XII. A Helping Hand: How Artificial Intelligence Can Help Financial Institutions Comply with AML/BSA Requirements

A. Introduction

On December 3, 2018, major American institutions, including the Board of Governors of the American Federal Reserve System, the Federal Deposit Insurance Corporation (FDIC), the Financial Crimes Enforcement Network (FinCEN), the National Credit Union Administration, and the Office of the Comptroller of the Currency (OCC; collectively, the Agencies) issued a joint statement (Joint Statement), encouraging banks to innovate and use contemporary approaches to strengthen their Anti-Money Laundering (AML) enforcement.[1] The Joint Statement was issued to encourage banks and lenders to try new technology in order to gather information on and combat financial threats, such as money laundering.[2] The agencies acknowledged that the implementation of new technology can unearth vulnerabilities in the current enforcement mechanisms, but the statement assured lenders that discovered vulnerabilities will not be penalized unless those vulnerabilities were present under their conventional detection

[1] Jesse-Ross Cohen, Chris Payne, & Peter Ruby, *Artificial Intelligence and Anti-Money Laundering: Risks and Rewards*, GOODMANS LLP (July 2, 2019), http://www.goodmans.ca/Doc/Artificial_Intelligence_and_Anti_Money_Laundering__Risks_and_Rewards?utm_source=Mondaq&amp;utm_medium=syndication&amp;utm_campaign=View-Original [https://perma.cc/C3AN-MRKU] (discussing the benefits of AI for AML purposes, specifically cutting expense and enforcement costs); BD. OF GOVERNORS OF THE FED. RESERVE SYS. ET AL., JOINT STATEMENT ON INNOVATIVE EFFORTS TO COMBAT MONEY LAUNDERING AND TERRORIST FINANCING 1 (2018) [hereinafter *Joint Statement*].

[2] Samuel Rubenfeld, *U.S. Encourages Banks to Innovate in Anti-Money Laundering Compliance*, WALL ST. J. (Dec. 3, 2018, 6:16 PM), https://www.wsj.com/articles/u-s-encourages-banks-to-innovate-in-anti-money-laundering-compliance-1543878973 (discussing the implications of the Joint Statement).

regimes.[3] The leniency in withholding penalties encourages banks and lenders to apply the technology.[4]

One particular recommendation was the use of Artificial Intelligence (AI).[5] Presently, the use of AI has grown exponentially. For example, in the healthcare industry, AI has been developed to recommend different treatments for patients, and even provide proper medicinal dosages.[6] Additionally, in the automotive industry AI has been prevalent in self-driving cars.[7] In the financial services sector, AI has grown in areas of lending, risk management, and trading.[8] Although the prospect of using AI is a new phenomenon, there has been some data that the use of AI can lead to more effective and efficient enforcement.[9] Following a brief overview of AML regulations and AI technology, discussing the benefits, drawbacks, current uses of AI in financial services, and forecasting the potential uses of AI in AML enforcement, the expanded use of AI may be warranted.

B. Definitions and Brief History

"Anti-money laundering refers to a set of laws, regulations, and procedures intended to prevent criminals from disguising illegally

[3] *Id*. ("The agencies also acknowledged testing new technology could identify vulnerabilities the banks may not have previously understood. They assured financial institutions that such an incident wouldn't always lead to a penalty, but would depend on the adequacy of the bank's existing compliance program.").

[4] *Id*. (asserting that the lack of a penalty will incentivize financial institutions to try using contemporary technology).

[5] *Id*. ("Administration nudges banks toward adopting new forms of technology, such as artificial intelligence . . .").

[6] Jake Frankenfield, *Artificial Intelligence (AI)*, INVESTOPEDIA, https://www.investopedia.com/terms/a/artificial-intelligence-ai.asp [https://perma.cc/D2JB-7E6B] (last updated June 13, 2019) (defining and describing AI, as well as listing examples of some contemporary use).

[7] *Id.*

[8] Arthur Bachinskiy, *The Growing Impact of AI in Financial Services: Six Examples*, TOWARDS DATA SCIENCE (Feb. 21, 2019), https://towardsdatascience.com/the-growing-impact-of-ai-in-financial-services-six-examples-da386c0301b2 [https://perma.cc/5TXV-C9SL] (stating several instances in which AI is used in the financial services).

[9] Cohen, Payne, & Ruby, *supra* note 1 (acknowledging that the use of AI in AML/BSA enforcement has reduced false positives and allowed for better allocation of human capital).

accumulated funds as legitimate income."[10] AML laws are used to target activities like market manipulation, trade of illegal goods, terrorist financing, and corruption of public funds.[11] In response to these illicit activities, AML laws rose to prominence in 1989 when a group of countries and organizations formed the Financial Action Task Force (FATF), with the goal of setting international standards in order to prevent money laundering in its various forms.[12]

Traditionally, AML monitoring systems segment customers by industry, business type, and size.[13] Although these rules have worked historically, there have been lingering issues with finding consistent transaction behavior that would signal actual illicit behavior.[14] The annual cost of AML compliance is estimated to be $23.5 billion in the United States and $20 billion in Europe.[15] Although these enforcement costs are steep, the results have been questionable, and many banks have been fined for their offenses.[16]

"Artificial Intelligence refers to the simulation of human intelligence in machines that are programmed to think like humans and mimic their actions."[17] Ideally, AI would be configured in such a way that it can rationalize and solve problems consistent with the regula-

[10] Will Kenton, *Anti Money Laundering (AML)*, INVESTOPEDIA, https://www.investopedia.com/terms/a/aml.asp [https://perma.cc/RW5L-DL5L] (last updated Sept. 10, 2019) (describing the history and purpose of AML).

[11] One of the most common techniques of laundering money is through a legitimate cash-based business owned by the laundering agent or organization. *Id*.

[12] *Id*. (chronicling the history of the inception for AML enforcement).

[13] Tim Mueller & Ellen Zimiles, *How AI Is Transforming the Fight Against Money Laundering*, WORLD ECONOMIC FORUM (Jan. 17, 2019), https://www.weforum.org/agenda/2019/01/how-ai-can-knock-the-starch-out-of-money-laundering/ [https://perma.cc/3EKS-SQTQ] ("With traditional monitoring systems, banks typically segment their customers by their industry, the type of business, size, as well as other factors.").

[14] *Id*. (implying that although data segmentation for these specific data sets has worked historically, it also leads to false positives that may drown out actual alerts of wrongdoing).

[15] *Id*. ("In the US alone, the cost of anti-money laundering ('AML') compliance is estimated at $23.5 billion per year. European banks come close with $20 billion spent annually.").

[16] *Id*. ("Over the last decade, 90% of European banks have been fined for AML-related offences; globally, banks have been fined approximately $26 billion over the last 10 years.").

[17] Frankenfield, *supra* note 6.

tor's enforcement goals.[18] AI has two types: supervised and unsupervised.[19] Supervised AI is trained using already categorized data to identity potentially suspicious action.[20] When a supervised AI program encounters potentially suspicious activity, it will alert a human counterpart and prompt them to ignore or elevate the notification to their superiors.[21] Through trial and error, humans can tweak the machines and set up new alerts that lead to more accurate detections and prevent false positives.[22] Unsupervised AI exposes the system to raw and uncategorized data, allowing the machine to identify patterns that may signal suspicious activity and categorize the data itself.[23] In both cases, AI relies on human intervention and requires human oversight and testing to ensure proper functionality.[24]

C. Current Regulations

The AML regime in the United States is primarily supported by the Bank Secrecy Act of 1970 (BSA).[25] The BSA was established for recordkeeping and reporting for private individuals, banks, and other financial institutions to help identify the source, volume, and

[18] *Id.* ("The ideal characteristic of artificial intelligence is its ability to rationalize and take actions that have the best chance of achieving a specific goal.").

[19] Mueller & Zimiles, *supra* note 13 (distinguishing the two types of AI).

[20] *Id.* ("With supervised learning, a model is trained using already categorized data to identify potentially suspicious transactions.").

[21] *Id.* (indicating the process of alerting for suspicious activity, and noting that a human counterpart is a secondary screener of these alerts).

[22] *Id.* (implying that although AI can alert enforcers of suspicious activity, it is not precluded from including some false positives and such false alerts require further configuration to provide for more accurate notifications).

[23] *Id.* ("With unsupervised learning, computer scientists expose the system to raw uncategorized data. Through interactions with the data, the computer system identifies patterns that might signal money laundering – and also suggest new ways to organize and analyse data.").

[24] Mueller & Zimiles, *supra* note 13 ("Even the best screening systems produce a high-rate of false positives that must be dispositioned by a human reviewer, by either clearing the alert, or escalating it for further review.").

[25] *History of Anti-Money Laundering Laws*, FINCEN, https://www.fincen.gov/history-anti-money-laundering-laws [https://perma.cc/S6EY-68EY] (last visited Sept. 8, 2019) ("The BSA was established in 1970 and has become one of the most important tools in the fight against money laundering."); Bank Secrecy Act of 1970, 31 U.S.C. §§ 5311–5316 (2001) (citing the statutory authority for the BSA).

movement of currency and other monetary instruments inside and outside of the United States.[26] In general, under the BSA, banks must: establish effective BSA compliance programs; establish effective customer due diligence and monitoring systems; screen against Office of Foreign Asset Control and other government lists; establish an effective suspicious activity monitoring and reporting process; and develop risk-based AML programs.[27] Specifically, the BSA requires financial institutions to: "(1) report cash transactions over $10,000 using the Currency Transaction Report (CTR); (2) properly identify persons conducting transactions; and (3) maintain a paper trail by keeping appropriate records of financial transactions."[28]

Wrongdoers who are familiar with the CTR requirement for transactions over $10,000 may attempt to "structure" their transactions.[29] "A structured transaction is a series of transactions, which individuals or entities may break up from a larger sum, in order to avoid regulatory oversight."[30] Theoretically, if an individual can break up a large sum into multiple smaller sums, that would not trigger the CTR because each transaction would presumably be under $10,000.[31] In order to combat structuring, the BSA allows financial institutions to file a Suspicious Activity Report (SAR).[32] The SAR allows financial institutions to file a report on a transaction that would not ordinarily be flagged under other reports (such as the CTR), if the activity gives rise to a suspicion that an account holder is attempting to hide something or make an illegal transaction.[33] Financial institutions report SARs to

[26] *Id*. (describing the purpose of the BSA and its overarching goals).

[27] *Bank Secrecy Act*, OCC, https://www.occ.treas.gov/topics/supervision-and-examination/bsa/index-bsa.html [https://perma.cc/QM8H-8GMQ] (last visited Nov. 10, 2019).

[28] *History of Anti-Money Laundering Laws*, *supra* note 25.

[29] *See* Julia Kagan, *Structured Transaction*, INVESTOPEDIA, https://www.investopedia.com/terms/s/structured-transaction.asp [https://perma.cc/S35Q-D2AH] (last updated Feb. 28, 2018) (defining a structured transaction and the motivations for individuals who try it).

[30] *Id*. (defining a structured transaction and how one could "structure" to avoid notifying enforcers).

[31] *See id*.

[32] Will Kenton, *Suspicious Activity Report (SAR)*, INVESTOPEDIA, https://www.investopedia.com/terms/s/suspicious-activity-report.asp [https://perma.cc/PPH3-VNJK] (last updated Sep. 24, 2019) (defining a SAR and explaining how and when it should be used).

[33] *Id*. (describing the purpose of the SAR, specifically to alert suspicious activity that doesn't reach the CTR report threshold).

FINCEN within thirty days of the purported activity, and clients are not notified that a SAR has been filed on their account.[34]

The BSA was also amended to incorporate provisions of the USA Patriot Act, requiring banks to adopt a customer identification program (CIP).[35] The CIP requires financial institutions to obtain, verify, and record information that identifies each person who opens an account.[36] Such information includes: name, date of birth, address, identification number, and other identifying documents such as a driver's license.[37] Corporations, partnerships, and other legal entities are also required to provide other information, such as: "its principal place of business, local office, employer identification number, certified articles of incorporation, government-issued business license, a partnership agreement, or a trust agreement."[38]

D. Implications of the Joint Statement

The Joint Statement attempts to encourage the use of contemporary technology to aid financial institutions in their AML/ BSA enforcement responsibilities. Within the Joint Statement, the Agencies granted financial institutions the ability to experiment with new pilot programs, with the hope of making AML enforcement more efficient.[39] The implementation of innovative approaches in the AML compliance programs will not result in additional regulatory expectations and financial institutions will not be subject to supervisory

[34] *Id*. (indicating that the SAR is sent to a secondary authority for review without the customer's knowledge; whereas a CTR would alert the customer that a report was filed on behalf of their transaction).

[35] *Bank Secrecy Act*, *supra* note 27 ("The BSA was amended to incorporate the provisions of the USA PARTRIOT ACT which requires every bank to adopt a customer identification program as part of its BSA compliance program.").

[36] *Customer Identification Program*, FINRA, https://www.finra.org/investors/customer-identification-program-notice [https://perma.cc/T4KD-KTUH] (last visited Nov. 10, 2019); 31 C.F.R. § 1020.220 (2018) ("Customer identification programs for banks, savings associations, credit unions, and certain non-Federally regulated banks.").

[37] *Id.*

[38] *Id*.

[39] *Joint Statement*, *supra* note 1, at 2 ("Pilot programs undertaken by banks, in conjunction with existing BSA/AML processes, are an important means of testing and validating the effectiveness of innovative approaches.").

criticism if their new programs prove unsuccessful.[40] For example, if AI identifies suspicious activity not otherwise identifiable under the current procedure, then the Agencies will not automatically assume that the traditional enforcement program is ineffective.[41] In addition, "to the extent necessary and appropriate, FinCEN will consider requests for exceptive relief under 31 CFR § 1010.970 to facilitate the testing and potential use of new technologies and other innovations, provided that banks maintain the overall effectiveness of their AML/BSA compliance programs."[42]

The language of the Joint Statement alludes to something akin to a "regulatory sandbox." A regulatory sandbox is a testing ground for a new innovation that is not protected by current regulations or supervised by a regulatory institution.[43] The sandbox can be used to determine whether such innovation can comply with strict financial regulations.[44]

Following the Joint Statement, the Agencies have made a commitment to partner with the private sector to modernize and innovate the AML/BSA compliance program.[45] "As part of this initiative, FinCEN will engage in outreach efforts that include dedicated times for financial institutions, technology providers, and other firms involved in financial services innovations to discuss the implication of their products and services, and their future applications

[40] *Id.* ("While the Agencies may provide feedback, pilot programs in and of themselves should not subject banks to supervisory criticism even if the pilot programs ultimately prove unsuccessful.").

[41] *Id.* ("For example, when banks test or implement artificial intelligence-based transaction monitoring systems and identify suspicious activity that would not otherwise have been identified under existing processes, the Agencies will not automatically assume the banks' existing processes are deficient.").

[42] *Id.* at 2–3; 31 C.F.R. § 1010.970 (2018) ("The Secretary, in his sole discretion, may by written order or authorization make exceptions to or grant exemptions from the requirements of this chapter.").

[43] *What Is a Regulatory Sandbox*, BBVA (Nov. 17, 2017), https://www.bbva.com/en/everything-need-know-psd2/ [https://perma.cc/PFY2-HQFE] (describing a regulatory sandbox).

[44] *Id.* (discussing the practical goal of using a regulatory sandbox).

[45] *Joint Statement*, *supra* note 1, at 3 ("FinCEN is launching an innovation initiative to foster a better understanding of the opportunities and challenges of BSA/AML-related innovation in the financial services sector.").

or next steps."[46] There is a strong possibility that other agencies may soon follow.[47]

E. Contemporary Uses of Artificial Intelligence

U.S. and international financial institutions have benefitted from the implementation of AI. The general benefits of using AI include: behavioral modeling, pattern mining algorithms, risk scoring, and anomaly detection.[48] The objective nature of AI has helped credit lending by allowing lenders to distinguish between riskier candidates.[49] For example, a leading automobile lending company has shown a 23% cut in losses due to its implementation of AI.[50] For risk management, AI can analyze risky consumers' histories and identify signs of potential issues in the future.[51] For example, Crest Financial has witnessed a significant improvement in risk analysis, without the delay of traditional data science, by using AI.[52] Banks and credit card companies have also utilized AI to detect credit card fraud by analyzing spending patterns.[53] Companies, such as Plaid, have created widgets that banks can use to help with detection and to secure financial transactions.[54] Finally, AI has been used in high-frequency trading to analyze structured and unstructured data and process the

[46] *Id*.

[47] *Id*. ("Similarly, each of the other Agencies has, or will establish, projects or offices that will work to support the implementation of responsible innovation and new technology in the financial system.").

[48] Cohen, Payne, & Ruby, *supra* note 1 ("Through machine learning algorithms and other techniques such as frequent patterning mining algorithms, behavioural modelling, risk scoring and anomaly detection, AI provides the opportunity for institutions and regulators to exponentially increase the scale and efficiency of AML detection and compliance programs.").

[49] Bachinskiy, *supra* note 8 (acknowledging an instance where AI has helped credit lenders).

[50] *Id*. (citing a report from tzestfinance.com that shows that "a top U.S. auto lender cut its losses by 23% annually").

[51] *Id*. (acknowledging an instance where AI has helped in risk management).

[52] *Id*. (citing a specific example of a company using AI to improve risk analysis).

[53] *Id*. (acknowledging that AI can also help with detecting credit card fraud through spending patterns).

[54] Bachinskiy, *supra* note 8 (citing a company that has created an application to aid banks in detecting credit card fraud detection and prevention).

data to trade in a fraction of the time.[55] As an example, Bloomberg launched the Alpaca Forecast AI Prediction Matrix that combines real-time market data provided by Bloomberg with advanced learning engines that can identify price movement patterns, which lead to more accurate market predictions.[56]

Several international financial institutions have also begun to implement AI in some capacity.

> [T]he Monetary Authority of Singapore is developing a tool for analysis of reports on suspicious activities while the central bank of Austria has developed a prototype for data validation. The central bank of Italy is using artificial intelligence techniques to predict price moves on the real estate market and the central bank of the Netherlands [uses AI] to anticipate potential liquidity problems at financial institutions.[57]

F. "The Black Box:" Issues, Compliance, and Bias

Although AI is seen as a contemporary solution to traditional problems, AI is not without its faults. The complex nature of AI has led to its being labeled a "Black Box."[58] "Generally, the Black Box Problem can be defined as an inability to fully understand an AI's decision-making process or predict the AI's decisions or outputs."[59] There are two types: "strong" (inability to predict AI operations at all) and "weak" (some predictability and variable ranking) black boxes.[60] The stronger the AI programs become, the more they could conceive

[55] *Id*. (acknowledging that the use of AI can even be implemented in high speed activities such as equity trading).

[56] *Id*. (indicating that a company has utilized AI to assist high frequency traders to assessing market action).

[57] Ana Fernandez, *Artificial Intelligence in Financial Services*, BANCO DE ESPANA, 4 (Mar. 29, 2019), https://ssrn.com/abstract=3366846, at 4 (discussing the issue of bias with AI and acknowledging some current uses of AI by central banks).

[58] Yavar Bathaee, *The Artificial Intelligence Black Box and the Failure of Intent and Causation*, 31 HARV. J.L. & TECH. 889, 905 (2018) (discussing the "black box" issue of AI and the spectrum of predictability of its operations).

[59] *Id*.

[60] *Id*. at 905–06 (Indicating that there are two forms of black box issues).

solutions to problems that humans may not have thought about, and thus, outperform their intended design.[61]

One particular issue that arises from this unpredictability involves tort litigation. For example, in order to establish a prima facie case for negligence, one must show that the plaintiff's injury was proximately caused by the defendant's breach of care.[62] Specifically, proximate cause is conditioned on whether the defendant's actions increases the rational probability of the injurious event occurring.[63] Unfortunately, if there is a lingering Black Box problem with AI, it would be extremely difficult to argue that the machine's actions were foreseeable. The unpredictability of strong Black Box AI can therefore hinder the victim's ability to collect compensation and shield potentially discriminative actions by the designers.[64] To combat this issue, some have presented the idea of vicarious liability between the machine and its operators.[65] In addition to litigation, explaining compliance with regulatory schemes presents another issue. For the purposes of AML, a problem may arise where, because of its unpredictable nature, banks are unable to show regulators whether the AI is complying with the detection requirements.[66]

The final issue that may arise from the implementation of AI is bias. When AI is computing data, it is seeking correlations that would maximize its predicative powers.[67] Ideally, the data that is

[61] Matthew U. Scherer, *Regulating Artificial Intelligence Systems: Risks, Challenges, Competencies, and Strategies*, 29 HARV. J.L. & TECH. 353, 363, 366 (2016) (discussing the legal implications, particularly in victim compensation, related to the unforeseeable nature of AI).

[62] KEITH HYLTON, TORT LAW: A MODERN PERSPECTIVE 100 (2016) (describing the prima facie elements for a negligence case).

[63] *Id.* at 229 (specifying the requirement of proximate causation in negligence cases).

[64] Scherer, *supra* note 61, at 366 ("Issues pertaining to foreseeability and causation thus present a vexing challenge that the legal system will have to resolve in order to ensure that means of redress exist for victims of AI-caused harm.").

[65] Bathaee, *supra* note 58, at 934–35 ("Notwithstanding the similarities between an AI and a human agent, a vicarious liability rule, such as *respondeat superior*, would make sense only in certain circumstances.").

[66] *See* Mueller & Zimiles, *supra* note 13 ("If the bank does not understand how its technology is monitoring for financial crime, it cannot explain how it is complying with regulations to its regulators.").

[67] Fernandez, *supra* note 57, at 5 ("Essentially, algorithms operate by seeking correlations that will maximize predictive power.").

inputted into the AI algorithms should be representative of the total population.[68] Without a data set that is representative, the AI would only register the baseline data that was originally inputted into the system, potentially leaving non-registered data out.[69] Therefore, the AI may be skewed to detect only a certain set of data, thereby creating a "bias" toward foreign data.[70] For example, because of potential bias, there may be lapses in alerts pertaining to certain job applicants or loan candidates because of an unfavorable data set in the AI.[71]

G. Artificial Intelligence and AML

Although AI technology is mature enough to be implemented by a financial institution's AML enforcement regime, continual development of the technology is necessary to prevent its misuse in the future. AI has two primary benefits for banks engaged in AML enforcement, it can: (1) increase the effectiveness and efficiency of crime investigation; and (2) increase the institution's risk management.[72] AI can also potentially help institutions slash expenses that arise from false positives and direct human exports to more productive areas.[73] IBM Watson Financial Services, for example, has suggested that using AI for AML enforcement can potentially decrease false positives by 30–50%, and allow decisions to be made 30–50% faster. Further, QuantaVerse was able to automate about 70% of time-consuming human work through AI.[74]

[68] *Id.* ("Algorithms must be trained with a huge volume of quality data, i.e. data that are representative of the total population.").

[69] *Id.* ("Otherwise any bias in the training sample may become a criterion to be met and thus an obstacle to equal opportunity.").

[70] *See id.*

[71] *Id.* ("[F]or example, in the case of job selection processes or loan origination)").

[72] Mueller & Zimiles, *supra* note 13 (highlighting the two primary benefits of using AI in AML/BSA enforcement).

[73] *Id.* (mentioning the economic and productivity benefits that can potentially arise from the use of AI).

[74] *Id.*; Sam Kalyanam, *Ending Vicious AML cycles: Why Repeating the Same Approach Is No Longer Sustainable*, IBM REGTECH INNOVATIONS BLOG (Sept. 19, 2018), https://www.ibm.com/blogs/insights-on-business/banking/ending-vicious-aml-cycles-why-repeating-the-same-approach-is-no-longer-sustainable/ [https://perma.cc/Z2W2-EKBS] (citing favorable statistics arising from AI's involvement in AML enforcement); Alaina Webster, *Thinking Outside the Black Box: Why AI in AML Makes Sense*, BANK NEWS (Jan. 2019),

Following the Joint Statement, regulators have given banks the option of using AI to review large transactions.[75] Instead of using the traditional enforcement approach, the use of AI to observe different patterns and create new and more relevant segments, i.e., by segmenting customers' transaction behaviors, has been encouraged.[76] Having the ability to segment customers by transaction behavior may help financial institutions identify structuring more effectively, and in turn file SARs more efficiently, by spotting instances where individuals constantly deposit amounts less than $10,000 in a short span of time.[77] Ayasdi AML, for example, uses advanced segmentation in order to create segments based on customer behavior and transactions.[78] By inputting customer data and using unsupervised AI, Ayasdi AML is able to monitor customer transactions to spot potential suspicious activity. HSBC has used Ayasdi AML to reduce its false positives and investigation volume by more than 20%.[79]

AI technology is mature enough to be applied today in more pressing matters.[80] Banks do not need to refashion their technology because the newer technology can complement and enhance their current systems.[81] Similarly, banks do not need to recruit computer

https://www.banknews.com/blog/thinking-outside-the-black-box/ [https://perma.cc/8Q55-UEB4] (citing a statistic that shows how AI is having a positive impact on allocation of human work).

[75] Mueller & Zimiles, *supra* note 13 (mentioning that AI may aid AML/BSA enforcement by being able to review a large set of transactions, and this approach is favored by the regulatory agencies if successful).

[76] *Id*. (clarifying how the use of AI, through a novel segmentation approach, can have beneficial effects).

[77] *See* Kagan, *supra* note 29; *see also* Kenton, *supra* note 32.

[78] Danielle Ghiglieri, *Symphony AyasdiAI Launches Next-Generation AI Solution for Anti-Money Laundering*, BUSINESS WIRE (Sept. 24, 2019), https://www.businesswire.com/news/home/20190924005402/en/ [https://perma.cc/74UN-JY6L] (discussing a particular AI product introduced and used for AML enforcement at a financial institution).

[79] *Id*. (citing an example of a bank receiving favorable results through the use of an AI platform).

[80] Mueller & Zimiles, *supra* note 13 (acknowledging that AI technology has grown enough to be of practical use).

[81] *Id*. ("Banks do not have to rip out and replace existing computer monitoring systems because the new technologies complement and enhance their legacy systems.").

scientists specializing in AI.[82] This convenience is also supplemented by the advent of open source coding and sharing, which allows developers of AI to outsource the coding scheme and cooperate with others in improving the functionality of the technology.[83]

Although AI can meet the pressing demands of AML compliance for financial institutions, the proper implementation and continual engagement in modifying AI for practical use is vital. Patrick Craig, the Financial Crime Technology Lead at Ernst and Young, recommends some approaches to proper AI adoption.[84] Craig believes that to produce an effective AML enforcement regime through AI, adopters need to: institute strong governance around the development and employment of AI; establish clear performance objectives; collaborate with other financial institutions, regulators, and vendors to make the AI mechanism transparent; test the AI continually; consider data and ethical implications (i.e., bias); and regularly review the AI for manipulative use.[85] Although AI can complement human enforcement, it cannot replace the human aspect of AML enforcement wholesale.[86] AI works optimally when it is paired with skilled investigators who can interpret the AI's alerts and take appropriate action.[87]

H. Conclusion

With the advent of improved technology, banks and regulators are encouraged to incorporate these innovations into their traditional enforcement regimes. The benefits of AI are apparent: they slash

[82] *Id.* ("At the same time, banks do not have to go to the trouble and expense of building massive teams of computer scientists specializing in AI.").

[83] Scherer, *supra* note 61, at 369–70 (discussing how the advent of open source technology has opened the door for AI technicians to receive aid from others who are similarly working to improve their own AI).

[84] Patrick Craig, *How to Trust the Machine: Using AI to Combat Money Laundering*, ERNST & YOUNG (Sept. 3, 2019) https://www.ey.com/en_us/trust/how-to-trust-the-machine--using-ai-to-combat-money-laundering [https://perma.cc/CVJ7-MVDD] (recommending various forms of due diligence for AI adopters involved in AML enforcement).

[85] *Id.* (recommending some specific steps to further improve AI for future use in AML enforcement).

[86] *Id.* (clarifying that the use of AI cannot completely eliminate the human aspect from the process because there needs to be a second decisionmaker to determine whether to elevate the alert to a superior).

[87] *Id.* (stressing the importance of having a knowledgeable human counterpart alongside the technology in order to improve the enforcement standards).

expense costs of traditional regulation, they aid risk management, they decrease false positives, and they help better allocate human capital on other areas of enforcement. The drawbacks are equally apparent: the Black Box issue, bias, and an aura of unpredictability surrounding the machine's decision-making process. Considering both the advantages and disadvantages, banks and regulators should strongly consider implementing AI into their AML enforcement regimes. Although AI can be placed into the current legacy system of most financial institutions, caution may be warranted. To exercise proper caution, institutions should take preventative measures in deploying the AI immediately into their enforcement networks. Testing the AI in an isolated environment with sample data and continually working with engineers to tweak and mold the AI may be the preferable route. By taking a more cautionary approach, institutions can hedge against the risk of bias and begin to understand the thought process of the AI as it begins to compute data. The potential rewards of AI arguably far outweigh the risk, and at a time where money-launderers may have the savvy to elude traditional detection, AI allows these institutions to fight back.

Shant Vosgueritchian[88]

[88] Student, Boston University School of Law (J.D. 2021).