Barrie VanBrackle

Parag Patel

Victor Razon

Potential applications of emerging technologies to anti-money laundering compliance programmes

Received (in revised form): 3rd November, 2022

Barrie VanBrackle*
Partner, Latham & Watkins LLP, USA

Parag Patel**
Partner, Latham & Watkins LLP, USA

Victor Razon***
Associate, Latham & Watkins LLP, USA

Barrie VanBrackle *is a partner in the Washington, DC office of Latham & Watkins. Barrie helps merchants, payment processors and FinTech vendors navigate key areas at the intersection of technology and finance. She regularly guides clients on transactions involving payment systems participants, including large merchants and financial technology companies, with respect to payment acceptance, payment issuance, co-brand agreements, payment card industry data security issues and payment regulatory matters. She also has significant experience advising corporate and private equity clients within the context of mergers and acquisitions and other FinTech investments. Barrie holds a BA from Johns Hopkins University and a JD from Washington University in St. Louis.*

Parag Patel *is a partner in the Washington, DC office of Latham & Watkins. Parag advises financial services companies, financial institutions and FinTechs on transactional and regulatory matters, with a particular focus on emerging payments, innovative technology, consumer and small-business lending, and banking. He has an extensive background in the regulation of money transmitters and other types of money services businesses and has helped dozens of FinTech startups navigate these rules at various stages of their business evolution. Parag holds a BA from the University of Georgia and a JD from the University of California, Berkeley School of Law.*

Victor Razon *is an associate in the Washington, DC office of Latham & Watkins. Victor advises traditional financial institutions, FinTechs and other companies on a range of regulatory and transactional matters, specifically in the context of emerging payment and lending services. Victor helps clients develop products and services and operate in accordance with applicable law and guidance, including anti-money laundering requirements. During law school, he worked for a variety of federal financial services regulators, including the Securities and Exchange Commission, the Consumer Financial Protection Bureau and the Department of the Treasury. Victor holds a BS from the University of Florida and a JD from the George Washington University Law School.*

Latham & Watkins LLP,
555 11th St NW,
Suite 1000,
Washington, DC 20004,
USA

**E-mail: barrie.vanbrackle@lw.com*
***E-mail: parag.patel@lw.com*
****E-mail: victor.razon@lw.com*

Journal of Financial Compliance
Vol. 6, No. 3 2023, pp. 248–258

2398-8053 (2023)

Abstract

The potential applications of emerging technologies to anti-money laundering (AML) compliance programmes present a variety of benefits and challenges to financial institutions. Recently, technologies such as machine learning and natural language processing, biometrics, geolocation, and blockchain and smart contracts have shown tremendous potential to bolster the AML compliance efforts of financial institutions. However, the use of these technologies in AML compliance programmes of financial institutions present a number of challenges.This paper discusses these emerging technologies, the potential applications of such technologies to AML compliance programmes of financial institutions, and the

associated benefits and challenges of these potential applications. This discussion is particularly important given increased regulatory scrutiny of financial institutions and their AML efforts in recent years.

Keywords: anti-money laundering, blockchain, artificial intelligence, biometrics, geolocation

INTRODUCTION

The Bank Secrecy Act (the BSA) is a compendium of federal statutes that serves as the United States' principal anti-money laundering (AML) and anti-terrorist financing statutes. The US Department of the Treasury's Financial Crimes Enforcement Network (FinCEN) is responsible for promulgating regulations that implement the BSA. The BSA applies to a 'financial institution', as defined under the BSA, which includes, without limitation, banks, credit unions, securities brokers and dealers, and money services businesses. Among other requirements, the BSA requires financial institutions to implement AML programmes.

To combat innovative bad actors, financial institutions have sought innovative ways to utilise the latest technologies to comply with their AML obligations. In recent years, certain emerging technologies have shown potential to improve the AML compliance programmes of financial institutions. Specifically, machine learning and natural language processing, biometrics, geolocation, as well as blockchain and smart contracts, present compelling potential to improve the efficiency of AML programmes. In fact, the US Congress has recently recognised the importance of emerging technologies in this space. The Anti-Money Laundering Act of 2020 (AMLA) directs FinCEN to brief Congress on the use of emerging technologies to combat money laundering, including artificial intelligence and distributed ledger technologies.[1]

Congress enacted the AMLA to improve information sharing and coordination among relevant government agencies and to modernise the BSA to address new money-laundering threats, among other reasons.[2] The AMLA amends the BSA to create new AML regulatory obligations and strengthen AML enforcement powers. It increases the rewards to whistleblowers for reporting AML violations, enhances penalties for repeat and egregious AML violations and enables law enforcement to subpoena foreign financial institutions that hold correspondent accounts in the US. These enhanced penalties are particularly significant because in 2020 alone, US financial institutions incurred roughly US$10bn in fines for AML and other compliance deficiencies.[3] In addition, FinCEN and state banking departments have recently assessed significant penalties against financial institutions for deficiencies in their AML compliance programmes.[4]

Further, earlier this year the Consumer Financial Protection Bureau (CFPB) announced it is invoking its authority to supervise nonbanks whose activities it reasonably believes pose risks to consumers.[5] The Dodd-Frank Wall Street Reform and Consumer Protection Act of 2010 granted this authority to the CFPB, which it invoked for the first time earlier this year[6] in response to the rapid growth of consumer offerings by nonbanks in recent years. This response will generally subject such nonbanks to the same supervisory standards applicable to banks.[7] Specifically, the rapid growth of financial technology companies (FinTechs) and the banking-as-a-service (BaaS) providers supporting FinTechs and banks (enabling FinTechs to embed banks' services into their consumer-facing applications by providing technical interfaces between FinTechs and banks) seems to have triggered this response from the CFPB.

However, the impact of this new oversight of nonbanks, including FinTechs and BaaS providers, remains to be seen. Due to this new federal oversight of nonbanks, banks should account for AML risks presented by nonbank partners in their AML programmes. Given this heightened regulatory scrutiny facing financial institutions and their nonbank partners, compliance departments should consider leveraging emerging technologies to improve the efficiency of AML programmes. This paper explores such uses and the associated benefits and challenges presented.

MACHINE LEARNING AND NATURAL LANGUAGE PROCESSING

Background

Machine learning is a branch of artificial intelligence and a method of teaching computers to learn from data, identify patterns and make decisions without human intervention. Machine learning algorithms are trained using statistical methods to analyse large datasets and provide insights about such data, which organisations then use to improve decision making. A machine learning algorithm generally consists of three parts: a decision process, an error function and an optimisation process.[8] A decision process is a series of steps that reviews the relevant data and guesses what kind of data pattern the algorithm should find.[9] An error function is a measure of how accurate such a guess was and quantifies the extent of the inaccuracy (if the guess was inaccurate).[10] An optimisation process updates the decision process based on the extent of the inaccuracy.[11] The machine learning algorithm will repeat this process until the algorithm meets a certain level of accuracy.[12]

The real-world application of machine learning algorithms started decades ago, but a recent resurgence in its use has occurred due to the growing amount and variety of data, declining costs of computer processing and data storage, and more powerful computer processing. Examples of recent real-world machine learning applications include self-driving cars and product recommendation features on e-commerce websites.

Natural language processing is a branch of artificial intelligence and a method of programming computers to understand, interpret and respond to human language. A computer's native language involves millions of ones and zeros that produce certain actions depending on their arrangement. The metaphors, sarcasm, idioms and other ambiguous qualities of human language pose challenges for a computer's native language to understand, interpret and respond to it.[13] Natural language processing divides human language into small, digestible pieces and enables computers to determine how these pieces create a particular meaning.[14] For example, word sense disambiguation is a function of natural language processing that enables computers to analyse a word with multiple meanings and determine which meaning is most appropriate in a particular context.[15] Another example is speech recognition, which is a function of natural language processing that enables computers to convert spoken language into text data.[16]

Natural language processing is not a new science but has been applied frequently in recent years because of increased availability of data, power of computer processing and interest in human communication with computers. Customer service chatbots, digital assistants like Apple's Siri, and e-mail spam detection features are examples of recent real-world natural language processing applications.

Potential applications of machine learning and natural language processing to AML programmes

Machine learning and natural language processing can significantly improve financial institutions' transaction monitoring. Many financial institutions deploy automated transaction monitoring systems, but have regularly reported dissatisfaction with such systems because of false positives — these systems generally produce a low proportion of quality alerts. In fact, a small proportion of alerts produced result in a financial institution submitting a Suspicious Activity Report (SAR) filing or finding a potential sanctions violation. For instance, a recent survey of US financial institutions found that roughly 4 per cent of suspicious transaction alerts resulted in those institutions filing a SAR and roughly 0.2 per cent of generated sanctions alerts at the larger institutions surveyed resulted in those institutions finding a potential sanctions violation.[17]

A financial institution could implement a machine learning and natural language processing algorithm that reviews all transaction alerts produced by its transaction monitoring system, analyses the outcome of each alert (eg whether compliance personnel filed a SAR or reported a sanctions violation), remove transaction alerts with a low likelihood of yielding results based on such analysis and therefore improve the quality of future transaction alerts manually reviewed by compliance personnel. The algorithm could also use the analysis of the outcomes of prior alerts to assign each future alert a risk score and organise alerts generated by level of risk presented. Natural language processing could enable the algorithm to 'read' the news, social media, sanctions lists and other publicly available information and use such data points as part of the algorithm's analysis of the transaction alerts. Such an algorithm would become increasingly more accurate as it analyses more transaction alerts over time, thus gradually and significantly decreasing the amount of time compliance personnel spend on manually reviewing transaction alerts. Given that the review of transaction alerts and converting such alerts into cases for further review accounts for a significant portion of the time spent during the SAR filing process, such an algorithm can save compliance personnel a lot of time.[18]

However, such an algorithm would only be as effective as the quality of the data it analyses.[19] Financial institutions should therefore ensure data collected is dependable, accessible and organised (eg by using quality storage methods such as cloud storage) and employ data scientists or similar personnel to manage such data and support compliance personnel. Further, regulators have emphasised that financial institutions relying on artificial intelligence tools in AML compliance should be able to explain the models used to regulators and consumers and monitor their performance regularly.[20] This task may prove difficult in the machine learning and natural language processing context because the models used may be sufficiently complicated to surpass human comprehension (ie 'black box' models).[21] Despite these challenges, machine learning and natural language processing present significant potential to improve the efficiency of transaction monitoring.

Certain financial institutions have obtained positive results from implementing machine learning in their AML compliance programmes. The Bank of Montreal (BMO) recently transferred approximately 50–60 per cent of its existing rules-based transaction monitoring to transaction monitoring based on machine learning or advanced analytics.[22] As of August 2022, BMO claimed

its AML compliance programme is roughly 25–35 per cent more efficient.[23] However, BMO has cautioned that bank regulators may be skeptical of such artificial intelligence tools because they are accustomed to rules-based systems for transaction monitoring. Therefore BMO meets quarterly with its own regulators to describe the technical steps involved in its use of artificial intelligence tools in AML compliance and to address any concerns with such use.[24]

BIOMETRICS

Background

Biometric data is data on an individual's physiological or behavioural traits. Many businesses, including financial institutions, have used some form of biometric data collection for identity verification and account access purposes, such as fingerprint scans. In recent years, customers have generally welcomed a shift to biometric-based account access because password-based account access has become relatively inconvenient for customers.[25] Recently, technology has facilitated the collection of new types of biometric data, such as heart and vein data, thermal data, keystroke data, and facial and iris data.[26]

Potential applications of biometrics to AML programmes

Over the last decade, financial institutions have regularly used biometric data for identity verification and account access purposes, such as fingerprint scanning or voice recognition through a financial institution's smart phone application. Recently, more advanced biometric methods for identity verification and account access purposes have been implemented, such as facial and iris recognition software. Generally, such software verifies an individual's identity by comparing the facial and eye features collected against a publicly available photograph of the individual or a separately provided photo identification, such as a driver's licence or passport.[27]

Implementing facial recognition or iris scan software to verify identities during customer onboarding and on an ongoing basis for account access could significantly improve financial institutions' know-your-customer (KYC) and anti-fraud efforts. These technologies identify individuals with an extremely high degree of accuracy. For instance, according to research published by the Center for Strategic & International Studies, facial recognition algorithms are generally accurate approximately 99.9 per cent of the time when clear reference images are used.[28] Another study found that a significant number of iris scanning software reviewed generally had similar levels of accuracy.[29] Further, these technologies rely on far more data points than older biometric verification methods, which makes identity fraud far more challenging. For example, identity verification through iris scanning generally relies on 260 identifying points, compared with 16 through fingerprint scanning.[30] However, these technologies are relatively inaccurate at identifying individuals with features that are less common in a given population (eg ethnic minorities).[31]

Nevertheless, the benefits of such technology should generally outweigh the risks. Financial institutions should consider leveraging facial and iris recognition software as an additional tool to improve identity verification and address fraud, especially given the associated risks from the increase in remote onboarding of new customers in the COVID-19 era. Some financial institutions have implemented such biometrics during the COVID-19 pandemic. For example, TD Bank recently added facial recognition biometrics (among other biometrics, including fingerprint and vocal recognition) to verify customers' identities through its mobile

application. It reported a resulting general improvement in the bank's identity verification efforts and a reduction of customer friction during onboarding.[32] However, prior to leveraging this technology, financial institutions should be aware that the collection of facial and iris data may present privacy issues. Some state privacy laws restrict the collection of consumers' biometric data, such as requiring informed consent before collection and prohibiting revenue generation from such data.[33] Such state laws may exempt biometric data collected by a financial institution from such requirements.[34] Financial institutions should review the privacy laws of each relevant state for any applicable requirements and exemptions prior to using facial or iris recognition software.

GEOLOCATION

Background

Geolocation data determines the precise physical location of any person or object and may be collected through various sources. Common sources include an internet user's Internet protocol (IP) address, which contains information that reveals the individual's physical location and an individual's use of cellular data on a mobile device, which reveals an individual's physical location through triangulation of the data signal between cellular towers.[35]

Potential applications of geolocation to AML programmes

Financial institutions have historically used geolocation data, particularly IP addresses, to verify a user's actual location during customer onboarding and ongoing customer due diligence. In recent years, US regulators have emphasised that financial institutions should rely on multiple sources of geolocation data.[36] For instance, aggregating geolocation data sourced from an IP address as well as cell tower, global positioning system (GPS) and/or Wi-Fi triangulation would enable financial institutions to verify a user's location with a far higher degree of confidence than using one such source. A multi-sourced approach would improve a financial institution's ability to understand user behaviour and detect suspicious activity by providing an accurate record of each user's usual locations and typical movement patterns. Some financial institutions rely on multi-sourced approaches to confirm a user's actual location and improve their initial and ongoing customer due diligence efforts. For example, People's United Bank relies on multiple sources in addition to an IP address to confirm a customer's actual location, including an anonymisation indicator/internet service provider, device language and a device identification number.[37]

Such multi-sourced approach may avoid issues from heavily relying on an IP address to verify a person's location, such as a person's use of a virtual private network (VPN) or domain name system (DNS) to mask the person's IP address and circumvent IP address monitoring (known as 'IP misattribution' or 'location spoofing').[38]

Financial institutions should effectively deploy the geolocation data once collected. The Office of Foreign Assets Control (OFAC) recently brought enforcement actions against certain entities for failing to use geolocation data in their possession to block transactions from and/or to sanctioned jurisdictions.[39] For instance, OFAC found that BitGo, a provider of secure digital wallet management services, had sufficient geolocation data to verify the actual location of its users (eg users' actual IP addresses) but failed to deploy such data to prevent users in sanctioned countries from transacting through digital currency wallets on BitGo's platform. Specifically, individuals

located in Crimea, Cuba, Iran, Sudan and Syria transacted 183 times on BitGo's platform over a four-year period, and BitGo had sufficient data to know the actual location of such users and did not implement internal controls to prevent these transactions. As a result, collecting sufficient geolocation data may not be enough to avoid regulatory scrutiny — financial institutions should deploy this data to ensure internal controls and processes are in place to prevent prohibited transactions.

Accordingly, financial institutions should use a multi-source approach for geolocation data and effectively deploy it to avoid such issues and improve customer onboarding and ongoing due diligence efforts. However, financial institutions should review state privacy laws before collecting such data, which may establish requirements and exemptions applicable to the collection of geolocation data by a financial institution in such a state.

BLOCKCHAIN AND SMART CONTRACTS

Background

A blockchain is a type of distributed ledger that is stored and maintained on each computer participating on the blockchain. Each participating computer stores and maintains a copy of the exact same ledger. Such computers constantly communicate to update and synchronise the ledger by verifying transactions (or other information) — a process known as 'consensus' — which confirms the validity of individual transactions (or other information) and the entire ledger by aggregating transactions into blocks of data. Generally, the consensus process results in a chain of immutable blocks of data.

Three main types of blockchains exist: public blockchains, private blockchains and consortium blockchains. In a public blockchain, anyone may join the network, participate in the consensus process, or access and maintain the ledger. A public blockchain is completely decentralised — no central authority can manipulate or otherwise control it.[40] Many cryptocurrencies, including Bitcoin, operate on a public blockchain. In contrast, a private blockchain has a single central network operator that controls who may join the network, participate in the consensus process, or access and maintain the ledger.[41] The central network operator may edit or delete blocks of data on the blockchain in its discretion. An example of a private blockchain is Ripple, which facilitates cryptocurrency exchange among certain businesses. A consortium blockchain has several network operators rather than one (in the case of a private blockchain) or zero (in the case of a public blockchain), which determine who may join the network, participate in the consensus process, or access and maintain the ledger.[42] A group of organisations with common goals may use a consortium blockchain to transfer data amongst themselves securely and efficiently, such as participants in a supply chain.[43]

A smart contract is a computer programme stored on a blockchain that improves the security, efficiency and impartiality of contract execution by eliminating the need for an individual to enforce an agreement. A smart contract digitises agreements by turning agreement terms into code that automatically executes once such terms are met. Smart contracts monitor data within the blockchain or from a third-party data source to determine whether the contract terms have been met and will execute only if such conditions are met and may not correspond to an actual legal contract.[44]

For example, a smart contract may be used to facilitate a property rental by programming the following terms into the smart contract: (i) if tenant sends landlord the agreed amount in cryptocurrency, then

tenant will receive a digital key to the property; and (ii) if landlord sends a digital key to the property to tenant, then tenant will send the agreed amount in cryptocurrency to landlord. If the tenant sends landlord the cryptocurrency or the landlord sends tenant the digital key to the property — whichever occurs first — the contract will enforce the agreement by executing the other party's obligation automatically via the blockchain (ie sending the cryptocurrency or the digital key, as applicable, to the respective accounts of landlord or tenant).

Potential applications of blockchain and smart contracts to AML programmes

US financial institutions could implement a consortium blockchain to decrease costs and improve outcomes associated with their customer identity verification and transaction monitoring obligations. A consortium blockchain could enable a participating financial institution to rely on KYC information collected, verified and stored on the consortium blockchain by one of the other participating financial institutions. In other words, each customer could complete the KYC process only once, rather than each time a participating financial institution begins a relationship with such customer, and such customer could share its KYC results securely with each participating financial institution it intends to use. This process could result in a digital profile for the customer stored on the consortium blockchain — covering biographic information, transaction types, dollar volume, expected origination, destination of transactions and frequency of transactions. A participating financial institution relying on this digital profile could reduce the significant amount of resources expended to complete KYC for a new customer. In fact, the process of collecting and verifying KYC information takes approximately 30 to 50 days on average for a financial institution to complete and costs approximately US$60m per year.[45]

Each participating financial institution could modify a customer's profile stored on the consortium blockchain to reflect updates to KYC information and/or each new transaction the customer engages in. Storing all customer data on a consortium blockchain could improve monitoring for suspicious transactions by enabling participating financial institutions to immediately notify other participating financial institutions of detected suspicious activity. Each participating financial institution would have immediate access to the suspicious transaction data and could rely on the information sharing provision under the BSA to share such suspicious transaction data with other participating financial institutions.[46] Such information sharing through the consortium blockchain would provide a clear, auditable and immutable record of the transaction data that the participating financial institutions found suspicious — as well as the KYC information the participating financial institutions relied on prior to opening customer accounts — which could streamline any regulatory review or internal review of such information.

Although no financial institutions have implemented a consortium blockchain to date, IBM has tested a proof-of-concept consortium blockchain among financial institutions for KYC purposes in partnership with HSBC, Deutsche Bank and several other major financial institutions.[47] This proof-of-concept consortium blockchain generally met its objectives, which included, among others, to: (i) 'define harmonized standards for the collection and validation of certain core document and information agreeable to all bank participants'; (ii) 'eliminate repetition of mundane documentary

tasks through collaboration and privacy-preserving sharing'; and (iii) 'digitize all corporate KYC information to preserve authenticity and accuracy'.[48]

Further, financial institutions could use smart contracts to improve transaction monitoring and reporting. Generally, the SAR filing process involves six stages: (i) maintaining a transaction monitoring system; (ii) reviewing transaction alerts; (iii) converting alerts into cases; (iv) reviewing the cases; (v) documenting the rationale behind whether to file a SAR and (vi) filing the SAR. Currently, financial institutions spend significant resources completing this process. In 2020, for instance, FinCEN estimated that compliance personnel at US financial institutions took roughly 20 minutes on average to complete steps (iv)–(vi) for each case and roughly 5.5m cases were created that year, which resulted in roughly US$91m in time spent on such review that year.[49] A financial institution could programme certain conditions precedent for filing a SAR into a smart contract based on transaction data and automatically populate the relevant information on a SAR form for submission to FinCEN (eg if a customer makes X transactions over Y dollar amount to an account located abroad within Z period of time, then populate and file a SAR). However, the review of certain transactions may require more subjectivity than a smart contract's logic permits (ie does not follow a strict 'if . . . then' format) and therefore financial institutions could rely on manual review in such situations. Accordingly, financial institutions could save significant amounts of time each year by using smart contracts to support transaction monitoring and reporting efforts.

However, implementing a consortium blockchain and smart contracts to improve AML compliance efforts presents several challenges. First, regulators generally have a lack of understanding of blockchain technology and have historically relied on legacy systems at financial institutions for compliance and reporting functions. In fact, financial institutions generally lack confidence in their regulators' understanding of emerging technologies used for BSA/AML compliance. Roughly 60 per cent of financial institutions surveyed in 2021 said their regulators stay up to date on technology in the BSA/AML space to the following extent: 'OK, poorly, or not at all'.[50] Regulators' lack of understanding is problematic because financial institutions would need their approval before using a consortium blockchain or smart contracts for KYC purposes. In addition, implementing a consortium blockchain would improve identity verification and transaction monitoring efficiency only if a significant number of financial institutions participated, which may be unlikely because of potential privacy law concerns and hesitance to share sensitive customer data with competitors. Further, the potential benefits of a consortium blockchain depends on a participating financial institution sharing accurate customer information. Implementing a consortium blockchain does not guarantee the accuracy of customer information shared, which could cause liability issues in the event a participating financial institution relies on inaccurate KYC information (eg a regulator may impose liability on both the relying and providing financial institutions for compliance failures resulting from the inaccurate information).

CONCLUSION

Machine learning and natural language processing, biometrics, geolocation, as well as blockchain and smart contracts have significant potential to improve financial institutions' AML compliance efforts. A financial institution should weigh the benefits and challenges discussed above and

determine if implementing any of these technologies would provide a net benefit to its AML compliance programme. Given the pace of technological change, financial institutions should monitor the market on an ongoing basis for new products and services that could improve their AML programmes.

References

(1) Notes to 31 U.S.C. § 5311.
(2) Notes to 31 U.S.C. § 5311 (discussing underlying purposes of the AMLA).
(3) Finbold (11th January, 2021) 'Bank Fines 2020', available at https://finbold.com/bank-fines-2020/#:~:text=The%20Bank%20Fines%202020%20report%20reveals%20the%20list%20of%20banks,personal%20data%20leaks%2C%20among%20others (accessed 31st July, 2022).
(4) Eg Financial Crimes Enforcement Network (17th March, 2022) 'FinCEN Announces $140 Million Civil Money Penalty against USAA Federal Savings Bank for Violations of the Bank Secrecy Act', available at https://www.fincen.gov/news/news-releases/fincen-announces-140-million-civil-money-penalty-against-usaa-federal-savings (accessed 5th August, 2022).
(5) Consumer Financial Protection Bureau (25th April, 2022) 'CFPB Invokes Dormant Authority to Examine Nonbank Companies Posing Risks to Consumers', available at https://www.consumerfinance.gov/about-us/newsroom/cfpb-invokes-dormant-authority-to-examine-nonbank-companies-posing-risks-to-consumers/ (accessed 2nd November, 2022).
(6) *Ibid*.
(7) *Ibid*.
(8) Berkeley School of Information (26th June, 2022) 'What Is Machine Learning (ML)?', available at https://ischoolonline.berkeley.edu/blog/what-is-machine-learning/ (accessed 31st July, 2022).
(9) *Ibid*.
(10) *Ibid*.
(11) *Ibid*.
(12) *Ibid*.
(13) IBM Cloud Learn Hub (n.d.) 'What Is Natural Language Processing?', available at https://www.ibm.com/cloud/learn/natural-language-processing (accessed 31st July, 2022).
(14) *Ibid*.
(15) *Ibid*.
(16) *Ibid*.
(17) Bank Policy Institute (29th October, 2018) 'Getting to Effectiveness – Report on US Financial Institution Resources Devoted to BSA/AML & Sanctions Compliance', available at https://bpi.com/wp-content/uploads/2018/10/BPI_AML_Sanctions_Study_vF.pdf (accessed 31st July, 2022).
(18) Federal Register, Vol. 85, No. 101, Fed. Reg. 31,598, 31,599 (26th May, 2020), available at https://www.govinfo.gov/content/pkg/FR-2020-05-26/pdf/2020-11247.pdf (accessed 31st July, 2022) (noting there is insufficient data available to calculate an accurate estimate of the time spent on this portion of the SAR filing process); RegTech Consulting LLC (2nd June, 2020) 'FinCEN's Estimate of the Costs and Burden of Filing SARs is Evolving, But Needs Private Sector Input', available at https://regtechconsulting.net/aml-regulations-and-enforcement-actions/fincens-estimate-of-the-costs-and-burden-of-filing-sars-is-evolving-but-needs-private-sector-input/ (accessed 31st July, 2022) (noting this portion of the SAR filing process is likely most burdensome in terms of time spent).
(19) The Royal Society (2017) 'Machine Learning: The Power and Promise of Computers that Learn by Example', available at https://royalsociety.org/~/media/policy/projects/machine-learning/publications/machine-learning-report.pdf, p. 94 (accessed 31st July, 2022).
(20) Monetary Authority of Singapore (n.d.) 'Principles to Promote Fairness, Ethics, Accountability and Transparency (FEAT) in the Use of Artificial Intelligence and Data Analytics in Singapore's Financial Section', available at https://www.mas.gov.sg/~/media/MAS/News%20and%20Publications/Monographs%20and%20Information%20Papers/FEAT%20Principles%20Final.pdf, p. 6 (accessed 31st July, 2022).
(21) Rudin, C. and Radin, J. (22nd November, 2019) 'Why Are We Using Black Box Models in AI When We Don't Need to? A Lesson from an Explainable AI Competition', Harvard Data Science Review, available at https://hdsr.mitpress.mit.edu/pub/f9kuryi8/release/7 (accessed 31st July, 2022).
(22) Lorinc, J. (19th August, 2022) 'Anti-money Laundering Can Benefit from AI – to a Certain Extent', Chartered Professional Accountants Canada, available at https://www.cpacanada.ca/en/news/pivot-magazine/ai-aml-tools (accessed 22nd November, 2022).
(23) *Ibid*.
(24) *Ibid*.
(25) Lovisotto *et al.* (n.d.) 'Mobile Biometrics in Financial Services: A Five Factor Framework', Department of Computer Science, University of Oxford, available at http://www.cs.ox.ac.uk/files/9113/Mobile%20Biometrics%20in%20Financial%20Services.pdf, p. 1 (accessed 1st August, 2022).
(26) Eg Patil, N.V. and Kadam, S. U. (2013) 'Thermal Recognition in Biometrics Approach', *International Journal of Recent Technology and Engineering*, Vol. 2,

No. 2, p. 1, available at https://www.ijrte.org/wp-content/uploads/papers/v2i2/B0602052213.pdf (accessed 1st August, 2022).
(27) Crumpler, W. (14th April, 2020) 'How Accurate are Facial Recognition Systems – and Why Does It Matter?' Center for Strategic and International Studies, available at https://www.csis.org/blogs/technology-policy-blog/how-accurate-are-facial-recognition-systems-%E2%80%93-and-why-does-it-matter (accessed 31st July, 2022).
(28) *Ibid*.
(29) Quinn, G. W., Grother, P. and Matey, G. (April 2018) 'IREX IX Part One Performance of Iris Recognition Algorithms', National Institute of Standards and Technology, available at https://nvlpubs.nist.gov/nistpubs/ir/2018/NIST.IR.8207.pdf (accessed 31st July, 2022).
(30) RecFaces (3rd December, 2020) 'What Are Iris and Retina Scanners, and How Do They Work?', available at https://recfaces.com/articles/iris-scanner#:~:text=According%20to%20the%20NIST%20(National,identification%20data%20using%20this%20method (accessed 31st July, 2022).
(31) Lohr, S. (9th February, 2018) 'Financial Recognition is Accurate, if You're a White Guy', The New York Times, available at https://www.nytimes.com/2018/02/09/technology/facial-recognition-race-artificial-intelligence.html#:~:text=When%20the%20person%20in%20the%20photo%20is%20a%20white%20man%2C%20the%20software%20is%20right%2099%20percent%20of%20the%20time (accessed 31st July, 2022).
(32) PYMNTS.com (March 2021) 'Digital Identity Tracker', available at https://www.pymnts.com/digital-identity-tracker-report/, p. 8 (accessed 2nd November, 2022).
(33) Eg 740 ILCS 14 *et seq*. (Illinois Biometric Information Privacy Act).
(34) *Ibid*.
(35) Marley, R. (4th December, 2018) 'Geolocation Technology and Its Benefits for KYC Verification', ShuftiPro, available at https://shuftipro.com/blog/geolocation-technology-benefits-kyc-verification/ (accessed 1st August, 2022).
(36) Eg Office of Foreign Assets Control (October 2021) 'Sanctions Compliance for the Virtual Currency Industry', available at https://home.treasury.gov/system/files/126/virtual_currency_guidance_brochure.pdf, p. 14 (accessed 31st July, 2022).
(37) GeoComply (21st April, 2021) 'People's United Bank Top Fraud Expert Speaks Out on FinCrime Trends and GeoLocation's Value in Fighting Fraud', available at https://www.geocomply.com/blog/peoples-united-bank-top-fraud-expert-speaks-out-on-fincrime-trends-and-geolocations-value-in-fighting-fraud/ (accessed 2nd November, 2022).
(38) *Ibid*.
(39) Eg Office of Foreign Assets Control (October 2021) 'Sanctions Compliance for the Virtual Currency Industry', available at https://home.treasury.gov/system/files/126/virtual_currency_guidance_brochure.pdf, p. 14 (accessed 31st July, 2022).
(40) Abrol, A. (10th March, 2022) 'Private Blockchain vs. Consortium Blockchain: A Comparison Guide', Blockchain Council, available at https://www.blockchain-council.org/blockchain/private-blockchain-vs-consortium-blockchain-a-comparison-guide/ (accessed 31st July, 2022).
(41) *Ibid*.
(42) *Ibid*.
(43) Businesswire (16th March, 2021) 'The Worldwide Blockchain Supply Chain Industry is Expected to Reach $3+ Billion by 2026', available at https://www.businesswire.com/news/home/20210316005759/en/The-Worldwide-Blockchain-Supply-Chain-Industry-is-Expected-to-Reach-3-Billion-by-2026---ResearchAndMarkets.com (accessed 31st July, 2022).
(44) Idelberger, F., Governatori, G., Riveret, R. and Sartor, G. (July 2016) 'Evaluation of Logic-Based Smart Contracts for Blockchain Systems', ResearchGate, available at https://www.researchgate.net/publication/303679677_Evaluation_of_Logic-Based_Smart_Contracts_for_Blockchain_Systems, pp. 3–4 (accessed 31st July, 2022).
(45) Van Oerle, J. and Lemmens, P. (May 2016) 'Distributed Ledger Technology for the Financial Industry', Chartered Alternative Investment Analyst Association, available at https://caia.org/sites/default/files/1.distributed_ledger_for_financial_industry.pdf (accessed 16th January, 2023); Moyano, J. P. and Ross, O. (15th November, 2017) 'KYC Optimization Using Distributed Ledger Technology', *Business & Information Systems Engineering* Vol. 59, pp. 411–423, available at https://link.springer.com/article/10.1007/s12599-017-0504-2#Fn1 (accessed 31st July, 2022).
(46) 31 C.F.R. § 1010.540.
(47) Curry, M. (21st September, 2018) 'Blockchain for KYC: Game-Changing RegTech Innovation', IBM, available at https://www.ibm.com/blogs/blockchain/2018/09/blockchain-for-kyc-game-changing-regtech-innovation/ (accessed 2nd November, 2022).
(48) *Ibid*.
(49) 85 Fed. Reg. 31,598, 31,606 (May 26, 2020), available at https://www.govinfo.gov/content/pkg/FR-2020-05-26/pdf/2020-11247.pdf (accessed 31st July, 2022).
(50) Thomson Reuters (2022) '2022 Thomson Reuters Anti-Money Laundering Insights Survey', available at https://legal.thomsonreuters.com/content/dam/ewp-m/documents/legal/en/pdf/reports/2022-thomson-reuters-anti-money-laundering-insights-survey-v2.pdf, p. 3 (accessed 31st July, 2022).