COMPLIANCE COMMITTEE
Subcommittee on Technology,
Cybersecurity and Data Privacy
&
Working Group on Artificial Intelligence
and Machine Learning

ARTIFICIAL INTELLIGENCE AND MACHINE LEARNING IN FINANCIAL SERVICES: OPPORTUNITIES AND CHALLENGES IN ANTI-MONEY LAUNDERING AND COMBATTING THE FINANCING OF TERRORISM

MARCH 2024

THE ASSOCIATION OF THE BAR OF THE CITY OF NEW YORK
42 West 44th Street, New York, NY 10036
212.382.6600 | www.nycbar.org

Table of Contents

I. Introduction

The compliance officers and other independent risk managers[1] of financial services companies and financial institutions[2] serve as essential gatekeepers to prevent, detect, and

[1] In the case of this report, a compliance officer or other independent risk manager is independent of line management, the sales force, and revenue generators and has stature and authority to provide objective and independent assessments.

[2] For purposes of this report, a financial institution is regulated if it meets the definition of financial institution within the meaning of the regulations of the Financial Crimes Enforcement Network (FinCEN). *See* 31 C.F.R. 1010.100(t) (2021), which defines a financial institution as (1) A bank (except bank credit card systems); (2) A broker or dealer in securities; (3) A money services business as defined in 31 C.F.R. 1010.100 (ff); (4) A telegraph company; (5) certain casinos; (6) certain card clubs; (7) A person subject to supervision by any state or federal bank supervisory authority; (8) A futures commission merchant; (9) An introducing broker in commodities; or (10) A mutual fund. Financial services companies are included alongside of financial institutions because even if some are not subject to the requirement to comply with FinCEN's regulations (such as investment advisers; certain insurance companies; and insurance brokers), they are often directly or indirectly required to comply with many of the anti-money laundering (AML) and combatting the financing of terrorism (CFT) laws (AML/CFT laws) by financial institutions, investors, third-party service providers, and other market participants. Frequently used acronyms are listed at Schedule B.

While registered investment advisers are not financial institutions under current law, on February 15, 2024, FinCEN published a Notice of Proposed Rulemaking in the Federal Register on Financial Crimes Enforcement Network: Anti-Money Laundering/ Countering the Financing of Terrorism Program and Suspicious Activity Report Filing Requirements for Registered Investment Advisers and Exempt Reporting Advisers https://www.govinfo.gov/content/pkg/FR-2024-02-15/pdf/2024-02854.pdf. (All websites last accessed on March 1, 2024.) The lack of a regulation covering investment advisers, and other reasons, explain why the Financial Action Task Force (FATF) continues to criticize the U.S. regarding its failure to comply fully with FATF Recommendation 10 (R.10.). "However, a few minor technical gaps remain, including the lack of explicit Beneficial Ownership (BO) requirements, mainly in relation to other trust relevant parties for legal arrangements. Limited measures have been taken to improve the occasional transaction threshold of USD 3,000 for Money Services Businesses (MSBs) and to improve gaps with regard to life insurance companies. In addition, Investment Advisers (IAs) are still not directly covered by the Bank Secrecy Act (BSA) obligations. Overall, the U.S. has addressed a number of the key identified deficiencies, but deficiencies (especially in relation to all types of legal arrangements) still remain. The U.S. is therefore re-rated as Largely Compliant with R.10." *See* FATF, *Anti-Money Laundering and Counter-Terrorist Financing Measures United States 3rd Enhanced Follow-up Report & Technical Compliance Re-Rating*, at p. 3 (Mar. 2020), https://www.fatf-gafi.org/en/publications/Mutualevaluations/Fur-united-states-2020.html.

FATF is the global money laundering and terrorist financing watchdog. It is also an inter-governmental body that sets international standards that aim to prevent illegal activities and the harm they cause to society. As a policy-making body, FATF works to bring about

remediate violations of laws, regulations, and internal policies and rules.[3] This is particularly true with compliance officers and independent risk managers who are responsible for AML and CFT compliance[4] (collectively, AML/CFT Compliance Officers).[5] The U.S. has long determined that the fight against money laundering and terrorist financing is critically important,[6] and under U.S. federal laws and the laws of several U.S. states, money laundering[7] and terrorist financing[8] are criminal offenses punishable by significant fines and imprisonment.

---

national legislative and regulatory reforms in these areas. FATF sets international standards to ensure national authorities can effectively go after illicit funds linked to drugs, trafficking, the illicit arms trade, cyber fraud, and other serious crimes. In total, more than 200 countries and jurisdictions have committed to implement the FATF's Standards as part of a coordinated global response to preventing organized crime, corruption, and terrorism. FATF was established in 1989 and is based in Paris.

[3] *See* N.Y. City Bar Assoc. Compliance Comm., *Chief Compliance Officer Liability in the Financial Sector*, N.Y. City Bar(Feb. 2020), https://s3.amazonaws.com/documents.nycbar.org/files/NYC_Bar_CCO_Framework.pdf.

[4] Many of these requirements are imposed by a combination of federal and state regulatory agencies and law enforcement. *See* Federal Financial Institutions Examination Council (FFIEC), *BSA/AML Examination Manual Appendix A: BSA Laws And Regulations*, https://bsaaml.ffiec.gov/manual/Appendices/02 [hereinafter FFIEC BSA/AML Examination Manual].

[5] For certain financial institutions and other U.S. Persons, the failure to detect and prevent money laundering and terrorist financing could lead to significant criminal and civil fines and penalties, as well as loss of a license granted by a licensing authority or prudential supervisor or revocation of a registration that has been accepted by a government agency. *See* 12 U.S.C. §1818(s); 31 C.F.R. Chapter X. The distinction between certain financial institutions and other U.S. Persons is necessary because certain financial institutions are required to comply with certain sections of 31 C.F.R Title X, but all U.S. Persons are required to comply with the requirements of the Office of Foreign Assets Control (OFAC) in 31 C.F.R. Chapter V. Criminal penalties exist for willful violations of the AML/CFT laws under 31 U.S.C. § 5322 and for structuring transactions to evade AML/CFT reporting under 31 U.S.C. § 5324(d).

[6] On June 30, 2021, FinCEN issued the AML/CFT National Priorities, which included eight categories of priorities: corruption; cybercrime; foreign and domestic terrorist financing; fraud; transnational criminal organization activity; drug trafficking organization activity; human trafficking and human smuggling; and proliferation financing. These priorities must be incorporated into AML/CFT Compliance Programs. *See Anti-Money Laundering and Countering the Financing of Terrorism National Priorities*, FinCEN (June 30, 2021), https://www.fincen.gov/sites/default/files/shared/AML_CFT%20Priorities%20(June%2030%2C%202021).pdf [hereinafter FinCEN AML/CFT Priorities].

[7] *See* 18 U.S.C. § 1956 and 18 U.S.C. § 1957; *See also* N.Y. PENAL LAW Article 470 (LexisNexis 2022).

[8] *See* 18 U.S.C. § 2339A–C and 21 U.S.C. § 960a; *See also* 50 U.S.C. § 1701–05, which criminalizes conduct in violation of executive orders prohibiting transactions with, among other things, nation-states that support international terrorism, designated terrorists, and terrorist groups. OFAC administers many of the CFT laws, and OFAC has issued regulations governing the activities of US Persons when it comes to these laws. 31 C.F.R. Chapter V. OFAC defines a U.S. Person as any U.S. citizen, permanent resident alien, entity organized

Under federal law, prudential supervisors[9] also make certain institution-affiliated parties[10] subject to fines and penalties in certain egregious cases, where they have played a significant role in the financial institution's failure to detect and prevent money laundering or terrorist financing. In fact, the roles and responsibilities of AML/CFT Compliance Officers are so important that they may become the subject of a government agency enforcement action when the government determines that an AML/CFT Compliance Program is flawed, and the flaws are attributable to the AML/CFT Compliance Officer.[11] Affiliated parties may also become

---

under the laws of the U.S. or any jurisdiction within the U.S. (including foreign branches), or any person in the U.S. *See* 31 C.F.R. § 560.314; *see also* N.Y. Penal Law Article 490.

[9] For these purposes, a prudential supervisor at the federal level includes the Board of Governors of the Federal Reserve System (Federal Reserve), the Office of the Comptroller of the Currency (OCC) and the Federal Deposit Insurance Corporation (FDIC). Prudential supervisors at the state level include governmental agencies that supervise banks and MSBs such as the New York State Department of Financial Services (DFS) and the California Department of Financial Protection and Innovation (DFPI). In the U.S., certain MSBs are required to register with FinCEN and obtain licenses from state prudential supervisors such as DFS and DFPI. In the case of financial institutions subject to federal prudential supervision, the federal prudential supervisors are required to impose a cease-and-desist order against the financial institution for certain AML/CFT Compliance failures, typically referred to as "program failures." See 12 U.S.C. § 1818(s)(3).

[10] *See* 12 U.S.C. § 1813(u). An "institution-affiliated party" includes (1) any director, officer, employee, or controlling stockholder (other than a bank holding company or savings and loan holding company) of, or agent for, an insured depository institution; (2) any other person who has filed or is required to file a change-in-control notice with the appropriate federal banking agency under 12 U.S.C. § 1817(j); (3) any shareholder (other than a bank holding company or savings and loan holding company), consultant, joint venture partner, and any other person as determined by the appropriate federal banking agency (by regulation or case-by-case) who participates in the conduct of the affairs of an insured depository institution; and (4) any independent contractor (including any attorney, appraiser, or accountant) who knowingly or recklessly participates in (A) any violation of any law or regulation; (B) any breach of fiduciary duty; or (C) any unsafe or unsound practice, which caused or is likely to cause more than a minimal financial loss to, or a significant adverse effect on, the insured depository institution.

[11] For instance, FinCEN imposed a $450,000 civil money penalty. *See* In the Matter of: Michael LaFontaine, Saint Croix County, WI, Number 2020-01 (Mar. 4, 2020), https://www.fincen.gov/sites/default/files/enforcement_action/2020-05-21/Michael%20LaFontaine-Assessment-02.26.20_508.pdf. FinCEN concluded that LaFontaine participated in the violations of the BSA and its implementing regulations. LaFontaine is a former Chief Operational Risk Officer (and, before that, Deputy Risk Officer, and Chief Compliance Officer) at U.S. Bank National Association. The OCC also imposed a $50,000 civil money penalty against LaFontaine. See In the Matter of: Michael S. LaFontaine, Former Chief Operational Risk Officer, U.S. Bank, N.A., Cincinnati, Ohio, AA-EC-2019-94 (Feb. 26, 2020), https://www.occ.gov/static/enforcement-actions/ea2020-011.pdf *See also*, In the Matter of Lia Yaffar-Pena, Order Instituting Administrative and Cease-and-Desist Proceedings, Pursuant to Sections 15(b) and 21C of the Securities Exchange Act of 1934, Making Findings, and Imposing Remedial Sanctions and a Cease-and-Desist Order, Release No. 79124, Securities and Exchange Commission (SEC) (Oct. 19, 2016),

subject to an enforcement action if they were a part of undermining or creating deficiencies in the AML/CFT Compliance Program.

The U.S. Anti-Money Laundering Act (AMLA) of 2020 has strengthened the AML/CFT laws and directed the appropriate authorities to modernize the AML/CFT laws to address new and emerging threats and encourage technological innovation and the adoption of new technology by financial institutions.[12] In seeking to ensure compliance with AML/CFT laws, and strengthen AML/CFT Compliance Programs, in many cases, AML/CFT Compliance Officers have turned to or are considering the use of advanced technologies (e.g., proprietary software, systems, and third-party support), including, artificial intelligence (AI) and machine learning (ML) (collectively, AI/ML).[13] To date, financial institutions are in different stages regarding AI/ML. Some of the largest have invested heavily in AI/ML or the exploration of AI/ML. Most smaller financial institutions have not invested heavily in either due primarily to the costs involved and the uncertainty regarding how much, if any, credit prudential supervisors and law enforcement would grant.[14] While the use of technology to support AML/CFT Compliance Programs (especially software and systems) is not new, and AML/CFT Compliance Officers have used technology for many decades, current forms of AI/ML and the

---

https://www.sec.gov/litigation/admin/2016/34-79124.pdf; *FINRA Fines Raymond James $17 Million for Systemic Anti-Money Laundering Compliance Failures, Former AML Compliance Officer Fined and Suspended*, Fin. Industry Regul. Auth. (May 18, 2016), http://www.finra.org/newsroom/2016/finra-fines-raymond-james-17-million-systemic-anti-money-laundering-compliance; *In the Matter of Charles Sanders*, Consent Ord., AA-EC-2015-92, OCC (Mar. 15, 2016), https://www.occ.gov/static/enforcement-actions/ea2016-038.pdf. *FinCEN Assesses $1 Million Penalty and Seeks to Bar Former MoneyGram Executive from Financial Industry*, Fin. Crimes Enforcement Network (Dec. 8. 2014), at https://www.fincen.gov/news/news-releases/fincen-assesses-1-million-penalty-and-seeks-bar-former-moneygram-executive; *U.S. Dep't of Treasury v. Haider*, No. 15-1518, 2016 WL 107940, at 3 (D. Minn. Jan. 8, 2016); and *U.S. Dep't of Treasury v. Haider* (S.D. N.Y. Dec. 18, 2014), https://www.fincen.gov/sites/default/files/shared/USAO_SDNY_Complaint.pdf.

[12] *See* The Bank Secrecy Act (BSA) the Anti-Money Laundering Act, 31 U.S.C. § 5311, https://www.fincen.gov/anti-money-laundering-act-2020 [hereinafter AMLA].

[13] There are many questions to be answered when considering whether to use AI/ML to strengthen AML/CFT Compliance. *See Federated Machine Learning in Anti-Financial Crime Processes Frequently Asked Questions*, FinRegLab (Dec. 2020), https://finreglab.org/wp-content/uploads/2020/12/FAQ-Federated-Machine-Learning-in-Anti-Financial-Crime-Processes.pdf.

[14] *See AML and AI: How AI is Changing the AML Landscape*, ComplyAdvatage, *https://complyadvantage.com/insights/aml-ai-how-ai-is-changing-the-aml-landscape/* (last visited Nov. 17, 2022). Some commentators have concluded that the use of AI/ML in AML/CFT Programs is a game changer. *See The Fight Against Money Laundering: Machine Learning is a Game Changer*, Mckinsey & Co., (Oct. 7, 2022), https://www.mckinsey.com/capabilities/risk-and-resilience/our-insights/the-fight-against-money-laundering-machine-learning-is-a-game-changer#/.

promised solutions for important use cases may present more opportunities and challenges than older technologies.[15]

The use of AI/ML is particularly important today to potentially increase efficiencies for historically labor intensive and unevenly effective compliance programs. Labor intensity has derived in part from the vast amounts of both structured and unstructured data that is generated and that must be considered.[16] The overwhelming majority of financial institution transactions are not suspicious or do not require the filing of a suspicious activity report (SAR). Given the volume of transactions, identifying the right suspicious activity is exceedingly difficult. Furthermore, historically available algorithms and other mathematical or statistical models are more basic than present day AI/ML systems.

Today, AI/ML is substantially more complex and therefore requires knowledge and skill sets that many traditional AML/CFT Compliance Officers may not have unless they have kept up to date on the uses of AI/ML in AML/CFT. In addition, it may be a bridge too far to expect such AML/CFT Compliance Officers to tackle complex AI/ML issues directly such as explainability and model bias and ensuring the right use of the AI/ML model's outputs. These AML/CFT Compliance Officers also may not have the experience to explain why they are using specific AI/ML systems and how such specific AI/ML systems help the financial institutions achieve their AML/CFT Compliance goals without causing other issues for the financial institutions and their customers. For some financial institutions, especially the largest

[15] This report aspires to help AML/CFT Compliance Officers understand and appreciate the opportunities and challenges related to AI/ML, especially with respect to AML/CFT Compliance Programs. In doing so, the report highlights some of the existing liabilities to AML/CFT Compliance Officers and their financial institutions under the AML/CFT Laws. The report has not focused on legal liability that might flow from the use of AI/ML because such liability is less clear and uncertain. However, it is worth noting and highlighting that others have focused on that issue. For instance, on February 6, 2023, the House of Delegates of the American Bar Association adopted Resolution 604, https://www.americanbar.org/content/dam/aba/directories/policy/midyear-2023/604-midyear-2023.pdf. Among other things, Resolution 604 provides that: (1) Developers, integrators, suppliers, and operators (Developers) of AI systems and capabilities should ensure that their products, services, systems, and capabilities are subject to human authority, oversight, and control; (2) Responsible individuals and organizations should be accountable for the consequences caused by their use of AI products, services, systems, and capabilities, including any legally cognizable injury or harm caused by their actions or use of AI systems or capabilities, unless they have taken reasonable measures to mitigate against that harm or injury; and (3) Developers should ensure the transparency and traceability of their AI products, services, systems, and capabilities, while protecting associated intellectual property, by documenting key decisions made with regard to the design and risk of the data sets, procedures, and outcomes underlying their AI products, services, systems and capabilities.

[16] *See* IBM, *Structured vs. Unstructured Data: What's the Difference? A Look into Structured and Unstructured Data, Their Key Differences and Which Form Best Meets Your Business Needs*, https://www.ibm.com/blog/structured-vs-unstructured-data/. While it is true that AML/CFT Compliance Officers have historically had to deal with vast amounts of data, today there are more laws and more government agencies and other stakeholders requiring AML/CFT Compliance Officers to create and review data, and government agencies now treat AML/CFT Compliance Officers as gatekeepers with potential liability that AML/CFT Compliance Officers have not been exposed/subject to in the past.

financial institutions that have heavily invested in AI/ML, this may be less an issue because AML/CFT Compliance Officers at those financial institutions might have a long history of working with advanced technologies, including technologies that use mathematical and statistical modelling, especially with respect to determining risk ratings of customers and transactions, investigating and identifying suspicious activity, eliminating false positives or false negatives on OFAC sanctions monitoring; and conducting other forms of due diligence.

Data is foundational to enabling models powered by AI/ML. Further, as stressed by the Bank of England (BoE) and the United Kingdom's Financial Conduct Authority (FCA) "[d]ata is at the core of financial services… [f]rom customer services to consumer credit, AML and anti-fraud analytics to investment management, financial services firms use AI for a range of business services."[17] Notwithstanding the risks and challenges, the transformative nature of AI/ML, and the increasing pace at which these technologies are adopted and improved, will continue to influence how AML/CFT Compliance Officers perform their responsibilities, while continuing to improve their AML/CFT Compliance Programs for financial services companies and financial institutions. The use and effectiveness of AI/ML will also influence the approaches and responses to AI/ML by regulatory agencies, law enforcement, policymakers, industry participants, data specialists, technologists, ethicists, and other stakeholders across the world.

This report[18] may serve as a resource for financial services companies and financial institutions and AML/CFT Compliance Officers who are implementing or considering implementing AI/ML systems into their AML/CFT Compliance Programs. The report (1) summarizes the definitions of AI/ML used by different regulatory agencies; (2) provides examples of how AI/ML may benefit a financial institution's AML/CFT Compliance Program; (3) describes the material risks and challenges with implementing AI/ML in AML/CFT Compliance Programs, and strategies for overcoming some of those risks and challenges; (4) discusses certain trends in AI/ML in AML/CFT Compliance; and (5) ends with a conclusion and some observations.

A. What Are the Definitions of Artificial Intelligence and Machine Learning?

At present, there is no single widely agreed upon definition of AI/ML in AML/CFT Compliance. According to Section VII.D of the FFIEC[19] IT Examination Handbook on

[17] *See* Bank of England & Financial Conduct Authority, *Final Report Artificial Intelligence Public-Private Forum* (Feb. 2022), https://www.bankofengland.co.uk/-/media/boe/files/fintech/ai-public-private-forum-final-report.pdf?la=en&hash=F432B83794DDF3F580AC5A454F7DFF433D091AA5 [hereinafter, the AIPPF Report].

[18] Schedule A identifies the professionals and City Bar committees that drafted or reviewed the report.

[19] The FFIEC was established on March 10, 1979, and is a formal interagency body empowered to prescribe uniform principles, standards, and report forms for the federal examination of financial institutions by the Federal Reserve, the FDIC, the National Credit Union Administration (NCUA), the OCC, and later the Consumer Financial Protection Bureau (CFPB), and to make recommendations to promote uniformity in the supervision of financial institutions. The federal and state prudential supervisors follow both the FFIEC IT

Architecture, Infrastructure, and Operations (FFIEC IT Handbook),[20] AI refers to the theory and development of systems that perform tasks or functions normally associated with human intelligence, such as reasoning, learning, and self-improvement. ML is a subset of AI in which components of AI systems are used to design a sequence of actions, which could improve upon and optimize algorithms automatically through experience, to perform tasks with limited human intervention. AI/ML algorithms can analyze large data sets quickly and identify complex patterns, which may be used to solve problems and generate predictions or categorizations. AI/ML can also allow management to personalize customer products and services and, in certain cases, analyze real-time data to help anticipate future behaviors. AI/ML can also augment decision-making by identifying patterns that a human may miss when analyzing data.

The BoE and the FCA take a more nuanced approach[21] to the definitions of AI/ML, while the draft European Commission (EC) regulation on AI is broad and includes statistical models and techniques that are not always considered to be AI.[22] For instance, the BoE and FCA previously defined AI as the theory and development of computer systems able to perform tasks that previously required human intelligence.[23] The German Bundesbank and BaFin have

---

Handbook (https://ithandbook.ffiec.gov/ https://ithandbook.ffiec.gov/it-booklets), which covers AI/ML, and the FFIEC BSA/AML Examination Manual (https://bsaaml.ffiec.gov/manual https://bsaaml.ffiec.gov/manual), which covers AML/CFT Compliance. As such, FFIEC manuals are critically important authoritative sources for regulated financial institutions and AML/CFT Compliance Officers. The FFIEC BSA/AML Examination Manual provides guidance to examiners for carrying out AML/CFT examinations. It also provides guidance on identifying and controlling risks associated with money laundering and terrorist financing and contains an overview of AML/CFT Compliance Program requirements, AML/CFT risks and risk management expectations, industry sound practices, and examination procedures. The FFIEC BSA/AML Examination Manual was developed collaboratively among federal and state banking agencies, FinCEN, and OFAC to ensure consistency in the application of the AML/CFT Compliance requirements.

[20] *See Architecture, Infrastructure, and Operations*, at 96, Fed. Fin. Inst. Examination Council (Jun. 2021), https://ithandbook.ffiec.gov/media/ywfm2ftz/ffiec_itbooklet_aio.pdf (AIO Booklet of the FFIEC IT Handbook) [hereinafter the FFIEC IT Handbook]..

[21] *See generally*, *AIPPF Report*, *supra* note 17.

[22] *See Proposal for a Regulation of the European Parliament and of the Council Laying Down Harmonized Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts*, COM (2021) 206 Final, European Comm'n (Jan. 26, 2024), https://data.consilium.europa.eu/doc/document/ST-5662-2024-INIT/en/pdf, intended as the final compromise text with a view to agreement which, as drafted, amends and supersedes the initial proposal adopted April 21, 2021 (Proposal for a Regulation laying down harmonized rules on artificial intelligence) [hereinafter the EU AI Act Draft].

[23] *See AIPPF Report*, *supra* note 17 ("As well as defining AI, it is important to consider the characteristics of AI applications and how they differ from non-AI applications that produce the same result. These characteristics may include the complexity of AI, its iterative approach, the use of hyperparameters, and the use of unstructured datasets.").

use a different approach in a recent publication.[24] Rather than use a specific definition of ML, the Bundesbank and BaFin set out various ML characteristics that create a boundary of what could be considered within and out of scope.[25]

B. What Are Some of the Use Cases[26] for AI/ML in the Financial Services Sector?

At the outset, to date, no US prudential supervisor requires regulated financial institutions to use AI/ML in AML/CFT Compliance Programs and it is unknown whether any will, even in the long term. Nonetheless, AI/ML use cases are rapidly increasing in the financial sector with AI/ML being adopted, in some cases, for compliance purposes, risk management purposes, and financial and credit risk purposes.[27] Further, the FFIEC IT Handbook indicates that AI/ML can be used for strengthening security controls (e.g., logical, and physical access anomaly analysis and use of facial recognition for authentication); to enhance compliance with applicable laws and regulations; and for detection and prevention of fraud or misconduct (e.g., AML/CFT, account compromise, and insider fraud).[28]

Specifically for AML/CFT Compliance Programs, AI/ML [29] may add value by analyzing a vast pool of data to flag any suspicious transactions and activity through:

---

[24] *See* Deutsche BundesBank and BaFin, *Machine Learning in Risk Models – Characteristics and Supervisory Priorities* (July 2021), https://www.bafin.de/SharedDocs/Downloads/EN/Aufsichtsrecht/dl_Ergebnisse_machinelles_Lernen_Risikomodelle_en.pdf?__blob=publicationFile&v=2.

[25] *See generally*, *AIPPF Report*, *supra* note 17.

[26] While the phrase "use case" is commonly used to refer to the use of AI/ML to address a specific subject matter such as AML/CFT Compliance Programs, the technical definition of use case is more exacting. See IBM Product Master 12.0 Fix Pack 10 Operating Systems: AIX, Linux, and Windows (Workbench only) (Last Updated: 2024-01-08), which defines a use case" as "built to refine a set of requirements based on a role or task. Instead of the traditional list of requirements that may not directly address the use of the solution, use cases group common requirements based on the type of role or goal. Use cases define what the users or roles are doing in the solution, a business process defines how they perform those functions," https://www.ibm.com/docs/en/product-master/12.0.0?topic=processes-defining-use-cases.

[27] *See $405+ Billion Artificial Intelligence Markets: Hardware, Software, Services, Machine Learning, Natural Language Processing, Big Data - Global Forecast to 2027*, Business Wire, (Nov. 29, 2022), https://www.businesswire.com/news/home/20221129005577/en/405-Billion-Artificial-Intelligence-Markets-Hardware-Software-Services-Machine-Learning-Natural-Language-Processing-Big-Data---Global-forecast-to-2027---ResearchAndMarkets.com.

[28] *See generally*, *FFIEC IT Handbook*, *supra note 19*.

[29] *See* Melissa Koide (FinRegLab CEO), *Testimony before the Senate Committee on Banking, Housing, and Urban Affairs on "Artificial Intelligence in Financial Services"*, at p.3, FinRegLab (Sept. 19, 2023), https://finreglab.org/wp-content/uploads/2023/09/FinRegLab-Senate-Banking-Testimony-9-19-23-.pdf [hereinafter M. Koide, Testimony].

- ***Enhanced Due Diligence and Know-Your-Customer (KYC) Processes:*** AI/ML can automate the customer on-boarding process, including checking customer information against sanctions and Politically Exposed Persons (PEPs)[30] lists, risk scoring for AML/CFT risk, adverse media screening, including with Natural Language Processing (NLP) solutions that are considerably more powerful than the traditional list matching, and client risk rating modeling.
- ***Monitoring of Customers Behavior and Transactions to Detect Suspicious Activity:*** AI/ML can optimize behavioral and transaction monitoring by applying smart segmentation of targeted customer populations, aiming to group customers under similar or homogenous profiles, with identical behavioral patterns, and detect abnormal activity and potential deviations.
- ***Improvement of the Quality of Reporting:*** AI/ML may be used to automate reports, including SARs, by pre-populating information through compilations of existing processed customer and transactions data.
- ***Fraud Detection:*** Machine learning models are often used to monitor bank account, credit card, or other financial transactions data to flag suspicious patterns, and may be combined with more traditional rules-based tools in connection with initial account opening and application processes. ML models also have the potential to dynamically update to reflect analysis of complex and large data sets and identify evolving fraud patterns.[31]

C. What Are Some of the Risks Associated With AI/ML?

Adopting AI/ML to enhance compliance systems can be a double-edged sword. Despite the benefits and added value that AI/ML may bring, financial institutions must be aware of and

[30] FATF and the United Nations Convention Against Corruption define PEP. The FATF is an independent inter-governmental body that develops and promotes policies to protect the global financial system against money laundering, terrorist financing and the financing of proliferation of weapons of mass destruction. The FATF Recommendations are recognized as the global AML and CFT standard. *See FATF Guidance Politically Exposed Persons (Recommendations 12 and 22)* (June 2013), https://www.fatf-gafi.org/content/dam/fatf-gafi/guidance/Guidance-PEP-Rec12-22.pdf.coredownload.pdf [hereinafter Guidance on PEP (2013)].The AML/CFT laws do not define PEP. PEP is commonly used in the financial services industry to refer to foreign individuals who are or have been entrusted with a prominent public function as well as to their immediate family members and close associates. *See generally*, *Guidance on PEP* 2013; *Wolfsberg Guidance on Politically Exposed Persons* (May 1, 2017), https://wolfsberg-group.org/news/28; *see also 31 C.F.R. 1010.605(p)* (Definition of Senior Foreign Political Figure), https://www.ecfr.gov/current/title-31/subtitle-B/chapter-X/part-1010#1010.605; and *Advisory on Human Rights Abuses Enabled by Corrupt Senior Foreign Political Figures and their Financial Facilitators*, FinCEN (June 12, 2018), https://www.fincen.gov/sites/default/files/advisory/2018-07-03/PEP%20Facilitator%20Advisory_FINAL%20508%20updated.pdf.

[31] *See M. Koide, Testimony*, *supra* note 29.

assess related potential risks as the utilization of AI/ML accelerates.[32] Some of the potential risks, which are also listed in the FFIEC IT Handbook,[33] are described below:

1. Underlying Data Used to Train AI/ML Models

One defining feature of AI/ML systems is its ability to process large volumes of both structured and unstructured data. The data may come from numerous sources such as, by way of example, transactional data, KYC profiles, online social media content, audio conversations, behavioral patterns, and satellite images used for sanctions vessel tracking. Although there is a vast variety of data that can be processed by AI/ML systems, data availability and quality issues might pose risks that also need to be considered.

Training data or the underlying input data used to develop AI/ML algorithms must meet high-quality standards, and any missing records, abnormal values,[34] or noise in data[35] will affect the expected results of AI/ML models. Data cleansing,[36] while costly, is essential in ensuring that AI/ML models are trained on accurate and relevant data. Validating aggregated data without knowing the structure of the underlying data also presents a risk because the underlying data may otherwise contain biases and inaccuracies.

In addition, AI/ML models in AML/CFT Compliance frequently rely on sensitive financial data, critical business data, and often nonpublic personal consumer information. In some cases, the data are unverified and contain errors. Similarly, if access to this sensitive data is not properly managed and secured, the data can be compromised and risks of data privacy

---

[32] *See Acting Comptroller of the Currency Michael J. Hsu's Remarks to the American Bankers Association Risk and Compliance Conference "Tokenization and AI in Banking: How Risk and Compliance Can Facilitate Responsible Innovation"* (June 16, 2023), https://occ.gov/news-issuances/speeches/2023/pub-speech-2023-64.pdf [hereinafter M. Hsu Remarks]. "Alignment is the core challenge. AI systems, which are generally based on neural networks, are not programmed explicitly like most software. They require training, and their outputs are not predictable. While this is part of their magic, it also creates a fundamental problem: since AI systems are built to "learn", they may or may not do what we want or behave consistent with our values. This alignment problem is inherent to all AI systems and is the focus of intense research. This alignment problem, in turn, creates a significant governance and accountability challenge. The more an AI system learns, the further it gets from its initial programming. This creates "opportunities for plausible deniability" should things go wrong. In addition, like most companies, banks generally must rely on third parties to develop and support their AI capabilities." *M. Hsu Remarks*, at p. 9.

[33] *See FFIEC IT Handbook*, *supra* note 19.

[34] "Abnormal data or outlier can be described as an observation that deviates so far from the rest of the observations that it can be suspected that it was produced by a different mechanism." *Outliers, Abnormal Data, Let's Take A Look at The Situation*, Aspexit (Apr. 9, 2019) (citing D.M. Hawkins, Monographs on Statistics and Applied Probability (1980)), https://www.aspexit.com/outliers-abnormal-data-lets-take-a-look-at-the-situation/.

[35] Noise in data refers to meaningless and potentially corrupt data.

[36] In general terms, data cleansing in this context refers to a process by which the quality and completeness of the data is assessed and assured. The process of data cleansing requires the involvement of both internal and external resources.

and protection including breaches; unfair use; financial loss; consumer harm; and reputational damage to the financial institutions can be magnified.

2. Complexity of AI/ML Models[37]

AI/ML models are becoming increasingly complex as modeling techniques and algorithms become more sophisticated and more stakeholders take part in modeling steps (e.g., data pre-processing; algorithms training; and ongoing monitoring of the models in production). Such increasing complexity may lead to several risks. For example:

- AI/ML models can at times be classified as 'black box' models categorized by the lack of access to their internal logic and functioning. They are not readily explainable and require additional techniques to justify how inputs are translated into corresponding outputs. This lack of explainability limits the ability to understand the approach and can reduce the confidence in the reliability of results.[38]
- Models need to be continuously retrained to adapt to changing behaviors and patterns. If models are not monitored and updated frequently, they can result in low model accuracy and prediction errors.[39]
- "A particular characteristic of some AI/ML is the ability for it to learn or evolve over time, especially as it captures new training data. Over time, this could result in drift (i.e., the AI approach could change) as it learns from the new data. This can present challenges for validating, monitoring, tracking, and documenting the AI/ML approach. It may be important to understand whether an AI/ML approach that was independently reviewed initially has significantly evolved over time (e.g., using an influx of new data). Dynamic updating can also affect how results are tracked over time. For example, initial performance thresholds chosen to monitor the approach could become less meaningful if the AI/ML approach has significantly changed to focus on different target outcomes. Similar risks can arise with AI/ML approaches that are not updated as their context evolves, since they are more closely tuned to their training data. For example, AI/ML approaches that are validated in one circumstance may not perform well in another, and an independent review conducted in a previous context may no longer be accurate in new circumstances."[40]
- Algorithms can reflect and amplify existing biases and reinforce them through the produced outcomes, particularly if not properly tested and validated.[41] The models that are trained on data sets that already contain non-compliant behaviors may not

[37] Some financial institutions, especially smaller financial institutions, have expressed frustration that complex AI/ML models are black boxes, and the relatively small number of AI/ML model providers tend to be inflexible in allowing adjustments to the models even when those adjustments are needed for risk management purposes. Another frustration is that the providers do not always have a satisfactory explanation for the refusal to allow changes.

[38] Google Cloud, *Explainable AI*, https://cloud.google.com/explainable-ai.

[39] Among the concerns expressed is that prudential supervisors and FinCEN may overreact to even one missed SAR.

[40] *See Request for Information and Comment on Financial Institutions' Use of Artificial Intelligence, Including Machine Learning*, at p.5, 86 Fed. Reg. (No. 60) 16,837 (Mar. 31. 2021), https://www.govinfo.gov/content/pkg/FR-2021-03-31/pdf/2021-06607.pdf.

[41] *Id.*

necessarily consider them as non-compliant and may see them as "normal." Therefore, the data should be cleansed to ensure any biases are removed.

These inherent risks[42] are one of the reasons the prudential supervisors issued guidance indicating that they do not require AML/CFT Compliance Programs to be based on AI/ML. Prudential supervisors have stressed that banks have wide latitude in determining whether to use models in AML/CFT Compliance Programs.[43]

3. IT Systems and Modeling Approaches Supporting the Models

AI/ML systems risk unreliability if they are not built under a suitable infrastructure and advanced modeling approach. Among other things:

- Interoperability between newer AI/ML and legacy IT systems makes it challenging to exploit the potential of innovative approaches. First, legacy IT systems are inefficient and slow due to significant loading times and lags that do not support AI/ML that requires high computational power. Second, legacy systems frequently are used in isolation because interconnection between the different systems can be difficult to achieve. This isolates information, and as a result, creates data silos that may not be accessible by AI/ML systems. Furthermore, legacy systems based on outdated hardware and software are more susceptible to cyberattacks and may not comply with newer regulations. Security and compliance risks become a concern when data protection measures are threatened. FATF points to outstanding operational and regulatory constraints such as legacy AML/CFT compliance systems and traditional regulatory frameworks and oversight mechanisms as a challenge.[44] In that regard, FATF notes that the complexities and costs involved in replacing or updating legacy systems make it challenging to exploit the potential of innovative approaches to AML/CFT Compliance for both industry and government.[45]
- Financial institutions should take care if using off-the-shelf AI/ML vendor solutions because the lack of thorough understanding and evaluation of how such solutions work

[42] For purposes of this report, inherit risk means the exposure to AML/CFT risk in the absence of any control environment being applied. This definition is used because AML/CFT Compliance Officers often conduct risk assessments, and they have to address both inherit risk and residual risk. Residual risk is the risk that remains after controls are in place.

[43] *See* Fed. Rsrv., et al, *Interagency Statement on Model Risk Management for Bank Systems Supporting Bank Secrecy Act/Anti-Money Laundering Compliance*, The Fed (Apr. 9, 2021), https://www.federalreserve.gov/newsevents/pressreleases/files/bcreg20210409a2.pdf.

[44] *See Artificial Intelligence and Machine Learning in Financial Services: A Compliance Perspective*, N.Y. City Bar (Oct. 21, 2021), https://www.nycbar.org/cle-offerings/webcast-artificial-intelligence-machine-learning-in-financial-services-a-compliance-perspective/.

[45] *See* FinCEN, *Anti-Money Laundering and Countering the Financing of Terrorism National Priorities*, U.S. Dep't of the Treasury (Jun. 30, 2021), https://www.fincen.gov/sites/default/files/shared/AML_CFT%20Priorities%20(June%2030%2C%202021).pdf.

can induce wrong results and issues with the traceability of the provenance of data, and their processing.[46]

- AI/ML hosting approaches (e.g., in-house solutions, cloud-based systems, hybrid cloud) if not carefully chosen, can expose financial institutions to security and data governance risks. Cloud-based hosting systems, in particular, present enhanced threats of data loss and breach, unauthorized access, and lack of control which may require a different risk appetite.
- The traditional, linear, and sequential approach to model development may no longer be appropriate for AI/ML models. In that sense, new sets of practices are maturing, like "MLOps," and "DevOps."[47] MLOps focuses on the intersection of data science and data engineering in combination with existing DevOps practices to streamline model delivery across the AI/ML development lifecycle. Adopting MLOps practices ensures faster time-to-market for AI/ML projects by delivering Productivity; Repeatability; Reliability; Auditability;[48] Data Quality; and Model Quality.[49]

The National Institute of Standards and Technology (NIST) provides a well-regarded summary of many of the differences between risks related to older technologies and risks related to the use of AI/ML.[50] NIST Appendix B identifies the following 14 key differences between the older technologies and current AI risks:

1. The data used for building an AI system may not be a true or appropriate representation of the context or intended use of the AI system, and the ground truth may either not exist or not be available. Additionally, harmful bias and other data quality issues can affect AI system trustworthiness, which could lead to negative impacts.
2. AI system dependency and reliance on data for training tasks, combined with increased volume and complexity typically associated with such data.

---

[46] *See News Release 2023-53 - Agencies Issue Final Guidance on Third-Party Risk Management*, OCC (June 6, 2023), https://www.occ.gov/news-issuances/news-releases/2023/nr-ia-2023-53a.pdf.

[47] DevOps is a set of practices, tools, and a cultural philosophy that automate and integrate the processes between software development and IT teams. It emphasizes team empowerment, cross-team communication and collaboration, and technology automation. *See Software Development DevOps*, Atlassian, https://www.atlassian.com/devops.

[48] Auditability is a critically important concept in AI/ML and needs further clarification. If auditability is defined narrowly, then it becomes akin to creating an audit trail (i.e., creating or identifying certain records), but not actually auditing the records. If auditability is defined broadly, then it becomes substantially similar to an audit conducted by an independent auditor, not by an automated system, software, or a machine. *See* Robert Mahari, Tobin South, and Alex "Sandy" Pentland, *Transparency By Design For Large Language Models*, Network Law Rev. (May 25, 2023), https://www.networklawreview.org/computational-three/.

[49] *See* Amazon SageMaker, *Developer Guide*, AWS Amazon, https://docs.aws.amazon.com/sagemaker/latest/dg/sagemaker-projects-why.html.

[50] *See Artificial Intelligence Risk Management Framework (AI RMF 1.0), Appendix B: How AI Risks Differ from Traditional Software Risks* (NIST AI 100-1 Appendix B) (Jan. 2023), https://nvlpubs.nist.gov/nistpubs/ai/NIST.AI.100-1.pdf.

3. Intentional or unintentional changes during training may fundamentally alter AI system performance.
4. Datasets used to train AI systems may become detached from their original and intended context or may become stale or outdated relative to deployment context.
5. AI system scale and complexity (many systems contain billions or even trillions of decision points) housed within more traditional software applications.
6. Use of pre-trained models that can advance research and improve performance can also increase levels of statistical uncertainty and cause issues with bias management, scientific validity, and reproducibility.
7. Higher degree of difficulty in predicting failure modes for emergent properties of large-scale pre-trained models.
8. Privacy risk due to enhanced data aggregation capability for AI systems.
9. AI systems may require more frequent maintenance and triggers for conducting corrective maintenance due to data, model, or concept drift.
10. Increased opacity and concerns about reproducibility.
11. Underdeveloped software testing standards and inability to document AI-based practices to the standard expected of traditionally engineered software for all but the simplest of cases.
12. Difficulty in performing regular AI-based software testing, or determining what to test, since AI systems are not subject to the same controls as traditional code development.
13. Computational costs for developing AI systems and their impact on the environment and planet.
14. Inability to predict or detect the side effects of AI-based systems beyond statistical measures.

4. Human Capital

AI/ML systems can automate multiple human tasks. However, as the use of AI/ML increases, the need for human assistance also increases, especially in the development of new use cases and applications. Similarly, as the use of human assistance increases, the likelihood of human errors also increases, and these errors can lead to incorrect and misleading decisions, with significant consequences. Perhaps one of the greatest potential benefits from the use of AI/ML systems comes from a strong human-AI/ML relationship. Humans should intervene at different steps of a model's conception, testing, and use, as a means to assure the AI/ML model is working as intended. Humans should be responsible for the fine-tuning of the models by giving feedback and adjusting predictions, if needed. If the computational power of AI/ML is not correctly combined with human expertise, models may perform less efficiently and effectively, and may create unnecessary barriers to achieving the desired improvements. Moreover, models can be misused by end users if the end users do not have a good understanding of how the outputs were generated. The potential for misuse is one of the reasons models must be regularly updated and audited. The automation of recurring processes and decision making can result in operational and productivity efficiencies (e.g., time and personnel reduction) by reducing (but not eliminating) human intervention.[51]

[51] *Id.* at 96-97.

5. Governance and Model Risk Management[52]

MRM frameworks aim to govern and validate the development of models, including AI/ML models, to ensure that they are correctly developed and used. MRM is crucial to mitigate model risks (e.g., untreated data quality issues; programming errors; bias in training data and models; and lack of model monitoring).

The complexity of AI/ML models, however, creates challenges for typical MRM functions. For example, the increased complexity of model inputs and the ways in which models evolve may make traditional MRM processes less effective. Monitoring outputs and performance may also make sense for AI/ML MRM rather than the more traditional MRM that focuses on assessment of inputs.

Reproducibility[53] is an important consideration for MRM teams, especially if model results require explainability later. Models may be stochastic[54] and hard to predict, which further affects reproducibility. The scale of AI/ML and data being used can also pose a challenge, since it is not clear which datasets, models, and metrics should be logged (e.g., test data; training data; live business data; source code; or explainability metrics), and for how long (e.g., weeks, months, years perhaps). Further, managing these governance metrics can come at a measurable cost to the MRM teams.

The absence or lack of an MRM framework can have severe consequences, exposing financial institutions to non-compliance risks, regulatory guidelines breaches, and potentially operational and financial losses. A comprehensive MRM framework should cover data quality, model design and construction, model performance and evaluation, governance, including roles and responsibilities, change management documentation and any operational process that might be affected by the model. MRM frameworks should also integrate a compliance management program to address all requirements, guidelines, and regulations from prudential supervisors on AI/ML use and development. There may also be other laws governing the use of AI/ML by financial institutions. In the U.S., for example, general artificial intelligence bills or resolutions were introduced in at least 17 states in 2022, and enacted in Colorado, Illinois, Vermont, and Washington.[55]

---

[52] One of the reasons the prudential supervisors do not require AML/CFT Compliance Programs to use models is that AML/CFT Compliance Program modeling is different in quality and scope from many other MRM programs. Some commentators have pointed out that there are no "true north" data from law enforcement and other sources and most algorithms are trained on bank SAR filings and other external information. This could lead to an "echo chamber" effect.

[53] Reproducibility is a principle that model development should be documented in a way that the process can be repeated with identical results. The interrelationship between auditability and reproducibility is critically important.

[54] Stochastic models are defined to have random probability distributions or patterns that may be analyzed statistically but may not be predicted precisely.

[55] *See Legislation Related to Artificial Intelligence*, National Conference of State Legislature (NCSL) (Aug. 26, 2022), https://www.ncsl.org/research/telecommunications-and-information-technology/2020-legislation-related-to-artificial-intelligence.aspx.

D. Recent Programs on AI/ML Sponsored by the City Bar

The City Bar has monitored continuously the increasing adoption of AI/ML in financial services and has brought together experts across the legal, regulatory, academic, and professional services fields to provide perspectives and guidance to understand and navigate latest developments in AI/ML, including in the use of AI/ML in AML/CFT Compliance.[56]

II. Recent Updates on AI/ML from Regulatory Agencies and Standard-Setting Organizations

For AML/CFT Compliance Officers, certain government agencies have greater influence over AML/CFT Compliance Programs than other government agencies. In the US, federal and state prudential supervisors, the SEC, FinCEN, OFAC, DOJ, local prosecutors, and main Treasury have the most influence over AML/CFT Compliance Programs.[57] Further following a functional regulation approach, AML/CFT laws and regulations will also be enforced by a financial institution's primary regulator or supervisor.[58] For example, the SEC (not the prudential supervisors) will enforce AML/CFT laws against broker dealers in securities and FinCEN (not the federal prudential supervisors) will enforce the AML/CFT laws against insurance companies and MSBs.

A. The Anti-Money Laundering Act of 2020

On January 1, 2021, Congress passed the AMLA, which many commentators consider to be the most significant reforms to AML/CFT laws since the USA PATRIOT Act in 2001. AMLA has made emerging technologies such as AI/ML a priority. The AMLA should strengthen and modernize AML/CFT infrastructure to reflect the capabilities of emerging technologies and new criminal methodologies. For instance, AMLA Section 6002(3) indicates that one of AMLA's purposes is to encourage technological innovation and the adoption of

---

[56] See Schedule C for a detailed list of some of the City Bar programs on AI/ML.

[57] Federal and state prudential supervisors exercise their influence primarily through laws and regulations; charters, licenses, consents, and other approvals; examination and supervision; investigations and enforcement actions; and guidance. FinCEN and OFAC exercise their influence primarily through laws and regulations; registrations (in the case of FinCEN) and specialized licenses (in the case of OFAC); investigations and enforcement actions; and guidance. DOJ, local prosecutors, and Treasury exercise their influence primarily through laws and regulations; investigations and enforcement actions; and guidance. FATF has indirect influence because it influences positions taken by national governments and policymakers, but FATF does not have jurisdiction over financial institutions in the US. The US Sentencing Commission through its sentencing guidelines and the US Attorneys Manual developed by DOJ are also influential. *See United States Sentencing Commission Guidelines Manual 2021*, USSC (2021), https://www.ussc.gov/guidelines/2021-guidelines-manual-annotated and *the U.S. Justice Manual (JM)* (previously known as the United States Attorneys' Manual (USAM)), U.S. Dep't of Justice (2018, as subsequently amended), https://www.justice.gov/jm/justice-manual.

[58] This does not mean that the primary regulator or supervisor will conduct the examinations. For instance, while FinCEN is the primary regulator for MSBs, it has delegated examination authority to the Internal Revenue Service (IRS).

new technology by financial institutions to more effectively counter money laundering and terrorist financing.[59] In addition, AMLA Section 6002(5)(D)(i) provides that FinCEN shall establish streamlined, including automated, processes to permit, as appropriate, the filing of noncomplex categories of SARs that reduce burdens imposed on persons required to report and do not diminish the usefulness of the reporting in combating financial crime, including terrorist financing.[60] Likewise, AMLA Section 6209(a) provides that Treasury, in consultation with the head of each agency to which the Treasury Secretary has delegated duties or powers in this area, "shall issue a rule to specify with respect to technology and related technology internal processes designed to facilitate compliance" with the AMLA requirements, the standards by which financial institutions are to test the technology and related technology internal processes. Treasury also emphasized, among other things, using innovative approaches such as AI/ML or other enhanced data analytics processes.[61]

B. Financial Action Task Force Report

In an analysis by FATF in July 2021, titled *Opportunities and Challenges of New Technologies for AML/CFT* (FATF Report),[62] FATF emphasized that new technologies have the potential to make AML/CFT Compliance measures faster, cheaper, and more effective.[63] The FATF Report expressly highlighted the following benefits:[64]

1. ***Digital Identity Solutions*** that can enable non-face-to-face customer identification/verification/authentication and updating of information. They can also improve authentication of customers for more secure account access and strengthen identification and authentication when onboarding and transactions are conducted in-

[59] *See U.S. Anti-Money Laundering Act 2020: Key Highlights*, ComplyAdvatage (May 5, 2022), https://complyadvantage.com/insights/us-anti-money-laundering-act-amla-2020/. *See also* AMLA, *supra* note 12, as amended by AMLA § 6002(3).

[60] 31 U.S.C. § 5318(g).

[61] 31 U.S.C. § 5318(o).

[62] *See* FATF, *Opportunities and Challenges of New Technologies for AML/CFT* (July 2021), https://www.fatf-gafi.org/content/dam/fatf-gafi/guidance/Opportunities-Challenges-of-New-Technologies-for-AML-CFT.pdf.coredownload.pdf [hereinafter FATF Report].

[63] *Id.* ¶ *6*:

> [T]hey can improve the implementation of FATF Standards to advance global AML/CFT efforts, ensure financial inclusion and avoid unintended consequences such as financial exclusion….Technology can facilitate data collection, processing and analysis and help actors identify and manage money laundering and terrorist financing (ML/TF) risks more effectively and closer to real time… Faster payments and transactions, more accurate identification systems, monitoring, record keeping and information sharing between competent authorities and regulated entities also offer advantages…. The increased use of digital solutions for AML/CFT based on Artificial Intelligence (AI) and its different subsets (machine learning, natural language processing) can potentially help to better identify risks and respond to, communicate, and monitor suspicious activity.

[64] *See generally*, *FATF Report*, *supra* note 62.

person, promoting financial inclusion, and combating money laundering, fraud, terrorist financing, and other illicit financing activities.[65]

2. ***Natural Language Processing*** that can support more accurate, flexible, and timely analysis of customer information and reduce inaccurate or false information and enabling more efficient matching and search for additional data. Better and more up-to-date customer profiles mean more accurate risk assessments, better decision-making, and fewer instances of unintended financial exclusion.[66]
3. ***AI/ML Technology-based Solutions*** that can be applied to big data can strengthen ongoing monitoring and reporting of suspicious transactions. These solutions can automatically monitor, process, and analyze suspicious transactions and other illicit activity, distinguishing it from normal activity in real time, while reducing the need for initial, front-line human review. AI/ML tools or solutions can also generate more accurate and complete assessments of ongoing customer due diligence and customer risk, which can be updated to account for new and emerging threats in real time.[67]
4. ***Application Programming Interfaces (APIs), Distributed Ledger Technology (DLT), Data Standardization, and Machine-Readable Regulations*** can help regulated entities in reporting more efficiently to supervisors and other competent authorities. The technologies also allow alerts, report follow-ups, and other communications from supervisors, law enforcement, or other authorities to regulated entities and their customers as well as communications among regulated entities, and between them and their customers. The application of more advanced analytics by regulators can also strengthen examination and supervision, including by potentially providing more accurate and immediate feedback.[68]

C. New York State Department of Financial Services

In March 2021, DFS held its first-ever Tech Sprint[69] on Digital Regulatory Reporting in the Virtual Currency Industry. The Tech Sprint opened on March 1, 2021, and culminated with "Demo Day" on March 12, 2021.[70] According to DFS, each Tech Sprint team worked to address one of several defined problem statements, such as the following:

- How can DFS achieve real-time or more frequent access to company financial data from virtual currency licensees and receive early warning signs of financial risks to the companies or their customers?
- How can DFS obtain real-time transaction data from its licensees and automatically analyze the data to safeguard against illicit financing risks?

---

[65] *Id.* ¶ 6-7.

[66] *Id.*

[67] *Id.*

[68] *Id.*

[69] Tech Sprints are a critically important part of any AML/CFT Compliance Program that uses advanced technology. In New York, DFS also has a strong set of AML/CFT Compliance laws, including the DFS's AML/CFT Compliance Program requirements under 3 N.Y.C.R.R. § 116.2 and DFS's transaction monitoring requirements under 23 N.Y.C.R.R. § 504.

[70] *Press Release - DFS Announces Details for its First-Ever Techsprint on Digital Regulatory Reporting in the Virtual Currency Industry*, N.Y. State Dep't of Fin. Sec'y (Jan. 21, 2021), https://www.dfs.ny.gov/reports_and_publications/press_releases/pr202101211.

- How can DFS use tools such as natural language processing, machine learning, and artificial intelligence to identify risks by processing and analyzing supervisory reports that are submitted by licensees in a wide range of formats?
- How can DFS use technology to facilitate information-sharing among licensees to help them more quickly identify and stop scams, ransomware strikes, and other criminal enterprises that put licensees and their customers at risk?

DFS takes a pragmatic approach to AI/ML, especially concerning the use of AI/ML to comply with DFS rules and regulations. DFS encourages responsible innovation and the practical use of AI/ML in, among other areas, AML/CFT Compliance Programs; transaction monitoring; cybersecurity; and virtual currencies. DFS does not require or forbid the use of AI/ML, but DFS does acknowledge that, if used responsibly, AI/ML could be used effectively to comply with the DFS's Cybersecurity and Transaction Monitoring Regulation.[71] For DFS supervised entities that use AI/ML, they must, at a minimum:

1. Develop and maintain the appropriate expertise in AI/ML;
2. Properly train appropriate staff in the use of AI/ML;
3. Properly supervise and monitor third-party vendors;
4. Conduct appropriate risk assessments; and
5. Use clear documentation.

D. Interagency Request for Information and Comment

In a Request for Information and Comment (RFI) published in the Federal Register on March 31, 2021, by the Federal Reserve, the CFPB, the FDIC, the NCUA, and the OCC (collectively, the Agencies) on the use of AI/ML by financial institutions, the Agencies expressed their support for responsible innovation by financial institutions that includes the identification and management of risks associated with the use of new technologies and techniques.[72]

---

[71] *See* N.Y. Comp. Codes R. & Regs. tit. 23 § 500.0 (2021); *See also* N.Y. Comp. Codes R. & Regs. tit. 3 § 504 (2021).

[72] *See* Request for Information and Comment on Financial Institutions' Use of Artificial Intelligence, Including Machine Learning, 86 Fed. Reg. 16,837 (Mar. 31, 2021), https://www.federalregister.gov/documents/2021/03/31/2021-06607/request-for-information-and-comment-on-financial-institutions-use-of-artificial-intelligence:

> [A]I has the potential to offer improved efficiency, enhanced performance, and cost reduction for financial institutions, as well as benefits to consumers and businesses. AI can identify relationships among variables that are not intuitive or not revealed by more traditional techniques. AI can better process certain forms of information, such as text, that may be impractical or difficult to process using traditional techniques. AI also facilitates processing significantly large and detailed datasets, both structured and unstructured, by identifying patterns or correlations that would be impracticable to ascertain otherwise. Other potential AI benefits include more accurate, lower-cost, and faster underwriting, as well as expanded credit access for consumers and small businesses that may not have obtained credit under traditional credit

E. OFAC Sanctions Screening and the Application of the OFAC Framework

OFAC's 2019 Framework for Compliance Commitments encourages financial institutions to employ a risk-based sanctions compliance program, which is anticipated to vary based upon a financial institution's size and sophistication; products and services; customers and counterparties; and geographic locations.[73] In support of the flexibility offered by this framework and its correspondent components, AI/ML can provide the following benefits:

- ***Screen Multiple Lists*** – Most large financial institutions screen multiple sanctions lists, and interfaces like APIs can play a key role.
- ***Fuzzy Matching*** – Sanctions screening depends on the ability of automated tools to effectively assess text that is similar but not quite the same.
- ***More Productive Investigations*** – Properly tuned automated solutions can allow for obvious false positives to be closed, with greater attention focused on the highest risk cases.
- ***Advanced Assessment of Hit Quality*** – Using technology such as Natural Language Processing to process text and infer entity attributes, such as age; nationality; or adverse information can increase hit quality. Hit quality is collected as a means to determine the accuracy of a hit and as a means to further limit the number of false positives and false negatives and thereby increase the quality of hits.

F. Department of Treasury National Risk Assessments

In its issuance of National Priorities that financial institutions should incorporate into their AML/CFT Compliance Programs, FinCEN specifically referenced Treasury's National Risk Assessments. Under the FinCEN guidance, AML/CFT Compliance Officers must review their risk assessments and make sure risks identified by Treasury in Treasury's National Risk Assessments are taken into account when the AML/CFT Compliance Officers conduct risk assessments for the regulated financial institutions.[74] Treasury defines proliferation financing as the financing of the proliferation of Weapons of Mass Destruction (WMD) and their delivery systems. WMD programs include the research, development, and deployment of delivery systems, including ballistic missiles and unmanned aerial vehicles. The definition of WMD encompasses chemical, biological, radiological, and nuclear weapons.[75] Treasury has identified North Korea and Iran as state actors posing the most significant threat.

---

underwriting approaches. AI applications may also enhance an institution's ability to provide products and services with greater customization.

[73] OFAC, *A Framework for OFAC Compliance Commitments*, U.S. Dep't of the Treasury (May 2, 2019), https://ofac.treasury.gov/media/16331/download?inline.

[74] *See FinCEN AML/CFT Priorities*, *supra* note 6, for a detailed discussion of FinCEN's National Priorities.

[75] *See* U.S. Dep't of the Treasury, *National Proliferation Financing Risk Assessment* (Feb. 2022), https://home.treasury.gov/system/files/136/2022-National-Proliferation-Financing-Risk-Assessment.pdf.

1. Department of the Treasury National Proliferation Financing Risk Assessment (February 2022) (Proliferation Financing Assessment)[76]

Among other trends, Treasury concluded that North Korea and Iran pose the most significant threats for the US. Meanwhile, China and Russia continue to engage in proliferation financing (PF) activities by expanding their efforts to acquire US-origin goods in violation of relevant expert control laws.[77] Since the Russian invasion of Ukraine in early 2022, these risks have increased significantly.

The report also notes that the illicit use of correspondent banking relationships by PF networks for PF activities continues to grow, especially in the maritime sector. PF networks are also exploiting the expansion of the digital economy by engaging in the mining and trading of virtual assets as well as hacking of virtual asset service providers (VASPs). The report specifically points to North Korea as becoming more sophisticated in engaging in malicious cyber activity against traditional financial institutions and VASPs.[78]

According to the Treasury, the threat to the US from proliferation networks arises from two factors. First, the role of the US dollar for a variety of cross-border financial activities and the sophistication of US-origin proliferation technology. Second, the PF networks acquire or attempt to acquire specific goods for WMD programs, some of which, depending on the specific needs of the proliferator, are of US origin and subject to the US export control regime.[79] For AML/CFT Compliance Officers, the OFAC and sanctions screening software used by the financial institutions must focus closely on geographic location (e.g., origination and destination of the goods or services) of transactions involving cross-border financial activity, and the underlying goods involved (e.g., the goods may not be used to assist with the development of WMD). AML/CFT Compliance Officers must make sure the underlying goods or technology does not violate any US export controls or restrictions.

2. Department of the Treasury National Money Laundering Risk Assessment (February 2022) (Money Laundering Risk Assessment)[80]

According to the Money Laundering Risk Assessment, among other significant risks, drug trafficking, money laundering, and corruption are significant risks:

a. Drug Trafficking

The Money Laundering Risk Assessment stresses that drug trafficking continues to pose a threat to public health in the U.S. and generates significant proceeds for the criminal organizations that supply the U.S. and global markets. Drug Trafficking Organizations (DTOs), engaged in the trafficking of a variety of drugs into the U.S., use numerous methods to launder proceeds, which remain predominantly cash based. The Drug Enforcement Administration estimates that DTOs continue to generate billions of dollars in illicit proceeds every year. The movement and laundering of proceeds associated with the illicit drug market in the U.S.

[76] *See Id.*

[77] *Id.*

[78] *Id.*

[79] *Id.*

[80] *See Id.*

continue to include traditional methods and techniques, such as bulk cash smuggling (BCS) and trade-based money laundering (TBML), although the COVID-19 pandemic caused some initial disruptions to DTOs using those methods due to travel restrictions and a slower global economy. Financial institutions, including banks and MSBs, remain vulnerable to exploitation by DTOs that use front and shell companies and third parties (including money mules) to wire proceeds from the U.S. to their base of operations. DTOs are growing more comfortable with darknet markets and the use of virtual assets to launder funds, although the size and scope of drug proceeds generated on the darknet and laundered via virtual assets remain low in comparison to cash-based retail street sales.

b. Professional Money Laundering Organizations

The Money Laundering Risk Assessment also notes that the use of professional money laundering organizations (PMLOs), networks, and third-party money launderers has not abated since previous risk assessments. Law enforcement has observed new trends with respect to PMLOs. For example, the FBI noted that these networks have co-opted unwitting and witting third parties (e.g., law firms, real estate agents, accountants, etc.) to bypass domestic regulatory AML/CFT controls and have used legal privilege[81] as a method to hide illicit activity. TBML is defined as the process of disguising the origin of criminal proceeds through the import or export of merchandise and trade-related financial transactions. There are various TBML methods that can be employed by professional launderers to include the use of money brokers. Money brokers are third parties that seek to purchase drug proceeds, at a discounted rate from drug cartels located in narcotics source countries (e.g., Colombia, Mexico), in the local

[81] Both the FATF and the Treasury view lawyers as essential gatekeepers to prevent illicit activities. Both have also emphasized that some lawyers use the attorney client and other privileges to shield law enforcement access to relevant information that could be used to uncover or prosecute illicit activity. Many lawyers have responded that they are required by ethical rules to represent their clients zealously within the full bounds of the law, and law enforcement would only be entitled to such information if an appropriate warrant or other legal process required the disclosure of such information. The assertion by law enforcement and the responses by lawyers to those assertions feed into a wider debate between law enforcement and lawyers regarding which governmental agencies should regulate lawyers. FATF and Treasury have made it clear that they believe lawyers should be subject to the requirement to have an AML/CFT Compliance Program. Lawyers have also made it clear that they are already regulated by, among others, the judiciary, and the ethical and other requirements of specific bar associations. *See ABA Resolution 100*, Am. Bar Ass'n. (Aug. 2023), which "Amends the Black Letter and Comments to Model Rule of Professional Conduct 1.16" (Declining or Terminating Representation), https://www.americanbar.org/news/reporter_resources/annual-meeting-2023/house-of-delegates-resolutions/100/; https://www.americanbar.org/content/dam/aba/directories/policy/annual-2023/100-annual-2023.pdf; and https://www.americanbar.org/content/dam/aba/administrative/news/2023/am-res/100.pdf. *See also, A Lawyer's Guide to Detecting and Preventing Money Laundering – A Collaborative Publication of the International Bar Association, the American Bar Association and the Council of Bars and Law Societies of Europe* (Oct. 2014), https://www.advocatenorde.nl/document/a-lawyers-guide-to-detecting-and-preventing-money-laundering and Laurel S. Terry and José Carlos Llerena Robles, *The Relevance of FATF's Recommendations and Fourth Round of Mutual Evaluations to the Legal Profession*, 42 FORDHAM INT'L L. J. 627 (2018), https://works.bepress.com/laurel_terry/87/.

currency where the drugs are sold and the illicit proceeds are generated (e.g., U.S. dollars in the U.S.). Money brokers often employ many individuals responsible for collecting narcotics proceeds and disposing of those proceeds, as directed by either the DTO or the money brokers who serve as PMLOs. The main objective of the money broker is to evade foreign exchange restrictions. This enables DTOs with cash located in the U.S. to transfer the value of that cash to other countries, principally Colombia and Mexico (depending on the location of the DTO), without having to transport U.S. currency physically across an international border. Furthermore, the use of a money broker allows all the participants to receive funds in their own currencies.

c. Corruption

The Money Laundering Risk Assessments, in 2018 and 2015, identified corruption as a priority money laundering threat, and President Joseph Biden in December 2021 signaled a redoubled emphasis on anti-corruption as a national security priority via the issuance of a U.S. Strategy on Countering Corruption, which includes curbing illicit finance as one of its key pillars. The US uses a number of legal authorities to combat foreign corruption. The Foreign Corrupt Practices Act (FCPA), among other things, makes it unlawful for certain classes of persons and entities to offer or pay money or anything of value to foreign government officials in order to obtain or retain business. The DOJ's Kleptocracy Asset Recovery Initiative focuses on investigation and litigation to recover the proceeds of foreign official corruption in the U.S., or which used the US financial system. As of 2021, the DOJ's Kleptocracy Asset Recovery Initiative had recovered and assisted in recovering and repatriating approximately $1.7 billion in assets and had an additional approximately $2.2 billion in assets restrained pending forfeiture litigation and forfeited pending return negotiations. Prosecutable domestic corruption often involves money laundering activity as individuals seek to disguise bribes paid to and received by corrupt officials. DOJ's Public Integrity Section handles federal cases involving embezzlement, bribery, and related crimes. As is the case with foreign corruption activity, domestic corruption often involves other crimes, ranging from tax evasion to contracting fraud. Recent domestic corruption cases have also involved unlawful campaign contributions, as both U.S. and foreign individuals have sought to illegally influence elections within the U.S. On December 22, 2023, President Biden signed into law the Foreign Extortion Prevention Act,[82] which criminalizes the demand side of foreign bribery.

G. Guidance Concerning the Difference between Domestic and International AI/ML

In August 2023, the U.S. Law Library of Congress released a report on *Regulation of Artificial Intelligence Around the World* (August 2023), which provides a list of jurisdictions in the world where legislation that specifically refers to AI or systems utilizing AI have been adopted or proposed.[83] Likewise, on August 23, 2023, the International Association of Privacy

[82] *See Press Release - Bipartisan, Bicameral Foreign Extortion Prevention Act Signed Into Law*, Sheldon Whitehouse (Dec. 26, 2023), https://www.whitehouse.senate.gov/news/release/bipartisan-bicameral-foreign-extortion-prevention-act-signed-into-law.

[83] Kayahan Cantekin, *Regulation of Artificial Intelligence Around the World*, Law Library of Congress (U.S). Glob. Legal Rsch. Directorate (GLRD) (Aug. 2023),

Professionals (IAPP) updated its *Global AI Legislation Tracker*[84] that identifies legislative policy and related developments in a subset of jurisdictions and provides commentary on the wider AI/ML context in specific jurisdictions, and lists index rankings provided by Tortoise Media. Similarly, according to the AIPPF Report, there have been several AI/ML governance principles around the world. However, the challenge remains in the application of such principles to specific AI/ML use cases and translating them in effective internal practices.[85] Jurisdictions such as the EU[86] have also progressed in their approach to regulating the use of AI/ML in financial services. In particular, the European Council proposal for draft regulation from April 2021, narrows the definition of high-risk use-cases, which may be useful for other jurisdictions to consider.[87]

The AIPPF Report highlights that it is important to avoid regulatory fragmentation where possible, which would help to ensure accountability and manage risks without curbing innovation. Regulations should aim to be flexible, and principle based.[88]

The AIPPF Report brings into focus one of the most difficult tasks for governmental agencies, especially those agencies that focus on the regulation of AI/ML. There are numerous laws and proposed laws not only in the U.S. and the UK, but also across North America, Europe, Australia, and Asia. These laws and proposed laws include restrictions on the use of algorithms, biometric surveillance systems, facial recognition processes, and other areas.

III. AI/ML Opportunities and Challenges

In many cases, AI/ML may present as many challenges as there are opportunities, especially in implementing AI/ML in AML/CFT Compliance Programs. For this reason, the Agencies issued guidance indicating that they do not require AML/CFT Compliance Programs to be based on AI/ML.[89] According to an Interagency Statement on Model Risk Management (MRM)[90] in response to concerns about the application of Supervisory Guidance on MRM,[91]

---

https://www.loc.gov/item/2023555920/ and https://tile.loc.gov/storage-services/service/ll/llglrd/2023555920/2023555920.pdf.

[84] *Global AI Legislation Tracker*, IAPP Rsch. and Insights (Aug. 25, 2023), https://iapp.org/media/pdf/resource_center/global_ai_legislation_tracker.pdf.

[85] *See AIPPF Report*, *supra* note 17.

[86] *See EU AI Act Draft*, *supra* note 21.

[87] *Id.* at 13-14.

[88] *See AIPPF Report*, *supra* note 17.

[89] *See* Bank Policy Institute Comment Letter, at p.13 (Nov. 16, 2020), https://bpi.com/wp-content/uploads/2020/11/BPI-Comment-Letter-re-FinCEN-AML-Program-Effectiveness-ANPRM-vF.pdf.

[90] *See* Fed. Rsrv., et al, *Interagency Statement on Model Risk Management for Bank Systems Supporting Bank Secrecy Act/Anti-Money Laundering Compliance*, the Fed (Apr. 9, 2021), https://www.federalreserve.gov/newsevents/pressreleases/files/bcreg20210409a2.pdf.

[91] *See* Fed. Rsrv., et al., *Supervisory Guidance on Model Risk Management, Fed.Rsrv. Supervision and Regul. Letter 11–7*, the Fed (Apr. 4, 2021), https://www.federalreserve.gov/supervisionreg/srletters/sr1107.htm and *see also*, FDIC,

banks have wide latitude in determining whether to use a model.[92] The Agencies support efforts by banks to innovate and update their AML/CFT Compliance systems and models to adapt quickly to an evolving threat environment.[93] Further recognizing that not all banks use models such as those described in the MRMG or have formalized MRM frameworks,[94] the Interagency Statement identifies cases to clarify how the MRMG may be a useful resource to guide a bank's MRM framework.[95] The Interagency Statement points out that regardless of whether a bank characterizes an AML/CFT Compliance system (or portions of that system) as a model, a tool, or an application, the risk management of such a system should be consistent with safety and soundness principles and should promote compliance with applicable laws and regulations.[96] For this and other purposes, financial institutions must be aware of the most common challenges that they might face to overcome them better.[97]

A. AI/ML Modeling Starts with Cleansing and Securing the Data

Some of the data that form the foundation for applying AI/ML in AML/CFT Compliance are often raw, unverified, and from varied sources. Data can be structured, semi-structured, or unstructured (e.g., customer and accounts details; transactions and assets; products and services; emails and chats; and behavioral information). Such variations represent challenges because data often come in a non-processed format, which needs preparation and cleansing to prevent the AI/ML system from learning from untrustworthy data or interpretating data incorrectly:

- Data can be fragmented, duplicated, inconsistent, inaccurate, and incomplete across a financial institution. Data should always be accessible, correctly captured, and integrated in the corresponding databases. An effective data supply is essential in terms of quality and quantity. Poor data quality will have immediate negative effects on the performance of AI/ML based monitoring systems.
- Data should be collected carefully with due consideration of laws and regulations. The following are examples of published regulatory guidance that provide guidelines on the data that can be collected for AML/CFT Compliance purposes, and how the data should be processed:

Adoption of Supervisory Guidance on Model Risk Management, Fin. Inst. Letter FIL-22-2017 (June 7, 2017), https://www.fdic.gov/news/financial-institution-letters/2017/fil17022.pdf (collectively, Model Risk Management Guidance or MRMG). The Interagency Statement provides that the MRMG, as with all supervisory guidance, does not have the force and effect of law.

[92] *Id.*

[93] *See Role of Supervisory Guidance*, 86 Fed. Reg. (NO.66) 18173 (Apr. 8, 2021), https://www.govinfo.gov/content/pkg/FR-2021-04-08/pdf/2021-07146.pdf. *See also*, 12 C.F.R. Part 262.

[94] *Id.*

[95] *Id.*

[96] *Id.*

[97] *See generally*, *AIPPF Report*, *supra* note 17.

The U.S. has federal and state laws that are actively enforced. For instance, The use of AI/ML can create or heighten consumer protection risks, such as risks of unlawful discrimination[98] or unfair, deceptive, or abusive acts or practices (UDAAP) under the Dodd-Frank Wall Street Reform and Consumer Protection Act (Dodd Frank),[99] unfair or deceptive acts or practices (UDAP) under the Federal Trade Commission Act (FTC Act), or privacy concerns.[100] Many states also have laws prohibiting UDAAP and UDAP and violations of consumer privacy. Indeed, in many cases, state laws provide more protections than the equivalent federal laws. As mentioned earlier in this Report, the use of facial recognition software and voice recognition software creates risks of illegal discrimination, and some states are currently regulating these areas. For example, California enacted the Bolstering Online Transparency Act to make it unlawful for a person or entity to use a bot to communicate or interact online with a person in California in order to incentivize a sale or transaction of goods or services or to influence a vote in an election without disclosing that the communication is by a bot.[101] California businesses are also required to provide notice to consumers regarding

---

[98] *See The Americans with Disabilities Act and the Use of Software, Algorithms, and Artificial Intelligence to Assess Job Applicants and Employees*, U.E. Equal Emp't Opportunity Comm'n (EEOC), https://www.eeoc.gov/laws/guidance/americans-disabilities-act-and-use-software-algorithms-and-artificial-intelligence; Apostol Vassilev, Harold Booth, and Murugiah Souppaya, *Mitigating Ai/Ml Bias In Context Establishing Practices for Testing, Evaluation, Verification, and Validation of AI Systems*, Nat'l Inst. of Standards and Tech. (NIST) (Nov. 9, 2022), https://www.nccoe.nist.gov/sites/default/files/2022-11/ai-bias-pd-final.pdf; Douglas MacMillan, *Eyes on the Poor: Cameras, Facial Recognition Watch Over Public Housing, Surveillance Cameras Purchased with Federal Crime-Fighting Grants are Being Used to Punish and Evict Public Housing Residents, Sometimes for Minor Rule Violations*, Wash. Post (May 16, 2023), https://www.washingtonpost.com/business/2023/05/16/surveillance-cameras-public-housing/; *Equitable Algorithms: How Human-Centered AI can Address Systemic Racism and Racial Justice in Housing and Financial Services*, Memorandum to Members, Comm. on Fin. Serv. from Fin. Serv. Comm. Majority Staff, U.S. House of Representatives Comm. on Fin. Serv. (May 4, 2021), https://democrats-financialservices.house.gov/uploadedfiles/hhrg-117-ba00-20210507-sd002.pdf and *Consumer Financial Protection Circular 2023-03 - Adverse Action Notification Requirements and the Proper Use of the CFPB's Sample Forms Provided in Regulation B*, Consumer Fin. Prot. Bureau (CFPB) (Sept. 19, 2023), https://www.consumerfinance.gov/compliance/circulars/circular-2023-03-adverse-action-notification-requirements-and-the-proper-use-of-the-cfpbs-sample-forms-provided-in-regulation-b/.

[99] *See Bulletin 2022-05: Unfair and Deceptive Acts or Practices That Impede Consumer Reviews*, CFPB (Mar. 2022), https://files.consumerfinance.gov/f/documents/cfpb_bulletin-2022-05_unfair-deceptive-acts-practices-impede-consumer-reviews.pdf and *see also, CFPB Chatbots in Consumer Finance*, CFPB (June 6, 2023), https://www.consumerfinance.gov/data-research/research-reports/chatbots-in-consumer-finance/chatbots-in-consumer-finance/.

[100] FTC Act of 1914, 15 U.S.C. § 45(c).

[101] *See* Senate Bill-1001, Chapter 892, Cal. Legislative Info. (Sept. 28, 2018), https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180SB1001.

their privacy practices.[102] In 2021, Colorado enacted SB 21-169, Protecting Consumers from Unfair Discrimination in Insurance Practices.[103] In 2019, Illinois enacted the Illinois AI Video Interview Act to restrict the use of AI in hiring.[104] In 2021, New York City enacted Local Law 144 to require employers to conduct bias audits of AI-enabled tools used for employment decisions.[105]

In the European Union, the 5th directive states: "In order to respect privacy and protect personal data, the minimum data necessary for the carrying out of AML/CFT investigations should be held in centralized automated mechanisms for bank and payment accounts, such as registers or data retrieval systems. It should be possible for Member States to determine which data is useful and proportionate to gather, taking into account the systems and legal traditions in place to enable the meaningful identification of the beneficial owners."[106] The EU specifically allows for the lawful processing of personal data where "processing is necessary for compliance with a legal obligation to which the controller is subject."[107] Accordingly, when processing personal data for the purposes of complying with an AML/CFT Compliance obligation, firms should ensure that such processing is necessary and proportionate in order to comply with their AML/CFT Compliance obligations.[108]

The following general principles must also be considered when cleansing and securing data:

- Using a limited set of internal data does not provide a holistic view for risk monitoring. Internal data needs to be enriched with external data. Open or commercial data sources (e.g., negative news, sanctions, and PEP lists), and web-scrapped data (e.g., social media and tweets and regulatory publications) can also be used to enrich data. For

---

[102] State of Cal. Off. of Atty. Gen., *California Consumer Privacy Act (CCPA)*, https://oag.ca.gov/privacy/ccpa.

[103] *See* Senate Bill 21-169 *Restrict Insurers' Use of External Consumer Data*, Colo. Gen. Assembly (2021), https://leg.colorado.gov/bills/sb21-169.

[104] *See* Ill. AI Video Interview Act (820 ILCS 42/), Ill. Gen. Assembly (2022), https://www.ilga.gov/legislation/ilcs/ilcs3.asp?ActID=4015&ChapterID=68.

[105] *See* N.Y. Dep't of Consumer and Worker Protection Local Law 144, City of N.Y.(2023), https://rules.cityofnewyork.us/wp-content/uploads/2023/04/DCWP-NOA-for-Use-of-Automated-Employment-Decisionmaking-Tools-2.pdf.

[106] *See Directive (EU) 2018/843 of The European Parliament and of The Council of 30 May 2018 Amending Directive (EU) 2015/849 on the Prevention of the Use of the Financial System for the Purposes of Money Laundering Or Terrorist Financing, and Amending Directives 2009/138/EC and 2013/36/EU (Text with EEA Relevance)*, 2018 O.J. (L 156), at 43-74, (Document 32018L0843) (June 19, 2018), https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32018L0843.

[107] *See Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation)*, Regulations I Art. 6.1, 2016 O.J. (L 119/36) (May 4, 2016), https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679.

[108] *Id.*

supervised learning approaches, labeling and annotating the target prediction variable may be required in the absence of complete training datasets. This can require substantial manual labor. The AIPPF Final Report indicates: "For AML and fraud detection, one fundamental problem can be that firms do not have access to ground truths."[109] One example is that regulators do not typically share which transaction SARs were helpful and which were not. This lack of relevant information affects the training as well as overall performance of the model and its wider applicability.[110]

- Financial institutions need to expand systems, processes, and procedures that protect data from unauthorized access and data corruption throughout their lifecycle, including risk assessments and security protocols, data encryption, hashing, tokenization, and key management practices that protect and ensure data governance across all applications and platforms.
- The efficacy of data cleaning depends significantly on a thorough understanding of the data. This comprehension serves as the foundation for identifying anomalies, outliers, and inter-variable dependencies. It guides major decision-making processes when dealing with missing values, duplicates, and variable semantics. A deep understanding facilitates precise data transformations, standardizations, and the establishment of meaningful quality metrics. It also acts as a safeguard against inadvertent data loss, ensuring that the cleaning process enhances data interpretability without compromising valuable information. In essence, the key to effective data cleaning lies in understanding the data, fostering accuracy, consistency, and reliability in the resultant dataset.

B. Rule-Based Approach vs Risk-Based Approach Dilemma

FATF and US authorities have stressed that a risk-based approach is the cornerstone of an effective AML/CFT Compliance Program. A risk-based approach requires governments, financial institutions, and other stakeholders to evaluate and understand the AML/CFT risks the financial system is exposed to and that need to be addressed.

Unlike the risk-based approach,[111] the rule-based approach requires compliance with rules without regard to the underlying risk. Both approaches are still widely used in AML/CFT Compliance Programs because both approaches are allowed in many FATF member countries. The FATF Report explains that the traditional rule-based approach has led to defensive compliance rather than the application of different mitigating measures to different levels of risk.[112] The response of the authorities to over-reporting in relation to under-reporting has further contributed to defensive actions.[113] Defensive AML/CFT Compliance Program

[109] *See AIPPF Report*, *supra* note 17, at 41.

[110] *Id.*

[111] According to FATF guidance, a risk-based approach means that countries, competent authorities, and banks identify, assess, and understand the money laundering and terrorist financing risk to which they are exposed, and take the appropriate mitigation measures in accordance with the level of risk.

[112] *See FATF Report*, *supra* note 62.

[113] Some commentators believe the response of the authorities to under-reporting has contributed to defensive actions (e.g., defensive SARs) as well because many regulated financial institutions perceive that regulatory agencies prioritize the use of a rule-based approach (i.e., ticking the box) when they examine, or at best a hybrid rule-based and risk-

frameworks are the result of regulatory or operational uncertainty and lack of trust in the strategies and mechanisms applied.[114] "Public and private sectors alike may lack trust in their own risk assessments because of their incomplete understanding of reality, lack of information and data, and lack of resources and tools to carry out solid, up-to-date, and comprehensive risk assessments."[115]

The appropriate transposition of risk-based measures holds some challenges and complexity. The changeover to the new risk-based systems generates extra costs during the transition period and requires an effective configuration and assessment to ensure its effectiveness. This becomes even more complex when financial institutions are adopting new technologies to support their AML/CFT Compliance systems in order to identify suspicious activity more accurately and efficiently.

The FATF Report asserts that the application of AI/ML based tools that allow for real time, quick, and more accurate data analysis may offer the solution to the issues identified above.[116] Such tools can partially or fully automate the process of risk analysis, allowing it to take account of a greater volume of data, and to identify emerging risks that do not correspond to already-understood profiles.[117] Such tools can also offer an alternative means of identifying risks in effect, acting as a semi-independent check on the conclusions of traditional risk analysis.[118]

C. Ethical AI/ML

Fairness in the use of AI/ML is now and will continue to be an important and challenging issue to address, in part, because there are so many types of bias to consider.[119]

The AIPPF provides a granular analysis of the risks.[120] The following risks to consumers could also appear in a similar form for AML/CFT Compliance use cases:

- ***Financial Exclusion*:** AI/ML systems may prevent certain customers from accessing a financial product or service. They may restrict the ability of customers to get credit or insurance and their ability to access certain investment products or even their ability to enter a relationship with financial institutions. AI/ML systems may also prevent customers from enjoying one or more benefits that they can reasonably expect from an

based examination. These regulated financial institutions, therefore, focus on regulatory risk, not necessarily on financial crime risk.

[114] *See FATF Report*, *supra* note 62.

[115] *Id.*

[116] *Id.*

[117] *Id.*

[118] *Id.*

[119] *See* Ninareh Mehrabi, Fred Morstatter, Nripsuta Saxena, Kristina Lerman, and Aram Galstyan, *A Survey on Bias and Fairness in Machine Learning*, Univ. of S. Cal. Info. Sci. Inst. (USC-ISI) (Jan. 25, 2022), https://arxiv.org/pdf/1908.09635.pdf?trk=public_post_comment-text.

[120] *See AIPPF Report*, *supra* note 17, at 42.

existing product or relationship such as their claims against an insurance policy, their ability to make payments, or engage in other transactions.[121] An example of this type of risk could be where a person does not have the information the AI/ML software requires in cases where the AI/ML software was trained using customers who always have such information (e.g., a birth certificate or a driver's license). Certain older Americans, for instance, may not have a birth certificate and certain lower income Americans may not have a driver's license, a birth certificate, or other government issued identification with a photograph. Similarly, AI/ML training data biases could result in harms like undermining financial inclusion for already marginalized communities, essentially a type of algorithmic de-banking.[122] "The pursuit of AML objectives can undermine financial inclusion in several ways. First, barriers to accessing the financial system that aim to deter criminals can also make access to financial products cumbersome or costly for legitimate users. Second, incentives for financial institutions to avoid doing business with criminal entities can prompt them to avoid doing business with individuals perceived to be high risk, regardless of their actual criminal intent. This practice, known as "de-risking", undermines financial inclusion and tends to disproportionately impose costs on low-income communities such as those relying on remittance payments. De-risking may also undermine AML efforts by forcing individuals to find alternative financial partners that lack sufficient AML capacity."[123]

- ***Competition Concerns*:** Certain consumers may experience unfavorable commercial outcomes compared to others when applying for or using a product or service. This could affect pricing, penalties, product conditions, or level of collateral.
- ***Breaching Personal Data Rights of Customers*:** AI/ML systems may lead to incremental disclosure of protected data or inappropriate engagement with customers that go against previously agreed terms and conditions (e.g., when a customer's video call is used by an algorithm to detect emotions without explicit consent).

---

[121] The AML/CFT Compliance area may not be as useful of an application of AI/ML when discussing financial inclusion or financial exclusion because AI/ML in AML/CFT Compliance will always be subject to human review whether that is in the context of opening an account or closing an account. Similarly, human review will be involved during risk grading; inclusion on a watchlist; transaction monitoring; investigating suspicious activity; or filing a SAR. While AI/ML may make those determinations more efficient, AI/ML will not replace human judgment in these cases.

[122] See Robert Mahari, Thomas Hardjono, and Alex Pentland (edited by Julie Stahlhut and Kevin McDermont), *AML by Design: Designing a Central Bank Digital Currency to Stifle Money Laundering*, MIT Media Lab (Aug. 29, 2022) at https://www.media.mit.edu/articles/aml-by-design-designing-a-central-bank-digital-currency-to-stifle-money-laundering/ and https://sciencepolicyreview.org/wp-content/uploads/securepdfs/2022/08/MITSPR-v3-191618003020.pdf.

[123] *Id*. *See also* Vijaya Ramachandran, *Mitigating the Effects of De-Risking in Emerging Markets to Preserve Remittance Flows*, Int'l Fin. Corp. World Bank Grp. (Nov. 2016), https://openknowledge.worldbank.org/server/api/core/bitstreams/1540e935-2a94-5c91-b7c5-5bf33cefcc90/content and Tracey Durner and Liat Shetret, *Understanding Bank De-Risking and Its Effects on Financial Inclusion*, Glob. Ctr. on Coop. Security (Nov. 2015), https://www-cdn.oxfam.org/s3fs-public/file_attachments/rr-bank-de-risking-181115-en_0.pdf.

A challenge that financial institutions face is protecting customers from unethical consequences of AI/ML models, and any inexplicable decisions that may be undertaken. According to the FATF Report,[124] although algorithmic decision making is an alternative to human subjectivity and prejudice, researchers are discovering that many AI/ML algorithms replicate the conscious and unconscious biases of their program developers, which leads to unfairly targeting as suspicious the financial activities of certain types of individuals and producing risk profiles and decisions that deny them access to certain financial products and services.

Biases may infiltrate algorithms due to multiple reasons:

- Data containing skewed and biased human decisions, inequities, and prejudice hypotheses made during the design of AI/ML models may infiltrate algorithms. Data completeness issues can also amplify biases. For example, in most SAR filings there is rarely a single data point that can be identified to make a case suspicious because this information is generally absent from the analyzed datasets. Oftentimes, humans are required to connect the dots to validate if the activity is suspicious. It becomes challenging to ensure the absence of human biases during the correction of the completeness of the "facts."
- Preprocessing issues: AML/CFT Compliance data are imbalanced. This means that there is an unequal distribution of classes in the training dataset, (e.g., the number of observations of proven cases of money laundering is small as compared to other non-suspicious cases). This can result in poor performance, specifically for the investigations that actually revealed suspicious activity. To correct this problem, the process would have to be recalibrated by applying some balancing techniques such as over-sampling the lower number of cases or under-sampling the higher number of cases. Mistakes can be observed when under-sampling-and-over sampling the training dataset, generating bias in the data (the lower number of cases are completely ignored vs. over-representation of the higher number of non-suspicious cases).
- Facial recognition technologies (FRTs) are a notable example to illustrate potential algorithm biases.[125] In AML/CFT Compliance, FRTs enable streamlined biometric identification and authentication, strengthening the KYC and AML/CFT Compliance onboarding and verification processes. However, many FRTs have produced materially incorrect results.[126] "Of the dominant biometrics in use (fingerprint, iris, palm, voice, and face), face recognition is the least accurate and is rife with privacy concerns. Police use face recognition to compare suspects' photos to mugshots and driver's license images; it is estimated that almost half of American adults – over 117 million people, as of 2016 – have photos within a facial recognition network used by law enforcement.

[124] *See FATF Report*, *supra* note 62.

[125] There has been significant recent research that may mitigate some of the problems with FRTs. *See* Joyce Yang, Patrick Grother, Mei Ngan, Kayee Hanaoka and Austin Hom, *Face Analysis Technology Evaluation (FATE) Part 11: Face Image Quality Vector Assessment Specific Image Defect Detection*, NIST Internal Report NIST IR 8485, Image Grp. Info. Access Div. Info. Tech. Lab., U.S. Dep't of Com. (Sept. 2023), https://doi.org/10.6028/NIST.IR.8485.

[126] *See* Alex Najibi, *Racial Discrimination in Face Recognition Technology*, Harvard Univ. The Graduate Sch. of Arts and Sci.(Oct. 24, 2020), https://sitn.hms.harvard.edu/flash/2020/racial-discrimination-in-face-recognition-technology/.

> This participation occurs without consent, or even awareness, and is bolstered by a lack of legislative oversight.[127] More disturbingly, however, the current implementation of these technologies involves significant racial bias, particularly against Black Americans. Even if accurate, face recognition empowers a law enforcement system with a long history of racist and anti-activist surveillance and can widen pre-existing inequalities."[128]

There has been a worldwide debate[129] on the proper and ethical use of biometric surveillance.[130] While the inevitable growth of this technology in the coming years can play a major role in enhancing public security and safety, there is just as much justification to argue that the technologies are susceptible to error. These errors can create a myriad of fundamental rights issues from illegal discrimination to pervasiveness and intrusiveness.

Within the EU,[131] FRTs fall under the General Data Protection Regulation (GDPR)[132] definition of personal data, thus declaring that biometric data cannot lawfully be shared with third parties without their consent. It is, however, noted that exceptions do include where these data are necessary for social protection law, employment, and social security. The EU AI Act draft released by the Council of the European Union proposes increased requirements on high-risk AI/ML applications, which include FRTs.[133] For example, facial recognition by the police is banned unless the images are captured with a delay, or the technology is being used to find missing children.[134]

---

[127] *See* Jennifer Lynch, *Face Off, Law Enforcement Use of Face Recognition Technology*, Elec. Frontier Found. (Apr. 2020), https://www.eff.org/files/2020/04/20/face-off-report-2020_1.pdf.

[128] *Id*.

[129] While this debate has been occurring worldwide, most banks in the US do not yet use biometric surveillance in the context of AML/CFT Compliance, and it is not at all certain how this debate will play out in the US. *See Biometric Technologies and Global Security*, Cong. Rsch. Serv. (CRS Reports) (Updated Jan. 30, 2023), https://crsreports.congress.gov/product/pdf/IF/IF11783.

[130] *See Facial Recognition: for a Debate Living Up to the Challenges*, Nat'l Comm. On Informatics and Liberty (CNIL) (Dec. 19, 2019), https://www.cnil.fr/sites/cnil/files/atoms/files/facial-recognition.pdf; *see also*, Ján Lunter, *The Ethical Implications and Legal Responsibilities of Biometric Data Security*, Solutions Rev. (Aug. 24, 2022), https://solutionsreview.com/identity-management/the-ethical-implications-and-legal-responsibilities-of-biometric-data-security/.

[131] *EU AI Act Draft Developments*, Future of Life Inst. (FLI), https://artificialintelligenceact.eu/developments/.

[132] *See Council Regulation 2016/679*, *supra* note 106, at 75.

[133] *See EU AI Act Draft*, *supra* note 22.

[134] *Id.* at 44.

Recent developments[135] in the UK show the government's commitment to providing guidance instead of over-regulating FRT—exemplified by the Information Commissioner's Office's papers discussing law enforcement and commercial FRT use and U.K.'s National AI Strategy.[136]

In the U.S., for example, Portland and Baltimore have implemented a ban on the use of FRT for commercial operations such as loyalty program subscriptions, customer profiling, targeting, and using facial expressions while purchasing a product.[137] Portland's ordinance does not ban all uses of the technology but rather prohibits facial recognition from being deployed in "places of public accommodation."[138] FRT users are still allowed to deploy the technology in distinctly private areas, but are prohibited from using it anywhere that is open to the general public. Proposed legislation in Massachusetts, Oregon, and Washington would institute similar bans.[139] On the other hand, Baltimore's recently enacted ban is much stricter in legislating that no individual or corporation—including the mayor and city council—can use any face surveillance system or information obtained from such a system.[140]

D. Explainable AI/ML

Multiple AI/ML systems are difficult to understand and interpret. It becomes challenging for experts within the AI/ML field to understand the logical explanation of the outputs and decisions of the algorithms. A model needs to be explainable to AML/CFT Compliance Officers, business users, auditors, regulatory bodies, and anyone else who is affected by its decisions.

The Autorité de Contrôle Prudentiel et de Résolution, Banque de France (ACPR),[141] the French Prudential and Resolution Authority, indicates that explainability "...encompasses

---

[135] *See* Taylor Kay Lively, *Facial Recognition in the US: Privacy Concerns and Legal Developments*, Asis Int'l (Dec. 1, 2021), https://www.asisonline.org/security-management-magazine/monthly-issues/security-technology/archive/2021/december/facial-recognition-in-the-us-privacy-concerns-and-legal-developments/.

[136] *National AI Strategy*, Sec'y of State for Digital, Culture, Media and Sport, HM Gov. (Sept. 2021), https://assets.publishing.service.gov.uk/media/614db4d1e90e077a2cbdf3c4/National_AI_Strategy_-_PDF_version.pdf.

[137] *See* Benjamin Stein, *Baltimore Bans Private Use of Facial Recognition Technology*, InfoLawGroup LLP (Aug. 27, 2021), https://www.infolawgroup.com/insights/baltimore-biometrics-ordinance-2021 and Benjamin Stein, *Portland's Facial-Recognition Ban Sees its First Lawsuit; Baltimore's Ban Expires*, InfoLawGroup LLP (Jan. 24, 2023), https://www.lexology.com/library/detail.aspx?g=56cb29c0-a933-4442-bad9-cd31cee7f462.

[138] *Id.*

[139] *Id.*

[140] The Baltimore ordinance was controversial and automatically expired on December 31, 2022, because there were not enough votes to renew it.

[141] ACPR is an independent administrative authority that exercises supervision of regulated French financial firms such as banks and insurance companies. It operates under the Bank of France.

two questions. On the one hand the "why" i.e., the question of transparency: the main associated issue is auditability. On the other hand, the "how" i.e., the question of interpretability, which affects the intelligibility of the system's behavior by human operators interacting with it and by customers, as well as social or ethical acceptance."[142]

Explainable AI/ML methods are varied and should be adapted to the considered stakeholders.[143] In the report, *Governance of Artificial Intelligence in Finance*, published in June 2020 by the ACPR, the objectives of an explanation are considered to vary greatly depending on the type of recipient targeted, and are summarized as the following:[144]

- Providing insights to domain experts and compliance teams.
- Facilitating the model's review by the engineering and validation teams.
- Securing confidence from the individuals impacted by the model's predictions or decisions.

---

[142] *See* Laurent Dupong, *ACR Tech Sprint on the Explainability of Artificial Intelligence*, at p. 3, ACPR Banque de France (Jan. 2022), https://acpr.banque-france.fr/en/acpr-tech-sprint-explainability-artificial-intelligence.

[143] *See* David Gunning, *Explainable Artificial Intelligence*, George Wash. Univ. (GWU) (Nov. 2017), https://nsarchive.gwu.edu/sites/default/files/documents/5794867/National-Security-Archive-David-Gunning-DARPA.pdf; Adam Zewe, *Building Explainability into the Components of Machine-Learning Models - Researchers Develop Tools to Help Data Scientists Make the Features Used in Machine-Learning Models More Understandable for End Users*, MIT News (June 30, 2022), https://news.mit.edu/2022/explainability-machine-learning-0630; P. Jonathon Phillips, Carina A. Hahn, Peter C. Fontana, Amy N. Yates, Kristen Greene, David A. Broniatowski and Mark A. Przybocki, *Four Principles of Explainable Artificial Intelligence*, NISTIR 8312, Nat'l Inst. of Standards and Tech., U.S. Dep't of Com. (Sept. 2021), https://doi.org/10.6028/NIST.IR.8312; David A. Broniatowski, *Psychological Foundations of Explainability and Interpretability in Artificial Intelligence*, NISTIR 8367, Nat'l Inst. of Standards and Tech., U.S. Dep't of Com. (Apr. 2021), https://doi.org/10.6028/NIST.IR.8367 and Duke Law Sch. and Thomson Reuters, *White Paper: Addressing Bias in Artificial Intelligence - The Current Regulatory Landscape*, Thomson Reuters (2023), https://www.thomsonreuters.com/en-us/posts/wp-content/uploads/sites/20/2023/08/Addressing-Bias-in-AI-Report.pdf. Collectively, these publications demonstrate the importance of explainability. The White Paper, for example, stresses the importance of explainability. "Through this concept of explainability, those affected by AI systems can both understand the outcome of AI decisions and challenge these outcomes where relevant." For AML/CFT Compliance Officers, this is a critically important point because regulatory agencies show strong support for requiring explainability, at some point explainability will be considered a best practice industry wide, and leading standard setters, including the FFIEC and NIST, support explainability. Finally, while courts have not yet addressed explainability in a material way, it is inevitable that they will be asked to do so.

[144] *See* Laurent Dupong, et al, *Governance of Artificial Intelligence in Finance*, ACPR Banque de France (June 2020), https://acpr.banque-france.fr/sites/default/files/medias/documents/20200612_ai_governance_finance.pdf.

Implementing Explainable AI/ML can become a challenge because it can be difficult to understand when the explainability is required, and what techniques and level of explainability are to be used. The two most common methods of explainability are:

- "Local explanatory methods provide an explanation for a decision made on a particular input data point (for instance, why a given credit application was granted to the applicant)."[145]
- "Global explanatory methods attempt to simultaneously explain the entirety of possible decisions (in this case, what are the general characteristics of the respective outcomes – acceptance or denial – of credit applications)."[146]

When Explainable AI/ML approaches and frameworks are deployed correctly, they promote regulatory transparency, add confidence in the final outputs, increase confidence of AML/CFT Compliance Officers in handling the AI/ML decisions, and help assess biases and other risks that might negatively affect the model. The FATF Report emphasizes that difficulties with the explainability and interpretability of digital solutions are key challenges for both industry and regulators that, in part, stem from the limited availability of relevant expertise and a lack of awareness of the potential of innovative technologies among AML/CFT Compliance Officers, both in industry and government.[147]

The interpretability and explainability of new technologies to prudential supervisors are key to securing support for these tools. Regulated entities must be able to explain, and remain responsible for, the principles and technical details of the innovative solutions before deploying those new technologies. Prudential supervisors must be able to understand the models used by AI/ML tools in order to determine their accuracy and their relevance to the identified risks.[148] Interpretability can come with a statistical cost in AI/ML and trigger potential trade-offs between accuracy and explainability. While added explainability enhances the opportunity to verify and contest a decision, it could also increase the probability of error due to a decrease in model accuracy and performance. AI/ML models that are considered to have higher performance are often based on more complex algorithms; as a result, they may lack sufficient interpretability or explainability and vice versa. The right balance should be reached, and the tradeoff decision should integrate the risk appetite of the financial institutions with regard to the implemented use cases.

E. Effectively Training and Maintaining AI/ML Models Based upon Ever-Involving Conditions

There is a general consensus that models only work if they are properly trained and maintained. In the absence of real-world cases, financial institutions must identify the proper method to train a model, and, in the face of rapidly changing conditions (data quality and distribution, behavior changes, model decay, feedback loops, model improvement, and other conditions), the frequency that a model should be trained. FATF has pointed out that the use of new technologies for AML/CFT Compliance can only truly become effective if systems are based on standardized data that are easier for technology developers to integrate into their tools,

[145] *Id.* at §11.3.

[146] *Id.*

[147] *See FATF Report*, *supra* note 62.

[148] *Id.*

easy to understand and explain to non-experts, and easy to communicate to counterparts and competent authorities when needed.[149] This issue also shows the importance of public authorities, particularly financial intelligence units such as FinCEN, providing reliable feedback to reporting entities on suspicious activity and AML/CFT Compliance cases that can be used for training purposes.[150] Training an AI/ML system based on real cases that have been verified as involving AML/CFT Compliance – if these were available – would offer a significantly better hit rate than training an AI/ML system to replicate the decisions of a human AML/CFT Compliance Officer about whether the appropriate suspicion threshold has been met.[151]

F. Cautious Regulatory Agency Support

In general, financial institutions have moved cautiously to identify and implement AI/ML in their AML/CFT Compliance Programs because they fear regulatory directives on the emerging technologies used. While many regulators recognize the potential benefits of using AI/ML in AML/CFT Compliance Programs, many also remain neutral or at least cautious because of the potential challenges of the implementation of AI/ML solutions.[152] This cautious approach, in part, may be the reason some financial institutions have expressed the view that more guidance is needed on AI/ML in AML/CFT Compliance.[153] Regulatory agency

[149] *Id.*

[150] *Id.*

[151] *Id.*

[152] An example of regulatory agency cautiousness is reflected by the June 16, 2023, remarks from the Acting Comptroller of the Currency: "How should banks and regulators approach rapid, potentially transformative innovations like tokenization and AI prudently? It helps to bear in mind three principles: (1) innovate in stages, (2) build the brakes while building the engine, and (3) engage regulators early and often. Innovating in stages requires discipline. The concept is simple: start with what can be controlled, expand only when ready, monitor carefully, adjust, and repeat... To build the brakes while building the engine, risk and compliance professionals need to be at the innovation table and have their voices heard. In the technology space, speed to market is an important factor in innovation. Slowing things down is seen as anti-innovative. Structurally and culturally, this casts the risk and compliance functions as barriers to innovation. In less regulated institutions, they tend to be ignored or pushed aside… There is a better way: by giving risk and compliance professionals a seat at the innovation table from the get-go and heeding their input. Empowering them to identify risks and risk mitigants will help ensure that the products and services that result will be safe, sound, fair, and trusted. This is what supervisors and the public expect, and it makes good long-term business sense. Asking for permission, not forgiveness, from regulators will help ensure the longevity of rapid and transformational innovations. The pressure to be a first mover and take advantage of network effects can incentivize firms to release first and engage with regulators later. This "ask for forgiveness" approach may work in certain technology contexts. But it doesn't work in banking and finance, where public trust is critical to long-term product success, and regulatory approval is a proxy for that trust." *See M. Hsu Remarks*, *supra* note 32.

[153] As indicated in this report, only the largest financial institutions are likely to have the resources and human capital to spend testing an AI/ML in AML/CFT Compliance approach over the length of time (i.e., years) necessary for regulatory agencies to become comfortable

cautiousness and industry mixed signals may also be the reason policymakers have been unsure how to address AI/ML, especially in AML/CFT Compliance. This problem is even more difficult for financial institutions that use AI/ML across borders because it is often extremely difficult to navigate or reconcile inconsistencies between and among multiple jurisdictions. FATF has made it clear that it is imperative that regulatory agencies on a global scale coordinate with these innovative technologies and continue to build the necessary knowledge and experience in AI/ML in AML/CFT Compliance.

G. Other Governance[154] Issues

As they adopt AI/ML in AML/CFT Compliance, financial institutions should put in place AI/ML governance frameworks, and review and refine existing ones. It can be challenging to build AI/ML governance frameworks that help financial institutions learn, govern, monitor, and mature AI/ML adoption:

- Careful consideration should be given to what AI/ML use cases should be prioritized. Those use cases can fail if proper scoping is not performed, leading to major operational and financial losses.
- Financial institutions might face challenges to ensure that sufficient oversight, challenge, and assurance requirements are met in AI/ML development and usage. This requires a solid development, validation, and testing approach, in addition to audit and documentation.
- Most financial institutions follow a three lines-of-defense model:
  - 1st Line of Defense (1LOD): Accountability of risks by the business;
  - 2nd Line of Defense (2LOD): Independent risk oversight and compliance monitoring, including AML/CFT Compliance Officers; and
  - 3rd Line of Defense (3LOD): Audit[155] and Assurance functions.
- Roles and responsibilities should be clearly defined within each line of defense and between the lines of defenses to ensure the right segregation of duties.

The AIFR points out that "there is an increase in the importance of monitoring for AI systems, but this is not always considered enough of a priority, especially during model

with such an approach. To date, pilot programs have been rather narrow, and in some cases, it has been difficult to obtain approval for pilot programs.

[154] AI/ML governance issues are a constant challenge across the board. For a more detailed discussion of the governance challenges in AI/ML, *see The Current State of AI Governance*, BABL AI Inc. & The Algorithmic Bias Lab (Mar. 13 2023), https://babl.ai/wp-content/uploads/2023/03/AI-Governance-Report.pdf.

[155] *See The IIA's Artificial Intelligence Auditing Framework Practical Applications - Part A Special Edition*, Inst. for Internal Auditors (IIA) Glob. Perspectives and Insights (Dec. 2017); and the IIA has subsequently revisited its framework, *see The Artificial Intelligence Revolution Part 2: Revisiting The IIA's Artificial Intelligence Framework*, IIA (Aug. 2023), https://www.theiia.org/en/content/articles/global-knowledge-brief/2023/august/the-artificial-intelligence-revolution-part-2-revisiting-the-iias-artificial-intelligence-framework/?_cldee=JPL7PTmVDvuQDv41GeY7iYLMAg65idUS8AUdk3-fs0VPf6ownK9i4iLoXa9Q-0zp&recipientid=contact-79ae810d9aa7487a9df647e9def0dc7e-fab191e95d8c422990a8563f82d525fd&utm_source=ClickDimensions&utm_medium=email&utm_campaign=MEM_Int_Standard&esid=4faf8e0d-eb48-ee11-a30d-00155dc12098.

validation stages. The validation step itself should ensure that there is appropriate monitoring in place for the model. Differentiating between validation and ongoing monitoring is important for managing AI model risks, especially because the latter may need to be real-time for certain AI models and conducted by 1LOD functions. Traditionally this was done periodically by the 3LOD and audit functions – an approach that may no longer be effective."[156] Striking the right balance between the scope of different lines of defenses can be challenging. This is often made more difficult in the monitoring of AI/ML systems due to the lack of relevant model risk and validation skills in the 1LOD teams, and lack of data science and AI skills in the 2LOD functions.

AI/ML deployment may involve third party vendors.[157] As a result, financial institutions are required to strengthen their third-party risk management strategy on aspects such as transparency and model interpretability; IT security issues; and other potential technology dependencies.[158]

Finding adequate human resources might add complexity to AI/ML implementation because it is not always easy to find the necessary subject matter expertise required to implement, challenge, and evaluate AI/ML systems effectively. Financial institutions should pay close attention to human-machine interaction because humans are involved in all steps of AI/ML models development, improvement, and usage. Further understanding of how humans and machines can better collaborate is key. Humans must remain in control in order to monitor and control risk.

Financial crime techniques are becoming more sophisticated and ensuring that models have a high performance (i.e., their predictions are accurate in production) can be very challenging. Financial institutions should enable the AI/ML in AML/CFT Compliance monitoring systems to adapt to any changes in behavior, technology, or in the financial institution (e.g., data distribution changes and population shifts in the training population; data quality issues; and decrease of model performance).

---

[156] *See AIPPF Report*, *supra* note 17, at 25-26.

[157] In some cases, there are heightened areas of risk where third-party vendors are deployed. For instance, in banking as a service (BaaS) models, often the third-party vendors are able to access bank products and services, but the bank itself may not have access to the customer and is dependent on the third-party vendor for KYC, due diligence, ongoing monitoring, and identifying suspicious transactions. Prudential supervisors are not likely to support this approach. "Depending on the specific circumstances, including the activities performed, such relationships may introduce new or increase existing risks to a banking organization. For example, in some third-party relationships, the respective roles and responsibilities of a banking organization and a third party may differ from those in other third-party relationships. Additionally, depending on how the business arrangement is structured, the banking organization and the third party each may have varying degrees of interaction with customers." *See Interagency Guidance on Third-Party Relationships: Risk Management*, OCC (June 6, 2023), https://www.occ.gov/news-issuances/news-releases/2023/nr-ia-2023-53a.pdf.

[158] These issues are often more serious when the third-party vendor does not have either a strong AML/CFT Compliance Program in place or is unregulated.

IV. Emerging Trends and Issues[159]

A. Do Third-Party Vendor AI/ML Solutions Provide Better Answers?

There is an extremely wide variety of third-party vendors who propose advanced solutions based on AI/ML for advanced AML/CFT Compliance systems. Using a third-party solution can be very tempting, but it can also expose the business to new risks and failures. US financial institutions should follow closely the Interagency Guidance on Third-Party Relationships: Risk Management (June 6, 2023)[160] and conduct a detailed risk assessment and consider multiple factors before choosing a third-party vendor solution.[161]

B. How Should Financial Institutions Address Metrics and Benchmarks?

In many cases, investing in AI/ML solutions will likely be both necessary and expensive. In the process, financial institutions should be able to:

- Establish short-term and long-term expectations linked to the implemented AI/ML use cases. Unrealistic expectations can hamper the project's performance and set it up for failure.
- Define metrics as a means to evaluate the effectiveness of the use of AI/ML systems in AML/CFT Compliance by financial institutions.[162]
- Establish benchmarks to identify the best-performing technologies in the industry.

C. Are the Current Laws and Governmental Agency Guidance Enough?

There is a consensus that current laws and governmental agency guidance have not kept pace with the speed of innovation. There is, however, a disagreement over whether new laws and new regulatory agency guidance could help or hurt the speed with which innovative

[159] This is not intended to be an exhaustive list of emerging trends and issues. Rather these are some of the major trends that AML/CFT Compliance Officers should follow.

[160] See Interagency Guidance on Third-Party Relationships: Risk Management, https://www.govinfo.gov/content/pkg/FR-2023-06-09/pdf/2023-12340.pdf.

[161] While it can be asserted that the Interagency Guidance does not have the force of law and is not required to be followed, such a position is extremely risky because examiners will follow the guidance and a bank's failure to do so could still lead to an examiner's conclusion that the bank acted in an unsafe and unsound manner.

[162] AML/CFT Compliance Officers should tailor the metrics and benchmarks needed for the use of AI/ML in AML/CFT Compliance to the risk profile and risk appetite of the financial institution. There is no currently available consensus on what to measure or what benchmarks to use. For more information on metrics and benchmarks in AI/ML, AML/CFT Compliance Officers may consider reviewing the NIST Workshop in June 2021, *see NIST Workshop on AI Measurement and Evaluation*, NIST (2021), https://www.nist.gov/news-events/events/2021/06/ai-measurement-and-evaluation-workshop.

technologies advance and the extent to which policymakers should tailor new laws to the specific technologies or apply current laws to new technologies. There is also disagreement regarding whether current governmental agency guidance is sufficient. In many cases, stakeholders have submitted comment letters to lay out the best guidance to policymakers and regulatory agencies.

As of the date of this analysis, there is no dedicated law in the US that regulates AI/ML comprehensively.[163] In fact, in the US, several organizations such as IBM and Open AI, and academics, have expressly requested the US government to regulate AI/ML.[164] Governments are working on AI/ML strategies and laws, but most AI/ML systems remain regulated, if at all, by other existing regulations (e.g., data and consumer protection or market competition laws).[165] There are examples of AI/ML guidance in the U.S. that are meant to be broadly applicable to the use of AI/ML. For instance, on January 7, 2020, the White House's Office of Science and Technology Policy released a draft *Guidance for Regulation of Artificial Intelligence Applications*, including ten principles for government agencies to consider when proposing new AI/ML regulations.[166] The main goals of the principles are to ensure engagement with and education of the general public; prevent any overreach or potential overregulation; and promote trustworthy AI/ML that is fair, transparent, and safe.[167] More recently, the White House released a 2023 strategic plan on artificial intelligence research and development.[168]

---

[163] In the absence of the comprehensive regulation of AI/ML at the federal level, many states have entered the field, adding to the uncertainty related to legal aspects of AI/ML. This also means that in many cases courts have stepped in to provide clarity. *See* George Wash. Univ. Law Sch. AI Litigation Database, https://blogs.gwu.edu/law-eti/ai-litigation-database/.

[164] *See* the written and oral testimony of Samuel Altman, CEO, OpenAI; Christina Montgomery, Chief Privacy & Trust Officer, IBM; and Gary Marcus, Professor Emeritus, New York University before the US Senate Committee on the Judiciary, Subcommittee on Privacy, Technology, and the Law. *See Oversight of A.I.: Rules for Artificial Intelligence*, U.S. Senate Comm. On the Judiciary (May 16, 2023), https://www.judiciary.senate.gov/committee-activity/hearings/oversight-of-ai-rules-for-artificial-intelligence.

[165] For an analysis of international laws and regulations covering AI/ML, *see Regulation of Artificial Intelligence Around the World.* Washington, D.C.: The Law Library of Congress, Glob. Legal Rsch. Directorate, (2023), https://www.loc.gov/item/2023555920/ and *see also*, *the Global AI Legislation Tracker*, IAPP Rsch. and Insights (Aug. 2023), https://iapp.org/media/pdf/resource_center/global_ai_legislation_tracker.pdf.

[166] *See* Russell Vought, *Guidance for Regulation of Artificial Intelligence Application*, Off. of Mgmt. and Budget, Exec. Off. of the President (Nov. 17, 2020), https://www.whitehouse.gov/wp-content/uploads/2020/11/M-21-06.pdf. *See also Blueprint for an AI Bill of Rights Making Automated Systems Work for the American People*, White House Off. of Sci. and Tech. Policy (Oct. 2022), https://www.whitehouse.gov/wp-content/uploads/2022/10/Blueprint-for-an-AI-Bill-of-Rights.pdf.

[167] *Id.*

[168] *See National Artificial Intelligence Research and Development Strategic Plan 2023 Update: A Report by the Select Committee on Artificial Intelligence of the National Science*

As discussed above, both the FFIEC and NIST have regularly provided valuable guidance. Policymakers in the U.S. House Financial Services Committee and the U.S. Senate Committee on the Judiciary Committee have held hearings on the use of AI/ML but have not yet reached any bipartisan agreements that would pass either committee.

The regulation of AI/ML also has been particularly challenging for states[169] because AI/ML regulation is unlikely to be effective or helpful if the laws are inconsistent. If some states decide to attract AI/ML business or promote innovation by using a light touch and other states decide to regulate AI/ML restrictively or manage innovation, then either or both approaches could lead to unhelpful or harmful consequences.

In China, a new set of regulations has been in place since March 2022. Those regulations aim to restrict the use by tech companies of algorithmic recommendations and provide more moral, ethical, fair, accountable, explainable, and transparent AI/ML algorithms.[170]

Perhaps the leader on legislating AI/ML is the EU.[171] On December 9, 2023, the European Parliament and the Council of the European Union announced a provisional agreement regarding the EU AI Act draft. In April 2021, the European Commission submitted its proposal for a European Union regulatory framework on AI; on December 9, 2023, the European Council updated the status of the EU AI Act, confirming on February 2, 2024 that a final compromise agreement had been reached.[172] The regulation could be the start of a global

---

and Technology Council, The White House, (May 2023), https://www.whitehouse.gov/wp-content/uploads/2023/05/National-Artificial-Intelligence-Research-and-Development-Strategic-Plan-2023-Update.pdf.

[169] *See AI Decision-Making Poses Unique Challenge for State Legislators, Regulators*, LexisNexis State Net Insights (Apr. 21, 2023), https://www.lexisnexis.com/community/insights/legal/capitol-journal/b/state-net/posts/ai-decision-making-poses-unique-challenge-for-state-legislators-regulators. "As of mid-April,144 measures containing the phrase "artificial intelligence" had been introduced in 33 states since the start of 2023, according to the LexisNexis® State Net® legislative tracking database. About 30 of the bills appear to deal substantially with AI governance or AI ethics issues—that is, with the automatic decision-making capabilities of AI which pose some of the thorniest problems for the technology."

[170] *See* Arjun Kharpal, *Chinese tech giants share details of their prized algorithms with top regulator in unprecedented move* (August 15, 2022), https://www.cnbc.com/2022/08/15/chinese-tech-giants-share-details-of-their-algorithms-with-regulators.html.

[171] On June 14, 2023, the European Parliament approved the world's first comprehensive regulation of AI/ML, the Proposal, *see Regulation of The European Parliament and of The Council Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts Com/2021/206 final*, EUR-Lex(EU) (Apr. 21, 2021), https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52021PC0206.

[172] *See* Council of the EU, Artificial intelligence act: Council and Parliament strike a deal on the first rules for AI in the world (December 9, 2023 updated February 2, 2024), https://www.consilium.europa.eu/en/press/press-releases/2023/12/09/artificial-intelligence-act-council-and-parliament-strike-a-deal-on-the-first-worldwide-rules-for-ai/.

standard for AI/ML oversight around the world through a potential "Brussels effect."[173] The EU AI Act proposes a risk-based approach to categories AI/ML use, and suggests extra checks for "high risk" uses that are likely to harm the health and safety or fundamental rights of natural persons (e.g., HR systems for recruitment; systems that help make decisions about law and justice; and medical monitoring).[174] The EU AI Act also prohibits some AI/ML uses like emotion recognition; discriminatory forms of biometric categorization; remote biometric identification; predictive policing systems; and the use of facial recognition in public places by law enforcement agencies.[175] The EU AI Act aims to protect humans from the worst side effects of AI/ML by ensuring accountability and transparency to the public as to which AI/ML systems are used, when, and for what purpose.[176] Likewise, the UK has taken a "pro-innovative approach" to regulating AI/ML.[177]

D. Can AI/ML Models Be Improved with Synthetic Data?

A key quality to the successful implementation of AI/ML in any industry is having both a historic and an up-to-date dataset from which the model may learn. Oftentimes, the issue is that very few financial institutions have a large enough database to train an algorithm. Data sharing between financial institutions or even internal departments can be difficult due to the sensitivity of information as well as regulations such as the GDPR or other restrictions in law.[178] In order to overcome this barrier and be able to integrate this technology effectively, the concept of synthetic data[179] to supplement AI/ML model development has been used. Synthetic data represents an abstraction of real data through its artificial creation of anonymizing original data, thus enabling them to be shared. Overall, an advantage of synthetic

---

[173] *See* Alex Engler, *The EU AI Act Draft Will Have Global Impact, But A Limited Brussels Effect*, Brookings (June 8, 2022), https://www.brookings.edu/articles/the-eu-ai-act-will-have-global-impact-but-a-limited-brussels-effect/.

[174] *See EU AI Act Draft*, *supra* note 22.

[175] *Id.*

[176] *Id.*

[177] *See* UK Government Policy paper, *A Pro-Innovative Approach to AI Regulation* (Mar. 29, 2023), https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1146542/a_pro-innovation_approach_to_AI_regulation.pdf and UK Information Commissioner's Officer *UK GDPR Guidance on AI and Data Protection* (Mar. 15, 2023), https://ico.org.uk/media/for-organisations/uk-gdpr-guidance-and-resources/artificial-intelligence/guidance-on-ai-and-data-protection-2-0.pdf.

[178] In the U.S., FinCEN permits certain financial institutions to share AML/CFT information that might be relevant to the use of AI/ML in AML/CFT Compliance such as the voluntary information sharing under Section 314b. *See 314b Fact Sheet*, FinCEN (Dec. 2020), https://www.fincen.gov/sites/default/files/shared/314bfactsheet.pdf.

[179] *See* Brian Eastwood, *What Is Synthetic–Data - And How Can It Help You Competitively?* MIT Management Sloan School (Jan. 23, 2023), https://mitsloan.mit.edu/ideas-made-to-matter/what-synthetic-data-and-how-can-it-help-you-competitively; Victor Dey, *How Synthetic Data Is Boosting AI at Scale*, Venture Beat (Mar. 15, 2023), https://venturebeat.com/ai/synthetic-data-to-boost-ai-at-scale/; Kim Martineau, *What Is Synthetic Data?* IBM (Feb. 8, 2023), https://research.ibm.com/blog/what-is-synthetic-data.

data is the scalable generation of additional data, which is a crucial input for AI/ML-based models. The application of these data also overcomes the issue of data privacy making it much easier for businesses to integrate AI/ML. However, synthetic data must accurately reflect realistic, fair, and accurate cases that affect real life human activity and transactions. Synthetic data must be properly trained, tested, and audited.

E. Is Information Sharing a Global AML/CFT Compliance Priority?

In general, and in the U.S. particularly, data sharing between financial institutions can have wider benefits by strengthening the understanding of global risks and vulnerabilities and providing an overall picture of the activities and transactions of customers with other financial institutions.[180] FATF Guidance on Private Sector Information Sharing considers data and information sharing critical for AML/CFT Compliance because multinational money laundering and terrorist financing schemes do not respect national boundaries. Barriers to information sharing may negatively impact the effectiveness of the efforts of AML/CFT Compliance Programs and conversely, inadvertently facilitate operations of such multinational criminal networks. This underscores the importance of having rapid, meaningful, and comprehensive sharing of information from a wide variety of sources, across the national and global scale. FATF has asserted that sharing information is key to promoting financial transparency and protecting the integrity of the financial system by providing financial institutions, and relevant competent authorities, the intelligence, analysis, and data necessary to prevent and combat money laundering and terrorist financing.[181]

Governments around the world have implemented information sharing initiatives:

- In the U.S., Section 6103 of the AMLA establishes the FinCEN Exchange to facilitate a voluntary public-private information-sharing partnership between law enforcement agencies, national security agencies, financial institutions, and FinCEN.[182]
- The Joint Money Laundering Intelligence Taskforce in the UK is a partnership between law enforcement and the financial sector to exchange and analyze information relating to money laundering and wider economic threats.[183]
- The UK Government Statement on Cross-border Information Sharing within Corporate Groups advised regulated entities of when it is acceptable to share information and set

[180] Data sharing will always be a challenge because data sharing raises many legal and social issues, and there are embedded structural barriers that must be addressed. *See* Gillian Diebold, *Overcoming Barriers to Data Sharing in the United States*, Ctr. for Data Innovation (Sept. 25, 2023), https://www2.datainnovation.org/2023-data-sharing-barriers.pdf.

[181] *See* FATF, *FATF Guidance - Private Sector Information Sharing* (Nov. 2017), https://www.fatf-gafi.org/en/publications/Fatfgeneral/Guidance-information-sharing.html.

[182] *See* AMLA, *supra* note 12.

[183] *See Improving the UK's Response to Economic Crime*, Nat'l Econ. Crime Ctr (NECC), Nat'l Crime Agency (NCA), https://www.nationalcrimeagency.gov.uk/what-we-do/national-economic-crime-centre.

out guidance on the cross-border sharing of information within corporate groups for the purpose of tackling economic crime.[184]

However, such information sharing can also raise a range of public policy concerns about how the information will be used, including confidentiality; data protection and privacy; and other general information sharing challenges. Modern techniques are being developed to bring responses to the identified risks, and to protect data from unauthorized access, and secure them in a way that allows sharing and analyzing without exposing them to breach risks.

F. How Are Tech Sprints Used to Enhance AI/ML in AML/CFT Compliance Programs?

To keep up with technological development and innovations, policymakers are exploring new approaches to frame technological innovation and its development. Many regulators encourage cooperation, and work to bring together financial institutions, financial technology companies, regulatory technology companies, and other vendors through creating regulatory sandboxes, innovation hubs, and the use of Tech Sprints.[185] Tech Sprints bring together participants from outside traditional financial services to create and develop proof of concepts as well as technology-based ideas. These events are effective in raising awareness of issues and creating potential solutions. Many of these Tech Sprints are open to a wide range of participants, and foster innovation through collaboration. The combination of different fields and backgrounds in one forum encourages an innovation of ideas that is ideal for exploring new territory such as AI/ML for AML/CFT Compliance use cases. Similarly, Tech Sprints help AML/CFT Compliance Officers see in real time the many problems associated with advanced technologies, and even a cursory review of the "tickets" created by the technology staff shows gaps in coverage; information asymmetries; timing flaws; API limitations; and record keeping challenges.

The use of Tech Sprints has proven to be so successful that regulators in the U.S. and UK not only encourage them, but also host them. Key outcomes from Tech Sprints both benefit the participants, and, when the results are made public, benefit the public at large. From a regulatory point of view, this signals interest in issues requiring industry-wide collaboration in order to innovate responsibly. Tech Sprints could be a laboratory for AML/CFT Compliance Officers to field test the use of technology, including AI/ML in AML/CFT Compliance Programs. Another outcome from Tech Sprints is the creation of new partnerships and relationships resulting in powerful cross border networks.

Government agencies, especially in the U.S. and Europe, have increasingly turned to Tech Sprints to help inform their decisions regarding AI/ML systems, including in AML/CFT Compliance. In the US, those agencies have included the DFS, the OCC, the Federal Reserve,

---

[184] *See Government Statement on Cross-Border Information-Sharing within Corporate Groups*, HM Treasury, (UK) (May 12, 2020), https://assets.publishing.service.gov.uk/media/5eb413f3d3bf7f5d3c74a2b2/Corporate_Group_Cross-Border_Sharing_-_public_statement_for_publication.pdf.

[185] *See* The Federal Reserve, OCC, and FDIC, *Joint Statement on Crypto-Asset Policy Sprint Initiative and Next Steps*, The Fed (November 23, 2021), https://www.federalreserve.gov/newsevents/pressreleases/files/bcreg20211123a1.pdf.

the FDIC, FinCEN, and OFAC. In Europe, those governments include France and the UK.[186] In May 2022, the UK FCA hosted its first ever CryptoSprint, engaging with the industry to seek industry views around the current market and design of an appropriate regulatory regime.[187] The goal of the program was to create industry engagement to develop a dynamic framework that supports innovation while protecting consumers. Additionally, in September 2022, the FCA held a joint Tech Sprint with the Payment Systems Regulator on Authorized Push Payment (APP) Fraud, which increased dramatically during the pandemic.[188] The Tech Sprint was focused on exploring solutions to identify and prevent APP Fraud, such as the identification of suspicious social media and fraudulent advertisement.[189]

In France, the ACPR held its first Tech Sprint between June and July 2021. The challenge was generating explanations to understand the behavior of credit risk predictive models based on AI/ML and only accessible as "black boxes."[190] The ACPR's Fintech-Innovation Hub acted as creator, organizer, and facilitator of the event – sometimes known as a regulatory hackathon. In doing so, it collaborated with four voluntary credit institutions that designed and trained AI/ML models on an agreed-upon use case, namely predicting which loans to individual customers are likely to default. Tech Sprint participants included professionals from fintech firms, banks, and other financial actors, as well as researchers and students in data or computer science. Those participants teamed up to play the role of "analysts." Their primary task was explaining the behavior of the predictive models and elucidating their nature and characteristics.[191]

V. Conclusion and Observations

While AML/CFT Compliance is required by law to be a priority for all regulated financial institutions, not all regulated financial institutions have the resources to use the most innovative technologies such as AI/ML to upgrade their AML/CFT Compliance Programs. This is an important issue, in part, because advances in technology, especially advances in AI/ML, are expected to continue to accelerate and improve the technology options available to AML/CFT Compliance Officers.[192] The enactment of AMLA and its implementing regulations, and the strong voice of FATF, are important in urging the modernization of AML/CFT Compliance Programs, including through the use of innovative technologies such as AI/ML. Whether or when AI/ML will be fully embraced in AML/CFT Compliance, however, likely will not be determined by either AMLA or FATF. Rather, each regulated

[186] *See CryptoSprint Outputs*, Fin. Conduct Authority (FCA), https://www.fca.org.uk/firms/cryptoassets/cryptosprint (last updated Feb. 23, 2023).

[187] *Id.*

[188] *See Authorised Push Payment Fraud Tech Sprint*, Payment Systems Regul. (PSR), https://www.psr.org.uk/news-and-updates/events/authorised-push-payment-fraud-techsprint/.

[189] *Id.*

[190] *See generally*, the discussions in § IV.F of this report.

[191] *Id.*

[192] *See GPT-4 Technical Report*, OpenAI (2023) (Mar. 27, 2023), https://arxiv.org/pdf/2303.08774.pdf.

financial institution will have to determine the degree to which it uses technologies such as AI/ML to enhance its AML/CFT Compliance Programs.

Some of the largest financial institutions have invested in AI/ML in their AML/CFT Compliance Programs because they concluded that AI/ML represents an integral solution to the multiple challenges they face in the AML/CFT Compliance area. For most smaller regulated financial institutions and even some of the largest financial institutions, there are simply too many areas of uncertainty and challenges, notwithstanding the numerous identified AI/ML opportunities. These uncertainties and challenges include, among other things, uncertainty around the regulatory framework; technical challenges related to the quality of the data and IT systems; explainability and model validation processes; what to do with legacy systems; the risk of bias and loss of control of the process; and the many human resources challenges.

It is likely that some of these concerns will be addressed in the short term because of the increased and frequent research, and the advances in technology, which are evolving at a rapid rate. The expectation is that the research and the advances in technology will improve the accuracy of the data, and, as a result of the improvement in the accuracy of the data, confidence in using AI/ML in AML/CFT Compliance will increase. The use of AI/ML in AML/CFT Compliance is also expected to increase because AI/ML has become an important topic of interest among governments around the world, especially with respect to national security issues where AML/CFT Compliance is paramount. The increased focus is particularly important because it means that AI/ML is no longer a purely technical topic for data scientists only. Rather AI/ML is now an important topic for numerous stakeholders in the financial systems around the world, including AML/CFT Compliance Officers.

There are certainly questions in AI/ML in AML/CFT Compliance that are still unanswered. To help AML/CFT Compliance Officers understand the current state of AI/ML in AML/CFT Compliance, we offer the following observations:

The Importance of AI/ML as a Tool to Improve AML/CFT Compliance Programs

1. AI/ML is an increasingly important tool used in some AML/CFT Compliance Programs, especially in transaction monitoring systems and in helping regulated financial institutions identify potentially suspicious transactions.
2. Sound data are essential to the effective functioning of AML/CFT Compliance Programs, including AI/ML systems, and the use of synthetic data may solve some of the problems with insufficient data.
3. The ability of governmental financial intelligence units, and other competent authorities, to offer more detailed feedback to financial institutions on which reports are of most utility to law enforcement, through automated processes, would help financial institutions train important AI/ML data and would also inform AML/CFT Compliance Officers and their teams and systems on how to use the data more efficiently and effectively.
4. Tech Sprints supplemented with AI/ML tools are an extremely effective tool that AML/CFT Compliance Officers can use to understand what information should be collected, maintained, and reviewed by them, and to verify the effectiveness of the technology they are utilizing. Government agencies are increasingly embracing Tech Sprints. A successful Tech Sprint requires the cooperation and close involvement of AML/CFT Compliance Officers and IT professionals.

AI/ML as a Short-Term, Intermediate Term or Long-Term Solution

5. While in the long-term AI/ML in AML/CFT Compliance may eventually replace existing rule-based systems, such a result is unlikely in the intermediate term. Presently, legacy systems, sometimes supplemented by AI/ML, are expected to remain in widespread use.
6. The pace of improvements to AI/ML will continue to put pressure on regulated financial institutions to embrace, at least in part, the use of AI/ML. To remain competitive and to keep up with best practices in the short-term and the long-term, many regulated financial institutions that have not embraced the use of AI/ML in their AML/CFT Compliance Programs will do so.

Material Obstacles to the Widespread Use of AI/ML in AML/CFT Programs

7. One obstacle to more widespread adoption of AI/ML systems in AML/CFT Compliance is perceived resistance from examiners and concerns that regulatory agencies will take action (e.g., a lookback, if the new system fails to identify suspicious transactions that were captured by the legacy system or identifies suspicious transactions that were not previously identified by the legacy system) if examinations find deficiencies in the analysis or methodology used to determine whether to use AI/ML or the application of AI/ML in AML/CFT Compliance Programs.
8. As a result of the fear of enforcement actions and other uncertainty, legacy systems persist, sometimes supplemented by AI/ML systems. In some cases, regulated financial institutions are conducting expensive and cumbersome parallel runs with no fixed sunset date for the legacy system.
9. At this point, not many regulated financial institutions are willing to replace legacy systems with AI/ML systems in AML/CFT Compliance Programs, and they are not willing to substitute AI/ML in AML/CFT Compliance for human judgment.
10. While financial institutions should consider the technological implications of AMLA and adopt the technologies that will help them fully abide by the law, many financial institutions are waiting for more clarity, more competitive pressure, and the creation of more risk mitigants before fully embracing the use of AI/ML in their AML/CFT Compliance Programs.

Schedule A

City Bar Compliance Committee

Clark Abrams*
Tiffany Archer, Secretary*
Patrick T. Campbell, Former Co-Chair
Rory M. Cohen, Co-Chair
Albert DeLeon*
Adam Felsenthal, Former Co-Chair
Doel Kar**
Mariya Komartsova*
Martin Pereyra*
Devi Shanmugham, Co-Chair
Jerome Walker*

City Bar Task Force on Digital Technologies

Clark Abrams, Subcommittee on Artificial Intelligence and Subcommittee on Law Enforcement and Regulatory Agency Activities in Digital Technologies
Robert Mahari, Subcommittee on Large Language Models, Co-Chair
Lorraine McGowen, Task Force, Co-Chair
Edward So, Task Force, Co-Chair
Jerome Walker, Task Force, Co-Chair***
Allieana Bao, Secretary to the Task Force

*Denotes member of the Compliance Committee's Subcommittee on Technology, Cybersecurity and Data Privacy and Working Group on Artificial Intelligence and Machine Learning.

**In addition to her membership on the Compliance Committee, and its Subcommittee on Technology, Cybersecurity and Data Privacy and Working Group on Artificial Intelligence and Machine Learning, Ms. Kar is a Director at Forensic Risk Alliance, a firm specializing in forensic accounting, data governance and compliance consulting. The City Bar thanks Ms. Kar and her colleagues at Forensic Risk Alliance, Rim Belaoud, Shivam Patel and Gerben Schreurs, for so generously sharing their expertise with the Compliance Committee as it was developing and refining this report.

***In addition to serving as Co-Chair of the Digital Technologies Task Force, Mr. Walker serves as Chair of the Working Group on Artificial Intelligence and Machine Learning.

Schedule B

Frequently Used Acronyms

AI means Artificial Intelligence

AI/ML means artificial intelligence and machine learning

AIPPF means the Artificial Intelligence Public-Private Forum

AML means anti-money laundering

AMLA means the U.S. Anti-Money Laundering Act of 2020

AML/CFT means anti-money laundering and combatting the financing of terrorism

BoE means Bank of England

BSA means Bank Secrecy Act

BO means Beneficial Ownership

CFT means combatting the financing of terrorism

CFPB means the Consumer Financial Protection Bureau

DFPI means the California Department of Financial Protection and Innovation

DFS means the New York State Department of Financial Services

DOJ means the U.S. Department of Justice

DTO means Drug Trafficking Organization

EC means European Commission

EDD means enhanced due diligence

EU means the European Union

FRT means Facial Recognition Technology

FATF means Financial Action Task Force

FFIEC means Federal Financial Institutions Examination Council

Federal Reserve means the Board of Governors of the Federal Reserve System

FDIC means the Federal Deposit Insurance Corporation

FCA means the United Kingdom's Financial Conduct Authority

FinCEN means the Financial Crimes Enforcement Network

IA means Investment Adviser

KYC means Know Your Customer

LOD means Line of Defense

ML means Machine Learning

MRM means Model Risk Management

MSB means Money Services Business

NIST means the National Institute of Standards and Technology

NLP means Natural Language Processing

OCC means the Office of the Comptroller of the Currency

OFAC means Office of Foreign Assets Control

PEP means Politically Exposed Persons

PMLO means Professional Money Laundering Organization

PF means proliferation financing

SEC means the U.S. Securities and Exchange Commission

SAR means suspicious activity report

TBML means Trade Based Money Laundering

Treasury means the U.S. Department of the Treasury

VASP means Virtual Asset Service Providers

Schedule C

Recent Programs on AI/ML Sponsored by the City Bar

The City Bar has monitored continuously the increasing adoption of AI/ML in financial services and has brought together experts across the legal, regulatory, academic, and professional services fields to provide perspectives and guidance to understand and navigate latest developments in AI/ML, including in the use of AI/ML in AML/CFT Compliance.

On October 21, 2021, the Compliance Committee, Subcommittee on Technology, Cybersecurity and Data Privacy, and AI/ML Working Group (Working Group) hosted the City Bar's first CLE program on how AI/ML is used in financial services; how the government regulates AI/ML and is considering regulating the use of AI/ML in financial services in the future; and the ethical considerations with using AI/ML in financial services.[193]

On January 26, 2022, the Working Group hosted a webcast with panelists who focused on the use of AI/ML in AML/CFT and Sanctions, particularly with respect to the detection and prevention of money laundering; terrorist financing; proliferation financing; fraud; cyberattacks; privacy violations; human trafficking and other priorities identified by FinCEN[194] and others pursuant to the Anti-Money Laundering Act of 2020 (AMLA), which includes the Corporate Transparency Act.[195] Among other things, the panelists covered a range of opportunities, challenges, emerging trends, and issues as they relate to data collection, storage and management; transaction monitoring and surveillance; conducting due diligence and investigations; sanctions screening and reporting to OFAC; PEP screening; suspicious activity and SARs reporting to FinCEN; model validation; third party vendor assistance; and examination and audit requirements.[196]

On September 29, 2023, the Banking Law Committee hosted an *Artificial Intelligence & Machine Learning Summit*, which focused on the need for attorneys to become familiar with the regulation, impacts, usage, and safety around AI/ML. This program featured a broad range of perspectives on the evolving regulatory and ethical issues arising out of legal AI/ML practices and provided an overview of how practical solutions affects and intersects practice

---

[193] *Artificial Intelligence and Machine Learning in Financial Services: A Compliance Perspective*, N.Y. City Bar (Oct. 21, 2021), https://www.nycbar.org/cle-offerings/webcast-artificial-intelligence-machine-learning-in-financial-services-a-compliance-perspective/.

[194] *See* FinCEN, *Anti-Money Laundering and Countering the Financing of Terrorism National Priorities*, U.S. Dep't of Treasury (June 30, 2021), https://www.fincen.gov/sites/default/files/shared/AML_CFT%20Priorities%20(June%2030%2C%202021).pdf.

[195] *See AMLA*, *supra* note 12.

[196] *Artificial Intelligence and Machine Learning in Financial Services: Opportunities and Challenges in Anti-Money Laundering and Combatting the Financing of Terrorism*, N.Y. City Bar (Jan. 26, 2022), https://www.nycbar.org/cle-offerings/artificial-intelligence-and-machine-learning-in-financial-services-opportunities-and-challenges-in-anti-money-laundering-and-combatting-the-financing-of-terrorism-ondemand/.

areas such as health; intellectual labor and employment; M&A: regulatory compliance in banking and finance; and diversity, equity & inclusion.[197]

October 24, 2023, the Compliance Committee hosted the *2023 Compliance Institute*, which focused on new and evolving laws and regulations, in an increasingly multi-jurisdictional environment that includes new and increasingly sophisticated technology, artificial intelligence, and machine learning solutions, together with the evolution of digital assets and cryptocurrencies, heightened demands by law enforcement agencies and regulators and potentially heightened personal liability.[198]

The Task Force, Compliance Committee, the Banking Law Committee, and White Collar Crime Committee also hosted an *Emerging Technologies Symposium* on February 23, 2024, which focused on, among other issues, AML/CFT issues in emerging technologies.[199] Similarly, on June 10, 2024, the Task Force is scheduled to host a Symposium on Artificial Intelligence focused on the Use of AI/ML in AML/CFT Compliance; the Use of AI in the New York Judicial System; the Use of Large Language Models and Generative Artificial Intelligence; and the Use of AI in Commerce and Finance, including Banking, Securities, Commodities, Insurance and Payments.

The City Bar also produced two podcasts on AI/ML. On August 1, 2023, the Working Group on Judicial Administration and Artificial Intelligence[200] recorded a podcast that focused on *Mata v. Avianca, Inc*[201] and AI in the courts.[202] On June 28, 2023, the Task Force Subcommittee on Artificial Intelligence recorded a podcast that focused on the transformations that AI/ML tools will make to legal services, and the challenges to evaluating and deploying those tools on behalf of clients.[203]

On February 15, 2024, the Task Force Subcommittee on Law Enforcement and Regulatory Agency Activities in Digital Technologies recorded a podcast titled *Fighting for*

---

[197] *Artificial Intelligence & Machine Learning Summit 2023*, N.Y. City Bar (Sept. 29, 2023), https://services.nycbar.org/EventDetail?EventKey=_WEB092923.

[198] *Compliance Institute 2023*, N.Y. City Bar (Oct. 24, 2023), https://services.nycbar.org/EventDetail?EventKey=OND102423&WebsiteKey=f71e12f3-524e-4f8c-a5f7-0d16ce7b3314.

[199] *Emerging Technologies Symposium*, N.Y. City Bar (Feb. 23, 2024), https://services.nycbar.org/EventDetail?EventKey=INS022324&WebsiteKey=f71e12f3-524e-4f8c-a5f7-0d16ce7b3314.

[200] This working group is a joint effort between the City Bar Council on Judicial Administration and the City Bar Task Force on Digital Technologies (Task Force).

[201] *Mata v. Avianca Inc.*, Case No. 1:22-cv-01461-PKC Document 54, (S.D.N.Y. June 22, 2023), https://cases.justia.com/federal/district-courts/new-york/nysdce/1:2022cv01461/575368/54/0.pdf?ts=1687525481.

[202] *The ChatPGT Case (Mata v. Avianca, Inc.) and AI in Courts: A Closer Look*, N.Y. City Bar (Aug. 1, 2023), https://www.nycbar.org/media-listing/media/detail/the-chatgpt-case-mata-v-avianca-inc-and-ai-in-courts-a-closer-look.

[203] *What to Make of It: The Great AI Retooling*, N.Y. City Bar (June 29, 2023), https://www.nycbar.org/media-listing/media/detail/what-to-make-of-it-the-great-ai-retooling.

National Security and Financial Stability in the Digital Tech Arena, including in AI/ML in AML/CFT, during the first quarter 2024.[204]

[204] *See* https://www.nycbar.org/podcasts/fighting-for-national-security-and-financial-stability-in-the-digital-tech-arena/?back=1&ref=media.