by the probability that law enforcement has underestimated the amount the bank has invested in compliance (50% or .50).

This suggests that banks may try to increase their investment in compliance to account for the possibility of law enforcement's estimation error. Now, they will invest $14.28 million (or $10 million divided by the probability of 70%). This amount of compliance is still less than the amount they would pay if they invested $10 million and were fined, however, it creates $4.28 million of dead weight loss or waste because the *optimal* amount of deterrence is $10 million, but the bank is spending an additional $4.28 million without seeing an appropriate increase in deterrence for this effort. Nevertheless, if the sanction is lowered from $150 to $120, banks would invest zero and expect to pay a $12 million penalty ($120 million multiplied by the 10% probability of imposition with no chance of estimation error by the government) which still creates waste of $2 million (although less than $4.28 million). As a result, more lenient (but still efficient) penalties can mitigate inefficient investment due to law enforcement error. In contrast, draconian penalties exacerbate the inefficiencies generated by the bank when the government is unable to accurately or perfectly estimate the bank's compliance effort.

On top of the inherent problem of interaction between harsh penalties and court error, draconian penalties are also intertwined with the second problem, low quality information. As mentioned above, when penalties are set sub-optimally high, banks are inclined to invest more in compliance programs and file more defensive reports, resulting in additional low-quality information. Even more disturbing, when more defensive reports are filed and the probability of detection is lowered because of limited resources available to law enforcement or financial crime regulators, sanctions would normally be raised to restore reduced deterrence effect. This results in a vicious cycle. As a result, the scale of penalties should be scrutinized.

Please note that the above example is replete with assumptions in order to create a more simplistic model that allows us to scrutinize the effect of large financial penalties on different actors' decisions. In reality, a number of other important factors (not considered here) play a role in the decision-making process. For example, financial institutions must decide the amount of spending on lobbying, actuarial analyses, litigation–all of which likely affect how much a given bank decides to invest into compliance with CDD measures. Likewise, regulatory bodies also have to navigate a set of interrelated decisions concerning maximizing penalties, retaining sanction funds, and securing political support for its budgetary requests.

3.4. Decreased Financial Inclusion

One last problem brought by AML enforcement is reduced financial inclusion. According to The World Bank, financial inclusion means that:

> . . . individuals and businesses have access to useful and affordable financial products and services that meet their needs – transactions, payments, savings, credit and insurance – delivered in a responsible and sustainable way. [164]

In big cities, financial inclusion is rarely an important issue. However, isolation from financial services is a pervasive and important problem for people in underdeveloped countries or rural areas in developing countries. Those excluded indirectly suffer from AML enforcement because when banks are faced with harsh penalties but have no effective way to enact compliance programs that save them from sanctions, banks will reduce the number of customers they serve based on their risk. As AML requirements get stricter, even law-abiding customers may have difficulty providing the appropriate documentation to verify their identity. While it may be easy to prove identity or verify income in countries that publicly store information (or using easy-to-access and reliable private information such as a pay stub), there are, nonetheless, cases where people lack official or privately-issued documents to support their identification (*e.g.*, self-employed farmer in Southeast Asia). When the law becomes stricter, banks abandon such customers to prevent further risk of being punished. Such abandonment is called "de-risking," which has substantially reduced financial inclusion. People who are categorized as "risky" or people who simply live in risky areas are denied access to financial services provided by banks. Such denial forces them to use informal and underregulated financial services and contributes to the growth of shadow banking. Consequently, those people are removed from regulatory oversight. It becomes more difficult for law enforcement agencies to get more information and to better combat money laundering.

3.5. Summary

The aforementioned four problems are the most significant encountered by banks or other players in the financial industry. From these problems, we can identify the three common players in any AML regime–law enforcement agencies, banks, and customers. These different players have different incentives. Law enforcement agencies wish to achieve optimal deterrence at the lowest cost. Banks seek to maximize their profit. Customers want access to inexpensive, complete and efficient financial services.

Two important issues arise from scrutinizing player behaviors. The first involves whether the players behave efficiently and, therefore, socially desirable ways. Three of the problems mentioned above are concerned with efficiency–whether banks can reduce the cost of compliance (problem 1) and produce more valuable information for law enforcement agencies (problem 2) without hindering customers'

[164] The World Bank, *Financial Inclusion: Overview,* https://www.worldbank.org/en/topic/financialinclusion/overview.

financial inclusion (problem 4).[165] These problems correspond to each players' incentives. The second issue involves distributional concerns about how costs and benefits are allocated among players. This inquiry can be insightful to further understand whether to qualify a proposal because of regressive distributive effects.

4. ANALYSIS

It is necessary to first briefly introduce liability regimes categorized by economic analysis, and apply the analysis to the bank's current AML obligations, followed by identification of the comparative advantages of banks as AML gatekeepers. Finally, the private incentives under the current regime must be addressed, including analysis of why private rational choices deviate from social optimality.

4.1. Liability Regimes and AML Compliance

There are two sections in this part. I will first introduce different types of liability regimes and then describe the circumstances in which they should be used. Next, I turn to investigate banks' compliance obligations under the current regime and what type of liability regime *should* be adopted to incentivize optimal levels of bank compliance.

4.1.1. Strict-Liability, Fault-Based, Harm-Based, and Act-Based Regimes

There are undeniably many ways to categorize different liability regimes. To be consistent with the methodology of this proposal, liability regimes are approached from the perspective of economic analysis. Professor Steven Shavell categorizes liability regimes in a 2x2 matrix along two axes: (1) the alternatives of harm-based and act-based on one axis, and (2) fault-based and strict-liability on the other axis.[166]

The difference between the entries on the vertical, first axis is based on when the liability attaches. A harm-based regime is characterized if the liability of the wrongdoer attaches *when the harm is created*. Alternatively, an act-based regime is characterized if the liability of the wrongdoer attaches just *after the misconduct occurs*.

The difference between the entries on the horizontal, second axis is the **condition of imposition of sanction**. A fault-based regime is governed by whether the misconduct is "desirable," that is, the gain of such misconduct outweighs the created harm. Alternatively, a strict-liability regime exists where the sanction is always imposed when harm is created by misconduct.[167]

The four types of regimes are shown below:

Table 1: Liability Regimes

	Strict Liability	**Fault-Based**

[165] Draconian penalties are not necessarily problematic. In fact, Becker's model implies that the higher the penalties are, the lower the probability of detection can be, which saves more resources. Hence, draconian penalties are not the core problem which must be addressed address, but resulting *effects* of such penalties resulting from errors made in fault-based regime. Accordingly, therefore, this Academic Proposal will focus on how best to mitigate the detrimental effect of such penalties instead of simply lowering the level of penalties.
[166] SHAVELL, *supra* note 10, at 474-479.
[167] *Id.*

Harm-Based	*e.g.*, felony murder	*e.g.*, negligent homicide
Act-Based	*e.g.*, safety regulation	*e.g.*, criminal attempt

Harm-Based Strict Liability. The regime of harm-based strict liability requires the lowest level of information for the law enforcement agency. The law enforcement agency need only know the level of harm in order to impose a sanction. However, because the actual sanction is always larger or at least equal to the harm (which requires a higher level of assets), the deterrence effect may be diluted. Additionally, the administrative cost of imposing sanctions is higher than fault-based regime because the sanction is unconditionally imposed whenever the harm is caused and known to the law enforcement agency.[168]

Harm-Based / Fault-Based Liability. In contrast, when the fault-based regime is employed, the law enforcement agency not only needs to know the level of actual harm, but also needs to know the likelihood of harm and the benefit to the wrongdoer from the misconduct, to determine whether the misconduct is "undesirable" and should be punished. However, this information is only required to decide whether to impose a sanction, but the expected sanction itself can be set above the level of actual level of harm because the sanction will not be imposed in situations where the wrongdoer is performing socially-desirable conduct. There is no chilling effect or over-deterrence associated with this higher sanction.[169] The conditional imposition of sanctions saves administrative costs, as well as enforcement costs, particularly for non-monetary sanctions.[170] However, the more demanding level of required information makes it more vulnerable to errors resulting from imperfect information. When the law enforcement agency has imperfect information and commits an error, it may over-deter and decrease desirable misconduct, incur enforcement costs and chill beneficial actions of law-abiding people. Such over-deterrence can be exacerbated by the higher-than-harm sanction. It is also possible that some undesirable misconduct is under-deterred.[171]

Act-Based Liability. In an act-based liability regime, the wrongdoer is liable immediately after the misconduct is completed. Because the harm is uncertain when the liability is imposed, the expected sanction should be set according to the *expected* harm instead of the *actual* harm. As a result, the law enforcement agency now needs to have information regarding the probability and the scale of expected harm (act-based strict liability) in addition to the gains associated with the misconduct (act-based fault-based liability).[172] Similarly, the act-based strict liability and act-based fault-based liability have the same advantages and disadvantages as their harm-based counterparts. However, the unique advantage for act-based liability is that it reduces the level of imposed sanction and therefore solves the judgment-proof problem, as well as saving enforcement costs.[173] This is the reason why act-based liability is always employed in response to misconduct that creates tremendous social harm, *e.g.*, most traditional crimes.

As described above, different liability regimes have their own merits. The application of each model is dependent on the information that the law enforcement agency has, the level of harm, the level of sanction, and the administrative and enforcement costs.

[168] *Id.* at 475.
[169] *Id.* at 466-467.
[170] *Id.* at 496-497.
[171] *Id.* at 497-499.
[172] *Id.* at 478.
[173] *Id.* at 501.

4.1.2. Banks' AML Compliance Obligations and Their Liability Regimes

General Compliance. Generally, banks have various AML compliance obligations. For example, the BSA requires financial institutions to establish an anti-money laundering program which includes (1) establishment of internal policies, procedures, and control, (2) appointment of a compliance officer, (3) ongoing employee training, and (4) an independent audit function to test the program.[174] However, only two of these requirements will be addressed—customer due diligence (CDD) and suspicious activities reports (SAR).

Customer Due Diligence. According to the Financial Crimes Enforcement Network (FinCEN), a CDD program includes four core requirements. Designated financial institutions are required to "establish and maintain written policies and procedures . . . 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;

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."[175]

The first core requirement, called a Customer Identification Program ("CIP"), generally includes the following components— (1) verification of the identity of the person seeking to open an account, (2) a maintenance record containing information collected for verification, and (3) a check of the customer's name against terrorist lists.

The second core requirement of CDD is targeted at corporate accounts and discovering a corporation's beneficial owner, which, by definition, includes individuals who either own at least a 25% of equity interest or carry significant responsibility or control.[176] This requirement prevents individuals from hiding their identity behind a corporate veil.[177]

The third core requirement, developing a risk profile of a customer, is defined by FinCEN as gathering appropriate information about a customer at the time of opening an account so as to develop a baseline against which to compare later transactions to assess whether a later transaction is suspicious. In practice, such information can include the type of the opened account, the services provided, the customer's income level, or other circumstantial facts.[178]

The last element of ongoing monitoring is an event-driven requirement to update information (as opposed to continually or periodic updates). Typically, banks are required to update a customer's profile

[174] 31 U.S.C. § 5318(h)(1)(A) – (D).
[175] Financial Crimes Enforcement Network, Information on Complying with the Customer Due Diligence (CDD) Final Rule, https://www.fincen.gov/resources/statutes-and-regulations/cdd-final-rule.
[176] Michael Levi, Federal Money Laundering Regulation: Banking, Corporate & Securities Compliance, 7A-6—7A-7 (2018).
[177] *Id.* at 7A-3.
[178] *Id*. at 6-36 – 6-37.

when they detect something relevant to reassess or reevaluation of the risk. Unexplained overseas funds transfer or significant change in the volume of customer activity can be examples.[179]

Both civil and criminal penalties may attach for violations of the above rules. For each single negligent violation of a BSA requirement, a penalty of not more than $500 may be assessed. However, for a pattern of negligent violations, an additional penalty not exceeding $50,000 can be imposed. In contrast, a willful violation can lead to penalties of up to $25,000. A separate violation is deemed to occur for each day, at each office, branch, or place of business at which a violation occurs.[180] Criminal penalties generally target individuals and can amount to $250,000 and/or imprisonment of up to five years.[181]

Suspicious Activity Reports. Financial institutions are required, at a minimum, to file SARs when an institution "knows, suspects, or has reason to suspect" that a transaction is suspicious as defined by the rule.[182] Although financial institutions enjoy discretion they remain obliged to conduct due diligence when determining whether or not the transaction is suspicious. Such due diligence includes an examination of the available facts, background, and possible purpose of the transaction.[183] Currently, financial institutions file reports to FinCEN. While there is no cost of filing, institutions incur costs in order to detect suspicious transactions and prepare reports before filing.[184] FinCEN received about 800,000 SARs in 2019.[185]

Several points are noteworthy. First, while filing immunizes financial institutions from penalties associated with SARs, institutions can still incur liability due to noncompliance with other AML components (*e.g.*, such as CDD or recordkeeping requirements).[186] Second, all information revealing the existence of SAR is confidential.[187]

Similar to the penalties associated with failure to comply with CDD rules, the violation of SAR rules leads to the possibility of both civil and criminal penalties. The former includes a $500 civil penalty for each single individual negligent violation and a penalty of up to $50,000 for a pattern of negligent activity. A willful SAR violation can lead to a civil penalty of up to $25,000 or the amount of the transaction (capped at $100,000).[188] Any person willfully violating SAR reporting requirements may suffer a fine of up to $250,000 and/or imprisonment of up to five years.[189]

Summary. According to the statute, all possible violations require (at a minimum) some level of fault (negligence) but do not require an occurrence of actual harm. Therefore, based on the categories described above, both liability regimes are act-based, fault-based liability regimes.

4.2. Bank's Comparative Advantage in Information Collection

As analyzed, the law enforcement relies on the information collected and generated by banks and other reporting entities. Many believe it is efficient to delegate such responsibility to banks due to their comparative advantages, including proximity to such information, professionality, and fewer conflicts of interest. Nevertheless, it is worth reexamining the accuracy of these claimed comparative advantages. It

[179] *Id.* at 6-37
[180] *Id.* at 7-8.
[181] *Id.* at 7-9.
[182] *Id.* at 14-19.
[183] *Id.*
[184] *Id.* at 12-3.
[185] Financial Crimes Enforcement Network, *Suspicious Activity Report Statistics (SAR Stats*), https://www.fincen.gov/reports/sar-stats.
[186] LEVI, *supra* note 40, 12-5.
[187] Id. at 14-33.
[188] *Id.* at 14-54.
[189] *Id.*

is first necessary to analyze the type of information currently collected by banks, and then analyze the areas in which banks have a comparative advantage.

Two Dimensions of Information. Under the current regime, banks collect customer-related information when conducting CDD and transaction-based information when the customer activates a transaction. Several differences can be drawn between these kinds of information. First, the timing of collection of both types of information is different. Banks usually collect customer-related information prior to building a business relationship or having accounts be opened. In contrast, financial institutions collect transaction-related information on an ongoing basis after each transaction occurs (and after the relationship has been formed). Second, the collection of customer-related information requires more effort from both banks and customers. A well-conducted CDD needs customer collaboration as well as bank verification. However, the collection of transaction-related information is relatively inexpensive and undemanding with the help of automated systems because most transactions, whether online or offline, are computerized.[190] In practice, however, modern AML compliance systems sometimes capture information that is not easily categories as either customer-related and transaction-based, for example, video archives of customer interactions. These supplemental materials have sometimes proven helpful to subsequent criminal investigations into potentially illegal conduct.

Similarly, banks are actually performing two types of actions with respect to information: collection and analysis. The bank collects the information and then analyzes it (as well as files reports where appropriate based on the analysis). The collection and analysis components of information-gathering are logically separable. For instance, a bank could turn over all collected information to a professional analysis company. The bank could also outsource its due diligence to other institutions to help verify the customer's identity.

These two dimensions of information generation create four subsets of information-generating roles: customer-related information collection, customer-related information analysis, transaction-related information collection, and transaction-related information analysis.

Interplay between CDD and SAR. The analysis of both customer-based and transaction-based information is interdependent. For example, to better detect a suspicious transaction, the bank needs to understand the customer's profile. Similarly, banks need to know the essence of planned transactions to determine the intensity of necessary customer due diligence and customer profile updates.

This interrelated relationship leads to the conclusion that the level of customer due diligence affects the accuracy of the detection of suspicious transactions. The knowledge of past or proposed transactions further determines the level of customer due diligence. For example, consider that a bank has information regarding a depositor's occupation and annual income—a custodian whose monthly salary is $3,000. That bank would be better positioned to detect the abnormality of a transaction of $500,000 in the customer's account as compared to a similar transaction in an account of high-income sports-team owner.

Similarly, banks may have different procedures for determining the suspiciousness of a small foreign exchange transaction, as compared to a million-dollar wire transfer. In one case, the bank may merely check the depositor's identification, but in the other would scrutinize carefully and require more documentation.

[190] LEVI, *supra* note 40, 12-15 – 12-16.

Interdependency as the salient feature of two-stage monitoring has rarely been mentioned in previous gatekeeper liability literature, yet it has significant implications for designing a liability regime. Specifically, when banks can be immune from liability simply by filing reports, they do not have incentives to conduct scrupulous due diligence, and the quality of their reports suffers substantially. As a result, to induce optimal investments in CDD, banks cannot be immunized from liability simply by virtue of having filed appropriate SARs.

Bank's Comparative Advantages. Even though the bank is currently obliged to shoulder all four subsets of information generation, the bank does not necessarily have a comparative advantage in creating all of them. The determinants of comparative advantage are effort, capacity, and quality. Between collection and analysis, banks are more likely to have comparative advantages in collecting as compared to analyzing information. The proximity to the information allows banks to enjoy some advantages in collecting information. For example, when collecting customer-related information, the bank employee can directly observe the document as well as the applicant's appearance. It is also inexpensive to collect transaction-related information for banks in this digital era because all transactions are stored on the computer. On the contrary, banks do not have a comparative advantage when it comes to *analyzing* the collected information. The efficacy of any AML information analysis is dependent on sample size. Sample size, in this sense, can be both cross-sectional and temporal. When the banking industry is fragmented, and each bank serves only a small group of customers, the bank is less likely to derive a meaningful result from such a small sample size of customers. Similarly, when the clientele is stable or few transactions are activated, the bank is also less likely to identify a new mode of suspicious transactions. Outsourcing the analysis to professional analysts can help aggregate the sample size and yield a more meaningful result. As a result, banks have lower comparative advantages in analyzing information.

However, even though banks seemingly have advantages in collecting information, it does not mean that the job may not be delegated or outsourced. For customer-related information, it is difficult to conclude that customer due diligence should definitely be conducted by a bank employee in the bank. However, it is undeniable that no other institutions can stand in a better position to collect transaction-related information because the primary source of information lies in the bank's system. Any other institution can never collect such information without access to the bank's system. Also, it seems absurd to require customers to "register" planned transactions before instructing banks to activate it. In short, banks have unique comparative advantages in collecting transaction-related information but replaceable comparative advantages in collecting customer-related information. When the market is fragmented, small banks ought not analyze information.

4.3. Private Incentives and Social Welfare

4.3.1. Law Enforcement Agencies

The primary purpose of law enforcement is to reduce crimes by deterring, incapacitating, and/or rehabilitating individuals. The first method takes a more ex ante perspective whereas the latter two are more grounded in ex post views. Only deterrence will be considered.

Assuming all actors are rational, criminals would perform a normal cost-benefit analysis when deciding to commit a crime. Crimes are harmful to society but beneficial to the individual wrongdoer. Accordingly, the government should punish criminals to deter them from committing socially harmful crimes. To achieve this goal, policymakers should set the expected sanction exactly equal to the generated social

harm. If wrongdoers are rational and risk-neutral, they are indifferent to any magnitude-probability combination of sanction so long as the expected sanction (*i.e.*, the amount or gravity of the sanction multiplied by probability of imposition) remains the same. While wrongdoers are indifferent, different combinations do have different implications for law enforcement. In particular, increasing financial penalties is less costly for the government than investing resources in increasing the probability of detecting wrongful activity. Doubling the financial penalty costs law enforcement little but halving the probability of its imposition requires heavy investments in investigating resources.

In the real world, monetary sanctions cannot be set extremely high for several reasons. First, wrongdoers are not infinitely rich, meaning they may be "judgement-proof" when the imposed monetary sanction is higher than their assets or income-earning ability. Limits on wrongdoers' wealth and income dilute the deterrent effect. Incarceration is one method to solve the limited-assets problem. However, when sanctions take a non-monetary (imprisonment) form, the costs to law enforcement of imposing his type of sanction increases. Unlike monetary sanctions, which merely involve wealth transfer and involve no efficiency implications, penal incarceration requires that the government construct prisons, and hire guards, etc. In addition, prisoners and their family members suffer a utility loss from these non-monetary sanctions. This makes the particular combination of a high non-monetary penalty, coupled with a low investment in detecting wrongdoing, even less appealing. Moreover, the low amount of deterrence from incarceration may provide another reason against increasing incarceration as a form of deterrence. While costly, enhancing the probability of detecting money laundering is necessary and desirable when compared with increasing the non-monetary sanction.

Assuming it is necessary and desirable to increase the probability of punishment, a system designer should attempt to minimize costs associated with such an approach. One answer is to introduce gatekeepers (banks in the AML context) or actors who are more capable of generating information required to impose a sanction. By directly observing customers' profiles and transactions, banks can access such information faster and identify abnormal patterns earlier than law enforcement. Therefore, delegation of collection and reporting of information to banks ought to reduce overall costs.

To induce banks to perform this role, policy makers must either reward banks for providing this information or punish them for noncompliance. Given the government's limited resources and budget, it would be hard to reward banks.[191] Therefore, it makes sense to punish banks for failing to comply with AML gatekeeping obligations. Law enforcement must then make two decisions— (1) setting expected sanctions on criminals for money laundering, and (2) setting expected sanctions on banks for noncompliance. As mentioned above, setting the expected sanction on criminals is constrained to a certain level of sanction based on the amount of marginal deterrence, imprisonment costs, and related probability of detection. As to setting the sanction on banks, Becker's model is again applicable. Sanctions should be monetary, and the judgment-proof issue (insufficient assets) is less likely to occur. Therefore, it would be rational for the law enforcement agency to set a higher monetary penalty and spend less money on enforcement (lower probability of imposition). Moreover, the more information law enforcement receives from banks, the easier and less expensive it is for law enforcement to apprehend criminals. They are also likely to be incentivized to set expected sanctions at too high of a level (to generate more information) because, here, law enforcement is not required to bear the cost of information generation.

[191] Unlike some whistleblower regimes, the ultimate goal of an AML regime is to punish individual criminals via imprisonment. Instead, in an SEC-type whistleblower regime, the ultimate entity on whom the sanction is imposed is a corporation whose penalty is monetary. Hence, it is viable to finance whistleblower rewards via the imposed penalties in those contexts; however, that is not possible in the AML context.

The incentive to save enforcement costs can consequently lead to draconian levels of penalties and sub-optimally high expected sanctions.

4.3.2. Banking System

In terms of incentive, banks are corporations whose primary goal is to maximize profits. To do so, banks should provide their services to the point where marginal revenue equals marginal cost. To illustrate how AML law plays a role in banks' incentives, the analysis is simplified and focuses on the business relationship between customers and banks.

On the revenue side, implementation of AML law does not have a definite effect on bank revenue. For example, it is imaginable that depositors are deterred by time-consuming verification processes and, therefore, engage in business relationships with fewer banks to reduce the time taken by verification. However, the result is that depositors will deposit their funds in fewer banks, with a different distribution of funds among the various banks, and the total amount of deposited monies will remain the same. In such a case, revenue does not necessarily decrease, however, each bank's relative market share might change. It is also possible that in some places (*e.g.*, China) people cannot live without bank accounts to either receive any wages or to use an almost exclusively electronic payment system. There, the elasticity of demand (a measure of how much demand changes in response to a change in price) can be so steep that demand for deposits would remain unchanged when AML law is implemented. It is empirically unclear how AML law affects banking institution's revenue streams.

In terms of costs, AML penalties could have potential ramifications for banks. A financial institution must choose between compliance or noncompliance. The former leads to investment in staffing, software, and programming. In concrete terms, banks need to recruit and train staff to meet AML standards. Banks would also install software and institute programs to better detect abnormal transactions. Some banks would even have to reform their organizational structure to implement best AML practices. All of these amount to massive costs. In contrast, should the bank choose not to comply, it faces harsh penalties. As a result, as a rational profit-maximizer, banks would try to strike a balance between compliance and noncompliance to minimize their expected overall expenditure. Additionally, banks would compare marginal cost and benefit for each group of customers. When a specific customer's marginal cost is higher than the marginal benefit provided to the bank, that customer would be rejected or not served by the bank. This is likely with a certain risky group of customers and is the motivating reason behind de-risking.

Under the current regime, it seems that banks trend towards choosing to comply with AML standards, as can be deduced from the fact that no banks have been repeatedly fined for the same type of fault. This high level of compliance implies that the cost of compliance is lower than the cost of expected sanctions, which means that it is inefficient and irrational to not comply. This may echo the proposition set forth in the preceding paragraph–the sanction level may not be optimal.

Compliance is desirable when the regime is well-designed, and the sanction reflects the real social cost. However, if the regime fails to account for externalities associated with compliance, it causes socially undesirable results. The current AML regime may be such an example. First, CDD obligations are not results-based, which prevents banks from obtaining information efficiently. When a customer opens several accounts at several banks, the customer is required to provide the same information and spend similar amounts of time simply to go through an identical verification process. This repetitive process is extremely inefficient. Nevertheless, because banks are threatened by harsh penalties, they care about the

bank's avoidance of penalties and not the socially optimal process. Accordingly, banks are motivated to conduct their own CDD process and deterred from using information collected by fellow banks. Secondly, SAR filing is also problematic. While setting the triggering standard for filing an SAR at the low level of "suspicion" may induce more information generation, it also invites banks to engage in defensive filing relative to normal transactions which trigger only negligible suspicion of money laundering, but which are almost certainly complaint with AML laws. Exempting banks from very high penalties, combined with the low cost of filing SARs, exacerbates such defensive filing. Defensive filing helps banks avoid huge fines but incurs huge social costs. It dilutes the information value of information provided to law enforcement. Bombarded with defensively filed reports and a limited budget, law enforcement is less capable of combating crime. To illustrate, a numerical example is provided below:

Example 2. *Suppose there are 100 transactions of which 20 are actual money-laundering-related transactions. Filing a SAR costs a bank $18, and the* ***expected*** *sanction for failure to file is $100. The law enforcement agency can handle or investigate a total of 15 cases due to budget constraints.*

Now, the banks can only identify (i.e., 100% sure) 10 out of 20 money-laundering-related transactions but are still 50% confident that the remaining 10 are also illicit money laundering. Also, it suspects (erroneously) that 25 of the remaining 80 transactions are illegal with 20% certainty.

When banks choose to file only when they are 100% certain (Scenario 1), all reports can be handled and investigated by the law enforcement agency (they would forward 10 transactions). When banks instead report solely because of a lower suspicion standard, say 50%, there are 20 transactions reported (Scenario 2). Here 15 cases will be investigated with five left untouched (but reported) by law enforcement. However, when the sanction is set high and banks file defensively, they will file 45 total reports (Scenario 3). The law enforcement agency can still only deal with 15 cases and would encounter difficulty sifting through the reports. Perhaps they will select randomly amongst the reported transactions (any random 15 of the 45). As a result, only 7 of the actual money laundering cases are investigated which is a worse outcome than both Scenarios 1 and 2. This example illustrates the banks behavioral responses to varying schemes. When expected sanction is far higher than filing costs, banks file defensively based on a low level of suspicion.

To summarize, banks weigh their private cost of compliance versus noncompliance in pursuit of profit maximization. Their ignorance of social costs incurred by their behavior should be calculated and incorporated into the AML regime to force them to internalize this cost. Concretely, we must focus on two flaws—how to encourage banks to save CDD costs without reducing information value, and how to prevent banks from engaging in defensive filing.

4.3.3. Social Welfare Implications

The preceding sections analyze how implementation of the current AML regime changes or affects different parties' incentives. To briefly review, law enforcement is motivated to impose higher sanctions on banks to induce as much information-generation as possible. Banks are attempting to escape harsh penalties and are likely over-complying (conducting CDD on their own and filing too many SARs). Facing time-consuming and laborious processes, customers may be deterred from purchasing financial services.

Although choices may be rational from the perspective of any individual party, that choice may reduce overall efficiency (socially). Law enforcement's goal is to maximize deterrence at the lowest cost. Their

choices may lead to too much information generation because they do not care whether the amount of generated information is justified by the cost absorbed by banks. The potential of financial inclusion is less relevant for law enforcement.

Secondly, requiring each bank to conduct their own CDD and preventing information sharing creates strong incentives to generate redundant information. Also, the exemption of liability by filing reports fails to force banks to internalize the cost of processing information. Hence, banks are filing too many reports. The redundant CDD process and defensive filing lead to a common result–banks are currently generating a low amount of valuable information.

Under the current regime, it is inefficient to require banks to produce redundant customer information and encourage them to file reports by fully exempting their liability. These actually decrease the value of information provided to any relevant regulatory authority. In addition, the broader concern regarding financial inclusion and regulation of shadow banking should be addressed by the government or receive more scrutiny to address these potential pitfalls of the current regime. The purpose of this proposal is to introduce and analyze a few possible reform policies to address these inefficiencies.

4.4. Summary

As demonstrated above, both CDD and SAR regimes currently operate on a fault-based liability scheme. However, under such a liability regime, the rational choices made by law enforcement and banks deviate from the socially optimal equilibrium. Law enforcement saves costs by outsourcing responsibility to conduct CDD/SAR to banks and induces information generation by imposing harsh penalties for bank noncompliance. In response, banks invest tremendous resources in compliance programs yet simultaneously file defensive reports and de-risk from particular demographic or geographic populations. Those circumstances fail to enhance deterrence and inhibit the role of banks as service providers that facilitate capitalism.[192]

5. SOLUTIONS

Based on the problems discussed above, it is necessary to propose several reform recommendations, each of which addresses the aforementioned problems. Commenting on some solutions proposed by other theorists, these recommendations are based on modifying liability regimes, encouraging information sharing, applying blockchain technology, and introducing private causes of action.

5.1. Modification of Liability Regime

5.1.1. Act-Based Liability for CDD

To optimize banks' CDD processes, an act-based liability regime should be adopted to induce the optimal level of due diligence.

Example 3. *Suppose a bank implements a CDD program that involves incurring fixed startup costs of $500 and variable costs of $10 per person. This program increases the probability of the bank being able to*

[192] *See* JOHN ARMOUR ET AL., PRINCIPLES OF FINANCIAL REGULATION 275-276 (2016).

accurately identify a suspicious transaction from 50% to 90%. In turn, the bank's program and filings increase law enforcement's chances of detecting and punishing money laundering from 20% to 50%.

For a person who commits a low-level offense of, say, extortion, the penalty will be set to $1,000. The social harm generated by this extortion crime is $500. Separately, banks will suffer a $100 penalty for failures to comply with AML laws. Further assume that there are two types of extortion criminals–100 high gain criminals whose penalty is $400 and 100 low gain criminals whose penalty is $300.

In the above example, if the bank ***does not*** implement the CDD regime, the extortion criminals face the following scenario. As a total class, they will be confronted with a $350 sanction. Here, the bank will only catch and file 50% of money laundering transactions. Separately, even if the bank fails to file a SAR, the government still has a 20% chance of catching that transaction. The sanction for this half of the money laundering transactions that flow through the bank is then 0.50 * 0.20 * $1,000 or $100. For the 50% of transactions that are caught and filed by the bank, law enforcement has a 50% chance of catching those filed transactions, meaning that the sanction for this half is 0.50 * 0.50 * $1,000 or $250. The total expected cost (or sanction) facing any person committing extortion is now $350 total. This means that the 100 high gain criminals will still commit the crimes because their expected gain outweighs the expected cost of $350. The other 100 low gain criminals will *not* engage in the criminal conduct.

However, with the help of the customer due diligence program, the expected sanction increases to $470. Now, the bank will catch 90% of transactions and, of those filed transactions, the government will catch and punish 50%. Now, for the transactions that are forwarded to law enforcement, the expected sanction is 0.90 * 0.50 * $1,000 or $450. The expected sanction for the 10% remaining, unfiled (or undetected by bank) transactions is 0.10 * 0.50 * $1,000 or $20. The total expected sanction facing the entire class of extortion criminals is now $470. All criminals are thus deterred.

The increased deterrence benefit from the CDD program is $50,000 (100 more criminals are deterred than before meaning that we can save $500 of social harm from being committed by 100 criminals for a total saved social cost of $50,000). This marginal benefit from the program outweighs the $2,500 cost incurred by implementing the CDD program ($500 + $10 * 200 total criminals). Therefore, the CDD program is socially desirable.

However, consider a harm-based liability regime where banks are ***not*** immunized from liability simply by filing suspicious reports. The bank would now face potential penalties for failing to file SARs. Rational banks must now decide whether it makes sense for them to file or not to file at all.

When a bank *files* (which happens 50% of the time), there is also a 50% chance that law enforcement discovers this crime leading to a total expected sanction of $25 (0.50 * 0.50 * $100 sanction for noncompliance with AML law). However, if the bank decides *not* to file, the total expected sanction harm will be only $20 because law enforcement only detects money laundering 20% of the time (0.20 * $100). Without immunity, rational banks will choose not to submit *any* reports, let alone incur costs to implement a CDD program.

Consider the addition of immunity to the example. Suppose filing incurs a small cost of $1 per report. Now, the bank will decide to file a report for every transaction because the bank would only have to pay $200 instead of implementing a $2,500 CDD program. However, the information value is diminished because the bank's filing of reports for *all* transactions is just as useless as not filing any reports at all.

As a result, the example illustrates how the liability regime for SAR filing affects the earlier decision regarding CDD. No matter whether immunity is granted, independent liability for CDD is desirable. Hence, an act-based liability regime should be adopted for the CDD program.

5.1.2. Strict Liability for SAR filing

Currently, SAR filing requirements are premised on fault-based liability. As discussed, fault-based liability regimes require more information, which has two implications. First, law enforcement incurs extra costs to investigate whether the failure to file met the standard of fault required for bank liability. Second, fault-based regimes incentivize banks to implement seemingly effective (but in fact inefficient) measures to pretend they are not negligent. Although banks may reduce *some* of their inefficient filing efforts due to immunity, banks may still find it rational to masquerade their behavior because it is impossible to report every transaction, and also because sanctions are fault-based and may be higher than the expected harm.

Shifting from fault-based liability to strict liability can not only save investigation costs but prevent overdeterrence stemming from errors estimating negligence and overly high sanctions. Moreover, some banks may actually refrain from introducing advanced measures because they are unrecognized by law enforcement despite their efficient or cost-effective nature. Rather, banks are forced to use inefficient measures because they are recognized by official law enforcement actors. Such inefficiency is exacerbated when the law enforcement agency has outdated knowledge about money laundering tactics or techniques.

To prevent inefficient investment in useless measures, this proposal suggests a shift from the fault-based liability to strict liability for failure to file SARs.

5.2. Encouraging Information Sharing

As discussed above, the CDD process is redundant and costly while arguably simultaneously yielding little valuable information. Therefore, policy makers should consider allowing the same information to be used by as many institutions as possible to maximize the benefit of information collection. Currently, information sharing focuses on information about "suspected customers and transactions" among financial institutions and law enforcement. The scope of shared information is rather limited and does not include all collected information.[193] This proposal argues for a broader information-sharing plan that allows more information to be used and shared by all reporting entities. This outcome could be achieved one of two ways. One method is to organize a centralized agency responsible for collecting all required customer information. Another method is a decentralized, industry-run information sharing mechanism.

5.2.1. Centralized Agency

The core problem of CDD is that each customer might engage in multiple business relationships with numerous banks or other reporting entities, and the costly and time-consuming CDD is undertaken for each, and produces similar information each time. Furthermore, when such business relationships are continuous, banks are also required to *update* the information, which is similarly repetitive and redundant. A centralized agency responsible for all front-end and follow-up information collection may be cost-saving and desirable.

[193] Levi, supra note 40, §8.

Imagine some of the transactions that a graduate might undertake—opening a checking and savings account at one bank, applying for a credit card from another, obtaining securities trading account from a broker, and applying for a loan for a new home from a lender. Many people engage in business relationships with multiple banks or reporting entities throughout their life. Under the current regime, each entity is required to conduct their own CDD—and each time incurring substantial costs. In addition, the customer must spend time collecting required documents to provide to the reporting bank or entity. However, creating a centralized agency would reduce monetary and temporal costs incurred by both regulated entities and the customer. The agency could also update a customer's profile for use by reporting entities, and the savings will increase the longer the agency is involved.

The centralized agency could be created by the government or some consortium of regulated reporting entities. Whether public or private, those subject to AML regulations can sign up as a member and pay a front-end proportional membership fee and one-time retrieval fee. The fees would go towards funding the agency and its employees. Further, to avoid distorting the price of financial services, the fee should be designed properly to reflect or approximate the real usage of information by reporting entities. For example, if a foreign money exchanger or a casino is charged the same amount as banks, that company will raise the price charged to procure their services. Demand is more inelastic for gambling or currency exchange services, meaning that customers are willing to incur the costs that would be passed onto them in these industries (as compared to banking). Thus, they are deterred from using such infrequent services provided by other entities who are charged similar fees. While the fee structure can have implications for the market, it is less problematic than the current practice because costs incurred under the current AML structure might already drive those customers out of the market. The fees charged by the centralized agency are foreseeably lower than costs incurred in the current regime. It must be determined whether the centralized agency or the reporting financial institutions should be responsible for defects or problems in the CDD process. Some would argue that the location of where the sanction is placed has no effect because monetary sanctions are always transmittable to counterparties. Therefore, it is likely that the costs of the penalties would ultimately be shared between banks and the centralized agency. However, in our case, when multiple reporting entities seek information from the centralized agency, it would be counterintuitive and indirect to impose sanctions on reporting entities.

First, the law enforcement agency should know all entities that have been asking for information about that money launderer. However, such information can only be accessed from the centralized agency. Accordingly, the law enforcement agency should obtain such information before making decisions.

Second, in terms of deterrence, the real harm from poor CDD outcomes is reduced accuracy of identification of suspicious transactions. The effectiveness of a CDD program has an impact on second-stage monitoring, because the centralized agency cannot adjust its level of scrutiny beforehand because the agency conducts the due diligence and collection and verification of information before the customer has opened a bank account. Accordingly, the agency can not foresee how many accounts the money launderer will open and what kind of service will be used. As a result, when sanctions are imposed on reporting entities, the aggregate sanction is likely to exceed optimal level and creates over-deterrence. The government may impose sanctions on multiple banks for the same failure which would create an inefficient (too punitive) outcome. It is, therefore, preferable and intuitive to impose sanctions on the centralized agency for information collection issues.

Lastly, other arguments counsel against the creation of a centralized agency. The first is whether a centralized CDD process loses a benefit inherent in multiple checks on the same customer—whether

detection of money laundering activity decreases (or launderers escape liability more easily) in the proposed central agency regime if the customer need only go through the process one time. It is more difficult to pass every CDD process at each bank. However, the missing element in this argument is the degree of similarity among different bank CDD programs. When the processes are near-identical, it is useless to conduct CDD multiple times by different banks. The result remains the same as a single bank or a centralized agency. If the processes diverge significantly, then multiple checks do create significant benefits. This issue requires empirical information to resolve. However, considering the required documents and standardized rules, it is likely that banks have substantially similar processes and each bank's additional CDD check produces little marginal benefit compared to the cost.

The second argument against a proposed centralized agency concerns privacy. Such an agency would store, control, and possibly share highly sensitive information with other reporting entities. In response, it is worth clarifying that no additional information is being collected above that collected in the current system. The difference is that in the current regime, the information is collected and possessed by different and isolated financial institutions. With the proposed centralized agency, that information would be owned by the agency and other entities that have business relationships with the customer. This requires a focus on two potential concerns—(1) the scope of released information, and (2) the diffuse or concentrated access to such information. This proposal would only impact the second of those two concerns and needs further investigation.

5.2.2. Multilateral Information Sharing Mechanisms Between Financial Institutions

Another method to encourage information sharing is to allow banks to rely on the information collected by other reporting entities. One possible iteration of this design could be a collaborative platform that allows quick and easy information sharing among industry actors that collect and rely upon AML / KYC information. The underlying rationale is similar to that underlying the creation of a centralized agency, to maximize the use of collected information and save redundant costs of information gathering. The major difference is that this proposed model has a disseminated information structure which has its own advantages and disadvantages.

A concrete explanation of this model can be illustrated as follows. First, banks are allowed to solicit information from other banks which already have a business relationship with the new customer. A customer who has a savings account at the Bank of America wishes to open a checking account at Chase. It would then be possible for Chase to solicit the customer's consent and contact Bank of America to ask for the required AML information. Now, Chase needs to perform only minimal verification to confirm the identity of the new customer to open the account. Chase saves on document collection, some verification costs, and electronic filing costs. In fact, inter-bank information sharing is not uncommon in other areas, such as credit ratings.

Nevertheless, compared to the centralized model, this model has a number of advantages. First, it can introduce market competition such that the bank that most efficiently collects and verifies customer data will be the information provider for the whole industry. Second, the scope of shared information is broader than the centralized model. Because the centralized agency itself is not a financial institution that facilitates customers' transactions, it does not possess any information regarding transactions. However, a reporting entity, such as a bank, does have information about the transaction history as well as an ongoing risk-profile regarding each of its customers. Such information can be more valuable than that

generated by a centralized agency. Moreover, the disseminated model mitigates privacy concerns to a degree.

Nevertheless, the disseminated model also comes saddled with several disadvantages. For example, the transaction cost can be high. Without collaboration of the customer, it is unlikely for the bank to know the other entities with which the customer has already transacted. Additionally, we can only rely on information flows if it moves in the direction from more credible to less credible actors. Ideally, information generated under better scrutiny processes would be used by other, less capable entities. Unlike a centralized agency as a single point of comparison or contact, a model using disparate, private actors would create difficulties in controlling the sequence of entities with which a customer transacts. If the customer first engaged with a local bank for a simple savings account and later wants to open a checking account at a big national bank, it is likely desirable that the larger entity conduct its own CDD process rather than using the CDD information obtained by the local bank. Almost definitively, the big bank is more reliable than a local saving and loan company. In such circumstances, the disseminated model might face practical problems when implemented. One other minor but unintended consequence might be that such a model can affect the market by granting those big banks comparative advantages. When all other banks rely on big banks to conduct CDD, customers are encouraged to open accounts provided by those institutions. Those big banks advantage in contacting customers and providing services.

Similar to the agency model, we must decide in the disseminated model where to impose liability for failure to conduct high quality CDD. We can either impose liability on banks that improperly *relied* on the information, or on the bank that *provided* faulty information (relying banks or provider banks). Again, if banks could pass on the costs associated with such information it makes no difference who is punished. If liability is imposed on provider banks, they will calculate a "risk premium" to reflect the increased potential costs that could be incurred from information sharing. The market enables the bank that is most capable and confident in its information quality to charge the lowest price for its provision of such information. Otherwise, relying banks that bear the cost of being sanctioned will do their best to solicit information from reliable banks that provide information. Both seem to be optimal and work well. Nevertheless, in the real world, customers might have different purposes for obtaining different types of financial services. The required information, even though largely overlapping, may vary according to the purpose. Hence, the sufficiency of information collection should be determined based on the services provided. For example, the bank providing international wire transfer service cannot merely rely on a customer profile collected by banks at which the customer only retains a checking account. Accordingly, law enforcement should be able to distinguish the difference and take corresponding actions. It is, therefore, less likely to impose sanctions on the providing banks without looking at the relying banks' practices. If the law enforcement agency failed to do so and attribute such failure to providing banks, then the flow of information will be hindered by the fear of unforeseeable and disproportionate penalties.

5.3. Applying Blockchain Technology

Separate from modifying the liability scheme and aforementioned institutional innovation, other new technologies may help complement those reform efforts.

Cryptocurrencies. Cryptocurrencies can pose serious new threats to an AML scheme.[194] Some consider cryptocurrency to be superior to both cash and other mediums of exchange within the current banking

[194] *See e.g.*, Raffaella Barone & Donato Masciandaro, *Cryptocurrency or Usury? Crime and Alternative Money Laundering Techniques* (BAFFI CAREFIN Ctr. Research Paper No. 2018-101), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3303871, [reader may require academic or account access].

system due to its transferability and anonymity. While possible, it is much more difficult and time consuming to transfer large amounts of money using cash–the core reason organized crime leaders need to launder their money.[195] However, cryptocurrency provides a similarly anonymous tool to transfer wealth at a faster pace and a lower cost. Also, compared to the conventional banking system under intensive supervision, criminals who hold cryptocurrency can transfer their wealth to other members without disclosing their identity.[196] Cryptocurrency, when treated as a closed-end system, is not meaningfully distinct from other digital assets that are unregulated (*e.g.*, online gambling currencies). All unregulated digital assets can be transferred anonymously and quickly. However, the gradual development of public recognition of cryptocurrency has transformed it into an open-end system, or one where the currency can be exchanged for fiat currency and become liquid. This process, as applied to cryptocurrency, also helps criminals to launder their money more easily. Now, criminals can use cryptocurrency as a medium when transacting illegal commodities such as drugs and weapons.[197] This medium eliminates the need for the placement stage of money laundering as conducted using normal mediums. As the public comes to recognize and use cryptocurrency as a medium, criminals can directly purchase tangible assets under legal protections afforded to cryptocurrency. The transaction of tangible assets allows the integration stage (where assets are converted into regular mediums) to be completed without governmental supervision. As a result, the existence of cryptocurrency and its widely accepted nature, can significantly facilitate money laundering.

Distributed Ledger. The blockchain technology underlying cryptocurrencies, especially a distributed ledger, can also be used to augment or complement AML compliance. Distributed ledgers allow information to be recorded and updated simultaneously in every block.[198] The distributed ledger transforms the conventional linear information flow into an information network, which ensures that every bank can know the latest status of each customer. The most noteworthy point of the distributed ledger is that a blockchain ensures the veracity of information during transmission. It is difficult, if not impossible, to hack and alter the information.[199] Therefore, from the perspective of combating crime, the distributed ledger is safer and more reliable. Adopting distributed ledger technology can enhance the efficiency of the reliance model. Each time the customer goes to *any* bank, the bank can update the customer's information. The latest collected information will then be appended to the customer information stored in other banks' databases.

The distributed ledger technology echoes the analysis of two-dimensional information. In previous sections, I focused on the information collection and concluded that customer-based information should only be collected once but transaction-based information should continue to be collected by respective banks. However, when it comes to analysis of data (rather than collection), a big data pool can generate more insights into a customer's transaction pattern and allows for better detection of abnormalities. A distributed ledger can aggregate data across all reporting entities. This model allows for all transaction information to be updated simultaneously at each bank's database for either further analysis of that transaction or to compare with future transactions.

However, it must be noted that this new technology does not solve the core problem. First, the main issue with inefficient CDD programs stems from redundant efforts to collect the same customer information. Adoption of a distributed-ledger model presumes the transferability of this information across banks.

[195] LEVI, *supra* note 40, 1-09.
[196] John W. Bagby, David Reitter & Philip Chwistek, *An Emerging Political Economy of the BlockChain: Enhancing Regulatory Opportunities*, Academy of Legal Studies in Business - National Proceedings 57 (2019).
[197] *Id.* at 26-27.
[198] *Id.* at 6.
[199] *Id.* at 7-8.

Therefore, a distributed ledger only improves the accuracy and the pace of information-sharing. The distributed ledger only improves but not alter the reliance model. While saving time and cost when transferring information exactly as collected and recorded by the bank, the distributed ledger still cannot guarantee the veracity of the information because the distributed ledger system only records and updates information collected by the bank and contains no inherent or independent truth-checking function. Accordingly, when a bank, intentionally or negligently, conducts unqualified CDD and updates the customer information, the erroneous information will be appended to the blockchain and appear accurate to other banks.

This convenient, fast technology also invites other problems. When information is updated automatically, it becomes more difficult to prevent erroneous information from polluting an error-free record. This can be a particularly acute problem when the error is already recorded in the "chain." A possible preliminary solution could be having other banks verify the information (setting aside the infeasibility of other banks verifying a transaction without their own transaction-level information). Even though they can verify such information, banks would have to collaborate to verify the updated information, which also inevitably generates redundant costs. At worst, due to free-rider problems, each information-receiving bank has insufficient incentive to correct the information and would make no effort to correct inaccuracies. From this point, the automatic nature of distributed ledger can be problematic because it does not prevent accumulation and sharing of erroneous information. In addition, the automatic nature of a distributed ledger can be problematic in terms of liability. When a system assigns liability for errors to relying banks (not providing banks), those entities can do nothing except for opting out of the distributed ledger network to escape liability. Allowing banks to opt-out undermines the system's expected effectiveness. However, insisting that banks remain in the system might degrade the quality of the information contained in the repository.

Aside from the interplay between blockchain-technology and information sharing, some other concerns could be raised. Any proposal must indicate which (and how many) actors would be involved in the distributed ledger. As the number of entities or institutions using the system increases, all parties would enjoy greater benefits from the larger amount of data generated and shared. However, there could be problems with allowing wider access to such a platform. For example, a group of malevolent individuals could set up a small money service simply to have access to the ledger and monitor when certain transactions or entities have triggered alarms or alerts within the database. Such a possibility undercuts the confidential nature of SARs– normally, SARs are not disclosed to the transacting customers. Second, if a policymaker adopted this multilateral, decentralized approach to data sharing, any proposal must decide whether FinCEN or law enforcement would be able to access the platform. On the one hand, access to the information could help facilitate resolving criminal investigations – sometimes law enforcement agencies use other information contained within the SARs to detect crimes other than money laundering itself. However, providing law enforcement with such access also brings up privacy and efficiency concerns. If FinCEN is able to review the database, would financial institutions still be required to flag suspicious activities or would they be exempt from any liability (as they are now) once they satisfactorily provide adequate information to the database? In addition, there could be separate privacy concerns given that this database would contain large amounts of personal transactional information. Now, that information is being provided to law enforcement in addition to financial institutions.

The introduction of blockchain technology aids in the quick and accurate transfer of information. However, it does not guarantee that the information input into the system is correct. To ensure the quality of information, banks would have to be able to opt-in to the distributed ledger network voluntarily to

adequately account for side effects stemming from the imposition of liability onto relying banks. In sum, distributed ledgers can only be a valuable means of transferring information (one aspect of an AML regime) instead of fully replacing the current AML model.

5.4. Introducing a Private Cause of Action

The solutions proposed in previous sections deal with modifying liability and reducing redundant costs of information generation. However, these partial solutions do not deal with the problem of defensive filing. Therefore, another solution must be proposed to combat this issue.

This problem has previously been identified and addressed by a theorist named Takáts. In his paper, he argued for increasing the cost of filing to reduce the overall total filed reports.[200] He also illustrated his solution mathematically. However, several questions can be raised in response to such a proposal. First, it is undeniable that increasing the cost of filing can reduce the number of filed reports and force banks to file only the most suspicious transactions. However, as mentioned above, when the expected sanction for a failure to report is exceptionally high and the cost of filing is comparatively negligible, it actually plays an insignificant role in reducing defensive reports. In contrast, if the filing cost is set high, it is also charged for those really suspicious reports. As a result, it is inevitably increasing the total cost of compliance for banks. The increased cost of compliance will exacerbate the problem of de-risking, which is not considered or addressed in Takáts' paper. Moreover, it is difficult to determine the optimal level of any penalties imposed in the real world. This is particularly true in the current regime where law enforcement is already incapable of reading and analyzing all reports filed and correctly identifying which are defensive. In such circumstances, the law enforcement agency is likely unable to accurately set the correct (or optimal) price of filing. Nevertheless, the concept of a higher filing cost is still illuminating. To address the problem of defensive reports, an AML regime should require collaboration from players who possess knowledge to identify which reports are defensive, and in this case, customers themselves ought to be able to verify the information.

In 2010, the British Civil Court of Appeals decided a case involving a customer, Jayesh Shah, and HSBC.[201] At issue was an SAR filed by HSBC after Mr. Shah sought to transfer money out of the country. HSBC had suspected the transaction violated AML laws and filed the SAR. In reply, Mr. Shah asked HSBC to prove the basis of their alleged suspicion. The court finally ruled that "the customer is entitled to proceed with a claim in breach of contract or duty" when the bank failed to carry out the customer's instruction due to suspicion about money-laundering connected to the transaction. This decision changed the landscape of AML regimes. Previously, bank customers could only seek judicial review to challenge decisions made by the governmental agency that had received the SARs from banks. This decision, however, addressed the lack of a private legal remedy for the delay of transactions halted by the filing of an SAR. The decision created conflicts between a bank's obligations to law enforcement under regulatory law and its duties to customers under contract law. On one hand, banks are prohibited from disclosing information regarding SAR filing. On the other hand, banks wish to avoid lawsuits brought by its customers. This case also confirmed that the defendant institution need not show that its suspicion was reasonable. Instead, the defendant institution need only show that its determination that a transaction was suspicious was not irrational.[202]

[200] Takáts, *supra* note 27.
[201] Shah v. HSBC Private Bank (UK) Ltd, 2009 WL 6454.

[202] Mikhail Reider-Gordon, *U.S. and International Anti-Money Laundering Developments*, 45 INT'L LAWYER 365, 377-378 (2011).

There are some important lessons in this case. First, it highlighted how banks face conflicting obligations to different parties. It also created an incentive for banks to take SAR filing more seriously. Additionally, it allowed another party with pertinent information to challenge the decision to file a SAR. Even though the court did not intend to address the problem of defensive filing, the decision might be helpful to mitigate such a problem.

Private parties, such as banks and their customers, may have more information and ability to effect change than the government. Governmental actors are quite removed from the transactions and only have access to information as provided by SAR reports filed by banks. Also, the resource constraint limits the government's capacity to read and process all reports filed by the reporting entities. As a result, due to the lack of information and capacity, the government does not have comparative advantage in identifying defensive reports.

Second, allowing customers to sue has other advantages. Incentivized by the damages, customers who strongly believe that the suspicion is unfounded will challenge the content of the report. However, natural separation can emerge. On one hand, a lawful customer who understands the essence of the transaction is able and willing to challenge the filed SAR so as to get compensation for damages. In addition, real money launderers will not initiate suits because bringing one will make their illicit scheme more likely to be detected. Therefore, both the ability and incentive of a lawful customer to challenge a wrongful SAR, and the worries that a money launderer would be caught by initiating suit, suggests that allowing customers to sue would be beneficial.

In detail, the final problem is the design of a regime which allows customers to sue. Conceptually, in order to keep the filing of SARs confidential, the disclosure of filing can be postponed until after the FIU's screening. When the FIU has scrutinized the report and found nothing suspicious or decided not to take action, then the release of such reports can pose little harm to investigation. Moreover, it is reasonable to limit the scope of released reports to only those that do not pass the threshold of further investigation because the filing cannot be said to be "defensive" when the FIU decides to take action after scrutiny. Once the reports have been examined and released, then the bank is allowed and mandated, in the proposed regime, to inform the customer regarding the filing. The customer can then decide to bring the lawsuit or not.

Questions remain about the possible claims. In fact, while difficult to prove the exact amount of harm, it is acceptable that harm is created by the filing itself in an information-sharing regime. When the filing is known to other financial institutions, the customer will likely have to go through a more stringent process of due diligence, and may even be discouraged from or denied certain services. Accordingly, one possible claim which would benefit the customer is the erasure of such records obtained by bringing a lawsuit. However, this proposal does not neglect the tremendous cost associated with litigation. Alternatively, a quicker and more simple way to resolve such disputes may be obtained using an electronic platform similar to those employed in cataloging customer complaints or resolving sales disputes on an online platform. Both parties would upload materials for third-party neutral arbitrators' reviews and decisions.

In fact, the proposed litigation regime is neither infeasible nor inconsistent with current rules. The current safe-harbor rule implies that the financial institutions cannot be liable to their customer for filing reports the breach of their duties to customers under contract law principles.[203] However, some contrary authority exists regarding the extent of this safe harbor provision. The statute appears to indicate (or

[203] 31 U.S.C. § 5318(g)(3)(A).

could be read as saying) that the immunity applies to all statements made in an SAR even if they are not made in good faith or based on probable cause.[204] However, some court decisions have stated that the protection applies only in the case where financial institutions have filed an SAR in good faith[205] or based on an objective identification of a possible violation of law.[206]

By introducing or encouraging the private cause of actions, banks are deterred from filing defensive reports. Compared to the filing-fee model proposed by Takáts, the probabilistic calculation of damages, combined with natural selection between lawful and unlawful customers, saves more cost without exacerbating decreased financial inclusion.

[204] LEVI, *supra* note 40, 14-51.
[205] *Lopez v. First Union Nat'l Bank of Florida*, 129 F.3d 1186, 1192–1193 (11th Cir. 1997).
[206] *Bank of Eureka Springs v. Evans*, 353 Ark. 438, 109 S.W.3d 672 (2003).

Appendices

1. Academic Proposal, 22-26 (Section 3), 38-49 (Section 5). [Compliance Costs, Liability Regime, Information Sharing, Blockchain]

2. Stavros Gadinis & Colby Mangels, *Collaborative Gatekeepers*, 73 Wash. & Lee L. Rev. 797 (2016). [Information Sharing, Liability Regime, Industry Self-Regulation]

3. The Great Chain of Being Sure About Things, The Economist (Oct. 31, 2015). [Blockchain, Distributed Ledgers]

4. Goldman Sachs, Profiles in Innovation: Blockchain 2 – 11, 71 – 7 (2016). [Compliance Costs, Blockchain]

5. Laura Noonan, Banks Face Pushback Over Surging Compliance and Regulatory Costs, Fin. Times (May 28, 2015). [Compliance Costs]

6. Matthew Britton, Could Blockchain Solve the KYC/AML Challenge?, BCS Consulting (Sept. 29, 2016). [Compliance Costs, Blockchain, Distributed Ledgers, Network Effects, Digital Identities]
7. Henry Engler, Blockchain Faces Maze of Regulatory Complexities, Questions and Challenges, Thomson Reuters (Feb. 23, 2016). [Blockchain, Centralized Agency]

8. FCA New Technologies and Anti-Money Laundering Compliance Report, 1 – 4, 11 – 3, 18 – 32 (2017). [Digital Identities, Blockchain, Regulatory Landscape]

9. FinCEN Joint Statement on Innovative Efforts to Combat Money laundering and Terrorist Financing (December 3,2018). [Regulatory Landscape, Centralized Agency]

10. Ross P. Buckley & Rebecca L. Stanley, *Protecting the West, Excluding the Rest: The Impact of the AML/CTF Regime on Financial Inclusion in the Pacific and Potential Responses*, 17 MEJ JIL 83, 84 – 7; 93 – 5; 100 – 5 (2016). [De-risking, Financial Inclusion]

11. Maria A. de Dios, *The Sixth Pillar of Anti-Money Laundering Compliance: Balancing Effective Enforcement with Financial Privacy*, 10 Brook J. Corp. Fin & Com. L. 495 – 500, 502 – 5; 507 – 12; 514 – 6 (2016). [Privacy Concerns, Regulatory Landscape]

12. Kevin Werbach, *Trust But Verify: Why the Blockchain Needs the Law*, 33 Berkeley Tech. L. J. 487, 507 – 13, 525 – 6, 534 – 41 (2018). [Distributed Ledgers, Centralized Agency, Blockchain, Regulatory Landscape]

13. Dirk A. Zetzsche, Ross P. Buckley & Douglas W. Arner, *The Distributed Liability of Distributed Ledgers: Legal Risks of Blockchain*, 2018 UILLR 1361 – 73 (2018). [Distributed Ledgers, Blockchain, Liability Regime]

Optional Materials

Appendix A

FFIEC BSA/AML Manual – Information Sharing
FFIEC BSA/AML Manual – Suspicious Activity Reporting
FFIEC BSA/AML Manual – Customer Due Diligence

Appendix B

FinCEN Guidance on Section 314(b) of the USA PATRIOT Act
FinCEN Section 314(b) Information Sharing Fact Sheet

Appendix C

Dirk A. Zetzsche, Ross P. Buckley & Douglas W. Arner, *The Distributed Liability of Distributed Ledgers: Legal Risks of Blockchain*, 2018 UILLR 1382 – 1404 (2018).

Appendix D

Academic Proposal, 17-22 (Sections 1-2), 26-38 (Section 4).

Appendix E

FCA Feedback on Distributed Ledger Technology Discussion Paper, 22 – 24 (2017).