HARVARD LAW SCHOOL
1525 Massachusetts Avenue
Cambridge, MA, 02138

Financial Regulation Case Study
Bank Secrecy Act, Anti-Money Laundering Law Compliance & Blockchain Technology

MEMORANDUM*

TO: Junior FinCEN Lawyer
RE: Recommendations Regarding Adopting Blockchain Technology for BSA/AML Compliance
DATE: November 2016

You are a junior attorney at the United States Department of the Treasury Financial Crimes Enforcement Network (FinCEN). FinCEN plays a critically important role in monitoring and enforcing financial crimes involving banks and other financial institutions. The organization takes this role very seriously, but is also trying to stay ahead of the curve when it comes to finding more effective ways of detecting illegal activity and fighting financial crime. The Director of FinCEN has been monitoring the news over the past year that a number of new startups are developing technology that utilizes blockchain technology with the goal of helping financial institutions comply with U.S. Anti-Money Laundering (AML) laws. The Director notes that financial institutions seem to be eager to test out blockchain technology in ways that not only increase their compliance with AML laws but also combat the rising costs of their current compliance schemes as well.

The Director wants you to look into the viability of these products using blockchain technology and make a recommendation as to whether FinCEN should assert a position in favor of encouraging the adoption of this type of technology for AML compliance. The Director would like to hear about the pros and cons of your recommendation. With FinCEN on the front lines of fighting financial crimes ranging from money-laundering violations to funding terrorist organizations and terrorism attacks, you understand the importance of FinCEN's role in the enforcement community. You are also cognizant that adopting new technology to help combat these crimes may be very helpful in the future. Ultimately, you understand that FinCEN giving its blessing for financial institutions to use new technology cannot come at the price of less-effective monitoring or enforcement.

The Bank Secrecy Act Origins 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 combatting 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]

---

* This case study was prepared by Dylan M. Aluise, Harvard Law School Class of 2017, under the supervision of Professor Howell E. Jackson. This case study is intended for educational purposes only and is not intended to offer legal advice.

[1] *Mission*, FINCEN, https://www.fincen.gov/about/mission (last visited Oct. 30, 2016).

[2] *History of Anti-Money Laundering Laws*, FINCEN, https://www.fincen.gov/history-anti-money-laundering-laws (last visited Oct. 30, 2016).

At the heart of the BSA compliance scheme is the goal of having financial institutions 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, authorities wanted to establish a paper trail of all customer transactions in order to follow the money to make it far more difficult for drug dealers to launder profits.[5] To accomplish this, the BSA established a broad mandate that financial institutions would be enlisted to help the government fight money-laundering through 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 passed 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 reasonably designed to ensure and monitor compliance with the reporting and recordkeeping requirements of the BSA and imposed sanctions on financial institutions that if they assisted customers in laundering money.[8] Later, the Annunzio-Wylie Anti-Money Laundering Act of 1992 expanded on the concept of CTR and established the requirement that financial institutions file reports whenever they detect suspicious activity.[9] The Annunzio-Wylie Act also granted 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 (USA PATRIOT Act) which imposed impressive new requirements on financial institutions with the goal of fighting terrorism.[11] The USA PATRIOT Act expanded AML requirements to all financial institutions subject to U.S. regulatory jurisdiction, provided the Secretary of Treasury with the authority to impose "special measures" on financial institutions that are of "primary money-laundering concern," augmented the existing BSA framework by strengthening customer identification procedures, imposed a 120 hour period in which financial institutions had to respond to regulatory requests for information, and improved information sharing between financial institutions and the U.S. government.[12]

The Current AML Compliance Regime

---

[3] *Bank Secrecy Act Anti-Money Laundering Examination Manual: Introduction*, FED. FIN. INSTITUTIONS EXAMINATIONS COUNCIL, https://www.ffiec.gov/bsa_aml_infobase/pages_manual/OLM_002.htm (last visited Oct. 30, 2016) [hereinafter Fed. Fin. Institutions Examinations Council will be referred to as FFIEC).

[4] Stavros Gadninis & 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 3; Gadinis & Mangels, *supra* note 4, at 861.

[9] 31 U.S.C. § 5318(g) (2012) (providing the Annuzio-Wiley Act's "Reporting of Suspicious Transactions" provision); *see* Gadinis & Mangels, *supra* note 4, at 869-70.

[10] Gadinis & Mangels, *supra* note 4, at 869-70.

[11] USA PATRIOT Act, Pub. L. No. 107-56, 115 Stat. 272 (2001); FFIEC, *supra* note 3.

[12] FFIEC, *supra* note 3

In total, the current BSA/AML compliance regime has several features which financial institutions must be aware of and comply with. The key features of AML compliance include the requirement that financial institutions file currency reports with the U.S. Department of the Treasury,[13] report suspicious transactions through Suspicious Activity Reports (SAR),[14] 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"),[15] and maintain a paper trail by keeping appropriate records of financial transactions.[16] These records 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.[17]

Two of the most robust compliance mechanisms are SARs (which require banks to detect and report any suspicious activity) and KYC programs (which require banks to 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: transactions with funds that come from illegal activities or that are designed to mask illegal activities, transactions that are designed to evade the BSA and its reporting requirements (such as the $10,000 CTR threshold), and any other unusual activity such as transactions which have no business or lawful purpose.[18] This scheme imposes the duty on a bank to both use its judgment when it comes to detecting suspicious activity and explain its suspicions to the government in the SAR it files.[19] The KYC programs require that a bank verify "the identity of individuals and businesses that are account holders and to be familiar enough with their banking practices so that transactions that are outside the norm can be readily identified."[20] Thus, a bank must have a system installed to collect relevant information about clients' backgrounds, business purposes, and anticipated account activities to be able to make such a determination.[21]

In many ways, the BSA/AML scheme imposes greater burdens on financial institutions than the compliance regimes of other financial laws. Outside of the AML requirements, many other financial regulatory schemes, such as the U.S. securities laws, require financial institutions to identify problematic

---

[13] 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).

[14] *Id.* at §§ 1010.320 (SAR requirement for banks); 1025.320 (SAR requirement for insurance companies).

[15] *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).

[16] *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 3.

[17] FFIEC, *supra* note 3.

[18] *See* 12 C.F.R. § 21.11(c); 31 C.F.R. § 1010.311; Gadinis & Mangels, *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), http://gao.gov/assets/160/155076.pdf (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).

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

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

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

clients or transactions, yet only impose heavy liability if the financial institution *knowingly* or *negligently* allowed such transactions to occur.[22] Conversely, the AML regime requires that financial institutions report clients and activities even if they have mere *suspicions* of misconduct.[23] Thus, financial institutions cannot be "willfully blind" when it comes to its customers or the transactions that it processes.[24]

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 feature (at a minimum): 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.[25] A "fifth pillar" was recently 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.[26] Due to regulators' reliance on banks to discover and report problematic customers and transactions, failure to comply with the AML regime imposes harsh sanctions on financial institutions with both civil or criminal penalties available to enforcement agencies.[27] In fact, a number of financial institutions have faced stiff fines not for processing fraudulent transactions, but because their compliance scheme and detection mechanisms were deemed insufficient.[28]

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 with bank affiliates and across different departments within the same bank, but with other financial institutions as well.[29] This inter-bank sharing mechanism was established by a USA PATRIOT Act safeharbor contained in Section 314(b) which allows for financial institutions to voluntarily share information with each other in order to better identify and report potential money laundering or terrorist activities.[30] Voluntarily participating in a Section 314(b) information exchange is strongly encouraged by FinCEN to help identify AML violations.[31]

As for the BSA scheme's effectiveness, a recent article reviewed the U.S. AML scheme found that the comprehensive set of BSA compliance requirements was effective in detecting and preventing money laundering operations and illegal financial activity.[32] Furthermore, underscoring one of the most

---

[22] Gadinis & Mangels, *supra* note 35, at 801-02.
[23] *Id.* at 802.
[24] *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.
[25] *See* 31 U.S.C. § 5318(h) (2012).
[26] *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).
[27] *See* 31 U.S.C. §§ 5321-22 (2012).
[28] *See* Samee Zafar, *Can Blockchain Prevent Money Laundering?*, Edgar, Dunn & Co. Mgmt. Consultants (Sept. 30, 2016), http://edgardunn.com/2016/09/can-blockchain-prevent-money-laundering (noting the case of Standard Chartered Bank where the bank was fined $300 million because the bank had below-par AML systems and controls).
[29] FINCEN, FIN-2014-A007, ADVISORY TO U.S. FINANCIAL INSTITUTIONS ON CREATING A CULTURE OF COMPLIANCE 3, note 2 (2014), https://www.fincen.gov/sites/default/files/shared/FIN-2014-A007.pdf.
[30] USA PATRIOT Act, Pub. L. No. 107-56, 115 Stat. 307 § 314(b) (2001); 31 C.F.R. § 1010.540.
[31] FINCEN, INFORMATION SHARING BETWEEN FINANCIAL INSTITUTIONS: SECTION 314(B) FACT SHEET (2013), https://www.fincen.gov/sites/default/files/shared/314bfactsheet.pdf.
[32] *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).

critical goals of the modern U.S. AML scheme, the effort to combat terrorists' access to financial resources has been "the most successful part" of the fight against terrorism since the September 11, 2001 attacks according to Daniel Benjamin, the former National Security Council Director for Transnational Threats.[33] However, some critics argue that no data have been collected and no tests have been conducted to thoroughly examine the effectiveness of the current scheme, and therefore the current system may not actually be the most effective.[34]

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 financial crisis have involved AML violations.[35] 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.[36] Currently, Goldman Sachs is facing a major investigation into its activities with respect to Malaysia's 1MDB development fund and whether the investment bank also violated U.S. AML laws.[37] Since 2009, financial institutions have been assessed over $12 billion in fines, penalties, and forfeitures for violations of the BSA/AML regime by not reporting suspicious transactions.[38] This period marks a dramatic increase in AML enforcement. From 2011-2015 the number of AML enforcement actions has risen 75%, and the dollar amount of penalties has increased by 431%.[39] In short, the U.S. AML regime has become a key tool for regulators to hold banks accountable and to combat fraud and other financial crimes as a critical detection and enforcement mechanism.[40] 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."[41]

The Growing Costs of AML Compliance

As the above section details, the central tenet of the current U.S. AML regime enlists private financial institutions as gatekeepers, placing burdens on banks to self-monitor compliance and issue reports to federal regulators.[42] Beyond the $12 billion plus in sanctions levied on financial institutions for AML violations over the past decade, banks are facing increasing costs to simply handle their compliance burdens. Banks have been spending increasing amounts of money adopting complex systems of compliance that utilize both dedicated compliance staff as well as new technology.[43] As an example, in his annual letter to shareholders in 2014, J.P. Morgan Chase CEO Jamie Dimon revealed

---

[33] *See* Anne L. Clunan, *The Fight against Terrorist Financing*, 121 POL. SCI. Q. 569, 569 (2006).
[34] *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.
[35] Stephen Grocer, *A List of the Biggest Bank Settlements*, Moneybeat (Blog), WALL ST. J. (June 23, 2014), http://blogs.wsj.com/moneybeat/2014/06/23/a-list-of-the-biggest- bank-settlements/; *see* Gadninis & Mangels, *supra* note 4, at 801.
[36] *See* Grocer, *supra* note 35; Gadinis & Mangels, *supra* note 35, at note 5, 801.
[37] Justin Baer, Tom Wright & Bradley Hope, *Goldman Probed Over Malaysia Fund 1MDB*, WALL ST. J. (June 7, 2016), http://www.wsj.com/articles/goldman-probed-over-malaysia-fund-1465257383.
[38] 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), http://gao.gov/assets/680/675987.pdf.
[39] Stephen Heifetz & Evan Abrams, *Dramatic Rise in FinCEN Enforcement*, STEPTOE INTERNATIONAL COMPLIANCE (BLOG), STEPTOE & JOHNSON LLP (Oct. 11, 2016), http://www.steptoeinternationalcomplianceblog.com/2016/10/dramatic-rise-in-fincen-enforcement/.
[40] *See* Gadinis & Mangels, *supra* note 35, at 801.
[41] Saperstein et al., *supra* note 34, at 1.
[42] *See generally* Gadninis & Mangels, *supra* note 5.
[43] *See* Gadinis & Mangels, *supra* note 5, at 874-75;

that the bank hired 8,000 new employees in 2013 to focus primarily on its BSA/AML compliance program and that its employees underwent 800,000 hours of compliance training.[44] From a larger compliance perspective, J.P. Morgan also has over 250,000 employees worldwide committed to focusing on various compliance issues.[45]

According to FinCEN's outreach report, a big bank alone might have over 80 lines of business, each with its own AML compliance officer.[46] Because of this, certain banks have faced added compliance costs (including AML and other compliance measures) totaling over $4 billion a year extra compared to pre-financial crisis.[47] This has also led to an increase in SAR reports from only 50,000 reports in 1996 to over 1,800,000 in 2015.[48] Ultimately, it is estimated that the total spending on AML compliance *alone* has grown from $3.6 billion in 2008 to an estimated $10 billion annual outlay in recent years.[49] Combined with sanctions, this represents nearly $18 billion in AML costs for financial institutions annually.[50] Due to these increases in compliance costs, banks are constantly looking for innovative ways to ensure compliance at a more cost-efficient level. However, management at the banks are aware that regulators are more focused than ever on compliance and any cutbacks or lapses in compliance procedures would likely be frowned upon.[51]

Blockchain Technology Background

Financial institutions are looking into many potential uses of blockchain technology.[52] However, it is important to first understand the origins of the technology and what the technology does. At its essence, a blockchain is a ledger. Blockchain technology first appeared in 2009 as the public ledger that recorded each transaction made using Bitcoins.[53] Bitcoins are digital currency traded peer-to-peer, and thus there needed to be an ability to verify transactions between two Bitcoin accounts and to ensure that the same Bitcoin would not be "spent" twice by the same person.[54] 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 processing the transactions, another new technology was created to solve the

---

[44] Jamie Dimon, *Dear Fellow Shareholders*, J.P. MORGAN CHASE 21, 23 (Apr. 8, 2015), https://www.jpmorganchase.com/corporate/investor-relations/document/JPMC-AR2014-LetterToShareholders.pdf; Anthony Effinger, *The Rise of the Compliance Guru—and Banker Ire*, BLOOMBERG (June 25, 2015), http://www.bloomberg.com/news/features/2015-06-25/compliance-is-now-calling-the-shots-and-bankers-are-bristling.

[45] *See* Monica Langley & Dan Fitzpatrick, *Embattled J.P. Morgan Bulks Up Oversight*, WALL ST. J., (Sep. 12, 2013), www.wsj.com/articles/SB10001424127887324755104579071304170686532.

[46] FINCEN, FINANCIAL INSTITUTIONS OUTREACH INITIATIVE: REPORT ON OUTREACH TO LARGE DEPOSITORY INSTITUTIONS 5 (2009), https://www.fincen.gov/sites/default/files/shared/Bank_Report.pdf; *see also* Gadinis & Mangels, *supra* note 5, at 883.

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

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

[49] WEALTHINSIGHT, 2020 FORESIGHT: THE IMPACT OF ANTI-MONEY LAUNDERING REGULATIONS ON WEALTH MANAGEMENT 6 (2013), http://www.marketresearch.com/product/sample-7717318.pdf; GOLDMAN SACHS, PROFILES IN INNOVATION: BLOCKCHAIN 71 (2016), http://www.the-blockchain.com/docs/Goldman-Sachs-report-Blockchain-Putting-Theory-into-Practice.pdf.

[50] Goldman Sachs, *supra* note 49, at 71.

[51] *See* Noonan, *supra* note 47.

[52] *See* Yassi Bello Perez, *8 Banking Giants Embracing Bitcoin and Blockchain Tech*, COINDESK (July 27, 2015), http://www.coindesk.com/8-banking-giants-Bitcoin-blockchain/.

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

[54] *Id.*

verification and double spending problems.[55] This technological breakthrough was the blockchain ledger. The blockchain would replace the trusted third-party and would serve as the ledger recording each transaction to be able to verify the payment history as well as proof of the number of Bitcoins associated with each Bitcoin owner's account at any given moment.[56]

This technology worked by acting as a distributed ledger of all transactions to ever occur. For Bitcoin, this blockchain ledger exists and is replicated on thousands of computers spread around the world (known as "nodes") and is made publicly available.[57] Each subsequent Bitcoin transaction would be recorded by adding another "block" to the "chain" and thus be reflected on the public ledger shared by each of the nodes.[58] But, despite being so open and publicly available, the blockchain is trustworthy and secure due to the fact that every single node must reflect the same ledger—producing a "consensus mechanism" whereby each of the nodes must be in agreement on how to update the blockchain for each transaction.[59] In this sense, it is the brute force of having thousands of computers in agreement that makes the blockchain virtually incorruptible and a trusted, public source of the "truth" or verification of each transaction.[60] 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, specialised nodes called miners will bundle Alice's proposal with other similarly reputable transactions to create a new block for the blockchain.[61]

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 blockchain by including a copy of the previous' block's hash. This is replicated all the way back to the initial block on the blockchain.[62] 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 to a transaction will necessarily cause a change to a block and therefore to the entire chain and will be rejected.[63] 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 which are constantly checking for uniformity. Therefore, the only way to fraudulently alter the ledger would be to hack 51% percent 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.[64] Here is another illuminating example:

> 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

[55] *Id.*
[56] *Id.*
[57] *Id.*
[58] *Id.*
[59] *Id.*
[60] *Id.*
[61] *Id.*
[62] *Id.*
[63] *Id.*
[64] *Id.*

> 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.[65]

Thus, the true value of the blockchain is its use as a trust/consensus technology: "the changes in the data are recorded into the blockchain when network participants agree that a transaction is legitimate in accordance with shared protocols and rules."[66] Beyond Bitcoin, blockchain has a number of 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."[67]

Potential Use of Blockchain for AML Compliance

Because of blockchain technology's ability to present the "truth" of a transaction or data for all parties with access to the blockchain, there have been many proposals about how to best adopt the blockchain to other uses beyond Bitcoin in the financial system. According to Julio Faura, the head of innovation at Santander Bank, "[blockchain's] distributed ledger is very elegant way to solve problems" in the financial services industry.[68] Goldman Sachs estimates that blockchain technology for AML and KYC compliance mechanisms can save financial institutions an estimated aggregate of $3-5 billion in cost savings.[69]

However, many banks may remain skittish about having customers' information available in a public database—which is where a closed "permissioned blockchain" is useful. While, the blockchain technology for Bitcoin is a public ledger, the technology can also be adapted to become private or "permissioned" and thus take advantage of a distributed ledger but with only certain parties able to view the data stored on that blockchain.[70] A permissioned blockchain behaves in the same way as a public distributed ledger, except that any entity which seeks to access the ledger must be validated or pre-approved.[71] Permissioned blockchains work where there is already an element of trust established between the participants—for instance, financial institutions that already have well-developed relationships with one another.[72] A recent study published by Barclays Bank posited that a permissioned blockchain would be a groundbreaking innovation in the AML/KYC space by having a centralized version of the "truth" be accessible on a consensus basis.[73] Barclays believes that this would stand in stark contrast to the system currently being employed in which "every bank, government department and law firm has their own paper copy of the truth."[74] The centralized ledger would thus essentially

---

[65] *Id.*
[66] Cliff Moyce, *How Blockchain Can Revolutionize Regulatory Compliance*, CORP. COMPLIANCE INSIGHTS (Aug. 10, 2016), http://corporatecomplianceinsights.com/blockchain-regulatory-compliance/.
[67] *Id.*
[68] Matthew Finnegan, *Why Banks Are Betting On the Blockchain - Not Bitcoin - To Transform The Financial Sector*, TECHWORLD (Aug. 4, 2016), http://www.techworld.com/e-commerce/why-banks-are-betting-on-blockchain-transform-financial-sector-3621840/.
[69] *See* Goldman Sachs, *supra* note 49, at 71.
[70] *See id.* at 10.
[71] *See id.*
[72] *See id.*
[73] SIMON TAYLOR, BARCLAYS BANK PLC, BLOCKCHAIN: UNDERSTANDING THE POTENTIAL 3 (2015), https://www.barclayscorporate.com/content/dam/corppublic/corporate/Documents/insight/blockchain_understanding_the_potential.pdf.
[74] *Id.*

eliminate a lot of the duplicative work and back-and-forth processes between these entities that is causing inefficiencies in the system.[75] These efficiencies are described below.

When a bank gains a new customer, the litany of KYC requirements is triggered to ensure that the customer is using 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, then much of the costly process of getting to "know" the customer could be avoided. [76] As an alternative to the current system, banks could access verified information about the new client based on the customer's compliance data and the procedures used to obtain that compliance data stored on the blockchain ledger.[77] In essence, the diligence and procedures done by one bank can be piggy-backed and enhanced by other banks to comply with their own internal procedures.[78] The blockchain would essentially be creating and storing 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—in effect creating a customer's "digital passport for transacting in financial services."[79] Banks could then amend and upload new data about the customer to the blockchain after each transaction is completed or if the customer's information has changed and been verified.[80] 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."[81] Conversely, in the current system, it is estimated that KYC requests can take 30-50 days to complete satisfactorily[82] and involve a lot of duplicative work by multiple institutions with potentially copious amounts of documentation that need to be obtained and verified each time the same customer opens up an account with a new financial institution. Furthermore, other stakeholders in the financial system might benefit as well—a recent study by Bain has shown that customers, too, are frustrated by the current KYC system whereby they have to reuse the same documentation and potentially wait weeks for access to a new bank account.[83]

Beyond the "on-boarding" of new clients, blockchain technology can also assist with other AML compliance demands on a transaction-by-transaction basis. Those critical of the current AML scheme have argued that the present approach encourages banks to hire more people and invest money to implement AML controls with an uncertain degree of effectiveness.[84] The current system places burdens on employees to comb through a financial institution's records and then check whether the the transactions were suspicious or whether they were in compliance with current rules and regulations—with much of this process duplicated on both sides of a single transaction.[85] These critics posit that blockchain technology would allow banks on both ends of a transaction to be able to quickly verify the credentials of all parties to a transaction.[86] Furthermore, with all of the transaction data stored and

---

[75] *See id.*
[76] *See* Moyce, *supra* note 66.
[77] *See id.*; Matthew Britton, *Could Blockchain Solve the KYC/AML Challenge?*, BCS Consulting (Sept. 29, 2016), http://www.bcsconsulting.com/blog/new-technology-can-enable-human-bank/.
[78] *See* Moyce, *supra* note 66.
[79] Britton, *supra* note 77.
[80] *See id.*
[81] Moyce, *supra* note 66; *see also* Britton, *supra* note 77.
[82] JEREON VAN OERLE & PATRICK LEMMENS, ROBECO, DISTRIBUTED LEDGER TECHNOLOGY FOR THE FINANCIAL INDUSTRY 13 (2016), https://www.robeco.com/images/201605-distributed-ledger-technology-for-the-financial-industry.pdf.
[83] *See* Matthias Memminger, Mike Baxter & Edmun Lin, *You've Heard of Fintech, Get Ready for 'Regtech'*, AM.BANKER (Sept. 7, 2016), http://www.americanbanker.com/bankthink/youve-heard-of-fintech-get-ready-for-regtech-1091148-1.html (noting also that "Half to three-quarters of onboarding requests never reach the final stage of account opening" wasting customers' time and effort).
[84] *See* Zafar, *supra* note 28.
[85] *See id.*
[86] *See id.*

verified on the distributed ledger, it may make it easier for banks and regulators to use algorithms to analyze and detect suspicious patterns and payments at an aggregate level.[87] This permissioned blockchain may not only hinder the ability for criminals to use financial institutions for illegal transactions, but also would allow banks to fully take advantage of a Section 314(b) sharing program to be able to immediately alert one another about a transaction or series of transactions that are suspicious and potentially illegal.[88] If a bank positively discovers a fraudulent transaction, then each bank where the customer has an account could be immediately alerted to prevent future fraudulent transactions.[89] Using such a system, stakeholders would no longer be receiving post-hoc reports about disaggregated transaction viewed on a more individualized basis, but would instead be able to monitor entire sets of transactions on an aggregated basis in real-time.[90]

Proponents of adopting blockchain for BSA/AML purposes note that regulators would stand to benefit greatly from this technology as well.[91] Regulators could take advantage of the technology to gain an inside view into each transaction posted on the blockchain as it is happening.[92] These proponents argue that the blockchain would allow regulators to take on a more proactive role in analyzing suspicious transactions or patterns alongside the banks that are monitoring them as well.[93] By having more eyes on the system at any given time, the potential for illegal activities escaping detection would likely decrease as a result. Thus, proponents conclude that this technology could dramatically reduce the time and effort spent on compliance under the current system and therefore decrease the growing costs of compliance, while also "improving the quality, accuracy and confidence of and in the process."[94]

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

Building off of this notion of the potential uses for blockchain in the KYC/AML space, a number of start up companies have begun to harness the underlying technology to build tools that could be used by banks and regulators to make compliance more efficient.[95] Some firms, such as Elliptic and Coinfirm, are using blockchain technology with an eye towards solving AML problems at financial institutions.[96] Another startup, Gem, is focused on digital identities and believes that it has potential applicability for AML compliance use in financial institutions.[97]

In addition, many established financial institutions have exploring ways to utilize blockchain technology either by developing their own technology or partnering with blockchain-based firms.[98] These financial institutions include Barclays, UBS, Deustche Bank, Santander, and Bank of America,

---

[87] *Id.*
[88] *See id.*
[89] Britton, *supra* note 77.
[90] *See* Moyce, *supra* note 66; Zafar, *supra* note 28.
[91] *See* Moyce, *supra* note 66.
[92] *See id.*
[93] *See id.*
[94] *Id.*
[95] *See* ACCENTURE, DISTRIBUTED CONSENSUS LEDGERS FOR PAYMENT (2015), https://www.accenture.com/t20151002T010405__w__/us-en/_acnmedia/Accenture/Conversion-Assets/DotCom/Documents/Global/PDF/Dualpub_22/Accenture-Banking-Distributed-consensus-ledgers-payment.pdf.
[96] *See id.*; Richard Kastelein, *Coinfirm and Billon Team Up to Better Blockchain AML and Compliance*, BLOCKCHAIN NEWS (Sept. 3, 2016), http://www.the-blockchain.com/2016/09/03/coinfirm-billon-team-better-blockchain-aml-compliance/.
[97] *See* Bryan Yurcan, *How Blockchain Fits into the Future of Digital Identity*, AM. BANKER (Apr. 8, 2016), http://www.americanbanker.com/news/bank-technology/how-blockchain-fits-into-the-future-of-digital-identity-1080345-1.html?zkPrintable=1&nopagination=1.
[98] *See* Finnegan, *supra* note 68.

among others.[99] Bank of America has already applied for 15 blockchain-based patents.[100] 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.[101]

Regulatory Reaction To This Point

At the Office of the Comptroller of the Currency's Forum on Supporting Responsible Innovation, Comptroller Curry noted that there is a significant opportunity for technology to reduce costs and and increase efficiency in BSA/AML compliance.[102] The OCC is one of the financial regulatory agencies in charge of monitoring and enforcing BSA compliance for national banks. However, other financial regulators have expressed some concerns. The Consumer Financial Protection Bureau (which does not enforce the BSA) has raised general concerns over vendors providing compliance-related services being too slow to adopt their technology to meet regulatory requirements.[103]

Some regulators overseas have taken an accommodating stance regarding adoption of innovative blockchain technology to potentially solving financial services problems. The U.K. Financial Conduct Authority is actively exploring potential uses of blockchain technology for financial services companies to meeting U.K. AML obligations. Christopher Woolard, an executive member of the FCA board, stated in a recent speech that the FCA is "particularly interested in exploring whether blockchain 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."[104] Similarly, Benedicte Nolens, the Senior Director of Hong Kong's Securities and Futures Commission, recently addressed the MIT Emtech conference and stated that blockchain has a real opportunity to address some "pretty significant inefficiencies" with the current KYC and AML system by removing duplicative efforts and creating a record of all checks carried out for each client.[105] However, many of these overseas regulators are similarly urging 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 up to innovative technology.[106] 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."[107]

U.S. regulators are similarly taking a somewhat measured approach thus far when it comes to blockchain technology, with regulatory acceptance being labeled as an "uphill battle."[108] At a recent

---

[99] *See id.*; Alice Woodhouse, *Blockchain Technology Can Help Banks Beat Money-Laundering, Hong Kong Regulator Says*, S. CHINA MORNING POST (June 8, 2016), http://www.scmp.com/business/banking-finance/article/1969769/blockchain-technology-can-help-banks-beat-money-laundering.
[100] Woodhouse, *supra* note 99.
[101] Avi Mizrahi, *IBM Successfully Tests Blockchain KYC with France's Crédit Mutuel Arkéa*, FIN. MAGNATES (June 30, 2016, 2:53 PM), http://www.financemagnates.com/cryptocurrency/innovation/ibm-successfully-tests-blockchain-kyc-with-frances-credit-mutuel-arkea/.
[102] *See* Katie Wechsler & Zachary Luck, *The Federal FinTech Promised Land*, 19 Fintech L. Rep. 2 (August 2016).
[103] *See id.*
[104] Christopher Woolard, Fin. Conduct Authority Dir. of Strategy and Competition, Speech at the FCA UK FinTech: Regulating for Innovation Conference (Feb. 22, 2016), https://www.fca.org.uk/news/speeches/uk-fintech-regulating-innovation.
[105] Woodhouse, *supra* note 99.
[106] *Id.*
[107] BANK OF ENG., OPEN BANK RESEARCH AGENDA 31 (2015), http://www.bankofengland.co.uk/research/Documents/onebank/discussion.pdf.
[108] Henry Engler, *Blockchain Faces Maze of Regulatory Complexities, Questions and*

conference, officials from the Federal Reserve expressed a number of concerns that they have over blockchain technology. David Mills, the Assistant Director of Operations and Payment Systems at the Federal Reserve noted that there were a number of risks the uses of such technology, cautioning 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."[109] Mills also sympathized with the notion that there appears to be a lack of consensus among the regulators with respect to blockchain technology, but noted that the regulators are eager to learn more about the technology.[110]

Finally, while FinCEN has not officially weighed in on blockchain's usage for KYC/AML compliance, a recent FinCEN enforcement case against a blockchain company garnered a lot of attention in 2015. Ripple Labs, a startup that uses blockchain technology to process and settle transactions between financial institutions. According to the company, "Ripple solutions lower the total cost of settlement by enabling banks to transact directly, instantly and with certainty of settlement."[111] However, Ripple was deemed by FinCEN to be facilitating transactions in violation of the BSA because they did not have proper AML protections in place.[112] Ripple was given a $700,000 fine—a significant blow for a startup company—and ordered to enhance the AML compliance across its platform.[113] In addition, many opined that the FinCEN's enforcement action against Ripple had the potential to created a chilling effect on banks and scare them away from partnering with some blockchain-based companies.[114] While Ripple's use of blockchain is not intended as an AML/KYC compliance tool, there remains a lot of uncertainty about how regulators would react to bank's adopting more robust uses of blockchain technology.[115]

Conclusion

The director of FinCEN would like to hear your recommendation about the potential uses of blockchain technology for BSA compliance. Considering that financial institutions will likely be hesitant to adopt the technology without the technology being legitimized in some form by regulatory bodies,[116] please evaluate the pros and cons with respect to FinCEN taking an affirmative stance encouraging or discouraging the use of this technology. How concerned should FinCEN be over privacy and security issues? Does the current system's duplicative processes serve as a useful filter to ensure that bad actors are caught? Will too much reliance on other banks' information in the blockchain allow for illegal transactions to slip through the cracks?

Challenges, Thomson Reuters (Feb. 23, 2016), https://blogs.thomsonreuters.com/answerson/blockchain-faces-maze-of-u-s-regulatory-complexities-questions-and-challenges/.

[109] *Id.*

[110] *Id.*

[111] *Company*, RIPPLE (last visited Oct. 30, 2016), https://ripple.com/company/.

[112] *See* Sarah Todd & Ian McKendry, *What Ripple's FinCEN Fine Means for the Digital Currency Industry*, AM. BANKER (May 6, 2015), http://www.americanbanker.com/news/bank-technology/what-ripples-fincen-fine-means-for-the-digital-currency-industry-1074195-1.html.

[113] *See id.*

[114] *See id.*

[115] *See* Goldman Sachs, *supra* note 49, at 77.

[116] *See id.*

APPENDIX:

Item 1 – FFIEC Introduction to the Bank Secrecy Act/Anti-Money Laundering Examination Manual

Item 2 – FFIEC Suspicious Activity Reporting Overview

Item 3 – FFIEC Customer Identification Program Overview

Item 4 – FinCEN Guidance on the Scope of Permissible Information Sharing Covered by Section 314(b) Safe Harbor of the USA PATRIOT Act & FinCEN Section 314(b) Information Sharing Fact Sheet

Item 5 – Stavros Gadinis & Colby Mangels, *Collaborative Gatekeepers*, 73 WASH. & LEE L. REV. 797 (2016).

Item 6 –*The Great Chain of Being Sure About Things*, THE ECONOMIST (Oct. 31, 2015).

Item 7 – GOLDMAN SACHS, PROFILES IN INNOVATION: BLOCKCHAIN (2016).

Item 8 – Laura Noonan, *Banks Face Pushback Over Surging Compliance and Regulatory Costs*, FIN. TIMES (May 28, 2015).

Item 9 – Matthew Britton, *Could Blockchain Solve the KYC/AML Challenge?*, BCS CONSULTING (Sept. 29, 2016).

Item 10 – Henry Engler, *Blockchain Faces Maze of Regulatory Complexities, Questions and Challenges*, THOMSON REUTERS (Feb. 23, 2016).

APPENDIX:

Item 1 – FFIEC Introduction to the Bank Secrecy Act/Anti-Money Laundering Examination Manual

Item 2 – FFIEC Suspicious Activity Reporting Overview

Item 3 – FFIEC Customer Identification Program Overview

Item 4 – FinCEN Guidance on the Scope of Permissible Information Sharing Covered by Section 314(b) Safe Harbor of the USA PATRIOT Act & FinCEN Section 314(b) Information Sharing Fact Sheet

Item 5 – Stavros Gadinis & Colby Mangels, *Collaborative Gatekeepers*, 73 WASH. & LEE L. REV. 797 (2016).

Item 6 –*The Great Chain of Being Sure About Things*, THE ECONOMIST (Oct. 31, 2015).

Item 7 – GOLDMAN SACHS, PROFILES IN INNOVATION: BLOCKCHAIN (2016).

Item 8 – Laura Noonan, *Banks Face Pushback Over Surging Compliance and Regulatory Costs*, FIN. TIMES (May 28, 2015).

Item 9 – Matthew Britton, *Could Blockchain Solve the KYC/AML Challenge?*, BCS CONSULTING (Sept. 29, 2016).

Item 10 – Henry Engler, *Blockchain Faces Maze of Regulatory Complexities, Questions and Challenges*, THOMSON REUTERS (Feb. 23, 2016).

Appendix Item 1

Bank Secrecy Act
Anti-Money Laundering
Examination Manual

Backward | Table of Contents | Forward

Introduction

This Federal Financial Institutions Examination Council (FFIEC) *Bank Secrecy Act (BSA) /Anti-Money Laundering (AML) Examination Manual* provides guidance to examiners for carrying out BSA/AML and Office of Foreign Assets Control (OFAC) examinations. An effective BSA/AML compliance program requires sound risk management; therefore, the manual also provides guidance on identifying and controlling risks associated with money laundering and terrorist financing. The manual contains an overview of BSA/AML compliance program requirements, BSA/AML risks and risk management expectations, industry sound practices, and examination procedures. The development of this manual was a collaborative effort of the federal and state banking agencies[1] and the Financial Crimes Enforcement Network (FinCEN), a bureau of the U.S. Department of the Treasury, to ensure consistency in the application of the BSA/AML requirements. In addition, OFAC assisted in the development of the sections of the manual that relate to OFAC reviews. Refer to Appendices A ("BSA Laws and Regulations"), B ("BSA/AML Directives"), and C ("BSA/AML References") for guidance.

STRUCTURE OF MANUAL

In order to effectively apply resources and ensure compliance with BSA requirements, the manual is structured to allow examiners to tailor the BSA/AML examination scope and procedures to the specific risk profile of the banking organization. The manual consists of the following sections:

- Introduction.
- Core Examination Overview and Procedures for Assessing the BSA/AML Compliance Program.
- Core Examination Overview and Procedures for Regulatory Requirements and Related Topics.
- Expanded Examination Overview and Procedures for an Consolidated and Other Types of BSA/AML Compliance Program Structures.
- Expanded Examination Overview and Procedures for Products and Services.
- Expanded Examination Overview and Procedures for Persons and Entities.
- Appendices.

The core and expanded overview sections provide narrative guidance and background information on each topic; each overview is followed by examination procedures. The "Core Examination Overview and Procedures for Assessing the BSA/AML Compliance Program" and the "Core Examination Overview and Procedures for Regulatory Requirements and Related Topics" (core) sections serve as a platform for the BSA/AML examination and, for the most part, address legal and regulatory requirements of the BSA/AML compliance program. The "Scoping and Planning" and the "BSA/AML Risk Assessment" sections help the examiner develop an appropriate examination plan based on the risk profile of the bank. There may be instances where a topic is covered in both the core and expanded sections (e.g., funds transfers and foreign correspondent banking). In such instances, the core overview and examination procedures address the BSA requirements while the expanded overview and examination procedures address the AML risks of the specific activity.

At a minimum, examiners should use the following examination procedures included within the "Core Examination Overview and Procedures for Assessing the BSA/AML Compliance Program" section of this manual to ensure that the bank has an adequate BSA/AML compliance program commensurate with its risk profile:

- Scoping and Planning.
- BSA/AML Risk Assessment.
- BSA/AML Compliance Program.
- Developing Conclusions and Finalizing the Examination.

While OFAC regulations are not part of the BSA, the core sections include overview and examination procedures for examining a bank's policies, procedures, and processes for ensuring compliance with OFAC sanctions. As part of the scoping and planning procedures, examiners must review the bank's OFAC risk assessment and independent testing to determine the extent to which a review of the bank's OFAC compliance program should be conducted during the examination. Refer to core examination procedures, "Office of Foreign Assets Control," page 152, for further guidance.

The expanded sections address specific lines of business, products, customers, or entities that may present unique challenges and exposures for which banks should institute appropriate policies, procedures, and processes. Absent appropriate controls, these lines of business, products, customers, or entities could elevate BSA/AML risks. In addition, the expanded section provides guidance on BSA/AML compliance program structures and risk management.

Not all of the core and expanded examination procedures will likely be applicable to every banking organization. The specific examination procedures that will need to be performed depend on the BSA/AML risk profile of the banking organization, the quality and quantity of independent testing, the financial institution's history of BSA/AML compliance, and other relevant factors.

BACKGROUND

In 1970, Congress passed the Currency and Foreign Transactions Reporting Act commonly known as the "Bank Secrecy Act,[2] which established requirements for recordkeeping and reporting by private individuals, banks[3], and other financial institutions. The BSA was designed to help identify the source, volume, and movement of currency and other monetary instruments transported or transmitted into or out of the United States or deposited in financial institutions. The statute sought to achieve that objective by requiring individuals, banks, and other financial institutions to file currency reports with the U.S. Department of the Treasury (U.S. Treasury), properly identify persons conducting transactions, and maintain a paper trail by keeping appropriate records of financial transactions. These records 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.

The Money Laundering Control Act of 1986 augmented the BSA's effectiveness by adding the interrelated sections 8(s) and 21 to the Federal Deposit Insurance Act (FDIA) and section 206(q) of

the Federal Credit Union (FCUA), which sections apply equally to banks of all charters.[4] The Money Laundering Control Act of 1986 precludes circumvention of the BSA requirements by imposing criminal liability on a person or financial institution that knowingly assists in the laundering of money, or that structures transactions to avoid reporting them. The 1986 statute directed banks to establish and maintain procedures reasonably designed to ensure and monitor compliance with the reporting and recordkeeping requirements of the BSA. As a result, on January 27, 1987, all federal banking agencies issued essentially similar regulations requiring banks to develop programs for BSA compliance.

The 1992 Annunzio–Wylie Anti-Money Laundering Act strengthened the sanctions for BSA violations and the role of the U.S. Treasury. Two years later, Congress passed the Money Laundering Suppression Act of 1994 (MLSA), which further addressed the U.S. Treasury's role in combating money laundering.

In April 1996, a Suspicious Activity Report (SAR) was developed to be used by all banking organizations in the United States. A banking organization is required to file a SAR whenever it detects a known or suspected criminal violation of federal law or a suspicious transaction related to money laundering activity or a violation of the BSA.

In response to 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 (USA PATRIOT Act). Title III of the USA PATRIOT Act is the International Money Laundering Abatement and Anti-Terrorist Financing Act of 2001. The USA PATRIOT Act is arguably the single most significant AML law that Congress has enacted since the BSA itself. Among other things, the USA PATRIOT Act criminalized the financing of terrorism and augmented the existing BSA framework by strengthening customer identification procedures; prohibiting financial institutions from engaging in business with foreign shell banks; requiring financial institutions to have due diligence procedures and, in some cases, enhanced due diligence (EDD) procedures for foreign correspondent and private banking accounts; and improving information sharing between financial institutions and the U.S. government. The USA PATRIOT Act and its implementing regulations also:

- Expanded the AML program requirements to all financial institutions.[5] Refer to Appendix D ("Statutory Definition of Financial Institution") for further clarification.
- Increased the civil and criminal penalties for money laundering.
- Provided the Secretary of the Treasury with the authority to impose "special measures" on jurisdictions, institutions, or transactions that are of "primary money-laundering concern."
- Facilitated records access and required banks to respond to regulatory requests for information within 120 hours.
- Required federal banking agencies to consider a bank's AML record when reviewing bank mergers, acquisitions, and other applications for business combinations.

ROLE OF GOVERNMENT AGENCIES IN THE BSA

Certain government agencies play a critical role in implementing BSA regulations, developing examination guidance, ensuring compliance with the BSA, and enforcing the BSA. These agencies include the U.S. Treasury, FinCEN, and the federal banking agencies (Board of Governors of the Federal Reserve System, Federal Deposit Insurance Corporation, National Credit Union Administration, and Office of the Comptroller of the Currency). Internationally there are various multilateral government bodies that support the fight against money laundering and terrorist financing. Refer to Appendix E ("International Organizations") for additional information.

U.S. Treasury

The BSA authorizes the Secretary of the Treasury to require financial institutions to establish AML

programs, file certain reports, and keep certain records of transactions. Certain BSA provisions have been extended to cover not only traditional depository institutions, such as banks, savings associations, and credit unions, but also nonbank financial institutions, such as money services businesses, casinos, brokers/dealers in securities, futures commission merchants, mutual funds, insurance companies, and operators of credit card systems.

FinCEN

FinCEN, a bureau of the U.S. Treasury, is the delegated administrator of the BSA. In this capacity, FinCEN issues regulations and interpretive guidance, provides outreach to regulated industries, supports the examination functions performed by federal banking agencies, and pursues civil enforcement actions when warranted. FinCEN relies on the federal banking agencies to examine banks within their respective jurisdictions for compliance with the BSA. FinCEN's other significant responsibilities include providing investigative case support to law enforcement, identifying and communicating financial crime trends and patterns, and fostering international cooperation with its counterparts worldwide.

Federal Banking Agencies

The federal banking agencies are responsible for the oversight of the various banking entities operating in the United States, including foreign branch offices of U.S. banks. The federal banking agencies are charged with chartering (National Credit Union Administration, and Office of the Comptroller of the Currency), insuring (Federal Deposit Insurance Corporation and National Credit Union Administration), regulating, and supervising banks.[6] 12 USC 1818(s)(2) and 1786(q) require that the appropriate federal banking agency include a review of the BSA compliance program at each examination of an insured depository institution. The federal banking agencies may use their authority, as granted under section 8 of the FDIA or section 206 of the FCUA, to enforce compliance with appropriate banking rules and regulations, including compliance with the BSA.

The federal banking agencies require each bank under their supervision to establish and maintain a BSA compliance program.[7] In accordance with the Patriot Act, FinCEN's regulations require certain financial institutions to establish an AML compliance program that guards against money laundering and terrorist financing and ensures compliance with the BSA and its implementing regulations. When the USA PATRIOT Act was passed, banks under the supervision of a federal banking agency were already required by law to establish and maintain a BSA compliance program that, among other things, requires the bank to identify and report suspicious activity promptly. For this reason, 31 CFR 1020.210 states that a bank regulated by a federal banking agency is deemed to have satisfied the AML program requirements of the USA PATRIOT Act if the bank develops and maintains a BSA compliance program that complies with the regulation of its federal functional regulator[8] governing such programs. This manual will refer to the BSA compliance program requirements for each federal banking agency as the "BSA/AML compliance program."

Banks should take reasonable and prudent steps to combat money laundering and terrorist financing and to minimize their vulnerability to the risk associated with such activities. Some banking organizations have damaged their reputations and have been required to pay civil money penalties for failing to implement adequate controls within their organization resulting in noncompliance with the BSA. In addition, due to the AML assessment required as part of the application process, BSA/AML concerns can have an impact on the bank's strategic plan. For this reason, the federal banking agencies' and FinCEN's commitment to provide guidance that assists banks in complying with the BSA remains a high supervisory priority.

The federal banking agencies work to ensure that the organizations they supervise understand the importance of having an effective BSA/AML compliance program in place. Management must be vigilant in this area, especially as business grows and new products and services are introduced. An

evaluation of the bank's BSA/AML compliance program and its compliance with the regulatory requirements of the BSA has been an integral part of the supervision process for years. Refer to Appendix A ("BSA Laws and Regulations") for further information.

As part of a strong BSA/AML compliance program, the federal banking agencies seek to ensure that a bank has policies, procedures, and processes to identify and report suspicious transactions to law enforcement. The agencies' supervisory processes assess whether banks have established the appropriate policies, procedures, and processes based on their BSA/AML risk to identify and report suspicious activity and that they provide sufficient detail in reports to law enforcement agencies to make the reports useful for investigating suspicious transactions that are reported. Refer to Appendices B ("BSA/AML Directives") and C ("BSA/AML References") for guidance.

On July 19, 2007, the federal banking agencies issued a statement setting forth the agencies' policy for enforcing specific anti-money laundering requirements of the BSA. The purpose of the *Interagency Statement on Enforcement of Bank Secrecy Act/Anti-Money Laundering Requirements* (Interagency Enforcement Statement) is to provide greater consistency among the agencies in enforcement decisions in BSA matters and to offer insight into the considerations that form the basis of those decisions.[9]

OFAC

OFAC administers and enforces economic and trade sanctions based on U.S. foreign policy and national security goals against targeted foreign countries, terrorists, international narcotics traffickers, and those engaged in activities related to the proliferation of weapons of mass destruction. OFAC acts under the President's wartime and national emergency powers, as well as under authority granted by specific legislation, to impose controls on transactions and freeze assets under U.S. jurisdiction. Many of the sanctions are based on United Nations and other international mandates, are multilateral in scope, and involve close cooperation with allied governments.

OFAC requirements are separate and distinct from the BSA, but both OFAC and the BSA share a common national security goal. For this reason, many financial institutions view compliance with OFAC sanctions as related to BSA compliance obligations; supervisory examination for BSA compliance is logically connected to the examination of a financial institution's compliance with OFAC sanctions. Refer to the core overview and examination procedures, "Office of Foreign Assets Control," pages 142 and 152, respectively, for guidance.

MONEY LAUNDERING AND TERRORIST FINANCING

The BSA is intended to safeguard the U.S. financial system and the financial institutions that make up that system from the abuses of financial crime, including money laundering, terrorist financing, and other illicit financial transactions. Money laundering and terrorist financing are financial crimes with potentially devastating social and financial effects. From the profits of the narcotics trafficker to the assets looted from government coffers by dishonest foreign officials, criminal proceeds have the power to corrupt and ultimately destabilize communities or entire economies. Terrorist networks are able to facilitate their activities if they have financial means and access to the financial system. In both money laundering and terrorist financing, criminals can exploit loopholes and other weaknesses in the legitimate financial system to launder criminal proceeds, finance terrorism, or conduct other illegal activities, and, ultimately, hide the actual purpose of their activity.

Banking organizations must develop, implement, and maintain effective AML programs that address the ever-changing strategies of money launderers and terrorists who attempt to gain access to the U.S. financial system. A sound BSA/AML compliance program is critical in deterring and preventing these types of activities at, or through, banks and other financial institutions. Refer to Appendix F ("Money Laundering and Terrorist Financing Red Flags") for examples of suspicious activities that may indicate money laundering or terrorist financing.

Money Laundering

Money laundering is the criminal practice of processing ill-gotten gains, or "dirty" money, through a series of transactions; in this way the funds are "cleaned" so that they appear to be proceeds from legal activities. Money laundering generally does not involve currency at every stage of the laundering process. Although money laundering is a diverse and often complex process, it basically involves three independent steps that can occur simultaneously:

- **Placement**. The first and most vulnerable stage of laundering money is placement. The goal is to introduce the unlawful proceeds into the financial system without attracting the attention of financial institutions or law enforcement. Placement techniques include structuring currency deposits in amounts to evade reporting requirements or commingling currency deposits of legal and illegal enterprises. An example may include: dividing large amounts of currency into less-conspicuous smaller sums that are deposited directly into a bank account, depositing a refund check from a canceled vacation package or insurance policy, or purchasing a series of monetary instruments (e.g., cashier's checks or money orders) that are then collected and deposited into accounts at another location or financial institution. Refer to Appendix G ("Structuring") for additional guidance.
- **Layering**. The second stage of the money laundering process is layering, which involves moving funds around the financial system, often in a complex series of transactions to create confusion and complicate the paper trail. Examples of layering include exchanging monetary instruments for larger or smaller amounts, or wiring or transferring funds to and through numerous accounts in one or more financial institutions.
- **Integration**. The ultimate goal of the money laundering process is integration. Once the funds are in the financial system and insulated through the layering stage, the integration stage is used to create the appearance of legality through additional transactions. These transactions further shield the criminal from a recorded connection to the funds by providing a plausible explanation for the source of the funds. Examples include the purchase and resale of real estate, investment securities, foreign trusts, or other assets.

Terrorist Financing

The motivation behind terrorist financing is ideological as opposed to profit-seeking, which is generally the motivation for most crimes associated with money laundering. Terrorism is intended to intimidate a population or to compel a government or an international organization to do or abstain from doing any specific act through the threat of violence. An effective financial infrastructure is critical to terrorist operations. Terrorist groups develop sources of funding that are relatively mobile to ensure that funds can be used to obtain material and other logistical items needed to commit terrorist acts. Thus, money laundering is often a vital component of terrorist financing.

Terrorists generally finance their activities through both unlawful and legitimate sources. Unlawful activities, such as extortion, kidnapping, and narcotics trafficking, have been found to be a major source of funding. Other observed activities include smuggling, fraud, theft, robbery, identity theft, use of conflict diamonds,[10] and improper use of charitable or relief funds. In the last case, donors may have no knowledge that their donations have been diverted to support terrorist causes.

Other legitimate sources have also been found to provide terrorist organizations with funding; these legitimate funding sources are a key difference between terrorist financiers and traditional criminal organizations. In addition to charitable donations, legitimate sources include foreign government sponsors, business ownership, and personal employment.

Although the motivation differs between traditional money launderers and terrorist financiers, the actual methods used to fund terrorist operations can be the same as or similar to those methods used by other criminals that launder funds. For example, terrorist financiers use currency

smuggling, structured deposits or withdrawals from bank accounts; purchases of various types of monetary instruments; credit, debit, or prepaid cards; and funds transfers. There is also evidence that some forms of informal banking (e.g., "hawala"[11]) have played a role in moving terrorist funds. Transactions through hawalas are difficult to detect given the lack of documentation, their size, and the nature of the transactions involved. Funding for terrorist attacks does not always require large sums of money, and the associated transactions may not be complex.

Criminal Penalties for Money Laundering, Terrorist Financing, and Violations of the BSA

Penalties for money laundering and terrorist financing can be severe. A person convicted of money laundering can face up to 20 years in prison and a fine of up to $500,000.[12] Any property involved in a transaction or traceable to the proceeds of the criminal activity, including property such as loan collateral, personal property, and, under certain conditions, entire bank accounts (even if some of the money in the account is legitimate), may be subject to forfeiture. Pursuant to various statutes, banks and individuals may incur criminal and civil liability for violating AML and terrorist financing laws. For instance, pursuant to 18 USC 1956 and 1957, the U.S. Department of Justice may bring criminal actions for money laundering that may include criminal fines, imprisonment, and forfeiture actions.[13] In addition, banks risk losing their charters, and bank employees risk being removed and barred from banking.

Moreover, there are criminal penalties for willful violations of the BSA and its implementing regulations under 31 USC 5322 and for structuring transactions to evade BSA reporting requirements under 31 USC 5324(d). For example, a person, including a bank employee, willfully violating the BSA or its implementing regulations is subject to a criminal fine of up to $250,000 or five years in prison, or both.[14] A person who commits such a violation while violating another U.S. law, or engaging in a pattern of criminal activity, is subject to a fine of up to $500,000 or ten years in prison, or both.[15] A bank that violates certain BSA provisions, including 31 USC 5318(i) or (j), or special measures imposed under 31 USC 5318A, faces criminal money penalties up to the greater of $1 million or twice the value of the transaction.[16]

Civil Penalties for Violations of the BSA

Pursuant to 12 USC 1818(i) and 1786(k), and 31 USC 5321, the federal banking agencies and FinCEN, respectively, can bring civil money penalty actions for violations of the BSA. Moreover, in addition to criminal and civil money penalty actions taken against them, individuals may be removed from banking pursuant to 12 USC 1818(e)(2) for a violation of the AML laws under Title 31 of the U.S. Code, as long as the violation was not inadvertent or unintentional. All of these actions are publicly available.

Backward | Table of Contents | Forward

Appendix Item 2

Bank Secrecy Act
Anti-Money Laundering
Examination Manual

Backward | Table of Contents | Forward

Suspicious Activity Reporting—Overview

Objective. *Assess the bank's policies, procedures, and processes, and overall compliance with statutory and regulatory requirements for monitoring, detecting, and reporting suspicious activities.*

Suspicious activity reporting forms the cornerstone of the BSA reporting system. It is critical to the United States' ability to utilize financial information to combat terrorism, terrorist financing, money laundering, and other financial crimes. Examiners and banks should recognize that the quality of SAR content is critical to the adequacy and effectiveness of the suspicious activity reporting system.

Within this system, FinCEN and the federal banking agencies recognize that, as a practical matter, it is not possible for a bank to detect and report all potentially illicit transactions that flow through the bank. Examiners should focus on evaluating a bank's policies, procedures, and processes to identify, evaluate, and report suspicious activity. However, as part of the examination process, examiners should review individual SAR filing decisions to determine the effectiveness of the bank's suspicious activity identification, evaluation, and reporting process. Banks, bank holding companies, and their subsidiaries are required by federal regulations[53] to file a SAR with respect to:

- Criminal violations involving insider abuse in any amount.
- Criminal violations aggregating $5,000 or more when a suspect can be identified.
- Criminal violations aggregating $25,000 or more regardless of a potential suspect.
- Transactions conducted or attempted by, at, or through the bank (or an affiliate) and aggregating $5,000 or more, if the bank or affiliate knows, suspects, or has reason to suspect that the transaction:
  - May involve potential money laundering or other illegal activity (e.g., terrorism financing).[54]
  - Is designed to evade the BSA or its implementing regulations.[55]
  - Has no business or apparent lawful purpose or is not the type of transaction that the particular customer would normally be expected to engage in, and the bank knows of no reasonable explanation for the transaction after examining the available facts, including the background and possible purpose of the transaction.

Footnote ×
Refer to Appendix G ("Structuring") for additional guidance.

A transaction includes a deposit; a withdrawal; a transfer between accounts; an exchange of currency; an extension of credit; a purchase or sale of any stock, bond, certificate of deposit, or other monetary instrument or investment security; or any other payment, transfer, or delivery by, through, or to a bank.

Safe Harbor for Banks From Civil Liability for Suspicious Activity Reporting

Federal law (31 USC 5318(g)(3)) provides protection from civil liability for all reports of suspicious transactions made to appropriate authorities, including supporting documentation, regardless of whether such reports are filed pursuant to the SAR instructions. Specifically, the law provides that a bank and its directors, officers, employees, and agents that make a disclosure to the appropriate

authorities of any possible violation of law or regulation, including a disclosure in connection with the preparation of SARs, "shall not be liable to any person under any law or regulation of the United States, any constitution, law, or regulation of any State or political subdivision of any State, or under any contract or other legally enforceable agreement (including any arbitration agreement), for such disclosure or for any failure to provide notice of such disclosure to the person who is the subject of such disclosure or any other person identified in the disclosure." The safe harbor applies to SARs filed within the required reporting thresholds as well as to SARs filed voluntarily on any activity below the threshold.[56]

Systems to Identify, Research, and Report Suspicious Activity

Suspicious activity monitoring and reporting are critical internal controls. Proper monitoring and reporting processes are essential to ensuring that the bank has an adequate and effective BSA compliance program. Appropriate policies, procedures, and processes should be in place to monitor and identify unusual activity. The sophistication of monitoring systems should be dictated by the bank's risk profile, with particular emphasis on the composition of higher-risk products, services, customers, entities, and geographies. The bank should ensure adequate staff is assigned to the identification, research, and reporting of suspicious activities, taking into account the bank's overall risk profile and the volume of transactions. Monitoring systems typically include employee identification or referrals, transaction-based (manual) systems, surveillance (automated) systems, or any combination of these.

Generally, effective suspicious activity monitoring and reporting systems include five key components (refer to Appendix S "Key Suspicious Activity Monitoring Components"). The components, listed below, are interdependent, and an effective suspicious activity monitoring and reporting process should include successful implementation of each component. Breakdowns in any one or more of these components may adversely affect SAR reporting and BSA compliance. The five key components to an effective monitoring and reporting system are:

- Identification or alert of unusual activity (which may include: employee identification, law enforcement inquiries, other referrals, and transaction and surveillance monitoring system output).
- Managing alerts.
- SAR decision making.
- SAR completion and filing.
- Monitoring and SAR filing on continuing activity.

These components are present in banks of all sizes. However, the structure and formality of the components may vary. Larger banks will typically have greater differentiation and distinction between functions, and may devote entire departments to the completion of each component. Smaller banks may use one or more employees to complete several tasks (e.g., review of monitoring reports, research activity, and completion of the actual SAR). Policies, procedures, and processes should describe the steps the bank takes to address each component and indicate the person(s) or departments responsible for identifying or producing an alert of unusual activity, managing the alert, deciding whether to file, SAR completion and filing, and monitoring and SAR filing on continuing activity.

Identification of Unusual Activity

Banks use a number of methods to identify potentially suspicious activity, including but not limited to activity identified by employees during day-to-day operations, law enforcement inquiries, or requests, such as those typically seen in section 314(a) and section 314(b) requests, advisories issued by regulatory or law enforcement agencies, transaction and surveillance monitoring system output, or any combination of these.

Employee Identification

During the course of day-to-day operations, employees may observe unusual or potentially suspicious transaction activity. Banks should implement appropriate training, policies, and procedures to ensure that personnel adhere to the internal processes for identification and referral of potentially suspicious activity. Banks should be aware of all methods of identification and should ensure that their suspicious activity monitoring system includes processes to facilitate the transfer of internal referrals to appropriate personnel for further research.

Law Enforcement Inquiries and Requests

Banks should establish policies, procedures, and processes for identifying subjects of law enforcement requests, monitoring the transaction activity of those subjects when appropriate, identifying unusual or potentially suspicious activity related to those subjects, and filing, as

appropriate, SARs related to those subjects. Law enforcement inquiries and requests can include grand jury subpoenas, National Security Letters (NSL), and section 314(a) requests.[57]

Mere receipt of any law enforcement inquiry does not, by itself, require the filing of a SAR by the bank. Nonetheless, a law enforcement inquiry may be relevant to a bank's overall risk assessment of its customers and accounts. For example, the receipt of a grand jury subpoena should cause a bank to review account activity for the relevant customer.[58] A bank should assess all of the information it knows about its customer, including the receipt of a law enforcement inquiry, in accordance with its risk-based BSA/AML compliance program.

The bank should determine whether a SAR should be filed based on all customer information available. Due to the confidentiality of grand jury proceedings, if a bank files a SAR after receiving a grand jury subpoena, law enforcement discourages banks from including any reference to the receipt or existence of the grand jury subpoena in the SAR. Rather, the SAR should reference only those facts and activities that support a finding of suspicious transactions identified by the bank.

National Security Letters

NSLs are written investigative demands that may be issued by the local Federal Bureau of Investigation (FBI) and other federal governmental authorities in counterintelligence and counterterrorism investigations to obtain the following:

- Telephone and electronic communications records from telephone companies and Internet service providers.[59]
- Information from credit bureaus.[60]
- Financial records from financial institutions.[61]

NSLs are highly confidential documents; for that reason, examiners will not review or sample specific NSLs.[62] Pursuant to 12 USC 3414(a)(3) and (5)(D), no bank, or officer, employee or agent of the institution, can disclose to any person that a government authority or the FBI has sought or obtained access to records through a Right to Financial Privacy Act NSL. Banks that receive NSLs must take appropriate measures to ensure the confidentiality of the letters and should have procedures in place for processing and maintaining the confidentiality of NSLs.

If a bank files a SAR after receiving a NSL, the SAR should not contain any reference to the receipt or existence of the NSL. The SAR should reference only those facts and activities that support a finding of unusual or suspicious transactions identified by the bank.

Questions regarding NSLs should be directed to the bank's local FBI field office. Contact information for the FBI field offices can be found at www.fbi.gov.

Transaction Monitoring (Manual Transaction Monitoring)

A transaction monitoring system, sometimes referred to as a manual transaction monitoring system, typically targets specific types of transactions (e.g., those involving large amounts of cash, those to or from foreign geographies) and includes a manual review of various reports generated by the bank's MIS or vendor systems in order to identify unusual activity. Examples of MIS reports include currency activity reports, funds transfer reports, monetary instrument sales reports, large item reports, significant balance change reports, ATM transaction reports, and nonsufficient funds (NSF) reports. Many MIS or vendor systems include filtering models for identification of potentially unusual activity. The process may involve review of daily reports, reports that cover a period of time (e.g., rolling 30-day reports, monthly reports), or a combination of both types of reports. The type and frequency of reviews and resulting reports used should be commensurate with the bank's BSA/AML risk profile and appropriately cover its higher-risk products, services, customers, entities, and geographic locations.

MIS or vendor system-generated reports typically use a discretionary dollar threshold. Thresholds selected by management for the production of transaction reports should enable management to detect unusual activity. Upon identification of unusual activity, assigned personnel should review CDD and other pertinent information to determine whether the activity is suspicious. Management should periodically evaluate the appropriateness of filtering criteria and thresholds used in the monitoring process. Each bank should evaluate and identify filtering criteria most appropriate for their bank. The programming of the bank's monitoring systems should be independently reviewed for reasonable filtering criteria. Typical transaction monitoring reports are as follows.

Currency activity reports. Most vendors offer reports that identify all currency activity or currency activity greater than $10,000. These reports assist bankers with filing CTRs and identifying suspicious currency activity. Most bank information service providers offer currency activity reports that can filter transactions using various parameters, for example:

- Currency activity including multiple transactions greater than $10,000.
- Currency activity (single and multiple transactions) below the $10,000 reporting requirement (e.g., between $7,000 and $10,000).
- Currency transactions involving multiple lower dollar transactions (e.g., $3,000) that over a period of time (e.g., 15 days) aggregate to a substantial sum of money (e.g., $30,000).
- Currency transactions aggregated by customer name, tax identification number, or customer information file number.

Such filtering reports, whether implemented through a purchased vendor software system or through requests from information service providers, will significantly enhance a bank's ability to identify and evaluate unusual currency transactions.

Funds transfer records. The BSA requires banks to maintain records of funds transfer in amounts of $3,000 and above. Periodic review of this information can assist banks in identifying patterns of unusual activity. A periodic review of the funds transfer records in banks with low funds transfer activity is usually sufficient to identify unusual activity. For banks with more significant funds transfer activity, use of spreadsheet or vendor software is an efficient way to review funds transfer activity for unusual patterns. Most vendor software systems include standard suspicious activity filter reports. These reports typically focus on identifying certain higher-risk geographic locations and larger dollar funds transfer transactions for individuals and businesses. Each bank should establish its own filtering criteria for both individuals and businesses. Noncustomer funds transfer transactions and payable upon proper identification (PUPID) transactions should be reviewed for unusual activity. Activities identified during these reviews should be subjected to additional research to ensure that identified activity is consistent with the stated account purpose and expected activity. When inconsistencies are identified, banks may need to conduct a global relationship review to determine if a SAR is warranted.

Monetary instrument records. Records for monetary instrument sales are required by the BSA. Such records can assist the bank in identifying possible currency structuring through the purchase of cashier's checks, official bank checks, money orders, or traveler's checks in amounts of $3,000 to $10,000. A periodic review of these records can also help identify frequent purchasers of monetary instruments and common payees. Reviews for suspicious activity should encompass activity for an extended period of time (30, 60, 90 days) and should focus on, among other things, identification of commonalities, such as common payees and purchasers, or consecutively numbered purchased monetary instruments.

Surveillance Monitoring (Automated Account Monitoring)

A surveillance monitoring system, sometimes referred to as an automated account monitoring system, can cover multiple types of transactions and use various rules to identify potentially suspicious activity. In addition, many can adapt over time based on historical activity, trends, or internal peer comparison. These systems typically use computer programs, developed in-house or purchased from vendors, to identify individual transactions, patterns of unusual activity, or deviations from expected activity. These systems can capture a wide range of account activity, such as deposits, withdrawals, funds transfers, automated clearing house (ACH) transactions, and automated teller machine (ATM) transactions, directly from the bank's core data processing system. Banks that are large, operate in many locations, or have a large volume of higher-risk customers typically use surveillance monitoring systems.

Surveillance monitoring systems include rule-based and intelligent systems. Rule-based systems detect unusual transactions that are outside of system-developed or management-established "rules." Such systems can consist of few or many rules, depending on the complexity of the in-house or vendor product. These rules are applied using a series of transaction filters or a rules engine. Rule-based systems are more sophisticated than the basic manual system, which only filters on one rule (e.g., transaction greater than $10,000). Rule-based systems can apply multiple rules, overlapping rules, and filters that are more complex. For example, rule-based systems can initially apply a rule, or set of criteria to all accounts within a bank (e.g., all retail customers), and then apply a more refined set of criteria to a subset of accounts or risk category of accounts (e.g., all retail customers with direct deposits). Rule-based systems can also filter against individual customer-account profiles.

Intelligent systems are adaptive and can filter transactions, based on historical account activity or compare customer activity against a pre-established peer group or other relevant data. Intelligent systems review transactions in context with other transactions and the customer profile. In doing so, these systems increase their information database on the customer, account type, category, or business, as more transactions and data are stored in the system.

Relative to surveillance monitoring, system capabilities and thresholds refer to the parameters or filters used by banks in their monitoring processes. Parameters and filters should be reasonable and tailored to the activity that the bank is trying to identify or control. After parameters and filters have been developed, they should be reviewed before implementation to identify any gaps (common money laundering techniques or frauds) that may not have been addressed. For example, a bank

Suspicious Activity Information, Part II of the SAR provides a number of categories with different types of suspicious activity. Within each category, there is the option of selecting "Other" if none of the suspicious activities apply. However, the use of "Other" should be limited to situations that cannot be broadly identified within the categories provided.

SAR Decision Making

After thorough research and analysis has been completed, findings are typically forwarded to a final decision maker (individual or committee). The bank should have policies, procedures, and processes for referring unusual activity from all business lines to the personnel or department responsible for evaluating unusual activity. Within those procedures, management should establish a clear and defined escalation process from the point of initial detection to disposition of the investigation.

The decision maker, whether an individual or committee, should have the authority to make the final SAR filing decision. When the bank uses a committee, there should be a clearly defined process to resolve differences of opinion on filing decisions. Banks should document SAR decisions, including the specific reason for filing or not filing a SAR. Thorough documentation provides a record of the SAR decision-making process, including final decisions not to file a SAR. However, due to the variety of systems used to identify, track, and report suspicious activity, as well as the fact that each suspicious activity reporting decision will be based on unique facts and circumstances, no single form of documentation is required when a bank decides not to file.[64]

The decision to file a SAR is an inherently subjective judgment. Examiners should focus on whether the bank has an effective SAR decision-making process, not individual SAR decisions. Examiners may review individual SAR decisions as a means to test the effectiveness of the SAR monitoring, reporting, and decision-making process. In those instances where the bank has an established SAR decision-making process, has followed existing policies, procedures, and processes, and has determined not to file a SAR, the bank should not be criticized for the failure to file a SAR unless the failure is significant or accompanied by evidence of bad faith.[65]

SAR Filing on Continuing Activity

One purpose of filing SARs is to identify violations or potential violations of law to the appropriate law enforcement authorities for criminal investigation. This objective is accomplished by the filing of a SAR that identifies the activity of concern. If this activity continues over a period of time, such information should be made known to law enforcement and the federal banking agencies. FinCEN's guidelines have suggested that banks should report continuing suspicious activity by filing a report at least every 90 calendar days. Subsequent guidance permits banks with SAR requirements to file SARs for continuing activity after a 90 day review with the filing deadline being 120 calendar days after the date of the previously related SAR filing. Banks may also file SARs on continuing activity earlier than the 120 day deadline if the bank believes the activity warrants earlier review by law enforcement.[66] This practice will notify law enforcement of the continuing nature of the activity in aggregate. In addition, this practice will remind the bank that it should continue to review the suspicious activity to determine whether other actions may be appropriate, such as bank management determining that it is necessary to terminate a relationship with the customer or employee that is the subject of the filing.

Banks should be aware that law enforcement may have an interest in ensuring that certain accounts remain open notwithstanding suspicious or potential criminal activity in connection with those accounts. If a law enforcement agency requests that a bank maintain a particular account, the bank should ask for a written request. The written request should indicate that the agency has requested that the bank maintain the account and the purpose and duration of the request. Ultimately, the decision to maintain or close an account should be made by a bank in accordance with its own standards and guidelines.[67]

The bank should develop policies, procedures, and processes indicating when to escalate issues or problems identified as the result of repeat SAR filings on accounts. The procedures should include:

- Review by senior management and legal staff (e.g., BSA compliance officer or SAR committee).
- Criteria for when analysis of the overall customer relationship is necessary.
- Criteria for whether and, if so, when to close the account.
- Criteria for when to notify law enforcement, if appropriate.

SAR Completion and Filing

SAR completion and filing are a critical part of the SAR monitoring and reporting process. Appropriate policies, procedures, and processes should be in place to ensure SARs are filed in a timely manner, are complete and accurate, and that the narrative provides a sufficient description of the activity reported as well as the basis for filing. FinCEN developed a new electronic BSA

Suspicious Activity Report (BSAR) that replaced FinCEN SAR-DI form TD F 90-22.47. The BSAR provides a uniform data collection format that can be used across multiple industries. As of April 1, 2013, the BSAR is mandatory and must be filed through FinCEN's BSA E-Filing System. The BSAR does not create or otherwise change existing statutory and regulatory expectations for banks.

The BSAR includes a number of additional data elements pertaining to the type of suspicious activity and the financial services involved. Certain fields in the BSAR are marked as "critical" for technical filing purposes. This means the BSA E-Filing System will not accept filings in which these fields are left blank. For these items, the bank must either provide the requested information or check the "unknown" box that is provided with each critical field. Banks should provide the most complete filing information available consistent with existing regulatory expectations, regardless of whether or not the individual fields are deemed critical for technical filing purposes.[68]

Banks should report the information that they know, or that otherwise arises, as part of their case reviews. Other than the critical fields, the addition of the new and expanded data elements does not create an expectation that banks will revise internal programs, or develop new programs, to capture information that reflects the expanded lists.[69] Refer to Appendix T for additional information on filing through the BSA E-Filing System.

Timing of a SAR Filing

The SAR rules require that a SAR be electronically filed through the BSA E-Filing System no later than 30 calendar days from the date of the initial detection of facts that may constitute a basis for filing a SAR. If no suspect can be identified, the time period for filing a SAR is extended to 60 days. Organizations may need to review transaction or account activity for a customer to determine whether to file a SAR. The need for a review of customer activity or transactions does not necessarily indicate a need to file a SAR. The time period for filing a SAR starts when the organization, during its review or because of other factors, knows or has reason to suspect that the activity or transactions under review meet one or more of the definitions of suspicious activity.[70]

The phrase "initial detection" should not be interpreted as meaning the moment a transaction is highlighted for review. There are a variety of legitimate transactions that could raise a red flag simply because they are inconsistent with an accountholder's normal account activity. For example, a real estate investment (purchase or sale), the receipt of an inheritance, or a gift, may cause an account to have a significant credit or debit that would be inconsistent with typical account activity. The bank's automated account monitoring system or initial discovery of information, such as system-generated reports, may flag the transaction; however, this should not be considered initial detection of potential suspicious activity. The 30-day (or 60-day) period does not begin until an appropriate review is conducted and a determination is made that the transaction under review is "suspicious" within the meaning of the SAR regulation.[71]

Whenever possible, an expeditious review of the transaction or the account is recommended and can be of significant assistance to law enforcement. In any event, the review should be completed in a reasonable period of time. What constitutes a "reasonable period of time" will vary according to the facts and circumstances of the particular matter being reviewed and the effectiveness of the SAR monitoring, reporting, and decision-making process of each bank. The key factor is that a bank has established adequate procedures for reviewing and assessing facts and circumstances identified as potentially suspicious, and that those procedures are documented and followed.[72]

For situations requiring immediate attention, in addition to filing a timely SAR, a bank must immediately notify, by telephone, an "appropriate law enforcement authority" and, as necessary, the bank's primary regulator. For this initial notification, an "appropriate law enforcement authority" would generally be the local office of the IRS Criminal Investigation Division or the FBI. Notifying law enforcement of a suspicious activity does not relieve a bank of its obligation to file a SAR.[73]

SAR Quality

Banks are required to file SARs that are complete, thorough, and timely. Banks should include all known subject information on the SAR. The importance of the accuracy of this information cannot be overstated. Inaccurate information on the SAR, or an incomplete or disorganized narrative, may make further analysis difficult, if not impossible. However, there may be legitimate reasons why certain information may not be provided in a SAR, such as when the filer does not have the information. A thorough and complete narrative may make the difference in determining whether the described conduct and its possible criminal nature are clearly understood by law enforcement. Because the SAR narrative section is the only area summarizing suspicious activity, the section, as stated on the SAR, is "critical." Thus, a failure to adequately describe the factors making a transaction or activity suspicious undermines the purpose of the SAR.

To inform and assist banks in reporting instances of suspected money laundering, terrorist financing, and fraud, FinCEN issues advisories and guidance containing examples of "red flags." In order to assist law enforcement in its efforts to target these activities, FinCEN requests that banks check the appropriate box(es) in the Suspicious Activity Information section and include certain key terms in

the narrative section of the SAR. The advisories and guidance can be found on FinCEN's website.[74]

By their nature, SAR narratives are subjective, and examiners generally should not criticize the bank's interpretation of the facts. Nevertheless, banks should ensure that SAR narratives are complete, thoroughly describe the extent and nature of the suspicious activity, and are included within the SAR. The BSAR will accept a single, Microsoft Excel compatible comma separated value (csv) file no larger than one (1) megabyte as an attachment as part of the report. This capability allows a bank to include transactional data such as specific financial transactions and funds transfers or other analytics which is more readable or usable in this format than it would be if otherwise included in the narrative. Such an attachment will be considered a part of the narrative and is not considered to be a substitute for the narrative. For example, narratives should not simply state "see attachment" if the bank included a csv attachment. As with other information that may be prepared in connection with the filing of a SAR, an attachment is considered supporting documentation and should be treated as confidential to the extent that it indicates the existence of a SAR.

More specific guidance is available in Appendix L ("SAR Quality Guidance") to assist banks in writing, and assist examiners in evaluating, SAR narratives.[75]

Notifying Board of Directors of SAR Filings

Banks are required by the SAR regulations of their federal banking agency to notify the board of directors or an appropriate board committee that SARs have been filed. However, the regulations do not mandate a particular notification format and banks should have flexibility in structuring their format. Therefore, banks may, but are not required to, provide actual copies of SARs to the board of directors or a board committee. Alternatively, banks may opt to provide summaries, tables of SARs filed for specific violation types, or other forms of notification. Regardless of the notification format used by the bank, management should provide sufficient information on its SAR filings to the board of directors or an appropriate committee in order to fulfill its fiduciary duties, while being mindful of the confidential nature of the SAR.[76]

Record Retention and Supporting Documentation

Banks must retain copies of SARs and supporting documentation for five years from the date of filing the SAR. The bank can retain copies in paper or electronic format. Additionally, banks must provide all documentation supporting the filing of a SAR upon request by FinCEN or an appropriate law enforcement or federal banking agency. "Supporting documentation" refers to all documents or records that assisted a bank in making the determination that certain activity required a SAR filing. No legal process is required for disclosure of supporting documentation to FinCEN or an appropriate law enforcement or federal banking agency.[77]

Prohibition of SAR Disclosure

No bank, and no director, officer, employee, or agent of a bank that reports a suspicious transaction may notify any person involved in the transaction that the transaction has been reported. A SAR and any information that would reveal the existence of a SAR, are confidential, except as is necessary to fulfill BSA obligations and responsibilities. For example, the existence or even the non-existence of a SAR must be kept confidential, as well as the information contained in the SAR to the extent that the information would reveal the existence of a SAR.[78] Furthermore, FinCEN and the federal banking agencies take the position that a bank's internal controls for the filing of SARs should minimize the risks of disclosure.

A bank or its agent may reveal the existence of a SAR to fulfill responsibilities consistent with the BSA, provided no person involved in a suspicious transaction is notified that the transaction has been reported. The underlying facts, transactions, and supporting documents of a SAR may be disclosed to another financial institution for the preparation of a joint SAR, or in connection with certain employment references or termination notices to the full extent authorized in 31 USC 5318(g)(2)(B). The sharing of a SAR by a bank or its agent with certain permissible entities within the bank's corporate organizational structure for purposes consistent with Title II of the Bank Secrecy Act is also allowed.

Any person subpoenaed or otherwise requested to disclose a SAR or the information contained in a SAR, except when such disclosure is requested by FinCEN or an appropriate law enforcement[79] or federal banking agency, shall decline to produce the SAR or to provide any information that would disclose that a SAR has been prepared or filed, citing 31 CFR 1020.320(e) and 31 USC 5318(g)(2)(A)(i). FinCEN and the bank's federal banking agency should be notified of any such request and of the bank's response. Furthermore, FinCEN and the federal banking agencies take the position that banks' internal controls for the filing of SARs should minimize the risks of disclosure.

Examiners should follow their respective agency's protocol on discovery of the improper disclosure of a SAR. Examiners also should ensure the bank has notified the appropriate federal banking agency and FinCEN of the improper disclosure.

Appendix Item 3

Bank Secrecy Act
Anti-Money Laundering
Examination Manual

Backward | Table of Contents | Forward

CORE EXAMINATION OVERVIEW AND PROCEDURES FOR REGULATORY REQUIREMENTS AND RELATED TOPICS

Customer Identification Program—Overview

Objective. *Assess the bank's compliance with the statutory and regulatory requirements for the Customer Identification Program (CIP).*

All banks must have a written CIP.[40] The CIP rule implements section 326 of the USA PATRIOT Act and requires each bank to implement a written CIP that is appropriate for its size and type of business and that includes certain minimum requirements. The CIP must be incorporated into the bank's BSA/AML compliance program, which is subject to approval by the bank's board of directors.[41] The implementation of a CIP by subsidiaries of banks is appropriate as a matter of safety and soundness and protection from reputational risks. Domestic subsidiaries (other than functionally regulated subsidiaries subject to separate CIP rules) of banks should comply with the CIP rule that applies to the parent bank when opening an account within the meaning of 31 CFR 1020.100.[42]

The CIP is intended to enable the bank to form a reasonable belief that it knows the true identity of each customer. The CIP must include account opening procedures that specify the identifying information that will be obtained from each customer. It must also include reasonable and practical risk-based procedures for verifying the identity of each customer. Banks should conduct a risk assessment of their customer base and product offerings, and in determining the risks, consider:

- The types of accounts offered by the bank.

- The bank's methods of opening accounts.
- The types of identifying information available.
- The bank's size, location, and customer base, including types of products and services used by customers in different geographic locations.

Pursuant to the CIP rule, an "account" is a formal banking relationship to provide or engage in services, dealings, or other financial transactions, and includes a deposit account, a transaction or asset account, a credit account, or another extension of credit. An account also includes a relationship established to provide a safe deposit box or other safekeeping services or to provide cash management, custodian, or trust services.

An account does not include:

- Products or services for which a formal banking relationship is not established with a person, such as check cashing, funds transfer, or the sale of a check or money order.
- Any account that the bank acquires. This may include single or multiple accounts as a result of a purchase of assets, acquisition, merger, or assumption of liabilities.
- Accounts opened to participate in an employee benefit plan established under the Employee Retirement Income Security Act of 1974.

The CIP rule applies to a "customer." A customer is a "person" (an individual, a corporation, partnership, a trust, an estate, or any other entity recognized as a legal person) who opens a new account, an individual who opens a new account for another individual who lacks legal capacity, and an individual who opens a new account for an entity that is not a legal person (e.g., a civic club). A customer does not include a person who does not receive banking services, such as a person whose loan application is denied.[43] The definition of "customer" also does not include an existing customer as long as the bank has a reasonable belief that it knows the customer's true identity.[44] Excluded from the definition of customer are federally regulated banks, banks regulated by a state bank regulator, governmental entities, and publicly traded companies (as described in 31 CFR 1020.315(b)(1) through (4)).

Customer Information Required

The CIP must contain account-opening procedures detailing the identifying information that must be obtained from each customer.[45] At a minimum, the bank must obtain the following identifying information from each customer before opening the account:[46]

- Name.
- Date of birth for individuals.
- Address.[47]
- Identification number.[48]

Based on its risk assessment, a bank may require identifying information in addition to the items above for certain customers or product lines.

Customer Verification

The CIP must contain risk-based procedures for verifying the identity of the customer within a reasonable period of time after the account is opened. The verification procedures must use "the information obtained in accordance with [31 CFR 1020.220] paragraph (a)(2)(i)," namely the identifying information obtained by the bank. A bank need not establish the accuracy of every element of identifying information obtained, but it must verify enough information to form a reasonable belief that it knows the true identity of the customer. The bank's procedures must

describe when it will use documents, nondocumentary methods, or a combination of both.

Verification Through Documents

A bank using documentary methods to verify a customer's identity must have procedures that set forth the minimum acceptable documentation. The CIP rule gives examples of types of documents that have long been considered primary sources of identification. The rule reflects the federal banking agencies' expectations that banks will review an unexpired government-issued form of identification from most customers. This identification must provide evidence of a customer's nationality or residence and bear a photograph or similar safeguard; examples include a driver's license or passport. However, other forms of identification may be used if they enable the bank to form a reasonable belief that it knows the true identity of the customer. Nonetheless, given the availability of counterfeit and fraudulently obtained documents, a bank is encouraged to review more than a single document to ensure that it has a reasonable belief that it knows the customer's true identity.

For a "person" other than an individual (such as a corporation, partnership, or trust), the bank should obtain documents showing the legal existence of the entity, such as certified articles of incorporation, an unexpired government-issued business license, a partnership agreement, or a trust instrument.

Verification Through Nondocumentary Methods

Banks are not required to use nondocumentary methods to verify a customer's identity. However, a bank using nondocumentary methods to verify a customer's identity must have procedures that set forth the methods the bank will use. Nondocumentary methods may include contacting a customer; independently verifying the customer's identity through the comparison of information provided by the customer with information obtained from a consumer reporting agency, public database, or other source; checking references with other financial institutions; and obtaining a financial statement.

The bank's nondocumentary procedures must also address the following situations: An individual is unable to present an unexpired government-issued identification document that bears a photograph or similar safeguard; the bank is not familiar with the documents presented; the account is opened without obtaining documents (e.g., the bank obtains the required information from the customer with the intent to verify it); the customer opens the account without appearing in person; or the bank is otherwise presented with circumstances that increase the risk that it will be unable to verify the true identity of a customer through documents.

Additional Verification for Certain Customers

The CIP must address situations where, based on its risk assessment of a new account opened by a customer that is not an individual, the bank will obtain information about individuals with authority or control over such accounts, including signatories, in order to verify the customer's identity. This verification method applies only when the bank cannot verify the customer's true identity using documentary or nondocumentary methods. For example, a bank may need to obtain information about and verify the identity of a sole proprietor or the principals in a partnership when the bank cannot otherwise satisfactorily identify the sole proprietorship or the partnership.

Lack of Verification

The CIP must also have procedures for circumstances in which the bank cannot form a reasonable belief that it knows the true identity of the customer. These procedures should describe:

- Circumstances in which the bank should not open an account.
- The terms under which a customer may use an account while the bank attempts to verify the customer's identity.
- When the bank should close an account, after attempts to verify a customer's identity have failed.
- When the bank should file a SAR in accordance with applicable law and regulation.

Recordkeeping and Retention Requirements

A bank's CIP must include recordkeeping procedures. At a minimum, the bank must retain the identifying information (name, address, date of birth for an individual, TIN, and any other information required by the CIP) obtained at account opening for a period of five years after the account is closed.[49] For credit cards, the retention period is five years after the account closes or becomes dormant. The bank must also keep a description of the following for five years after the record was made:

- Any document that was relied on to verify identity, noting the type of document, the identification number, the place of issuance, and, if any, the date of issuance and expiration date.
- The method and the results of any measures undertaken to verify identity.
- The results of any substantive discrepancy discovered when verifying identity.

Comparison With Government Lists

The CIP must include procedures for determining whether the customer appears on any federal government list of known or suspected terrorists or terrorist organizations. Banks will be contacted by the U.S. Treasury in consultation with their federal banking agency when a list is issued. At such time, banks must compare customer names against the list within a reasonable time of account opening or earlier, if required by the government, and they must follow any directives that accompany the list.

As of the publication date of this manual, there are no designated government lists to verify specifically for CIP purposes. Customer comparisons to Office of Foreign Assets Control lists and 31 CFR 1010.520 (commonly referred to as section 314(a) requests) remain separate and distinct requirements.

Adequate Customer Notice

The CIP must include procedures for providing customers with adequate notice that the bank is requesting information to verify their identities. The notice must generally describe the bank's identification requirements and be provided in a manner that is reasonably designed to allow a customer to view it or otherwise receive the notice before the account is opened. Examples include posting the notice in the lobby, on a Web site, or within loan application documents. Sample language is provided in the regulation:

> IMPORTANT INFORMATION ABOUT PROCEDURES FOR OPENING A NEW ACCOUNT — To help the government fight the funding of terrorism and money laundering activities, federal law requires all financial institutions to obtain, verify, and record information that identifies each person who opens an account. What this means for you: When you open an account, we will ask for your name, address, date of birth, and other information that will allow us to identify you. We may also ask to see your driver's license or other identifying documents.

Reliance on Another Financial Institution

A bank is permitted to rely on another financial institution (including an affiliate) to perform some or all of the elements of the CIP, if reliance is addressed in the CIP and the following criteria are met:

- The relied-upon financial institution is subject to a rule implementing the AML program requirements of 31 USC 5318(h) and is regulated by a federal functional regulator.[50]
- The customer has an account or is opening an account at the bank and at the other functionally regulated institution.
- Reliance is reasonable, under the circumstances.
- The other financial institution enters into a contract requiring it to certify annually to the bank that it has implemented its AML program, and that it will perform (or its agent will perform) the specified requirements of the bank's CIP.

Use of Third Parties

The CIP rule does not alter a bank's authority to use a third party, such as an agent or service provider, to perform services on its behalf. Therefore, a bank is permitted to arrange for a third party, such as a car dealer or mortgage broker, acting as its agent in connection with a loan, to verify the identity of its customer. The bank can also arrange for a third party to maintain its records. However, as with any other responsibility performed by a third party, the bank is ultimately responsible for that third party's compliance with the requirements of the bank's CIP. As a result, banks should establish adequate controls and review procedures for such relationships. This requirement contrasts with the reliance provision of the rule that permits the relied-upon party to take responsibility.

Other Legal Requirements

Nothing in the CIP rule relieves a bank of its obligations under any provision of the BSA or other AML laws, rules, and regulations, particularly with respect to provisions concerning information that must be obtained, verified, or maintained in connection with any account or transaction.

The U.S. Treasury and the federal banking agencies have provided banks with Frequently Asked Questions (FAQ), which may be revised periodically. The FAQs and other related documents (e.g., the CIP rule) are available on FinCEN's and the federal banking agencies' Web sites.

Backward | Table of Contents | Forward

Appendix Item 4

Department of the Treasury
Financial Crimes Enforcement Network

GUIDANCE

FIN-2009-G002
Issued: June 16, 2009
Subject: Guidance on the Scope of Permissible Information Sharing Covered by Section 314(b) Safe Harbor of the USA PATRIOT Act

The Financial Crimes Enforcement Network ("FinCEN") is issuing this interpretive guidance to clarify the application of the rule implementing section 314(b) (the "314(b) rule")[1] of the USA PATRIOT Act (the "Act").[2] Specifically, this guidance clarifies that a financial institution participating in the section 314(b) program may share information relating to transactions that the institution suspects may involve the proceeds of one or more specified unlawful activities ("SUAs") and such an institution will still remain within the protection of the section 314(b) safe harbor from liability.

Section 314(b) permits two or more financial institutions and any association of financial institutions to "share information with one another regarding individuals, entities, organizations, and countries suspected of possible terrorist or money laundering activities."[3] Section 314(b) establishes a safe harbor from liability for a financial institution or an association of financial institutions that voluntarily chooses to share information with other financial institutions for the purpose of identifying and, where appropriate, reporting possible money laundering or terrorist activity.[4] To avail itself of the section 314(b) safe harbor, a financial institution must comply with the requirements of the implementing regulation, including provision of notice to FinCEN, taking reasonable steps to verify that the other financial institution has submitted the requisite notice, and restrictions on the use and security of information shared.[5]

---

[1] 31 CFR § 103.110.

[2] Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act of 2001 ("USA PATRIOT Act") Pub. L. No. 107-56, 115 Stat. 272 (2001).

[3] Pub. L. No. 107-56, § 314(b). Consistent with the broad intent underlying section 314(b) of the Act, the 314(b) rule defines "money laundering" by reference to sections 1956 and 1957, Title 18, United States Code, which in turn include the conducting of a transaction involving the proceeds of a specified unlawful activity.

[4] 31 CFR § 103.110(b)(5).

[5] 31 CFR § 103.110(b)(2)-(b)(4).

FINANCIAL CRIMES ENFORCEMENT NETWORK

Information Sharing Between Financial Institutions

Section 314(b) Fact Sheet

What is Section 314(b)?

Section 314(b) of the USA PATRIOT Act provides financial institutions with the ability to share information with one another, under a safe harbor that offers protections from liability, in order to better identify and report potential money laundering or terrorist activities. 314(b) information sharing is a voluntary program, and FinCEN strongly encourages information sharing through Section 314(b).

What are the Benefits of 314(b) Voluntary Information Sharing?

While information sharing under the 314(b) program is voluntary, it can help financial institutions enhance compliance with their anti-money laundering/ counter-terrorist financing (AML/CFT) requirements, most notably with respect to:

- Gathering additional and potentially invaluable information on customers or transactions potentially related to money laundering or terrorist financing, including previously unknown accounts, activities, and/or associated entities or individuals.
- Shedding more comprehensive light upon overall financial trails, especially if they are complex and appear to be layered amongst numerous financial institutions, entities, and jurisdictions.
- Building a more comprehensive and accurate picture of a customer's activities where potential money laundering or terrorist financing is suspected, allowing for more precise decision-making in due diligence and transaction monitoring.
- Alerting the contacted financial institution to customers about whose suspicious activities it may not have been previously aware.
- Facilitating the filing of more comprehensive and complete SARs than would otherwise be filed in the absence of 314(b) information sharing.
- Aiding in identifying and collectively stemming money laundering and terrorist financing methods and schemes.

- Facilitating efficient SAR reporting decisions - for example, when a financial institution obtains a more complete picture of activity through the voluntary information sharing process and determines that no SAR is required for transactions that may have initially appeared suspicious.[1]

Who is Eligible to Participate in 314(b)?

Financial institutions subject to an anti-money laundering program requirement under FinCEN regulations, and any association of such financial institutions, are eligible to share information under Section 314(b). This currently includes the following types of financial institutions:

- Banks (31 CFR 1020.540)
- Casinos and Card Clubs (31 CFR 1021.540)
- Money Services Businesses (31 CFR 1022.540)
- Brokers or Dealers in Securities (31 CFR 1023.540)
- Mutual Funds (31 CFR 1024.540)
- Insurance Companies (31 CFR 1025.540)
- Futures Commission Merchants and Introducing Brokers in Commodities (31 CFR 1026.540)
- Dealers in Precious Metals, Precious Stones, or Jewels (31 CFR 1027.540)
- Operators of Credit Card Systems (31 CFR 1028.540)
- Loan or Finance Companies (31 CFR 1029.540)
- Associations consisting of the financial institutions listed above[2]

What Information can be Shared Under 314(b)?

Under 314(b), financial institutions or associations of financial institutions may share information with each other regarding individuals, entities, organizations, and countries for purposes of identifying, and, where appropriate, reporting

1. For more information on the benefits of voluntary information sharing under Section 314(b), including examples of ways in which SAR narratives have referenced 314(b), see Issue 23 of the SAR Activity Review – Trends, Tips & Issues at http://www.fincen.gov/news_room/rp/files/sar_tti_23.pdf.
2. In July 2012, FinCEN issued an administrative ruling which clarified the meaning of "association of financial institutions." For more information, see FIN-2012-R006 (http://www.fincen.gov/news_room/rp/rulings/pdf/FIN-2012-R006.pdf)

activities that may involve possible terrorist activity or money laundering. FinCEN has issued guidance clarifying that, if 314(b) sharing participants suspect that transactions may involve the proceeds of specified unlawful activities under money laundering statutes, information related to such transactions can be shared under protection of the 314(b) safe harbor.[3]

In cases where a financial institution files a SAR that has benefited from 314(b) information sharing, FinCEN encourages financial institutions to note this in the narrative in order for FinCEN to identify and communicate additional examples of the benefits of the 314(b) program. Please note, however, that while information may be shared related to possible terrorist financing or money laundering that resulted in, or may result in, the filing of a SAR, Section 314(b) does not authorize a participating financial institution to share a SAR itself or to disclose the existence of a SAR.[4]

How do Financial Institutions Participate in 314(b)?

While FinCEN encourages 314(b) information sharing due to the many benefits of the program, financial institutions may voluntarily choose whether or not to participate. FinCEN regulations (31 CFR 1010.540) set forth the requirements that must be satisfied in order to benefit from 314(b) safe harbor protection, as outlined below. Sharing information without satisfying these conditions does not by itself subject an institution to penalty under FinCEN regulations, since 314(b) participation is voluntary; however, a financial institution will only benefit from the safe harbor protection if it follows the conditions for participation in the program:

1) Submit a Notification to FinCEN

Information regarding the 314(b) notification process, including on-line notification, is available on FinCEN's website (http://www.fincen.gov/statutes_regs/patriot/section314b.html). Financial institutions or associations of financial institutions interested in participating in the 314(b) program must complete and submit a 314(b) notification. All notifications are processed within two business days of receipt, and participants will receive an acknowledgment via e-mail.

3. Specified unlawful activities listed in 18 U.S.C. § § 1956 and 1957 include an array of fraudulent and other criminal activities. For more information, see FIN-2009-G002 (http://www.fincen.gov/statutes_regs/guidance/pdf/fin-2009-g002.pdf).

4. SAR confidentiality standards are governed by applicable SAR regulations. See, e.g., 31 CFR 1020.320.

2) Sharing information with other 314(b) participants

Prior to sharing information under 314(b), financial institutions must take reasonable steps, such as checking the FinCEN 314(b) participant list, to verify that the other financial institution has also submitted a notification to FinCEN. To facilitate the identification of 314(b) program participants, the notification acknowledgement will contain details of participation as well as the link and information required to access the most recent 314(b) participant list. FinCEN updates the list on a daily basis. Financial institutions may establish policies and procedures that designate more than one person with the authority to participate in the financial institution's 314(b) program.[5]

3) Safeguard Shared Information and use only for AML/CFT Purposes

Financial institutions and associations must establish and maintain procedures to safeguard the security and confidentiality of shared information, and must only use shared information for the purpose of:

- Identifying and, where appropriate, reporting on activities that may involve terrorist financing or money laundering;
- Determining whether to establish or maintain an account, or to engage in a transaction; or
- Assisting in compliance with anti-money laundering requirements.

Updating Point of Contact Information and Additional Resources

Any changes, updates or deletions of current 314(b) notifications should be submitted to FinCEN via e-mail at frc@fincen.gov. For additional questions related to 314(b) information sharing, FinCEN can be reached via phone at 1-800-767-2825 (1-800-SOS-BUCK) or via e-mail at frc@fincen.gov

5. For more information, see Issue 18 of the SAR Activity Review – Trends, Tips & Issues at http://www.fincen.gov/news_room/rp/files/sar_tti_18.pdf.

Appendix Item 5

Washington and Lee Law Review

Volume 73 | Issue 2 Article 6

Spring 4-1-2016

Collaborative Gatekeepers

Stavros Gadinis
University of California - Berkeley

Colby Mangels University of California - Berkeley

but instead helped create them.[317] More specifically, two critical elements of the regime, the imposition of regulatory requirements on big and small gatekeepers alike, and the standardization of reports, were introduced at the insistence of large banks. That said, we have not yet explained how this regime has worked in practice. The next Part explores this question and shows how gatekeepers and regulators have collaborated in their efforts to implement the modern anti-money-laundering regime.

V. The Anti-Money-Laundering Regime in Practice

This Part discusses the operation of the anti-money-laundering regime on the ground. It helps address two critical concerns about the collaborative gatekeeper model. First, how might gatekeepers react to the requirement that clients provide early warning to regulators, and report client activity that seems suspicious? Will gatekeepers be able to separate the suspicious from the innocuous, and will they be willing to pass on this information to regulators? Second, how might regulators respond? Will they make full use of suspicious activity reports (SARs), or will they set these aside in favor of other priorities and sources of information?

As the subpart below discusses, financial institutions across the United States, representing all segments of the market and diverse lines of business, are increasingly submitting SARs in recent years.[318] This widespread embrace of suspicious activity reporting indicates a shift in the way the industry approaches money laundering: Instead of withholding information out of concerns about betraying clients, financial institutions have come to view reporting as an obligation equally applicable to all. To carry out this mission, financial institutions created populous compliance departments, structured under specific regulatory guidelines and operating under regulatory supervision.[319] They

317. *See supra* Part IV.D (discussing customer due diligence and reporting law).

318. *See infra* Part V.A (discussing the volume and quality of SAR filings).

319. *See* Bruce Kelly, *Firms Pumping Millions into Their Compliance Departments to Keep Regulators at Bay*, INV. NEWS (Oct. 26, 2014), http://www.investmentnews.com/article/20141026/REG/310269996/firms-pumping-millions-into-their-compliance-departments-to-keep (last visited Apr. 1, 2016)

have also invested heavily in modern technology for data analysis and sharing to scout for violations, explore and analyze surrounding circumstances, and submit and review reports.[320] This compliance infrastructure has greatly expanded gatekeepers' information processing capacity, thus boosting their chances of actually catching misconduct. But it has also changed dynamics within gatekeepers, blunting the conflict of interest between gatekeeper firms and their employees. That is, the new compliance infrastructure utilizes a broad range of employees, as well as technological infrastructure, to flag suspicious activities, rather than leaving this task to those employees who courted a particular client, and who are most likely to suffer from conflicts of interest. The industry's embrace of SARs and the related compliance infrastructure suggest that the proposed theoretical framework is not entirely impracticable.

Are these investments paying off? Does the information gathered through suspicious activity reporting have any value for enforcement authorities? The paragraphs below show that regulators believe that SARs reveal a lot and thus devote significant time and resources in reviewing SARs. They review SARs not only to fight money laundering, but also to combat diverse types of financial crime and non-criminal fraud.[321] Indeed, since the introduction of the SAR filing obligation, criminal cases targeting money laundering, as well as convictions, have generally increased.[322] These developments illustrate that gatekeepers' intimate knowledge of their clients' business models, and their ability to distinguish between legitimate business proposals and potentially fraudulent ventures at an early stage, are proving valuable to regulators. They thus

---

(explaining that firms are spending millions of dollars for their compliance departments) (on file with the Washington and Lee Law Review).

320. *See* PETER REUTER & EDWIN M. TRUMAN, CHASING DIRTY MONEY: THE FIGHT AGAINST MONEY LAUNDERING 100 (2004) (estimating that capital costs account for two-thirds of anti-money-laundering compliance costs).

321. *See infra* Part V.B (discussing SAR filings that relate to other issues other than money laundering).

322. *See* REUTER & TRUMAN, *supra* note 320, at 109–13 (noting that money laundering adjudications increased from 1,159 in 1994 to 1,420 in 2001). Similarly, money-laundering convictions over the same period increased from 81% to 88%. *Id.* at tbl.5.2.

highlight the potential of collaborative gatekeeping as a blueprint for reforming financial regulation.

A. Volume and Quality of SAR Filings Indicates Industry Buy-In

U.S. financial institutions, though initially apprehensive about filing SARs, quickly espoused the practice with eagerness. In 1996, there were about 50,000 SARs filed with FinCEN;[323] by 2003, the SARs filed per year had risen to over 300,000.[324] Ten years later, in 2013, filed SARs had exceeded 1,600,000.[325] During this period, FinCEN has intensified its efforts to police submission of suspicious activity reports and has imposed fines some view as extraordinarily large.[326] The Department of Justice has criminally prosecuted financial institutions for anti-money-laundering violations, putting some out of business.[327]

To put SARs' increase in perspective, it is worth contrasting them to Currency Transaction Reports (CTRs), triggered for every transfer of over $10,000 through the financial system.[328] The volume of CTRs has remained relatively stable over the same period, ranging from about 12 million in 1996 to over 14 million in 2011.[329] The comparison between CTRs and SARs also reveals that financial institutions are selective about submitting a SAR. In 2011, there were over 14 million CTRs filed, compared to about

---

323. U.S. DEP'T OF TREASURY FIN. CRIMES ENFORCEMENT NETWORK, THE SAR ACTIVITY REVIEW: BY THE NUMBERS 1 (2004), www.fincen.gov/news_room/rp/files/sar_by_numb_03.pdf.

324. *Id.*

325. SAR STATS TECHNICAL BULL, *supra* note 28, at 1.

326. *See* David Zaring & Elena Baylis, *Sending the Bureaucracy to War*, 92 IOWA L. REV. 1359, 1414 (2007) (noting two instances of $30 million fines).

327. *See id.* at 1415 ("$43 million in combined criminal and civil fines against Riggs Bank . . . put the bank of out of business.").

328. *See* FED. FIN. INST. EXAMINATION COUNCIL, CURRENCY TRANSACTION REPORTING—OVERVIEW, https://www.ffiec.gov/bsa_aml_infobase/pages_manual/OLM_017.htm (last visited Feb. 26, 2016) (explaining that multiple transactions equaling $10,000 or more are treated as a single transaction) (on file with the Washington and Lee Law Review).

329. U.S. DEP'T OF TREASURY FIN. CRIMES ENFORCEMENT NETWORK, ANNUAL REPORT 2011, 7 (2011) [hereinafter ANNUAL REPORT 2011, http://www.fincen.gov/news_room/rp/files/ annual_report_fy2011.pdf.

1.4 million SARs.[330] Fears that filers would simply submit a SAR for every client that crosses their institution's doorstep and thus dilute SARs' signaling value, seem to not have materialized. Instead, it seems that the suspicions threshold pushes filers to think hard about when to alert regulators to client activity.

All segments of the market have contributed to the increase in suspicious activity reporting. Financial institutions from across the nation, big and small, in one or in multiple lines of business, are increasingly reporting their suspicions to authorities.[331] Such diversity in filers indicates that many market participants come to view reporting suspicions to regulators as their obligation. As one compliance officer stated: "There has been a cultural change in the banking industry. Before we were focusing more on the customer, now we have to focus more on compliance."[332] Indeed, finance professionals currently consider SARs as the main channel through which the U.S. government collects intelligence about money laundering.[333]

The exponential increase in SARs represents a staggering growth in the amount of tips bank regulators are receiving about money laundering. How informative are these tips for enforcement authorities? Generally, regulators treat SARs as an important source of information about financial misconduct, suggesting that many disclosures are of high quality. Reports by regulators that regularly review SARs, such as the Federal Reserve and the FDIC, have stated that they see little evidence of defensive filing, such as reports that provide only skeletal information in an effort to discharge a regulatory obligation without triggering an investigation.[334] As further discussed

---

330. *See id.* (providing a comparison of the volume of the different reporting methods).

331. *See, e.g.*, U.S. DEP'T OF TREASURY FIN. CRIMES ENFORCEMENT NETWORK, THE SAR ACTIVITY REVIEW: BY THE NUMBERS 4 (2013) https://www.fincen.gov/news_room/rp/files/btn18/sar_by_numb_18.pdf (describing filers from different segments of the market); U.S. DEP'T OF TREASURY FIN. CRIMES ENFORCEMENT NETWORK, THE SAR ACTIVITY REVIEW: TRENDS, TIPS & ISSUES 15 (2006) [hereinafter TRENDS, TIPS & ISSUES 2006], https://www.fincen.gov/news_room/rp /files/sar_tti_10.pdf (discussing filings by state).

332. NEIL KATKOV, TRENDS IN ANTI-MONEY LAUNDERING 2011, at 5 (2011).

333. *See* REUTER & TRUMAN, *supra* note 320, at 106 (explaining that SARs are viewed as being more informative).

334. *See* MONEY LAUNDERING: NEEDED IMPROVEMENTS, *supra* note 279, at 19

below, many regulators invest significant time and effort in reviewing SARs every month, which highlights the importance of SARs for their agenda.[335] As Andrew Ceresney, Director of the SEC's enforcement division, put it:

> The SEC receives tens of thousands of tips and referrals every year from many different sources including investors, whistleblowers and SROs. But SARs coming from broker-dealers often stand out from this pack in terms of reliability because the best ones contain allegations of wrongdoing that are described clearly and comprehensively, but also concisely. This reduces the amount of research and assessment that is needed before determining whether and how to act. [336]

This does not mean that all reports are equally informative. Unfortunately, examining SAR disclosures themselves is not possible for researchers, as they are confidential by law.[337] But regulatory institutions have described their use of SARs in a variety of annual overviews and statements.[338] This evidence suggests that the quality of information provided through SARs varies, with some reports providing important leads for enforcement actions, and others offering little of substance.[339] FinCEN itself has stated that a number of reports do not fully sketch the reported suspicious activity, by failing to answer basic questions such as "who, what, when, were, why, and how."[340] In

---

(noting that "[b]oth banks have a policy of not filing suspicious CTRs").

335. *See infra* Part V.E (discussing collaborative regulators).

336. Andrew Ceresney, *Remarks at SIFMA's 2015 Anti-Money Laundering and Financial Crimes Conference*, Feb 25, 2015, http://www.sec.gov/news/speech/022515-spchc.html (last visited Jan. 21, 2016) (on file with the Washington and Lee Law Review).

337. *See* 31 U.S.C. § 5318(g)(2) (2012) (explaining that neither the reporting institution nor government may disclose the information contained in the SAR).

338. *See* U.S. DEP'T OF TREASURY FIN. CRIMES ENFORCEMENT NETWORK, THE SAR ACTIVITY REVIEW: TRENDS, TIPS & ISSUES 1 (2013) [hereinafter TRENDS, TIPS & ISSUES 2013] ("The SAR Activity Review—Trends, Tips & Issues is a product of continual dialogue and collaboration among the nation's financial institutions, law enforcement officials and regulatory agencies to provide meaningful information about the preparation, use and value of Suspicious Activity Reports . . . .").

339. *See generally* REUTER & TRUMAN, *supra* note 320, at 107; Ceresney, *supra* note 336.

340. U.S. DEP'T OF TREASURY FIN. CRIMES ENFORCEMENT NETWORK, REPORT ON OUTREACH TO DEPOSITORY INSTITUTIONS WITH ASSETS UNDER $5 BILLION 30

light of the enormous volume of reported cases, some variation in SAR quality is, perhaps, not very surprising. As FinCEN concludes, the vast majority of filed SARs are generally in line with regulatory guidance in describing activity as suspicious.[341]

An indirect way of assessing SARs' potential impact is to explore whether the increase in filings has changed the landscape for enforcing anti-money-laundering laws. Indeed, U.S. data suggest that, as SAR filings have increased, so has the number of money laundering cases brought and the number of convictions won by criminal authorities.[342] To give one example, regulators report that between 2003 and 2012, depository institutions reported over 200,000 cases of suspected insider abuse, such as cases where bank employees used client funds for personal gain.[343] In more than half of these cases, the executives involved were subsequently fired or suspended.[344] These connections are only tentative because confidentiality rules prevent researchers from connecting a specific SAR to a specific conviction. That said, the fact that regulators, the only persons with the full picture, make extensive use of available SARs suggests that they find much that is useful in these reports.

B. SAR Filings Besides Money Laundering

Perhaps one of the most staggering aspects of SAR submissions is that the vast majority of reported cases do *not* involve money laundering.[345] Indeed, only 27% of all SARs submitted to FinCEN in 2014 ended up concerning money

(2011) [hereinafter DEPOSITORY INSTITUTIONS WITH ASSETS UNDER $5 BILLION], www.fincen.gov/news_room/rp/reports/pdf/Banks_Under_$5B_Report.pdf.

341. *See id.* (mentioning that, although the SARs are typically consistent with what is suspicious activity, many of them are filled out incorrectly).

342. *See* Elod Takats, *A Theory of "Crying Wolf": The Economics of Money Laundering Enforcement* 28 (Int'l Monetary Fund Working Paper No. 07/81, 2007) (explaining that "the number of money laundering convictions measures how efficient SARs are in providing useful evidence to convict criminals").

343. TRENDS, TIPS & ISSUES 2013, *supra* note 338, at 12.

344. *Id.* at 13.

345. *See generally SAR Stats*, U.S. DEP'T OF TREASURY FIN. CRIMES ENFORCEMENT NETWORK [hereinafter *FinCEN SAR Stats*], https://www.fincen.gov/news_room/rp/sar_by_number.html (last visited Apr. 1, 2016) (on file with the Washington and Lee Law Review).

laundering.[346] As regulators quickly realized, money laundering occurs through actions that are common in many different types of fraud. Typical activities that trigger money laundering suspicions involve transactions with no apparent economic purpose, use of multiple locations or accounts for a common goal, questionable or false documentation, counterfeit instruments, etc. All these machinations are not exclusive to money launderers, but could easily involve tax evasion, insider trading, consumer fraud, identity theft, and a host of other activities—either fraudulent, criminal, or both.[347] As a result, SARs have opened a window into diverse criminal undercurrents in the financial system.

This extensive review of SAR information has opened regulators' eyes to problems they did not clearly see before. For example, depository institutions clearly identified elder abuse as a rising trend in financial fraud, as older Americans need to manage sizeable resources but are not as technologically savvy.[348] A stream of SARs prompted FinCEN to conduct an extensive report and to identify practices that indicate elder abuse.[349] Moreover, SARs help regulators collect intelligence about new structures or tools in the financial system, particularly when these new tools can also facilitate misconduct. For example, when bitcoins emerged as a successful virtual currency, SARs were crucial in providing the government with information about the bitcoin ecosystem and shaping regulatory guidance.[350]

---

346. According to FinCEN, of the 2,413,447 activities reported in 2014 by depository institutions, only 672,136 involved money laundering. *Exhibit 5: Number of Filings by Type of Suspicious Activity by Depository Institutions*, FINCEN (2015), https://www.fincen.gov/news_room/rp/files/SAR02/Section_2-Depository_Institution_SARs.xls.

347. *See generally FinCEN SAR Stats*, *supra* note 345.

348. *See,* U.S. DEP'T OF TREASURY FIN. CRIMES ENFORCEMENT NETWORK, ADVISORY TO FINANCIAL INSTITUTIONS ON FILING SUSPICIOUS ACTIVITY REPORTS REGARDING ELDER EXPLOITATION 1 (2011), https://www.fincen.gov/statutes_regs/guidance/pdf/fin-2011-a003.pdf (crediting financial institutions' increased reporting of elder abuse as motivation for advisory).

349. *See id.* ("Analysis of SARs reporting elder financial exploitation can provide critical information about specific frauds and potential trends, and can highlight abuses perpetrated against the elderly.").

350. *See* U.S. DEP'T OF TREASURY FIN. CRIMES ENFORCEMENT NETWORK, REQUEST FOR ADMINISTRATIVE RULING ON THE APPLICATION OF FINCEN'S REGULATIONS TO A VIRTUAL CURRENCY TRADING PLATFORM (2014),

SARs have also contributed a lot of granular information to well-known weaknesses of the financial system, thus aiding regulators in addressing long-standing problems with significant social consequences. Mortgage fraud, which ran rampant in the period before the 2007 collapse of the subprime market, has been targeted by FinCEN intelligence gathering efforts.[351] As a result, the Federal Housing Agency has been able to use nearly 100,000 mortgage loan fraud SARs as the basis for subsequent action.[352] Another example of a well-known regulatory effort where SARs have made significant contributions is the fight against various forms of insider abuse, such as insider trading, breach of fiduciary duties, and other ways of using executive privileges for personal advantage.[353]

These examples of issues that SARs have helped address, outside of money laundering, are a further indication of the value of SARs as efforts to gather intelligence. At the same time, gatekeepers are not obliged to submit SARs for all types of financial fraud; these diverse SARs are submitted because money laundering sometimes intersects with other types of crimes.[354] The extension of the suspicious activity reporting requirement seems likely to draw regulators' attention to much more misconduct.

---

http://www.fincen.gov/news_room/rp/rulings/pdf/FIN-2014-R011.pdf (discussing FinCEN's policy and implementation responses to virtual currency issues).

351. *See* Press Release, U.S. Dep't of the Treasury, Federal, State Partners Announce Multi-Agency Crackdown Targeting Foreclosure Rescue Scams, Loan Modification Fraud (Apr. 6, 2009), https://www.treasury.gov/press-center/press-releases/Pages/tg83.aspx (last visited Feb. 26, 2016) ("To this end, Treasury and FinCEN announced an advanced targeting effort already underway to combat fraudulent loan modification schemes and coordinate ongoing efforts across agencies to investigate fraud and assist with enforcement and prosecutions.") (on file with the Washington and Lee Law Review).

352. ANNUAL REPORT 2011, *supra* note 329, at 39.

353. *See* TRENDS, TIPS & ISSUES 2013, *supra* note 338, at 12–13 (describing a rise in the reporting of insider relationships between 2003 and 2009).

354. *See* 31 C.F.R. §§ 1010.300–340 (2015) (identifying when financial institutions must file a SAR).

C. Compliance Process and Technology Behind Suspicious Activity Reporting

How are SARs produced? The paragraphs that follow explain that gatekeeper firms have made major investments in personnel and technology to comply with their regulatory obligations. Technological innovations are already allowing computers to flag many suspicious transactions, so that firms need not rely solely on front-line employees who might face conflicts of interest.[355] While these investments are sizeable, survey data suggests that firms do not find these burdens impossibly heavy.[356] The existence of this compliance infrastructure makes the extension of the collaborative gatekeeper model to other fields more plausible.

The resources devoted by financial institutions into staffing their anti-money-laundering compliance programs show the extent of private industry participation in this regulatory effort.[357] To start with a captivating example: J.P. Morgan, the largest U.S. bank by assets,[358] has 8,000 employees working solely on anti-money-laundering compliance—more than the Treasury Department and the Federal Reserve combined.[359] J.P. Morgan has about 15,000 employees working on regulatory compliance (including anti-money laundering) and 250,000 employees worldwide.[360] In large banks with multinational

355. *See* TRENDS, TIPS & ISSUES 2006, *supra* note 331, at 52 ("While a computer may flag activity for review, it is the person looking at the screen who should determine whether a series of transactions is a reportable event.").

356. *See infra* notes 379–403 and accompanying text (providing data suggesting that firms have come to terms with the regulatory obligations).

357. *See* REUTER & TRUMAN, *supra* note 320, at 100 (estimating the cost of compliance as exceeding $3 billion per year).

358. *See* Erik Holm, *Ranking the Biggest U.S. Banks: A New (Old) Entrant in Top 5*, WALL STREET J. (Dec. 10, 2014), www.blogs.wsj.com/moneybeat/2014/12/10/ranking-the-biggest-u-s-banks-a-new-old-entrant-in-top-5 (last visited Feb. 26, 2016) (noting the bank's reported $2.5 billion dollars in assets as of late 2014) (on file with the Washington & Lee Law Review).

359. *See* J.P. MORGAN, ANN. REP. 2013, at 12 (2014) http://investor.shareholder.com/common/download/download.cfm?companyid=ONE&fileid=742266&filekey=2bd13119-52d2-4d78-9d85-a433141c21ae&filename=01-2013AR_FULL_09.pdf (describing the firm's "industry leading Anti-Money Laundering" program).

360. *See* Monica Langley & Dan Fitzpatrick, *Embattled J.P. Morgan Bulks Up Oversight*, WALL STREET J. (Sept. 12, 2013), www.wsj.com/articles/SB

presence, anti-money-laundering operations include one large team that concentrates information and coordinates action, and specialized officers working on the many different lines of business in the institution.[361] Big banks can have over eighty different lines of business, each with a dedicated anti-money-laundering officer.[362] A medium-sized bank with over $100 billion in assets would typically have about 200 anti-money-laundering officials.[363] Even the smallest banks, with up to $1 billion in assets, typically have ten or fewer anti-money-laundering officials.[364] Many of these officials started their careers as front-line employees and have a good understanding of the institution's client relationships, while others have worked in other compliance positions or in larger banks.[365]

The expanding size of anti-money-laundering departments has boosted financial institutions' compliance firepower, but it is modern technology that has really revolutionized their monitoring philosophy. Financial institutions have developed software that recognizes specific transaction patterns, based on typologies sketched out on the basis of past investigations and violations.[366] This software can be enriched and adapted over time, "learning" more violations and modern techniques for money laundering. Overall, banks' newly automated systems are capable of identifying unusual patterns in transactions by sifting

---

10001424127887324755104579071304170686532 (last visited Jan. 21, 2016) ("J.P. Morgan Chase & Co., facing a host of regulatory and legal woes, plans to spend an additional $4 billion and commit 5,000 extra employees this year to clean up its risk and compliance problems, according to people close to the bank.") (on file with the Washington and Lee Law Review).

361. U.S. DEP'T OF TREASURY FIN. CRIMES ENFORCEMENT NETWORK, REPORT ON OUTREACH TO LARGE DEPOSITORY INSTITUTIONS 5 (2009) [hereinafter OUTREACH TO LARGE DEPOSITORY INSTITUTIONS], https://www.ffiec.gov/bsa_aml_infobase/documents/FinCEN_DOCs/FIOI_Bank_Report_Large_DIst_200910.pdf.

362. *Id.*

363. KATKOV, *supra* note at 332, at 6.

364. *Id.*

365. DEPOSITORY INSTITUTIONS WITH ASSETS UNDER $5 BILLION, *supra* note 340, at 12.

366. *See* OUTREACH TO LARGE DEPOSITORY INSTITUTIONS, *supra* note 361, at 15 ("Banks build typologies gleaned from previous investigations into their investigative strategy, creating risk models that assist the monitoring tools to identify suspicious activity.").

through multiple data points in a manner that manual laborers would find hard to imitate.

Because software typology relies on past events, it cannot catch fraudulent transaction structures that appear for the first time. To improve their alertness to money laundering novelties, financial institutions have tried an alternative approach: they use software that observes metrics of client behavior and compares them to a "peer group" of clients that are expected to behave in similar ways over time.[367] Peer groups vary by line of business, client background, geography, and other factors. In addition, most banks assess not only individual clients, but also a line of business as a whole, in terms of susceptibility to money laundering.[368]

Financial institutions' use of technological advances has been one of the primary drivers of the increase in SARs, according to finance professionals and regulators interviewed for a GAO study.[369] That said, referrals from front-line employees continue to contribute a significant amount of the cases that ultimately result into a SAR.[370] In some banks, software-generated referrals amount to 75% of total SAR candidate cases.[371] In other banks, the picture is reversed: software contributes only 20% of their referrals.[372]

The increased use of software in anti-money-laundering supervision has allowed financial institutions to outsource a significant portion of their compliance heavy lifting. This can reduce conflicts of interest significantly, by empowering many individuals besides front-line employees to report on suspicious activities. There are about twenty providers of anti-money-laundering software in the world.[373] Among financial

367. *See id.* at 14 (explaining that "peer groups may by segmented by LOBs, product types, geography and/or account types").

368. *See id.* at 6–7 (explaining the various ways banks access suspicious activity).

369. MONEY LAUNDERING: NEEDED IMPROVEMENTS, *supra* note 279, at 17.

370. *See* OUTREACH TO LARGE DEPOSITORY INSTITUTIONS, *supra* note 361, at 2 ("[B]anks unanimously indicated that they believe their best source of information . . . comes from referrals by front-line branch personnel and relationship managers.").

371. *Id.* at 16–17.

372. *Id.*

373. KATKOV, *supra* note at 332, at 3.

institutions, 90% find themselves running their software in house in collaboration with outside vendors, while 10% outsource their software management completely.[374] Of course, developing sophisticated software solutions and staffing populous compliance departments do not come without a cost. According to a recent survey, the aggregate global expenditure in anti-money-laundering supervision in 2011 reached $5 billion per year, with $1.2 billion spent on software and $3.8 billion devoted to staff and other operational expenses.[375]

These costs are contributing to a growing trend in structuring compliance departments: increasing integration between anti-money laundering and general fraud operations. From a substantive perspective, it is becoming clear that, through anti-money-laundering supervision, institutions receive alerts about other types of fraud.[376] Anti-money-laundering technology can be readily used, with just a few alterations, against financial fraud more generally.[377] Many institutions find that modern solutions applied in anti-money laundering deliver superior results compared to antiquated fraud detection systems.[378] The pressure to contain costs is particularly strong in smaller institutions, which have started to use the same staff as both anti-money laundering and anti-fraud compliance officers.[379]

Perhaps because gatekeepers directly reap some of the benefits of the early detection of client fraud, they have come to terms with these significant compliance costs. Periodic surveys of the top global banks suggest that large majorities find the anti-money-laundering regulatory burden acceptable.[380] The

374. *Id*. at 12–13.

375. *Id*. at 4.

376. *See* OUTREACH TO LARGE DEPOSITORY INSTITUTIONS, *supra* note 361, at 10 (discussing the connection between money laundering and financial fraud).

377. *See id.* at 11 (reporting regulators' push to encourage financial institutions to use their fraud resources to combat money laundering).

378. KATKOV, *supra* note at 332, at 29.

379. *See* DEPOSITORY INSTITUTIONS WITH ASSETS UNDER $5 BILLION, *supra* note 340, at 2, 12 (mentioning the need for staff at smaller institutions to play multiple roles).

380. More specifically, KPMG surveyed a wide variety of professionals in the financial industry involved in anti-money laundering in dozens of countries. Eighty-four percent of respondents in the 2004 survey believed the regulatory burden was acceptable, 93% of respondents in the 2007 survey believed the

significant investments firms have made to combat money laundering indicate that implementing the collaborative model has proven feasible in this field. Rather than setting up compliance systems from scratch, it seems likely that firms would draw on their existing infrastructure if called on to give early warning about a broader range of fraudulent activities. In short, while the expansion of the collaborative gatekeeper model to a broad range of crimes would undoubtedly involve significant costs, experience with the AML regime suggests these might not be insurmountable.

D. Filing a SAR: Efforts for Investigation and Drafting by Front-Line Employees, Compliance Officers, and Management

To assess how effectively the "suspicious activity" threshold helps filers distinguish between dubious and harmless transactions, one can look at the process for filing an SAR. Compliance officers receive information about many potentially suspicious situations but proceed with filing in a small subset of these cases. To draw on one available example, a small financial institution conducted 439 investigations in 2009 but decided to file in only thirty-nine cases. Thus, institutions seem to put serious thought into the potential violations hidden in the situation at hand, rather than simply filing a report even in remotely suspicious cases, so as to avoid any regulatory sanctions.

Investigating a potentially suspicious transaction requires significant personnel commitment.[381] In many institutions, the

---

regulatory burden was either acceptable or should be increased, while 85% of respondents in the 2011 survey found the burden acceptable. KPMG, GLOBAL ANTI-MONEY LAUNDERING SURVEY 2014, 7 (2014), https://www.kpmg.com/KY/en/IssuesAndInsights/ArticlesPublications/PublishingImages/global-anti-money-laundering-survey-v3.pdf. This question was not repeated in the 2014 survey. *Id.* While most AML professionals found the overall burden acceptable, they also desired various reforms to the system, notably more guidance and closer cooperation with regulators. *See generally id.* at 7; KPMG, GLOBAL ANTI-MONEY LAUNDERING SURVEY 2011: HOW BANKS ARE FACING UP TO THE CHALLENGE 9 (2011), https://www.kpmg.com/CN/en/IssuesAndInsights/ArticlesPublications/Documents/Global-Anti-Money-Laundering-Survey-O-201109.pdf.

381. *See generally* OUTREACH TO LARGE DEPOSITORY INSTITUTIONS, *supra* note 361.

Appendix Item 6

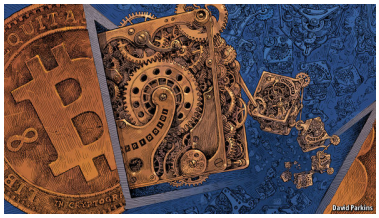
The Economist

Blockchains

The great chain of being sure about things

The technology behind bitcoin lets people who do not know or trust each other build a dependable ledger. This has implications far beyond the cryptocurrency

Oct 31st 2015 | From the print edition



WHEN the Honduran police came to evict her in 2009 Mariana Catalina Izaguirre had lived in her lowly house for three decades. Unlike many of her neighbours in Tegucigalpa, the country's capital, she even had an official title to the land on which it stood. But the records at the country's Property Institute showed another person registered as its owner, too—and that person convinced a judge to sign an eviction order. By the time the legal confusion was finally sorted out, Ms Izaguirre's house had been demolished.

It is the sort of thing that happens every day in places where land registries are badly kept, mismanaged and/or corrupt—which is to say across much of the world. This lack of secure property rights is an endemic source of insecurity and injustice. It also makes it harder to use a house or a piece of land as collateral, stymying investment and job creation.

Such problems seem worlds away from bitcoin, a currency based on clever cryptography which has a devoted following among mostly well-off, often anti-government and sometimes criminal geeks. But the cryptographic technology that underlies bitcoin, called the "blockchain", has applications well beyond cash and currency. It offers a way for people who do not know or trust each other to create a record of who owns what that will compel the assent of everyone concerned. It is a way of making and preserving truths.

That is why politicians seeking to clean up the Property Institute in Honduras have asked Factom, an American startup, to provide a prototype of a blockchain-based land registry. Interest in the idea has also been expressed in Greece, which has no proper land registry and where only 7% of the territory is adequately mapped.

A place in the past

Other applications for blockchain and similar "distributed ledgers" range from thwarting diamond thieves to streamlining stockmarkets: the NASDAQ exchange will soon start using a blockchain-based system to record trades in privately held companies. The Bank of England, not known for technological flights of fancy, seems electrified: distributed ledgers, it concluded in a research note late last year, are a "significant innovation" that could have "far-reaching implications" in the financial industry.

The politically minded see the blockchain reaching further than that. When co-operatives and left-wingers gathered for this year's OuiShare Fest in Paris to discuss ways that grass-roots organisations could undermine giant repositories of data like Facebook, the blockchain made it into almost every speech. Libertarians dream of a world where more and more state regulations are replaced with private contracts between individuals—contracts which blockchain-based programming would make self-enforcing.

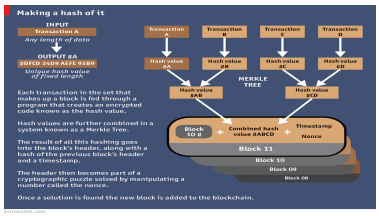
The blockchain began life in the mind of Satoshi Nakamoto, the brilliant, pseudonymous and so far unidentified creator of bitcoin—a "purely peer-to-peer version of electronic cash", as he put it in a paper published in 2008. To work as cash, bitcoin had to be able to change hands without being

diverted into the wrong account and to be incapable of being spent twice by the same person. To fulfil Mr Nakamoto's dream of a decentralised system the avoidance of such abuses had to be achieved without recourse to any trusted third party, such as the banks which stand behind conventional payment systems.

It is the blockchain that replaces this trusted third party. A database that contains the payment history of every bitcoin in circulation, the blockchain provides proof of who owns what at any given juncture. This distributed ledger is replicated on thousands of computers—bitcoin's "nodes"—around the world and is publicly available. But for all its openness it is also trustworthy and secure. This is guaranteed by the mixture of mathematical subtlety and computational brute force built into its "consensus mechanism"—the process by which the nodes agree on how to update the blockchain in the light of bitcoin transfers from one person to another.

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, specialised nodes called miners will bundle Alice's proposal with other similarly reputable transactions to create a new block for the blockchain.



This entails repeatedly feeding the data through a cryptographic "hash" function which boils the block down into a string of digits of a given length (see diagram). Like a lot of cryptography, this hashing is a one-way street. It is easy to go from the data to their hash; impossible to go from the hash back to the data. But though the hash does not contain the data, it is still unique to them. Change what goes into the block in any way—alter a transaction by a single digit—and the hash would be different.

Running in the shadows

That hash is put, along with some other data, into the header of the proposed block. This header then becomes the basis for an exacting mathematical puzzle which involves using the hash function yet again. This puzzle can only be solved by trial and error. Across the network, miners grind through trillions and trillions of possibilities looking for the answer. When a miner finally comes up with a solution other nodes quickly check it (that's the one-way street again: solving is hard but checking is easy), and each node that confirms the solution updates the blockchain accordingly. The hash of the header becomes the new block's identifying string, and that block is now part of the ledger. Alice's payment to Bob, and all the other transactions the block contains, are confirmed.

This puzzle stage introduces three things that add hugely to bitcoin's security. One is chance. You cannot predict which miner will solve a puzzle, and so you cannot predict who will get to update the blockchain at any given time, except in so far as it has to be one of the hard working miners, not some random interloper. This makes cheating hard.

The second addition is history. Each new header contains a hash of the previous block's header,

which in turn contains a hash of the header before that, and so on and so on all the way back to the beginning. It is this concatenation that makes the blocks into a chain. Starting from all the data in the ledger it is trivial to reproduce the header for the latest block. Make a change anywhere, though —even back in one of the earliest blocks—and that changed block's header will come out different. This means that so will the next block's, and all the subsequent ones. The ledger will no longer match the latest block's identifier, and will be rejected.

Is there a way round this? 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. This rule stops the occasions when two miners find the solution almost simultaneously from causing anything more than a temporary fork in the chain

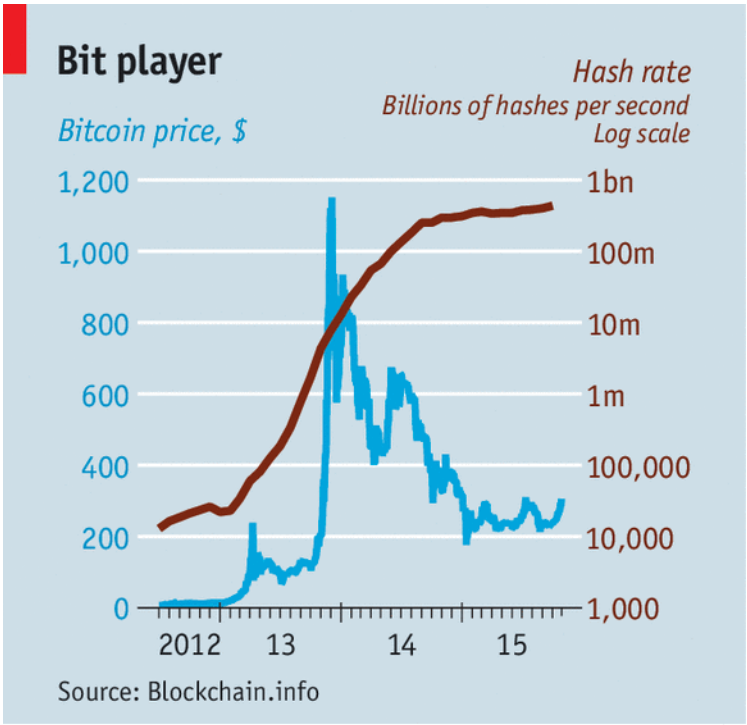
the solution almost simultaneously from causing anything more than a temporary fork in the chain. It also stops cheating. To force the system to accept her new version Alice would need to lengthen it faster than the rest of the system was lengthening the original. Short of controlling more than half the computers—known in the jargon as a "51% attack"—that should not be possible.

Dreams are sometimes catching

Leaving aside the difficulties of trying to subvert the network, there is a deeper question: why bother to be part of it at all? Because the third thing the puzzle-solving step adds is an incentive. Forging a new block creates new bitcoin. The winning miner earns 25 bitcoin, worth about $7,500 at current prices.

All this cleverness does not, in itself, make bitcoin a particularly attractive currency. Its value is unstable and unpredictable (see chart), and the total amount in circulation is deliberately limited. But the blockchain mechanism works very well. According to blockchain.info, a website that tracks such things, on an average day more than 120,000 transactions are added to the blockchain, representing about $75m exchanged. There are now 380,000 blocks; the ledger weighs in at nearly 45 gigabytes.

Most of the data in the blockchain are about bitcoin. But they do not have to be. Mr Nakamoto has built what geeks call an "open platform"—a distributed system the workings of which are open to examination and elaboration. The paragon of such platforms is the internet itself; other examples include operating systems like Android or Windows. Applications that depend on basic features of the blockchain can thus be developed without asking anybody for permission or paying anyone for the privilege. "The internet finally has a public data base," says Chris Dixon of Andreessen Horowitz, a venture-capital firm which has financed several bitcoin start-ups, including Coinbase, which provides wallets, and 21, which makes bitcoin-mining hardware for the masses.



Economist.com

For now blockchain-based offerings fall in three buckets. The first takes advantage of the fact that any type of asset can be transferred using the blockchain. One of the startups betting on this idea is Colu. It has developed a mechanism to "dye" very small bitcoin transactions (called "bitcoin dust") by adding extra data to them so that they can represent bonds, shares or units of precious metals.

Protecting land titles is an example of the second bucket: applications that use the blockchain as a truth machine. Bitcoin transactions can be combined with snippets of additional information which then also become embedded in the ledger. It can thus be a registry of anything worth tracking closely. Everledger uses the blockchain to protect luxury goods; for example it will stick on to the blockchain data about a stone's distinguishing attributes, providing unchallengeable proof of its identity should it be stolen. Onename stores personal information in a way that is meant to do away

with the need for passwords; CoinSpark acts as a notary. Note, though, that for these applications, unlike for pure bitcoin transactions, a certain amount of trust is required; you have to believe the intermediary will store the data accurately.

It is the third bucket that contains the most ambitious applications: "smart contracts" that execute themselves automatically under the right circumstances. Bitcoin can be "programmed" so that it only becomes available under certain conditions. One use of this ability is to defer the payment miners get for solving a puzzle until 99 more blocks have been added—which provides another incentive to keep the blockchain in good shape.

Lighthouse, a project started by Mike Hearn, one of bitcoin's leading programmers, is a decentralised crowdfunding service that uses these principles. If enough money is pledged to a project it all goes through; if the target is never reached, none does. Mr Hearn says his scheme will both be cheaper than non-bitcoin competitors and also more independent, as governments will be unable to pull the plug on a project they don't like.

Energy is contagious

The advent of distributed ledgers opens up an "entirely new quadrant of possibilities", in the words of Albert Wenger of USV, a New York venture firm that has invested in startups such as OpenBazaar, a middleman-free peer-to-peer marketplace. But for all that the blockchain is open and exciting, sceptics argue that its security may yet be fallible and its procedures may not scale. What works for bitcoin and a few niche applications may be unable to support thousands of different services with millions of users.

Though Mr Nakamoto's subtle design has so far proved impregnable, academic researchers have identified tactics that might allow a sneaky and well financed miner to compromise the block chain without direct control of 51% of it. And getting control of an appreciable fraction of the network's resources looks less unlikely than it used to. Once the purview of hobbyists, bitcoin mining is now dominated by large "pools", in which small miners share their efforts and rewards, and the operators of big data centres, many based in areas of China, such as Inner Mongolia, where electricity is cheap.

Another worry is the impact on the environment. With no other way to establish the bona fides of miners, the bitcoin architecture forces them to do a lot of hard computing; this "proof of work", without which there can be no reward, insures that all concerned have skin in the game. But it adds up to a lot of otherwise pointless computing. According to blockchain.info the network's miners are now trying 450 thousand trillion solutions per second. And every calculation takes energy.

Because miners keep details of their hardware secret, nobody really knows how much power the network consumes. If everyone were using the most efficient hardware, its annual electricity usage might be about two terawatt-hours—a bit more than the amount used by the 150,000 inhabitants of King's County in California's Central Valley. Make really pessimistic assumptions about the miners' efficiency, though, and you can get the figure up to 40 terawatt-hours, almost two-thirds of what the 10m people in Los Angeles County get through. That surely overstates the problem; still, the more widely people use bitcoin, the worse the waste could get.

Yet for all this profligacy bitcoin remains limited. Because Mr Nakamoto decided to cap the size of a block at one megabyte, or about 1,400 transactions, it can handle only around seven transactions per second, compared to the 1,736 a second Visa handles in America. Blocks could be made bigger; but bigger blocks would take longer to propagate through the network, worsening the risks of forking.

Earlier platforms have surmounted similar problems. When millions went online after the invention of the web browser in the 1990s pundits predicted the internet would grind to a standstill: *eppur si muove*. Similarly, the bitcoin system is not standing still. Specialised mining computers can be very energy efficient, and less energy-hungry alternatives to the proof-of-work mechanism have been proposed. Developers are also working on an add-on called "Lightning" which would handle large numbers of smaller transactions outside the blockchain. Faster connections will let bigger blocks propagate as quickly as small ones used to.

The problem is not so much a lack of fixes. It is that the network's "bitcoin improvement process" makes it hard to choose one. Change requires community-wide agreement, and these are not people to whom consensus comes easily. Consider the civil war being waged over the size of blocks. One camp frets that quickly increasing the block size will lead to further concentration in the mining

camp frets that quickly increasing the block size will lead to further concentration in the mining industry and turn bitcoin into more of a conventional payment processor. The other side argues that the system could crash as early as next year if nothing is done, with transactions taking hours.

A break in the battle

Mr Hearn and Gavin Andresen, another bitcoin grandee, are leaders of the big-block camp. They have called on mining firms to install a new version of bitcoin which supports a much bigger block size. Some miners who do, though, appear to be suffering cyber-attacks. And in what seems a concerted effort to show the need for, or the dangers of, such an upgrade, the system is being driven to its limits by vast numbers of tiny transactions.

This has all given new momentum to efforts to build an alternative to the bitcoin blockchain, one that might be optimised for the storing of distributed ledgers rather than for the running of a cryptocurrency. MultiChain, a build-your-own-blockchain platform offered by Coin Sciences, another startup, demonstrates what is possible. As well as offering the wherewithal to build a public blockchain like bitcoin's, it can also be used to build private chains open only to vetted users. If all the users start off trusted the need for mining and proof-of-work is reduced or eliminated, and a currency attached to the ledger becomes an optional extra.

The first industry to adopt such sons of blockchain may well be the one whose failings originally inspired Mr Nakamoto: finance. In recent months there has been a rush of bankerly enthusiasm for private blockchains as a way of keeping tamper-proof ledgers. One of the reasons, irony of ironies, is that this technology born of anti-government libertarianism could make it easier for the banks to comply with regulatory requirements on knowing their customers and anti-money-laundering rules. But there is a deeper appeal.

Industrial historians point out that new powers often become available long before the processes that best use them are developed. When electric motors were first developed they were deployed like the big hulking steam engines that came before them. It took decades for manufacturers to see that lots of decentralised electric motors could reorganise every aspect of the way they made things. In its report on digital currencies, the Bank of England sees something similar afoot in the financial sector. Thanks to cheap computing financial firms have digitised their inner workings; but they have not yet changed their organisations to match. Payment systems are mostly still centralised: transfers are cleared through the central bank. When financial firms do business with each other, the hard work of synchronising their internal ledgers can take several days, which ties up capital and increases risk.

Distributed ledgers that settle transactions in minutes or seconds could go a long way to solving such problems and fulfilling the greater promise of digitised banking. They could also save banks a lot of money: according to Santander, a bank, by 2022 such ledgers could cut the industry's bills by up to $20 billion a year. Vendors still need to prove that they could deal with the far-higher-than-bitcoin transaction rates that would be involved; but big banks are already pushing for standards to shape the emerging technology. One of them, UBS, has proposed the creation of a standard "settlement coin". The first order of business for R3 CEV, a blockchain startup in which UBS has invested alongside Goldman Sachs, JPMorgan and 22 other banks, is to develop a standardised architecture for private ledgers.

The banks' problems are not unique. All sorts of companies and public bodies suffer from hard-to-maintain and often incompatible databases and the high transaction costs of getting them to talk to each other. This is the problem Ethereum, arguably the most ambitious distributed-ledger project, wants to solve. The brainchild of Vitalik Buterin, a 21-year-old Canadian programming prodigy, Ethereum's distributed ledger can deal with more data than bitcoin's can. And it comes with a programming language that allows users to write more sophisticated smart contracts, thus creating invoices that pay themselves when a shipment arrives or share certificates which automatically send their owners dividends if profits reach a certain level. Such cleverness, Mr Buterin hopes, will allow the formation of "decentralised autonomous organisations"—virtual companies that are basically just sets of rules running on Ethereum's blockchain.

One of the areas where such ideas could have radical effects is in the "internet of things"—a network of billions of previously mute everyday objects such as fridges, doorstops and lawn sprinklers. A recent report from IBM entitled "Device Democracy" argues

report from IBM entitled "Device Democracy" argues that it would be impossible to keep track of and manage these billions of devices centrally, and unwise to to try; such attempts would make them vulnerable to hacking attacks and government surveillance. Distributed registers seem a good alternative.

The sort of programmability Ethereum offers does not just allow people's property to be tracked and registered. It allows it to be used in new sorts of ways. Thus a car-key embedded in the Ethereum blockchain could be sold or rented out in all manner of rule-based ways, enabling new peer-to-peer schemes for renting or sharing cars. Further out, some talk of using the technology to make by-then-self-driving cars self-owning, to boot. Such vehicles could stash away some of the digital money they make from renting out their keys to pay for fuel, repairs and parking spaces, all according to preprogrammed rules.

What would Rousseau have said?

Unsurprisingly, some think such schemes overly ambitious. Ethereum's first ("genesis") block was only mined in August and, though there is a little ecosystem of start-ups clustered around it, Mr Buterin admitted in a recent blog post that it is somewhat short of cash. But the details of which particular blockchains end up flourishing matter much less than the broad enthusiasm for distributed ledgers that is leading both start-ups and giant incumbents to examine their potential. Despite society's inexhaustible ability to laugh at accountants, the workings of ledgers really do matter.

Today's world is deeply dependent on double-entry book-keeping. Its standardised system of recording debits and credits is central to any attempt to understand a company's financial position.

Whether modern capitalism absolutely required such book-keeping in order to develop, as Werner Sombart, a German sociologist, claimed in the early 20th century, is open to question. Though the system began among the merchants of renaissance Italy, which offers an interesting coincidence of timing, it spread round the world much more slowly than capitalism did, becoming widely used only in the late 19th century. But there is no question that the technique is of fundamental importance not just as a record of what a company does, but as a way of defining what one can be.

Ledgers that no longer need to be maintained by a company—or a government—may in time spur new changes in how companies and governments work, in what is expected of them and in what can be done without them. A realisation that systems without centralised record-keeping can be just as trustworthy as those that have them may bring radical change.

Such ideas can expect some eye-rolling—blockchains are still a novelty applicable only in a few niches, and the doubts as to how far they can spread and scale up may prove well founded. They can also expect resistance. Some of bitcoin's critics have always seen it as the latest techy attempt to spread a "Californian ideology" which promises salvation through technology-induced decentralisation while ignoring and obfuscating the realities of power—and happily concentrating vast wealth in the hands of an elite. The idea of making trust a matter of coding, rather than of democratic politics, legitimacy and accountability, is not necessarily an appealing or empowering one.

At the same time, a world with record-keeping mathematically immune to manipulation would have many benefits. Evicted Ms Izaguirre would be better off; so would many others in many other settings. If blockchains have a fundamental paradox, it is this: by offering a way of setting the past and present in cryptographic stone, they could make the future a very different place.

From the print edition: Briefing

Appendix Item 7

EQUITY RESEARCH | May 24, 2016

Goldman Sachs

Is the hype around blockchain justified? Since Bitcoin introduced the world to the concept of secure distributed ledgers, much has been written about their potential to address other business problems. But the discussion often remains abstract, focusing on the opportunity to decentralize markets and disrupt middlemen. In the latest in our **Profiles in Innovation** series, we shift the focus from theory to practice, examining seven real-world applications of blockchain, such as enhancing trust in the Sharing Economy, building a distributed smart grid, lowering the cost of title insurance, and changing the face of finance across capital markets, trading and control. We identify, itemize, and quantify the players, dollars and risks for blockchain to reach its full potential.

James Schneider, Ph.D.
(917) 343-3149
james.schneider@gs.com
Goldman, Sachs & Co.

Alexander Blostein, CFA
(212) 357-9976
alexander.blostein@gs.com
Goldman, Sachs & Co.

Brian Lee, CFA
(917) 343-3110
brian.k.lee@gs.com
Goldman, Sachs & Co.

Steven Kent, CFA
(212) 902-6752
steven.kent@gs.com
Goldman, Sachs & Co.

Ingrid Groer, CFA
+61(2)9321-8563
ingrid.groer@gs.com
Goldman Sachs Australia Pty Ltd

Eric Beardsley, CFA
(917) 343-7160
eric.beardsley@gs.com
Goldman, Sachs & Co.

PROFILES IN INNOVATION

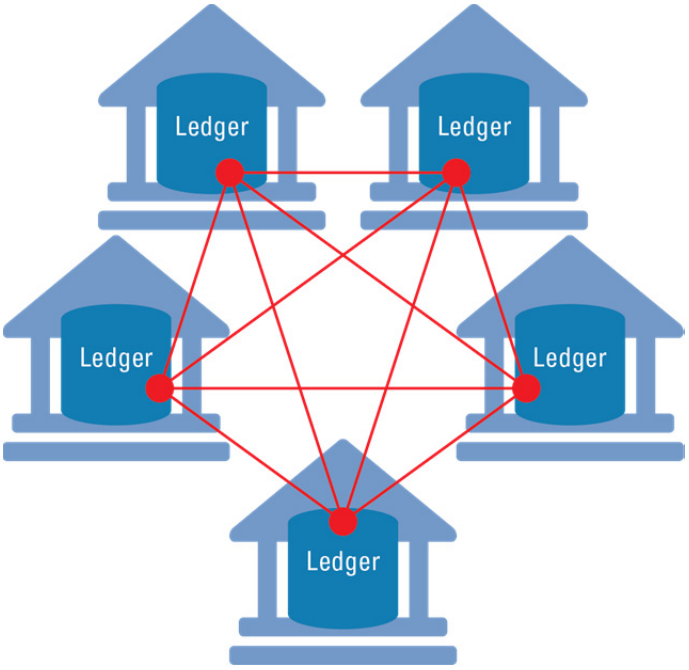
BLOCKCHAIN

Putting Theory into Practice

The Goldman Sachs Group, Inc.

markets), multiple parties already maintain duplicate databases containing information about the same transactions. And in many cases, the data pertaining to the same transaction is in conflict – resulting in the need for costly, time-consuming reconciliation procedures between organizations. Employing a distributed database system like blockchain across organizations can substantially reduce the need for manual reconciliation, thus driving considerable savings across organizations. In addition, in some cases (see our discussion of AML) blockchain offers the potential for organizations to develop common or "mutual" capabilities that eliminate the need for duplication of the same effort among multiple organizations.

Exhibit 3: The blockchain ledger is distributed across multiple locations, each of which is connected via a data link. This illustration shows a "permissioned" blockchain composed of a fixed number of trusted counterparties.



Source: Goldman Sachs Global Investment Research.

Blockchain: Public or private?

We expect private or "permissioned" blockchains to dominate most commercial applications. The distributed ledger used for Bitcoin is a public ledger that can be read from or written to by anyone who wishes to transact, making it an ideal vehicle for public transactions between individuals who don't know each other. In fact, the public nature of the Bitcoin ledger is one of the most appealing and novel features of the distributed database. Yet for many high-volume commercial transactions (for example, in securities transactions between counterparties or sharing information between commercial partners in a supply chain), trust is already established among the participants – and in many cases they desire transaction privacy. Private or "permissioned" blockchains behave in the same way as the public blockchain, except that the identity of anyone who attempts to access the blockchain must be validated against a list of pre-validated market IDs. We believe that the vast majority of commercial blockchain applications – particularly in capital markets – are likely to use private or permissioned blockchains.

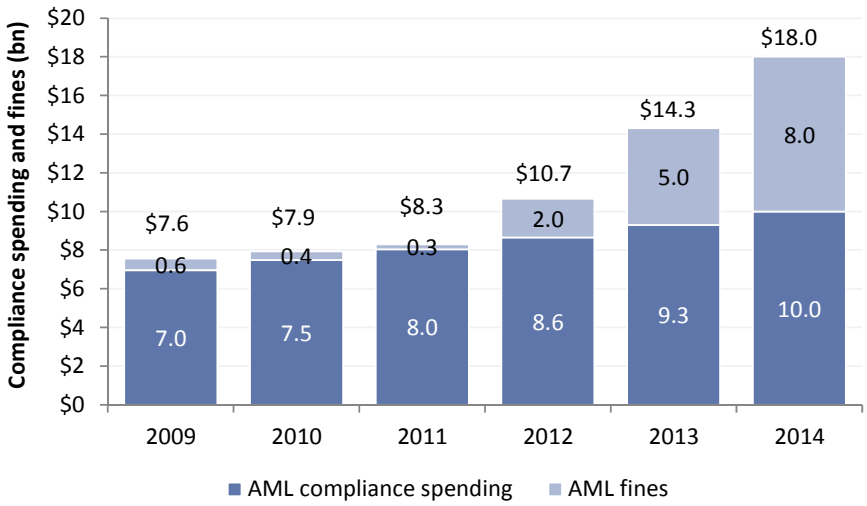
Case Study 7: AML and KYC Compliance

We believe blockchain has the opportunity to streamline and potentially transform anti-money laundering (AML) compliance procedures. By using a distributed database of payment transactions to better validate counterparty information, financial institutions could substantially reduce the false positive rate in transaction surveillance – which requires significant manual intervention today. In addition, over the long term we think a shared database of validated customer information could help streamline the KYC process that is involved in client onboarding. Together, we believe blockchain could drive between $3bn and $5bn in industry cost savings through reduction in personnel and in AML regulatory penalties.

What is the opportunity?

AML compliance spending totals ~$10bn annually. Money laundering (i.e., disguising the proceeds of illegal activity such as drug trafficking, financial fraud, etc. so as to appear to originate from legitimate sources or activities) is a serious problem in the international financial system. The World Bank estimates that the volume of money laundering is between $2.0tn and $3.5tn annually (3%-5% of global GDP). In an effort to combat this problem, regulators have instituted far-reaching guidelines for banks' in-house AML compliance programs. Still, third-party data suggests that less than ~1% of money laundering is detected, and banks have incurred significant regulatory penalties as a result. **Inclusive of regulatory penalties, total AML compliance costs borne by banks amount to ~$18bn annually** (AML fines alone totaled $8bn in 2014). We see an opportunity for blockchain to streamline AML monitoring procedures by "mutualizing" financial transaction information via a distributed ledger, which could drive meaningful industry cost savings in transaction surveillance and, potentially, in KYC onboarding.

Exhibit 70: AML compliance costs and regulatory fines continue to reach new highs
AML compliance spending + AML regulatory fines, 2009-2014 ($bn)



Source: Accenture, Celent.

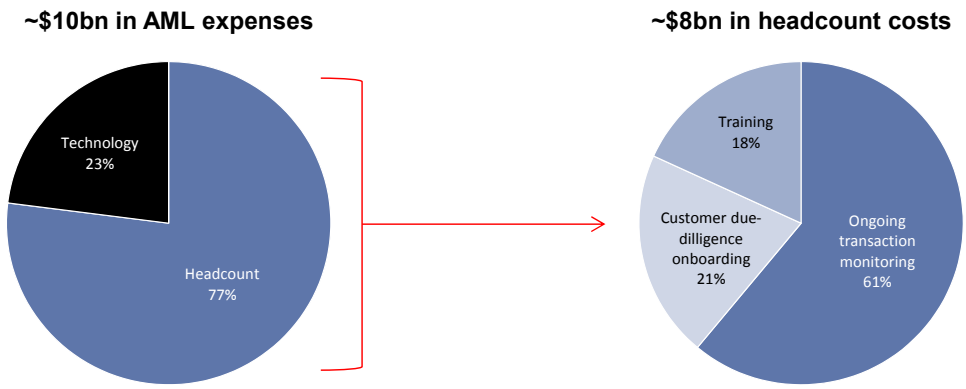
What are the pain points?

Implementation of AML requirements is highly labor intensive. In order to comply with evolving anti-money laundering regulations, financial institutions expend significant resources to develop and maintain their AML compliance programs. Although banks do automate many aspects of these procedures, the vast majority of AML budgets are dedicated to compliance personnel who manually scrutinize suspicious payment transactions and onboard new clients. We believe the existing banking system faces several structural problems that underscore the need for such manual oversight and the high cost structure involved in carrying out AML compliance programs:

- **Lack of data "mutualization" between banks leads to duplicate effort in client onboarding.** When a new client relationship is formed, financial institutions conduct a thorough customer due-diligence (CDD) process in accordance with "know your customer" (KYC) regulations. While the complexity of select retail and institutional account ownership structures requires manual review, KYC checks are often duplicative. In most jurisdictions, banks are required to independently vet prospective accounts even when the account has already been vetted by another bank. We estimate that proper KYC due diligence can cost $15k-$50k per client.
- **Lack of account codification leads to significant false-positive rates in transaction surveillance.** Although banks rely on transaction monitoring software to screen for suspicious behavior, our checks suggest that 2%-5% of all payment transactions are manually reviewed by compliance personnel to determine if money laundering has actually occurred. In such instances, false positive rates are ~99.9%. In the vast majority of cases, we believe this is not the result of deficiencies in monitoring software as much as it is due to poor transaction data quality (e.g., missing sender/receiver identification details). Whether or not money laundering has occurred, monitoring systems sound alerts when wire transfer information pertinent to the formation of an audit trail is either syntactically misrepresented or incomplete – and we believe this manual reconciliation process amounts to ~$6bn in costs borne by the industry.

As a result of these factors, financial institutions employ large numbers of people to carry out AML compliance programs. **Between onboarding, transaction monitoring, and recruitment personnel, we estimate that headcount costs represent nearly 80% of total AML budgets.** We believe much of these costs are a result of structural inefficiencies in the mutual flow of reliable information between financial counterparties, which requires the manual intervention of compliance personnel to facilitate the process.

Exhibit 71: AML operating costs largely consist of headcount costs
Illustrative breakdown of AML budget expense structure



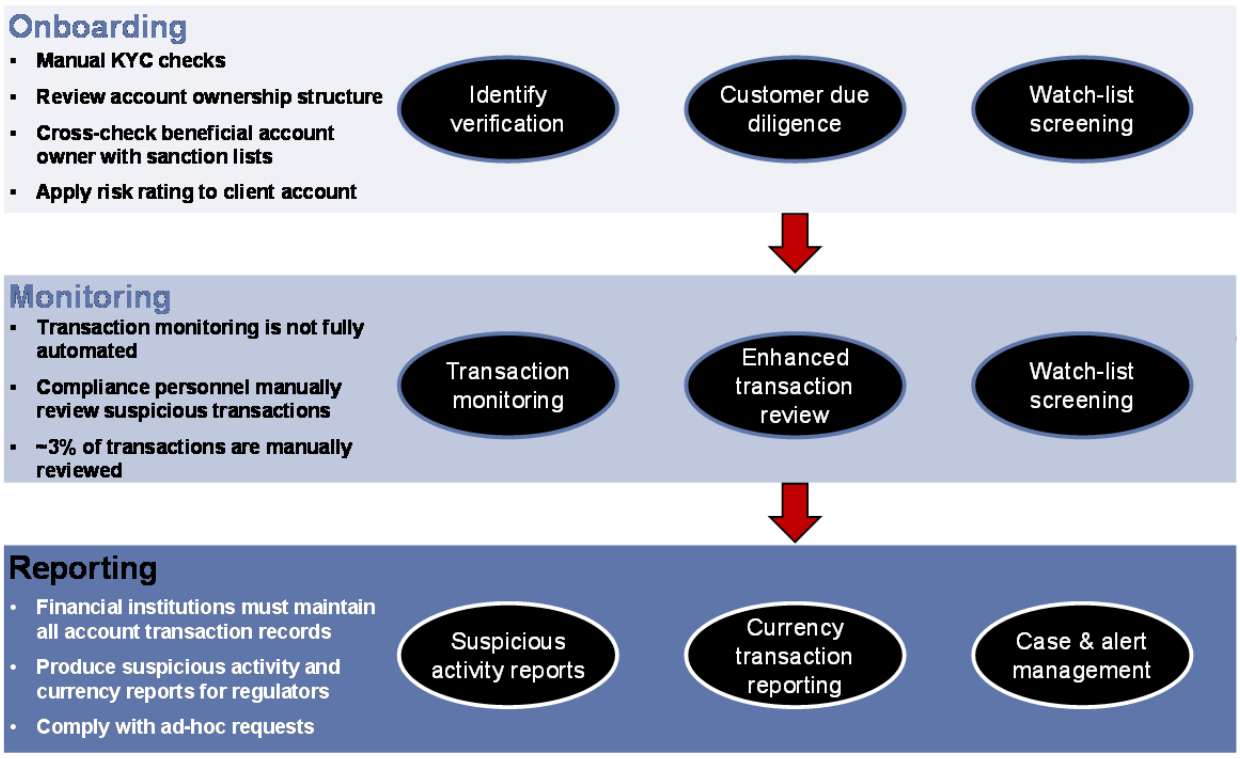
Source: Celent, Goldman Sachs Global Investment Research.

What is the current way of doing business?

Financial institutions implement AML procedures in several phases. Whether opening a bank account or moving money between accounts, financial intuitions employ AML procedures to mitigate counterparty risk in each step. We highlight the following phases to this process below:

- **Onboarding:** When a client seeks to open an account, banks conduct an exhaustive customer due-diligence process to verify customer identity and beneficial ownership of the account, and cross-check this data against sanctions lists. Given the complexities of select retail and institutional account ownership structures, KYC checks comprise a significant manual component.
- **Monitoring:** Once a client is on board, banks perform real-time and remedial transaction surveillance using advanced data analytics (typically provided by an external software vendor). We note that compliance personnel will manually review alerted transactions on a daily basis. Our checks suggest that 2%- 5% of all payment transactions are alerted, and these carry a ~99.9% false positive rate.
- **Reporting:** Financial institutions must maintain all necessary records on transactions, both domestic and international, as well as customer due-diligence information in order to comply swiftly with regulatory requests. Banks often prepare suspicious activity and currency transaction reports for authorities as well.

Exhibit 72: AML implementation procedures are highly manual
AML implementation phases



Source: Goldman Sachs Global Investment Research.

How does blockchain help?

Blockchain has the potential to improve structural pain points and ultimately streamline AML compliance. We believe new distributed database technology enabled by blockchain, in combination with enhanced policies and procedures, could significantly shore up the following pain points in today's system. **While we recognize that technology by itself is insufficient to address many of these structural challenges, we think systems could enhance procedures while enabling significant cost reductions:**

- **Secure codification of account details could enable greater transparency and efficiency in transaction surveillance.** By codifying the rules tied to completeness of account information (sending and receiving party details, legal entity information, etc.) that is part of every payment transaction, blockchain could improve the transparency of payment transactions and reduce the false positive rate. We believe this would reduce the labor overhead required to reconcile alert transactions with underlying money-laundering activity.
- **Distributed ledgers of present and past transactions would simplify recordkeeping and audit procedures.** Financial institutions could use a blockchain-based system to store an historical record of all transactions (including documents shared and compliance activities undertaken) on behalf of each client. Because all transactions tied to a particular client could be traced automatically, this record could be used to provide evidence that a bank has acted in accordance with AML demands, and enable it to quickly comply with regulatory requests.
- **Secure, distributed databases of client information shared between institutions could help reduce duplicative efforts in customer onboarding.** Each financial institution is required to conduct KYC checks for new accounts in order to validate the origin and associations of individuals, corporations, and sub-entities. In principle, financial institutions having a longstanding relationship with a client could potentially help "credentialize" that client with other institutions by providing supporting evidence of client associations through a secure, permissioned process facilitated by blockchain. While this would not completely eliminate the KYC burden for other financial institutions, it could potentially reduce the number of manual onboarding steps and reduce customer due-diligence costs.

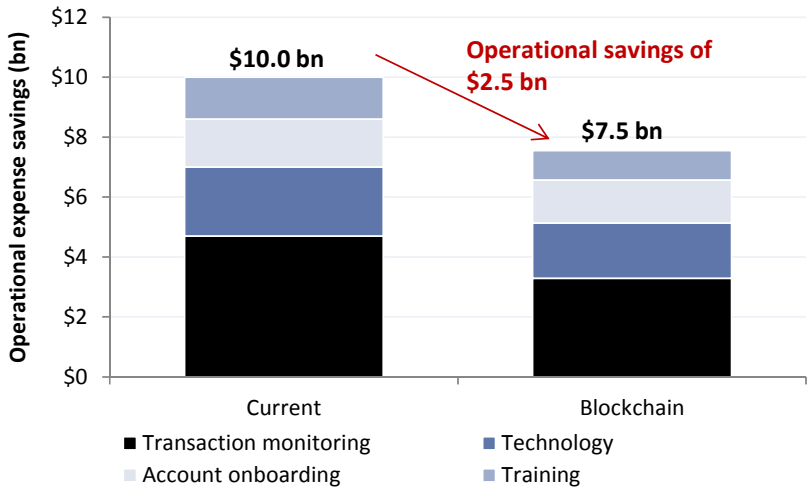
By streamlining these processes, blockchain could help reshape AML compliance implementation process. As a result of greater data integrity and accessibility, we believe the reliance on manual labor to conduct KYC checks and scrutinize suspected instances of laundering activity could be substantially reduced – thus allowing for potentially significant cost savings from reduced headcount. We would also expect blockchain to help improve counterparty risk as client information becomes more easily verifiable and systematic "misses" are reduced, potentially reducing monetary fines for financial institutions.

Quantifying the opportunity

We estimate that blockchain could drive substantial cost savings between $3bn and $5bn by reducing compliance personnel, technology expenses, and AML penalties. From an operational standpoint, we believe blockchain could introduce meaningful headcount efficiencies as manual aspects of transaction monitoring and onboarding procedures would be streamlined. While we do not believe blockchain by itself is a cure-all for inefficiencies in AML compliance, we believe the underlying technology – in conjunction with improved industry data policies and standards – could meaningfully increase the transparency of transactions. **In our base case, we estimate that blockchain could drive $2.5bn in operational cost savings** (headcount + technology). We break down our cost assumptions by function below:

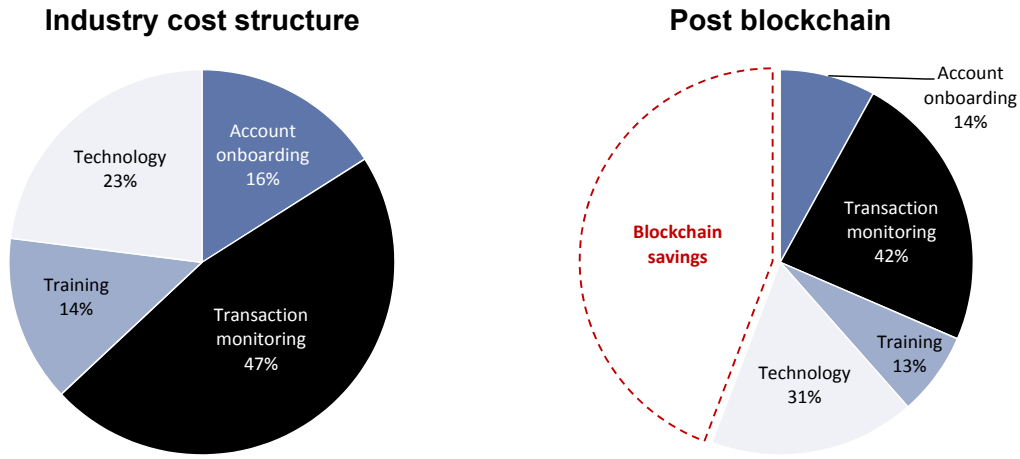
- **Customer onboarding: Modest cost savings with streamlined KYC effort.** We estimate blockchain could decrease customer onboarding headcount by 10%, introducing ~$160mn in cost savings. While a shared database of client information could eliminate duplicative aspects of KYC for select accounts with precedent banking relationships, we expect banks would still need to run customer diligence checks when the prospective account is a private company and/or individual setting up a bank account for the first time – or if the pre-existing customer data's authenticity is questionable (e.g., validated only by a single source). Importantly, blockchain would not remove banks' KYC liability, and thus we think banks will remain cautious when onboarding new accounts given AML penalties, despite improvements in customer data transparency and security.
- **Transaction monitoring: Meaningful efficiencies due to fewer "false positives" and less manual intervention.** We estimate blockchain could decrease transaction monitoring headcount by 30%, allowing for as much as $1.4bn in cost savings. We believe capturing and tracking customer information with blockchain in conjunction with unique client identifiers could introduce greater transparency to transaction surveillance. Since a large proportion of false positives are tied to transactions with incomplete information, we believe this could significantly reduce the number of false positives, thereby lowering the number of compliance personnel necessary to reconcile alerted transactions.
- **Training and technology: Significant cost savings resulting from less headcount and greater security.** We estimate blockchain could decrease training headcount by 30%, introducing ~$420mn in cost savings, tied solely to the reduction in headcount savings noted above. Over the long term, blockchain could lower technology expenses by 20% ($400mn-500mn in cost savings), given less reliance on proprietary systems.

Exhibit 73: We estimate blockchain could drive $2.5bn in operational cost savings
Estimated industry headcount operating expenses currently vs post-blockchain ($bn)



Source: Celent, Goldman Sachs Global Investment Research.

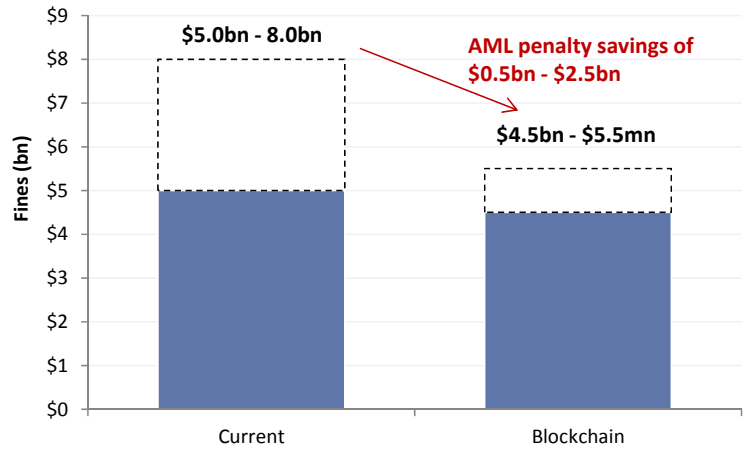
Exhibit 74: Labor-intensive AML implementation expenses could see significant reduction
Estimated industry operating expense composition currently vs post-blockchain



Source: Goldman Sachs Global Investment Research.

Wildcard: Higher capture rates could potentially reduce AML regulatory fines. Banks incurred approximately $8bn in AML regulatory fines in 2014, according to an Accenture report. While it is highly unlikely that money-laundering risk would be fully eliminated if payment transactions were linked to blockchain, we would expect that "capture rates" would improve in the presence of more-effective systems with more extensive audit and tracing capability. In addition to specific instances of money laundering violations, programmatic deficiencies associated with transaction monitoring procedures have driven significant penalties in recent years – and we think these systematic fines could probably be substantially reduced with better systems in place. **In our base case we estimate that AML penalties could be reduced by 10% to 40% - generating cost savings of $0.5 - $2.5bn annually.**

Exhibit 75: Blockchain could drive between $0.5 - $2.5bn in AML penalty savings annually
Estimated AML penalties currently and post-blockchain



Source: Accenture, Goldman Sachs Global Investment Research.

**Numbers may not sum due to rounding.*

Exhibit 76: In our base scenario, blockchain could drive $3.0bn - $5.0bn in total cost savings
Cost savings by operating expense line item

	Current		Blockchain		
Operating Expenses	Absolute cost (bn)	% of total	Absolute cost (bn)	% of Opex	Savings (bn)
Account onboarding	$1.6	10%	$1.4	13%	**$0.2**
Transaction monitoring	$4.7	28%	$3.3	29%	**$1.4**
Training	$1.4	8%	$1.0	9%	**$0.4**
Technology	$2.3	14%	$1.8	16%	**$0.5**
AML fines	$5.0 - $8.0	39%	$2.5 - $5.0	33%	**$0.5 - $2.5**
Total	**$15.0 - $18.0**		**$10.0 - $12.5**		**$3.0 - $5.0**

Source: Goldman Sachs Global Investment Research.

Who could be disrupted?

We believe blockchain could potentially have the most impact on AML software providers. We note that most financial institutions, particularly smaller-sized banks, rely on externally provided AML software solutions to screen for suspicious transaction activity and sanction-list filtering. In our view, the companies most exposed to our assumption of reduced technology spending are Actimize, Mantas, Prime Associates, ACI Worldwide, SAS Institute, and Infrasoft. While we believe the prospect for commercialization of blockchain is a longer-term phenomenon, we think it is reasonable for AML software providers to react in advance of this trend, potentially spurring greater automation and cost saving efforts over the medium term.

Challenges to adoption

Critical mass of counterparty information. We believe a critical mass of information is needed in order for data to be commercially reliable. For example, in cases where there is a scarcity of validated counterparty information (e.g., validated only by a single source), we expect banks would still need to run their own KYC checks and/or transaction surveillance to independently corroborate client information.

Regulatory reform. Regulatory reform that supports blockchain-based applications will be needed before financial institutions are able to embrace the technology. While blockchain will likely not remove banks' AML liability, blockchain-based distributed ledgers will need to be legitimized by governing bodies (i.e., fiat currency) in order for banks to comfortably rely on them as a source of counterparty information.

Infrastructure development. The development of blockchain-based infrastructure that operates in conjunction with existing industry standards is needed for commercial adoption. For example, we note that wire transfer information (e.g., ABA routing numbers) will need to be tied to a blockchain index to improve the security of money movement transactions. As such, we believe considerable investment is needed to implement requisite infrastructure.

Appendix Item 8

Libor investigation

Banks face pushback over surging compliance and regulatory costs

Call for lenders to rein in billions of dollars in extra expenses incurred since financial crisis

MAY 28, 2015 by: **Laura Noonan**

The world's biggest banks are coming under increasing pressure to control soaring compliance and regulatory costs, with investors, analysts and even some bank executives asking if lenders can do more to rein in the billions of dollars in extra annual costs they have incurred since the financial crisis.

The additional outlay — up to $4bn a year for some banks — covers demands ranging from checks to prevent money-laundering, to requirements to give more data to regulators for stress tests.

Against the backdrop of the multibillion-dollar fines (http://next.ft.com.ezp-prod1.hul.harvard.edu/content/23fa681c-fe73-11e4-be9f-00144feabdc0) for compliance breaches and the mandatory nature of new regulatory demands, investors and analysts have traditionally supported the higher spending, which some bank executives privately describe as a "blank cheque" approach.

Now, the tide is turning. "All I see are cases where compliance costs are going up, and that is a massive challenge for these banks," says a top 10 investor in several banks including HSBC and Standard Chartered. "Every time I see the

management teams, it is the first thing I raise with them."

Bankers say their ability to reduce compliance costs is severely constrained, as regulators are more focused than ever on compliance (http://next.ft.com.ezp-prod1.hul.harvard.edu/content/fab70d48-00a2-11e5-a908-00144feabdc0) and would probably frown on cutbacks. Regulators say the quality of spending is important, while investors believe there is still a case for cost discipline.

"There is a very clear risk banks will overspend," says Patrick Lemmens, a senior portfolio manager at Robeco, pointing to the swelling demands and the fact that it is "very difficult to grasp" what makes up banks' regulatory and compliance spending.

Banks make only ad hoc disclosures about their compliance and regulatory spending. The detail of those disclosures varies greatly. Barclays and Credit Suisse are among the big banks that disclose no data at all.

"We haven't so far demanded evidence that they are not falling into that trap [overspending]," says Richard Buxton, head of UK equities at Old Mutual Global Investors. "Maybe we are at fault." Another large UK banks investor says his company "probably hasn't spent enough time" scrutinising the costs.

On Citigroup's last earnings call, an analyst fruitlessly pushed for confirmation that the average salary for its 26,000 compliance staff was about $60,000. At StanChart's annual meeting, chairman Sir John Peace said the rise in executives earning more than $1m was largely because of compliance hiring.

In depth

Libor scandal (http://www.ft.co

Not everyone agrees

m.ezp-prod1.hul.harvard.edu/indepth/libor-scandal)

Regulators across the globe probe alleged manipulation by US and European banks of the London interbank offered rate and other key benchmark lending rates

Further reading (http://www.ft.com.ezp-prod1.hul.harvard.edu/indepth/libor-scandal)

that more disclosure would help. "Knowing the amount would not tell me if it was being spent well," says Justin Bisseker, banking analyst at Schroders, adding that it was "very dangerous" to benchmark banks given their different structures and needs.

No one disputes the significance of the costs. Citi recently admitted 59 per cent of its expenses savings were "being consumed by additional investments that we're making in regulatory and compliance activities". Analysts and investors express universal frustration with banks that blame compliance spending for missed cost targets.

Bank insiders admit overspending is a potential issue and say some efficiencies will be found. One banker who sits on the executive board of a large European bank says his compliance spending is not put through the same scrutiny as other costs.

"It can be a bit chaotic and certainly there is a bit of inefficiency in this," says a consultant whose company does compliance work for banks. "That's an inevitable consequence of the fact they have had to sort this stuff quickly".

The consultant adds that while banks can push consultants quite hard on costs for some types of projects, when it comes to compliance, the consultancies have more pricing power because banks "haven't got enough compliance resources themselves" even though they have hired thousands.

A senior executive at an investment bank says that after a big compliance issue is uncovered, “the immediate reaction is to hire a lot of people, and bring in externals to fix the problem”. Later, there is a more process-driven set-up, which allows banks to “optimise a little bit”, he adds.

Optimising can take lots of different forms. A divisional chief financial officer working for a large US investment bank says his company initially had unskilled people screening emails at a rate of 200 messages a day, and then discovered skilled people could do 1,000 a day, without costing five times as much.

Technology can do even more, analysing word flow and syntax to screen for the emails most likely to be problematic, and assigning a risk factor to the messages. “If an email is very well written and has good punctuation, it’s less likely [to have an issue],” the CFO says.

Marianne Lake,

In depth

Forex trading probes (http://www.ft.com.ezp-prod1.hul.harvard.edu/topics/themes/Forex_trading_probes)

After the manipulation of Libor is rigging foreign currency markets the next big scandal to hit some of the world’s biggest banks?

Further reading (http://www.ft.com.ezp-prod1.hul.harvard.edu/topics/themes/Forex_trading_probes)

JPMorgan’s finance chief, has spoken publicly about optimising regulatory and compliance spending, but many banks are not yet tackling the cost issue.

"Shareholders would be very reluctant about kicking up a huge fuss about compliance overspending because the downside of not doing it could be phenomenal," says Mr Bisseker of Schroders.

For some, even wasted spend is good spend.

"My sense is that banks believe that their best defence lies in being able to evidence that they've done all they can to minimise the frequency/severity of breaches," says a banking analyst who asked not to be named.

Several senior bankers say they believe that the fact they had spent massively on compliance would serve as a defence if any compliance issues arise — regardless of whether their spending was efficient or effective.

Regulators do not agree. "There is no compensation procedure that will result in a count up of money spent on compliance [set] against breaches," says one regulator. "Certainly, quality is more important than the amounts spent."

Additional reporting by Martin Arnold in London, Tom Braithwaite and Ben McLannahan in New York

What banks have said and done on compliance costs

JPMorgan

JPMorgan employed 4,000 additional compliance staff in 2013 and spent an extra $1bn on controls, Jamie Dimon, the bank's CEO, told staff in a November 2013 memo. The spending came as the lender agreed to pay large fines to settle a range of compliance issues including the London whale.

Deutsche Bank

Deutsche's 2014 results included €1.3bn in extra regulatory-related spending, the bank said. Some €500m was described as "temporary or one off", another €400m was related to regulatory projects which have not yet been completed" and the final €400m was for "incremental headcount to

comply with additional regulatory requirements" and extra charges such as bank levies.

Credit Suisse

Credit Suisse does not disclose details of compliance and regulatory spending. In its 2014 annual report the bank said regulation was "increasingly more extensive and complex". "In recent years, costs related to our compliance with these requirements and the penalties and fines sought and imposed on the financial services industry by regulatory authorities have all increased significantly and may increase further," the statement added.

Citigroup

In April, John Gerspach, Citi's finance boss, said that about half the bank's $3.4bn efficiency savings were being "consumed by additional investments that we're making in regulatory and compliance activities".

UBS

UBS spent SFr900m ($946m) on regulatory demands in 2014. "SFr400m of this is permanent, and we must overcome these increases to achieve our cost reduction targets," Tom Naratil, chief financial officer, told investors in February.

HSBC

In September 2013, HSBC said it would take on 3,000 more compliance staff, bringing the total number working in compliance to more than 5,000. That number has since increased to more than 7,000, according to the bank's latest annual reports. The 2013 hiring came after the bank was fined a record $1.9bn for money laundering.

Appendix Item 9

Could Blockchain solve the KYC/AML challenge?

Matthew Britton

29th September, 2016

With the advent and evolution of new technologies such as distributed ledger technology (DLT) and Artificial Intelligence (AI), many opportunities are arising for banks to reduce their IT and operational costs through mutualisation or automation of their non-differentiating processes. While this will have a beneficial impact on their cost bases, the more proactive banks will recognise the opportunity to either reinvest the savings in value-add, customer–focused services, or reinvent their business processes to make them more customer-friendly – technology will be the great enabler.

As blockchain and DLT reach the peak of the Gartner Hype Cycle, they are being touted as solutions for improving many different processes across financial services. While this may be true in the long run, there will be many fewer applications in the short term where DLT can be more easily incorporated. It's clear from the discussions at SIBOS this week that the industry is starting to focus on three particular use-cases as the first applications using DLT: trade finance, cross-border payments, and KYC/AML; in this blog we look at KYC and AML.

KYC processes are currently expensive, inefficient, and deliver a poor customer

KYC processes are currently expensive, inefficient, and deliver a poor customer experience. It can take up to 50 days to onboard a large corporate through all the necessary checks, with multiple pieces of documentation needing to be produced and verified. While this is painful for clients, it is also a huge burden for banks for what is a non-revenue generating, non-differentiating process. On top of this, fines for incorrectly discharging KYC responsibilities can be huge. AML checks have a similar problem – large operations teams are needed to handle transactions failing AML checks, but typically these run with a >99% false positive rate, resulting in massive inefficiencies.

The industry tried to resolve some of the duplication in KYC by setting up KYC utilities – third-party companies which took on the burden of KYC checks on behalf of the banks (for a fee), and then disseminated each customer's verified documentation to multiple banks as required. This presents a better experience for the customer (they only have to provide documentation once) and a more efficient service for the banks. However, due to a lack of collaboration, four or five competing KYC utilities have emerged resulting in a fragmented market which, while providing some improvements, does not deliver the benefits that could be realised for banks and corporates if a single utility was used.

In this environment, blockchain's attributes of security, distributed data, and decentralisation, appear to provide a potential solution to improving both efficiency and the customer experience by reducing processing costs and enabling the banks to focus on more customer-focussed activity.

The solution would involve a blockchain-based registry, a distributed database of verified customer data, which all banks could access. When a corporate approaches a new bank to open an account the bank will be able to access their pre-verified information from their node on the blockchain. In due course, corporates would be able to upload, amend and delete their information on the blockchain as required. This is not too dissimilar from the model today with KYC utilities but assumes that all banks would use one blockchain network (as opposed to multiple KYC utilities), and would enable near real-time dissemination of updated, verified customer data to all the banks, as well as benefitting from the inherent increased security that blockchain delivers through cryptographic hashing. However, these benefits do not appear to be large enough to justify the significant effort required to implement this change across the industry – as with

the majority of blockchain use-cases, benefits are magnified through the network effect, so the more banks that sign up, the greater the efficiencies that can be realised.

The real selling point of using blockchain is the ability to create, and subsequently use, digital identities. Once a corporate has had their documentation verified once, a digital identity could be created for that customer – this is essentially their digital passport for transacting in financial services and would be appended to every transaction they undertake, effectively

'signing' the transactions for them. This digital identity would store all relevant information about the customer from addresses, account details, director's details, PEPs etc which could be used during AML / transaction monitoring, thus increasing the accuracy of the monitoring and reducing the likelihood for false positives. Taking this further, banks that positively identify a fraudulent transaction could distribute details of that transaction globally to all connected banks, thus preventing the opportunity for further fraud.

This potential model of using a digital identity provides significant benefits over the simple usage of blockchain for KYC, namely:

- Enhanced customer experience through only having to submit documentation once, increased security (less opportunity for identity theft), and fewer transactions being flagged as false positives and stalling transaction flows. In due course, a digital identity could be used across many industries, not just for financial transactions
- Reduced operational costs for banks through not having to KYC-check every customer (if they've already been checked and given a digital identity), and fewer operational staff needed for handling false positives
- Increased security through near real-time distribution of updated KYC documentation, verified digital identities, and the opportunity to share, in near real-time, fraudulent transaction details
- Increased transparency for regulators as both the immutability of the blockchain, and the opportunity for regulators to have nodes on blockchain networks, support the ability to get a full, transparent audit trail of all transactions

While there is great potential for blockchain to improve efficiency in the KYC/AML space, there are still a number of challenges that need to be overcome to make this a reality (over and above some of the generic challenges with blockchain):

- Privacy – corporates will not want all banks (or indeed other customers) to see their KYC documentation or digital identity if they don't have a relationship with them. Similarly, when corporates exit a relationship with a bank they will want the right to be 'forgotten' – given the immutable nature of blockchain technology, how will this be managed?
- Standardisation – all banks within one jurisdiction are required to confirm to the same KYC rules and regulations, so standardisation in this domain is relatively simple. However, there are two challenges where increased standardisation would further enhance the benefits of using blockchain for KYC. Firstly, cross-jurisdictional standardisation of KYC requirements across different regional and national regulators. Secondly, the standardisation of the banks' own onboarding checks relating to their own risk appetite and customer profiling

- Liability – if one bank verifies a customer (through KYC checks) and that digital identity is then used by a different bank, who is liable in the event of a fraudulent transaction by that customer? How frequently should customers be re-verified, and who is responsible for that re-verification?
- Single Point of Failure – does the creation of a single global KYC / identity blockchain create a target for hackers and cyber-terrorists?

Whilst there is immense potential in the application of blockchain technology for KYC, digital identities and AML, there are challenges that need to be addressed to make this a viable proposition that customers, banks and regulators are all willing to adopt. As with all blockchain use-cases, the power of the technology is driven by the network effect so this can only be successful with collaboration amongst market participants to work toward a mutually beneficial solution which enables them all to focus on the customer.

Appendix Item 10

Blockchain faces maze of regulatory complexities, questions and challenges

Published on 23 Feb 2016 by Henry Engler

Blockchain technology could drive enormous efficiencies in global financial transactions but regulatory acceptance will be a huge challenge.

While the U.S. financial sector is working feverishly on finding common solutions and standards for blockchain, the technical backbone for bitcoin that has shown promise in transforming transactions systems, regulatory acceptance will be an uphill battle. The complex regulatory environment, with multiple agencies likely to voice their own unique concerns and questions, runs the risk of slowing down progress and ultimate adoption unless there is greater coordination among various interests.

That view was widespread at a conference on blockchain sponsored by the Brookings Institution last week. The meeting brought together industry professionals, financial technology firms, venture capitalists and federal and state regulators. While there is no doubt U.S. regulators are keenly interested in the emergent technology and see the potential it holds for streamlining financial services, those working to harness blockchain's firepower said there needed to be a one stop shop for coordinating multiple regulatory concerns.

"I don't know who to even call," said Charlie Cooper, managing director at R3 CEV, a consortium of more than 40 banks working on blockchain applications, when asked how he would engage U.S. regulators to gain their approval.

"Unless I've got a lobbying firm to have a specialist in all these organizations . . . it's

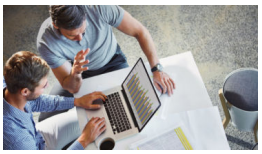
Related posts

Automatic Exchange of Information (AEOI) in an age of rising protectionism

25 Oct 2016 · 5 minute read

From an informal to formal economy: How technology and information offer a pull-through mechanism

25 Oct 2016 · 5 minute read



Higher Standards: Building and keeping customer relationships the right way

25 Oct 2016 · 5 minute

almost like the universe is so big that we don't know where to start," he added. "To the extent we can unify as companies . . . we need a unified front to talk to at the federal and state level."

To illustrate the challenges, Cooper pointed to the question of "settlement finality" in financial transactions, and how agencies differ in terms of how they define the concept. For example, both the Securities Exchange Commission and

Commodity Futures Trading Commission have different rules on what constitutes final settlement of transactions.

"If we are out talking to those two organizations, if they have two different rules on settlement finality, what do we do," asked Cooper.

Blockchain technology is like a digital central ledger that acts as a custodian of information. The information is transparent, and held in a shared database, without any middlemen or central authority. For regulators, the potential for an enhanced and more timely understanding of global transactions is seen as invaluable in their efforts to contain systemic risk.

Clearing and settlement is one of the major processes in financial markets where blockchain technology could drive enormous efficiencies, say experts. In the securities world, current settlement of transactions between buyer and seller takes place three days (T+3) after the trade is executed. Under a blockchain governed market, the settlement would be virtually instantaneous.

"The regulatory community should ask itself the question: how do we approach this," he added.

Coordinating role for FSOC and Federal Reserve

In order to filter the numerous nuances of multiple agency regulations and concerns, some suggested that the Financial Stability Oversight Council (FSOC) might be well positioned to take a lead role in coordinating federal and state regulatory agencies.

"There is some potential for the FSOC to take more of a leadership role in this area in bringing agencies together," said Michael Barr, professor of law at Michigan Law School, and previously a

read

U.S. Treasury official who helped to develop and pass the DoddFrank Act.

Barr also suggested that FSOC might give the Federal Reserve greater sway among U.S. regulators in addressing regulatory issues on blockchain.

For their part, Federal Reserve officials at the conference offered a laundry list of issues that concern them in evaluating blockchain's introduction into financial services.

David Mills, assistant director for operations and payment systems at the Fed, said in addition to basic issues such as AML and KYC, and privacy and security, there were questions regarding operational and legal risk, as well as dispute resolution when "things go wrong." In addition, the Fed was interested in the role of information under a blockchain governed universe and how that might change.

Echoing the view of blockchain advocates , who argue that regulators would have a better view into potential systemic risks under the new technology, Mills pointed to possible tradeoffs or risks of having an unfettered oversight of financial transactions.

"You may have better information from a regulatory point of view, and better ability to improve AML concerns or systemic events," said Mills. "But how do we understand the limits of rich information and the tradeoff over the privacy of individuals. We need to strike a balance between the two."

"It will be helpful to try to understand the nuances and complexities of what goes on in these types of transactions," he added. "The more we understand the easier it will be to have a discussion."

In response to the complaint over the lack of harmonization among various U.S. regulators, Mills appeared sympathetic.

"We definitely hear those kinds of complaints," he said. "But I think the suggestion of really educating all parties is part of the challenge."

"We are all trying to figure things out," Mills added. "We are very open and we want to learn . . . Learning isn't just in one place."