FINANCIAL REGULATION INNOVATION LAB

SHAPING THE FUTURE OF FINANCIAL REGULATION

FinTech Scotland®

WHTE PAPER SERIES

"USING AUTOMATION AND AI TO COMBAT MONEY LANUDERING"

In collaboration with

University of Strathclyde Glasgow

University of Glasgow

FRIL White Paper Series

USING AUTOMATION AND AI TO COMBAT MONEY LAUNDERING

Devraj Basu* Godsway Korku Tetteh*

*University of Strathclyde

March 2024

ABSTRACT: Money laundering, which is the criminal activity of processing criminal proceeds to disguise their origin is one of the gravest problems faced by the global economy, and its size is growing rapidly. It is estimated that 2- 5% of the global GDP or US$800 billion to US$2 trillion is being laundered every year across the globe. Banks have begun to understand that their legacy rules-based systems cannot effectively mitigate risks related to money laundering. There is a need to embrace advanced technology that can effectively solve their problems of getting involved in money laundering cases. This white paper outlines a case study focusing on the effectiveness and limitations of Artificial Intelligence (AI) in detecting and preventing money laundering activities. It will provide an overview of the design, architecture, implementation, and testing of such a strategy.

Strategic Alignment: FinTech Research & Innovation Roadmap 2021-31; Khalifa Review of UK FinTech; EU's Anti-Money Laundering Directives (existing); EU's Anti-Money Laundering (AML) Regulation (ongoing); EU's Transfer of Funds Regulation (existing); EU's Anti-Money Laundering Authority (ongoing); UK's Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations.

FinTech Research & Innovation Roadmap 2021-31 Sub-Theme: Simplifying Compliance.

Table of Contents

1. PROBLEM STATEMENT

The scale of global money laundering and financial crime is significant. The World Bank, the International Monetary Fund (IMF), the European Union, and others publish estimates of what they consider to be the total global figure of all activities related to money laundering and financial crime. The estimates vary with the consensus being that 2%-5% of global GDP is laundered every year within the global financial system – somewhere between £2tn-£5tn[1]. Current banking and other financial institution (FI) systems environments are simply inadequate to arrest money laundering proactively, despite the fact that globally banks spend somewhere between 2%-5% of total annual revenues on their overall risk and financial crime divisions[2]. This in a July 2013 report, they stated:

> *The root cause of these problems is often a failure in governance of money laundering risk, which leads, among other things, to inadequate anti-money laundering resources and a lack of (or poor quality) assurance work across the firm.*
>
> *This often focuses on whether processes have been followed rather than on the substance of whether good AML judgements are being made*[3].

The increasing globalization of financial transactions is also driving the rise of financial crime. As more companies operate across borders, tracking and monitoring financial transactions becomes more difficult. As more transactions happen online, there is a growing need to monitor and detect fraudulent transactions via digital channels. Moreover, the increasing use of digital currencies has created new challenges for Anti-Money Laundering (AML) compliance. Digital currencies are decentralized and difficult to trace, which makes it easier for cybercriminals to launder money using these currencies.

---

[1] https://www.imf.org/external/pubs/ft/fandd/2018/12/imf-anti-money-laundering-and-economic-stability-straight.htm

[2] https://www.mckinsey.com/~/media/McKinsey/Business%20Functions/Risk/Our%20Insights/Financial%20crime%20and%20fraud%20in%20the%20age%20of%20cybersecurity/Financial-crime-and-fraud-in-the-age-of-cybersecurity.ashx

[3] https://www.fca.org.uk/publication/corporate/anti-money-laundering-report.pdf

In response to the scale of this problem, Governments worldwide are implementing stricter AML regulations, and financial institutions are under increasing pressure to comply with these regulations. There is also growing awareness of the impact of financial crime on society. Financial crime can have significant social and economic consequences, including funding terrorism, drug trafficking, and other illegal activities. Penalties for inadequate or non-compliance have been growing and the gross amount of fines for money laundering offenses over the 2008-2022 period is around $55 billion[4]. The US has led the way, chalking up $37bn of the fines, followed by roughly $11bn in Europe, the Middle East and Africa, and just over $5.1bn in Asia-Pacific. In 2022, financial institutions were fined over $8 billion for AML-related infractions. BNP Paribas, UBS, Goldman Sachs, JP Morgan, HSBC, and Standard Chartered top the league tables in terms of fines for money laundering and related offenses since the financial crisis. The violations that received the biggest penalties leaned toward repeated violations and failure to effectively calibrate AML measures with a firm's risk profile. These included deficient customer due diligence processes, failure to monitor politically exposed persons and high-risk entities, inadequately staffed compliance teams, and insufficient source of funds and source of wealth checks.

Bank AML fines in 2022 reached far and wide across the globe, totaling over $2 billion in civil monetary penalties. In December 2022, the United States Department of Justice (DoJ) settled a long-running probe into Danske Bank, Denmark's largest bank. Because of the investigation, Danske Bank agreed to forfeit over USD 2 billion, with USD 1.2 billion going to the DoJ, USD 178.6 million to the Securities and Exchange Commission, and USD 612.4 million to Denmark's Special Crime Unit[5]. A separate settlement with the Securities and Exchange Commission related to misleading investors over AML compliance failures in Estonia. The bank agreed to pay a penalty of USD 413 million to settle the case, however, this sum also includes the previously mentioned payment of USD 178.6 million. The FCA also fined several banks for failing to conduct sufficient

[4] https://www.ft.com/content/7a4821e6-96f1-475c-ae55-6401e402061f

[5] *"Danske Bank lied to U.S. banks about its deficient anti-money laundering systems, inadequate transaction monitoring capabilities, and its high-risk, offshore customer base in order to gain unlawful access to the U.S. financial system."*

~ Kenneth Allen Polite Jr, Assistant Attorney General of the Justice Department's Criminal Division

checks for money laundering and terrorist financing, while processing deposits from customers in high-risk countries. In one case, the FCA noted that a bank had also failed to undertake the required checks for some politically exposed persons and had inadequate compliance staff to perform the work required. In December 2022, the UK's Financial Conduct Authority (FCA) fined Santander Bank GBP 107.7 million for repeated AML compliance failures. These include inadequate systems and processes for the verification of customer information regarding the banking business that they would be carrying out. The FCA also highlighted Santander's failure "to properly monitor the initial amount declared by the customers with the actual turnover of the client."[6] The Financial Crimes Enforcement Network (FinCEN) levied USAA Federal Savings Bank (USAA FSB) with a USD 140 million fine in March "for willful violations of the Bank Secrecy Act (BSA) and its implementing regulations." In particular, USAA FSB admitted that it intentionally failed to implement and manage an appropriate AML program. Most recently, Binance the cryptocurrency exchange agreed to pay more than $4.3 billion in penalties on criminal charges related to money laundering and breaching international financial sanctions to the DoJ[7]. This is the first major money laundering fine for a digital currency entity and the transactions appear to be related to ransomware attacks, child sexual abuse, large-scale hacks, narcotics trading, and terrorist financing.

The foregoing indicates the pressure on FIs to find innovative strategies and solutions for striking a balance between loss reduction, client experience, operating efficiency, and regulatory compliance. The area of regulatory technology or RegTech has emerged to provide solutions to problems of regulatory compliance. In its simplest form, RegTech is the application of technology to improve the efficiency of regulatory compliance in areas such as regulatory reporting, identity management, risk management, and in our setting money laundering. RegTechs provide efficient workflow engines that improve the productivity of the regulatory journey, whilst others

[6] *"Santander's poor management of their anti-money laundering systems and their inadequate attempts to address the problems created a prolonged and severe risk of money laundering and financial crime."*

~ Mark Steward, FCA Executive Director of Enforcement and Market Oversight

[7] https://www.ft.com/content/d10af983-1376-457f-9709-815e04ba59fb

automate and improve the necessary reporting output standards required by the regulator. In their ongoing research study, Deloitte (2020) has identified over 350 RegTech companies globally that fit into one of the categories listed above[8]. The global **AML market size** was valued at **USD 1.32 billion in 2022** and is expected to grow at a compound annual growth rate (CAGR) of 15.9% from 2023 to 2030. AML solutions can help financial institutions identify and investigate transactions that are suspicious or outside of the normal behaviour of the account holder reducing the risk of fraud and financial crime. The technologies deployed incorporate data analytics, machine learning, natural language processing (NLP) which we will discuss in the Solutions section, but it is important to understand that all of these technology improvements are taking place under the restrictions of a bounded framework of existing regulatory infrastructure that is, in the main, analogue, or paper-based at its core. Banks and other FIs within the UK jurisdiction operate in a 'silo' environment where data and transaction flow sharing is generally prohibited or discouraged due to privacy laws (such as GDPR) which makes large-scale deployment of technologies difficult. Thus incorporating the innovative solutions that we will discuss in the Solutions sections will likely require a re-organization of banks' and financial institutions' workflows.

2. LITERATURE REVIEW

2.1 Automation and anti-money laundering

Money laundering which is defined as "the process by which proceeds from a criminal activity are disguised to conceal their illicit origin"[9] occurs in three main stages. The first stage is the placement stage where illicit proceeds of crime are first introduced into the financial system. The second stage is the layering stage during which criminals attempt to conceal the source of the illicit funds by engaging in multiple transactions and transfers. The final stage of money laundering is the integration stage. At this stage, the illicit money is fully integrated into the formal economy making it difficult to distinguish or detect[1]. The early detection of money

[8] https://www2.deloitte.com/lu/en/pages/technology/articles/regtech-companies-compliance.html

[9] https://www.imf.org/external/np/leg/amlcft/eng/aml1.htm

laundering at the initial stages of the money laundering cycle is required to enhance the efficiency and effectiveness of AML systems. The methods and techniques employed by criminals to launder proceeds of crime are referred to as typologies. Money laundering typologies are in constant evolution[10]. The adaptability of AML systems to the ever-changing landscape of financial crime is therefore indispensable in the fight against these crimes.

Money laundering poses significant risks to the UK economy while the costs associated with current AML regimes are extremely high. Fraud costs the UK about £190bn each year and money laundering-enabled serious organised crime is estimated to cost the country about £37bn annually. At the same time, about £90 trillion worth of transactions change hands every year in the UK. The high volume of transactions makes identification of suspicious transactions nontrivial especially when such illicit activities are overshadowed by large volumes of legitimate transactions. Automation of AML systems and processes offers some hope, but banks in the UK still rely on manual verification processes which are time-consuming and costly[11]. For example, a study by the Financial Conduct Authority on a sample of 2000 firms in the UK shows that these firms spent over £650 million a year on dedicated staff to combat financial crimes including money laundering[12].

Automation of AML systems and processes is necessary but current approaches are inefficient. A study reveals that current AML systems in the financial services industry follow a linear process where data sources are connected to a rules-based system[2]. This approach begins with data collection and data processing followed by transaction screening and monitoring. The authors identified four main layers of AML frameworks. The first layer is comprised of the data layer. This layer is characterized by the collection, management, and storage of both internal and external data. Internal data in this case refers to data sources that are internal to the firm such as customer profiles and transaction records whereas external data sources are external to the firm and may include social media and news portals. The second layer is the screening and monitoring layer. This layer includes transaction screening where transactions are screened prior to execution to comply with sanctions. Name screening is carried out under this layer to identify

[10] https://www.imf.org/external/np/leg/amlcft/eng/aml1.htm

[11] https://www.fca.org.uk/news/speeches/turning-technology-against-financial-crime

[12] https://www.fca.org.uk/news/speeches/turning-technology-against-financial-crime

payments relating to legal or natural persons that have been blacklisted by regulatory authorities. In addition, transaction monitoring is performed to identify suspicious activities. Subsequently, client profile monitoring is conducted to have up-to-date information on the client. The third layer is the alert and event layer which triggers suspicious transaction alerts for further investigation by human evaluators. The large volume of suspicious alerts requires time and effort to be reviewed by human evaluators. The final layer is the operational layer where human agents determine whether a transaction should be blocked, released, or reported to regulatory authorities.

Rules-based systems are not able to detect small value transactions that fall under defined threshold limits and AML systems based on such systems face significant false positives problems. False positives arise when there are transactions that are highlighted as suspicious based on a defined set of rules, but which do not pose any risk to the financial institution. Also, rules-based solutions do not have the adaptability or learning ability to uncover new money laundering schemes by criminals [3].

2.2 Achieving efficiency through machine learning and artificial Intelligence

Possible automation solutions have been offered to overcome the challenges in existing AML systems. An earlier study proposed a Bayesian network (BN) approach that is designed based on AML rules to identify suspicious transactions [4]. Based on customers' transaction behaviour the Bayesian network approach is designed to assign a baseline money laundering score to each customer and a suspicious transaction alert is triggered if customers' current transaction behaviour deviates from their historical transaction patterns. A two-stage solution to detect suspicious or unusual transactions has also been proposed[5]. The first stage models consumer behaviour using past transactional records while the second stage monitors new transactions by comparing them with original patterns to identify suspicious transactions. Other solutions exist to enable financial institutions to detect anomalies in financial transitions[6]. The first stage is the data pre-processing stage which includes data normalisation, noise removal, and dimension reduction. The second stage is clustering which relies on unsupervised learning techniques to segment data items into various groups based on defined criteria. This stage is followed by the final stage which is the computation of the anomaly index. The anomaly index measures the deviation of transactions (amount and frequency) from the established behaviour of the cluster

the customer belongs to. In this case higher values of the index correspond to the higher levels of the suspicion[6].

Neural networks and abnormality indicators can equally be employed to detect suspicious transactions and reduce the proportion of false positives[7]. This process primarily involves the assignment of risk metrics to variables using fuzzy logic and money laundering typologies. Subsequently, unsupervised algorithms are employed to generate risk clusters. Finally, the riskiest clusters are identified using abnormality indicators based on variable variances. Such systems are designed to improve both self and group comparisons in AML systems. Other approaches combined statistical and expert-based techniques to achieve efficiency and reduce false positives. This technique generates automatic rules using distributed tree-based machine learning algorithms such as Decision Tree, Random Forest, and Gradient Boosting while integrating expert rules in the model [8].

Social network analysis techniques can be used to visualise and detect criminal networks in the banking system. This approach can yield greater efficiency given that it does not rely only on a single data domain but data from multiple sources including administrative datasets [9]. Social network analysis can predict the risk profile of customers and identify criminal networks[10]. While social network analysis comes in handy to unravel the structure of criminal organisations, other advanced techniques such as machine learning, data mining, and data clustering are required to extract knowledge about criminal networks [9].

The application of artificial intelligence and machine learning techniques can help financial institutions achieve greater efficiency while reducing the time and costs associated with manual inspection. Intelligent AML systems monitor transactions in real time and detect suspicious transactions. These systems can learn and adapt thereby enabling financial institutions to detect new money laundering schemes as they arise. Intelligent AML systems can employ an enterprise-wide approach and screen every suspicious transaction as opposed to approaches that only look out for specific behavioural patterns [3]. In addition, deep learning methods, natural language processing, and the integration of unstructured external data sources such as news items and social media information into AML systems can enable financial institutions to achieve greater efficiency [2]. Deep learning is an advanced form of machine learning that is comprised of

artificial neural networks with the capability to learn from high amounts of data autonomously thereby engendering machine-enabled resolution of complex problems without human intervention[13]. Artificial intelligence and machine learning technology-based solutions can enable financial institutions to automatically monitor, process, and analyse suspicious transaction activities and differentiate such illicit transactions from normal ones in real-time[14]. A recent report by Financial Action Task Force (FATF) suggests that the financial services industry is beginning to embrace new technologies with cloud capabilities to centralise and process big data. The report shows that this new technique employs machine learning to detect financial crimes. This dynamic risk assessment tool incorporates existing typologies on money laundering, accounts for the social linkages between entities that are linked to suspicious transactions, and quantifies the suspicious behaviour of an entity with respect to its historical behaviour on the one hand and peer groups of similar characteristics on the other. The report further reveals that the use of artificial intelligence is not only relevant for the identification of suspicious transactions but machine learning with natural language processing and cognition capabilities combined with robotic process automation can help simplify and interpret large volumes of unstructured regulatory documents and facilitate automatic regulatory reporting.

A report by McKinsey and Company demonstrates how a large US bank was able to overcome the high rate of false positives in anti-money laundering (AML) alerts using a combination of machine learning approaches and the incorporation of new data elements. Initially, the bank employed a two-stage suspicious transaction verification procedure where transactions were first screened by a team of experts to eliminate false positives before escalating to the next team for further investigation. However, this process was overtaxing, and the underlying database was found to incompletely identify customers and transactions.

"By adding more data elements and linking systems through machine-learning techniques, the bank achieved a more complete understanding of the transactions being monitored" leading to

13 https://www.fatf-gafi.org/content/dam/fatf-gafi/guidance/Opportunities-Challenges-of-New-Technologies-for-AML-CFT.pdf.coredownload.pdf

14 https://www.fatf-gafi.org/content/dam/fatf-gafi/guidance/Opportunities-Challenges-of-New-Technologies-for-AML-CFT.pdf.coredownload.pdf

a significant reduction in false positive rates.[15] AI-driven anti-money laundering frameworks are more effective than rules-based systems[16] in transaction screening, monitoring, and identification of suspicious activities with lower rates of false positives. Artificial Intelligence becomes even more powerful in AML when combined with contextual data[17].

The use of Artificial Intelligence and machine learning comes with significant risks that require careful consideration. A recent report by the IMF revealed that Artificial Intelligence especially Generative AI poses significant risk to the financial system[11]. Potential areas of major concern include data privacy, embedded bias, robustness, explainability, cyber security, and financial stability. Huge amounts of data are required to train machine learning models. Any leakage in the trained dataset can lead to the disclosure of sensitive information and undermine data privacy. Bias in underlying AI algorithms has the potential to engender discrimination in access to financial services especially when these algorithms work in favour of a particular group or region. The robustness of AI models is crucial in AML systems given that inaccurate predictions can lead to wrong conclusions. Explainability or the ability to interpret GenAI systems could pose a significant risk to AML systems given that financial institutions require transparency to meet their regulatory obligations. Artificial intelligence and quite recently generative AI are equally susceptible to cyberattacks which can be exploited by criminals to disrupt AML systems. The hallucinations associated with GenAI for example can spread misinformation in financial reporting with significant implications for financial stability [11].

3. SOLUTION FRAMEWORK

In response to the increasing demands of and penalties from AML laundering banks and financial institutions have sought to re-think and expand their compliance and control frameworks. Solution providers have sought to meet expanding demand through innovations in their core

15 https://www.mckinsey.com/~/media/mckinsey/business%20functions/risk/our%20insights/mckinsey%20on%20risk%20issue%204%20winter%202018/mckinsey-on-risk-issue-4.pdf

16 https://learn.napier.ai/hubfs/eBooks/AI_financial_crime_typologies.pdf

17 https://learn.napier.ai/hubfs/eBooks/AI_financial_crime_typologies.pdf

technology, how they position themselves in the control framework, and which segments of the market they emphasize. The overall scope of the market has also increased to include non-financial organizations such as merchants. The market for machine learning platforms will continue to increase as banks and financial institutions expand their data science and machine learning capabilities and as vendors advance model development, guidance, and documentation. A number of institutions are interested in more “pre-packaged” solutions that do not require them to invest heavily in data science capabilities. This has seen a significant rise in Software-as-a Service solutions and an increasing push for offerings targeting non-data scientists. Regulators are becoming less averse to the adoption of advanced detection systems, such as those that machine learning platforms and ecosystems leverage. Yet, along with increased adoption of solutions with advanced analytics has come the need to provide more transparency for regulators.

Historically, conventional detection solutions were self-contained, purpose-built systems focused on one use case (or a relatively narrow grouping of very similar use cases) that tightly coupled signal processing and signal risk analysis. Through the increased adoption of data analytics capabilities financial institutions discovered that they were able to aggregate the output of discrete purpose-built detection systems and feed them into what many practitioners refer to as a “risk engine.” The amplification of benefits, particularly for complex attack vectors such as money laundering, derives from examining the predictive value of greater and greater ranges of characteristics throughout not just the entirety of the journey but of the history of the relationship. Advancements in processing power, data management, and analytics capabilities led innovative solution providers in this space to build highly integrated, multilayer control frameworks capable of tightly integrating and switching highly specialized best-in-breed signal detection controls with advanced event risk assessment and decision-support engines re-usable across a variety of use cases. These frameworks could be bespoke for institutions that can afford to build these, which enables the FI to find an optimal combination of best-in-class signal detection systems with next-generation risk engines that offer agile data integration capabilities and powerful risk modelling features. They could also be eco-system centric, which allows for a more “out-of-the-box” implementation using well recognized vendors that is less technically complex and could be perceived as less risky than the bespoke solution.

We will next focus on the main underpinning technologies for the three main use cases, name screening, transaction screening, and transaction monitoring that we wish to consider. We begin by outlining the main drivers for the adoption of these technologies. Regulatory pressure is a major driver as outlined in the first section and this is closely related to dissatisfaction with current systems for surveillance. Most rules-based surveillance platforms generate a high volume of false positive alerts, driving up costs and headcount. Moreover, many suspicious and unusual events go undetected. Many legacy systems cannot bring disparate data sets together and unlock their value.

Increasing internal pressure for operational efficiency also drives increased technology adoption. The trend of AML functions augmenting staff cannot continue because of the prohibitive cost. Yet financial crime will continue to escalate, regulatory expectations and scrutiny will increase, and transactions will grow in volume and get faster. Client experience demands are also an important factor driving technology adoption in this context. Machine learning techniques can more easily and quickly digest and orchestrate vast data sources, enabling richer and more complete intelligence, further disrupting financial crime across the customer life cycle. Platform and ecosystem-based approaches can also propel more innovative approaches to fighting financial crime, by breaking down silos. There is increased demand for such innovative solutions for example in the UK Government's recent Economic Crime and Corporate Transparency Bill[18].

It is useful to split developments into two categories, those related to systems architectural change from an infrastructural perspective and those related to the technologies that typically sit within these new environments and bring with them new ways of solving regulatory problems.

Banks, their system architects, and software developers are turning their attention to cloud-native architectures as a path to customer-focused continuous innovation where new code can be deployed as and when the business needs to adjust to threats and opportunities in the external environment. Rapid innovation in the data management layer of cloud-native architectures, particularly in NOSQL[19] technologies, creates opportunities for banks to stream

[18] https://www.gov.uk/government/publications/economic-crime-and-corporate-transparency-bill-2022-factsheets/fact-sheet-information-sharing-measures

[19] https://www.mongodb.com/nosql-explained

transactional data from their core systems into secondary architectures. These include data lakes, which use NoSQL technologies to store data in their native formats, whether these are structured, semi-structured or unstructured.

Assuming the bank maintains sound governance that ensures data entering the lake is cleansed and classified, then analysts, data scientists, and software developers can find and access data for transformation and downstream processing by predictive algorithms of machine learning.
This approach allows banks to gain an accurate picture of their customers' spending, loan, preference patterns, and to identify transactional patterns indicative of financial crime.
The importance of this two-speed architecture and data lake concepts is summarized in the following extract from a recent McKinsey paper on the future of monitoring risk in banking.

> *The supporting IT infrastructure and data could take a variety of forms, although the most recent trends lean toward a "two- speed architecture" and data lakes. A two-speed architecture decouples the bank's IT architecture into a slower, reliable back end (e.g., the bank's core IT systems, often the legacy systems) and a flexible, agile front-end that is customer-facing. A data lake gathers and stores all types of data, structured and unstructured, internal and external. Data entering the bank need not follow strict rules (as would be required of data entering an enterprise data warehouse). Instead, the users of the data define the rules when they extract the data from the lake. By combining this flexibility with Google-like search technology, the data lake provides banks with a step-change that helps them leverage their data for multiple purposes, ranging from marketing to risk to finance. The scope and flexibility of the system help banks use big data tools for complex data investigation and analysis*[20].

The availability of cost-effective access to vast amounts of cloud-based computing power is also a very significant development. Both Amazon and Microsoft through their AWS and Azure offerings now offer easy and cost-effective access to any Bank or FI that wishes to build its own cloud-based environment. In addition, these companies and others – in particular, Google – provide a large range of tools to help with the creation of efficient big data repositories resident

---

20 https://www.mckinsey.com/~/media/mckinsey/dotcom/client_service/risk/pdfs/the_future_of_bank_risk_management.ashx

in the cloud. Google has created several innovative tools, including the capability of easily building a high-performance machine-learning environment using Tensor Processing Units (TPUs)[21].

Inside and around the new systems architectures will sit a range of individual technologies whose primary purpose will be to address the main business challenges of the RegTech ecosystem. The most relevant in our setting are natural language processing , network analytics and machine learning.

NLP excels at the automated analysis of huge quantities of unstructured data, and it is a powerful resource for financial institutions as they combat fraud, money laundering, and criminal enterprise generally. A number of technology companies are deploying NLP as part of the overall KYC/AML customer profile. Typical use is in quicker understanding of the context and sentiment of articles and other information related to the entity under review during an extended customer due diligence (CDD) review. With NLP, it is about both the content and the context, as certain content might, taken alone, ring alarm bells, but when viewed in context, it means something entirely different. NLP applies this logic to its processing, taking context into account. This helps whittle down incidences, which previously identified as fraudulent. In financial crime compliance and AML, NLP reads new sources to find mentions of suspects or 'bad actors' and understands what those sources are saying about the individuals concerned. NLP can speed up the review process by over 60% by eliminating false positives from news analysis on an individual[22].

Network analytics specifically focusses on identifying and forecasting connections, relationships and influence among individuals and groups – it mines transactions, interactions and other behavioural information that may be sourced from social media. In a financial crime context, banks can use network analytics to identify links and patterns that traditional monitoring systems would not identify[23]. It is worth highlighting that Network analytics differs from SMA (Social Media Analytics) in that the former is trying to identify patterns of financial transactional

[21] https://cloud.google.com/tpu

[22] https://www.ibm.com/downloads/cas/WKLQKD3W

[23] https://www.mckinsey.com/industries/financial-services/our-insights/banking-matters/network-analytics-and-the-fight-against-money-laundering

behaviour between connected groups of individuals whereas the latter is concerned with identifying predictive patterns of behaviour among individuals.

There are three kinds of machine learning, supervised, unsupervised and reinforcement learning. In supervised learning, the system tries to learn relationships and interpret data based on labelled examples provided. In unsupervised learning, the system tries to discover data points with similar characteristics, and unsupervised learning is characterized by the lack or paucity of labelled data points. In reinforcement learning the system tries to learn based on trial and error using feedback provided by humans. Machine learning methods can be used to set fraud transaction monitoring thresholds based on an analysis of risk data and decide whether to trigger a fraud alert based on customer profile information. This allows human analysts to focus on high priority alerts while the lower risk alerts can be resolved in bulk or used to train newer analysts. Unsupervised machine learning can help uncover more bad actors using weak correlates and identify true actors operating behind the scenes using identity clustering to seek out hidden relationships. Machine learning methods can be used to find optimal combinations of rules and priorities and allow for more effective tuning of rules-based thresholds using methods such as Bayesian hyper-parameter tuning. This process can also be carried out using typologies instead of rules where the expert can focus on selecting the right set of typologies and let the machine learning system generate the right risk indicators and calibrate the relevant thresholds. Machine learning anomaly detection pinpoints atypical or abnormal behaviours by looking at multiple weak signals that combine to identify a higher risk than they would alone.

We now discuss a number of best-in-breed providers who have developed innovative AML platforms. Featurespace is a Cambridge based start-up that designed its ARIC Risk Hub as an enterprise AML and fraud transaction monitoring platform, leveraging advanced rules and machine learning models to deliver real-time and explainable detection. The ARIC Risk Hub leverages advanced, explainable anomaly detection to enable clients to automatically identify risk, catch new attacks, and identify suspicious activity in real-time. Using supervised and unsupervised machine learning techniques, ARIC Risk Hub delivers predictive risk scores on current activity based on past customer behaviour, while also spotting new attack types. ARIC Risk Hub is recognized for its predictive power, explainability, and ability to scale in high-volume

low-latency environments. ARIC Risk Hub enables customers to develop a range of risk models using a variety of modeling techniques within their model development environment or to import risk models developed on external platforms by way of PMML or data studio products. Once the models are developed, tested, and trained, ARIC Risk Hub houses a variety of tools for deploying, managing, and monitoring models as well as managing alerts and investigations. ARIC Risk Hub was engineered for high availability, resiliency, and easy integration with other systems. The platform can support multitenancy, with model customization capabilities at the subtenant level, making it appealing to large, complex deployments such as those common among processors and acquirers. While the model development platform enables customers to develop risk models based on virtually any use case, most of its clients have gravitated toward applications specific to transaction monitoring for both fraud and AML, application fraud and KYC, holistic cross-channel interaction monitoring, and cross-product customer risk scoring. Clients also use ARIC Risk Hub to complement existing tools within their financial crime ecosystem, such as scoring events using ARIC Adaptive Behavioral Analytics models and using ARIC Risk Hub as an orchestration layer. They successfully completed the PETS challenge securing a place as one of the UK winners. The winners of the challenge, which was convened to drive innovation in Privacy-Enhancing Technologies that reinforce democratic values, were announced at President Biden's second Summit for Democracy. The winning solutions combined different PETs to allow the AI models to learn to make better predictions without exposing any sensitive data. The prizes encouraged the development of innovative solutions that address practical data privacy concerns in real-world scenarios.

Feedzai has built its solution as an omnichannel financial crime platform that clients can expand and adapt as their business grows and their risk evolves. Feedzai's platform combines a flexible range of model development and deployment mechanisms to detect fraud and money laundering activities in real time—empowering data scientists to build their own models, enabling the import of third-party models, and providing professional services resources to build custom models for its clients. The combination of its rules-based risk scoring engine and diverse algorithms enables large data set analysis in milliseconds, offering real-time decision-making capabilities. It leverages graph-based techniques to surface different AML and fraud typologies, such as mule accounts, layering tactics, triangle schemes, structuring, ATO, and bot attacks. Their platform fully automates the entire model building pipeline, from feature engineering to

model training, hyperparameter tuning, model selection, and accelerating model creation. Leveraging machine learning to actively monitor deviations to expected model behaviour (e.g., changes in input data, sudden attacks, and model degradation), Feedzai's automated model monitoring can optimize model performance and responsiveness. Moreover, Feedzai's automated rules system uses machine learning to provide rules recommendations with demonstrable value.

4. CONCLUSION

This white paper focuses on the effectiveness and limitations of Artificial Intelligence (AI) in detecting and preventing money laundering activities. Thus, this paper discusses the challenges with existing AML systems in the financial services sector and highlights possible automation solutions that can be leveraged to drive efficiency in combating financial crimes. The paper identifies the false positives problem as a major challenge with rules-based AML systems and views manual verification processes in the identification of suspicious transactions as tasking and costly. The paper recommends the adoption and integration of AI into AML systems to simplify compliance while achieving greater efficiency at reduced costs. Finally, the paper discusses emerging risks associated with AI models and anticipate that financial institutions will take the necessary steps to reduce their risk exposure in AI-driven AML systems.

References

1. Schneider, F. and U. Windischbauer, *Money laundering: some facts.* European Journal of Law and Economics, 2008. **26**(3): p. 387-404.
2. Han, J., et al., *Artificial intelligence for anti-money laundering: a review and extension.* Digital Finance, 2020. **2**(3-4): p. 211-239.
3. Gao, S. and D. Xu, *Conceptual modeling and development of an intelligent agent-assisted decision support system for anti-money laundering.* Expert Systems with Applications, 2009. **36**(2): p. 1493-1504.
4. Khan, N.S., et al., *A Bayesian Approach for Suspicious Financial Activity Reporting.* International Journal of Computers and Applications, 2013. **35**(4).
5. Perez, D.G. and M.M. Lavalle, *Outlier Detection Applying an Innovative User Transaction Modeling with Automatic Explanation*, in *2011 IEEE Electronics, Robotics and Automotive Mechanics Conference*. 2011. p. 41-46.
6. Larik, A.S. and S. Haider, *Clustering based anomalous transaction reporting.* Procedia Computer Science, 2011. **3**: p. 606-610.
7. Rocha-Salazar, J.-d.-J., M.-J. Segovia-Vargas, and M.-d.-M. Camacho-Miñano, *Money laundering and terrorism financing detection using neural networks and an abnormality indicator.* Expert Systems with Applications, 2021. **169**.
8. Vorobyev, I. and A. Krivitskaya, *Reducing false positives in bank anti-fraud systems based on rule induction in distributed tree-based models.* Computers & Security, 2022. **120**.
9. Dreżewski, R., J. Sepielak, and W. Filipkowski, *The application of social network analysis algorithms in a system supporting money laundering detection.* Information Sciences, 2015. **295**: p. 18-32.
10. Fronzetti Colladon, A. and E. Remondi, *Using social network analysis to prevent money laundering.* Expert Systems with Applications, 2017. **67**: p. 49-58.
11. Shabsigh, G. and E.B. Boukherouaa, *Generative Artificial Intelligence in Finance: Risk Considerations*, in *NOTE/2023/006*. 2023, International Monetary Fund.

About the Authors

Dr. Devraj Basu is Senior Lecturer in Finance in the Accounting and Finance department at Strathclyde Business School. His area of academic research is financial markets, covering equity markets, commodity markets and alternative investments, as well as quantitative finance. He has published in top ranked international peer reviewed journals as well as top industry journals. He is actively involved in Regtech having set up the Regtech Forum which bring together industry, academia and government both within Scotland and internationally. The goal of the Regtech Forum is to help understand the fast moving Regtech landscape and how Scotland and the UK can position themselves to become leading global players. He has helped design Strathclyde's MSc in Financial Technology, the UK's first master's program in Fintech.

Email: devraj.basu@strath.ac.uk

Dr. Godsway Tetteh is a Research Associate at the Financial Regulation Innovation Lab (FRIL), University of Strathclyde. Previously, he worked as a Knowledge Exchange Associate with the Financial Technology (FinTech) Cluster at the same university. Prior to this, he was a Tutor at the Cambridge Centre for Alternative Finance at the University of Cambridge. There he contributed to building the capacity of FinTech entrepreneurs, regulators, and policymakers from across the globe on FinTech and Regulatory Innovation. He also served as a Public Policy Tutor at the United Nations University-MERIT. Godsway has a Ph.D. in Economics from Maastricht University in the Netherlands with a specialisation in Economics of Innovation. He has a Master of Science degree in Global Economy from the University of Glasgow, UK, and a Bachelor of Arts degree in Geography and Resource Development from the University of Ghana. His research focuses on the impacts of digital technologies and financial innovations (FinTech) on financial inclusion, welfare, and entrepreneurship in developing countries. He has previously examined the effects of local digital lending development, digital infrastructure, and mobile money in developing countries. He currently works on the Financial Regulation Innovation project that focuses on the application of technologies to drive regulatory innovations (RegTech) and efficiency in financial regulation compliance. Godsway has published in reputable journals including Small Business Economics.

Email: godsway.tetteh@strath.ac.uk

GET IN TOUCH

For further information,
please contact us at
FRIL@FinTechscotland.com

FinTech Scotland®