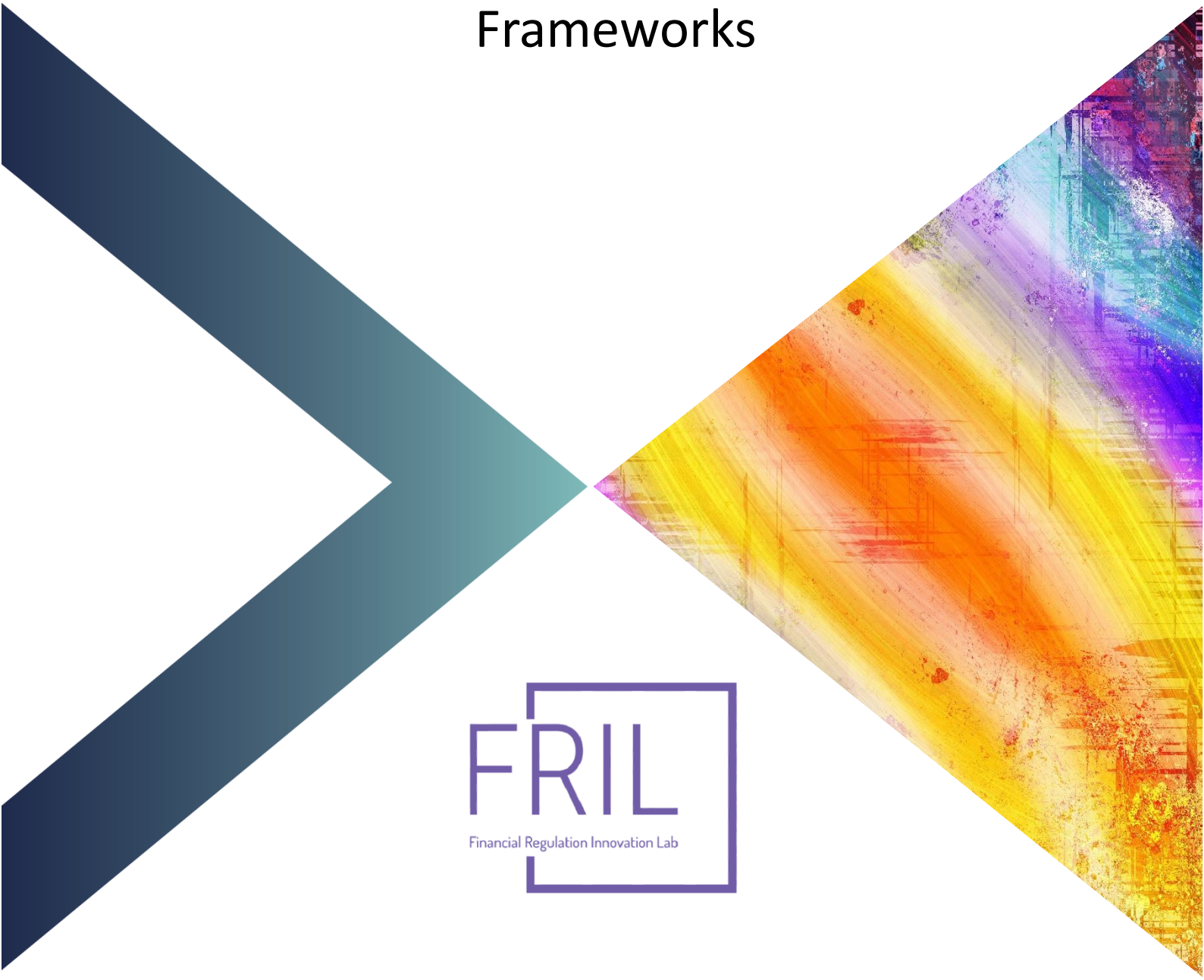
ISSN: 3033-4136
DOI: https://doi.org/10.17868/strath.00091081

Enhancing Financial Crime Detection By Implementing End-to-end AI Frameworks



FRIL
Financial Regulation Innovation Lab

FinTech Scotland®

University of Glasgow

University of Strathclyde Glasgow

in collaboration with

sopra steria

Financial Regulation Innovation Lab

Who are we?

The Financial Regulation Innovation Lab (FRIL) is an industry-led collaborative research and innovation programme focused on leveraging new technologies to respond to, shape, and help evolve the future regulatory landscape in the UK and globally, helping to create new employment and business opportunities, and enabling the future talent.

FRIL provides an environment for participants to engage and collaborate on the dynamic demands of financial regulation, explore, test and experiment with new technologies, build confidence in solutions and demonstrate their ability to meet regulatory standards worldwide.

What is Actionable Research?

FRIL will integrate academic research with an industry relevant agenda, focused on enabling knowledge on cutting-edge topics such as generative and explainable AI, advanced analytics, advanced computing, and earth-intelligent data as applied to financial regulation. The approach fosters cross sector learning to produce a series of papers, actionable recommendations and strategic plans that can be tested in the innovation environment, in collaboration across industry and regulators.

Locally-led Innovation Accelerators delivered in partnership with DSIT, Innovate UK and City Regions

Department for Science, Innovation & Technology

UKRI Innovate UK

GLASGOW CITY REGION

FRIL White Paper

Enhancing Financial Crime Detection By Implementing End-to-end AI Frameworks

Kal Bukovski* Jonny Cooper* Dr Devraj Basu**

** Sopra Steria*

***University of Strathclyde*

October 2024

Abstract: Economic crime, encompassing money laundering, fraud, scams, and various other illegal financial activities, continues to evolve with the emergence of sophisticated Artificial Intelligence (AI) technologies. This white paper explores the dual-edged nature of AI in the financial sector. While AI tools are increasingly being exploited by criminals to commit financial crimes, they also hold the key to more robust and effective detection and prevention strategies. This paper delves into the array of AI techniques currently leveraged by malicious criminals, including deepfake technologies, phishing and spear phishing, automated social engineering, credential stuffing, synthetic identity fraud and others. Furthermore, it provides a comprehensive analysis of AI techniques capable of countering these threats. Key focus areas include Neural Networks for unusual patterns and behaviours, gradient boosting algorithms for risk assessment, reinforcement learning for optimisation of decision making, Markov chains for temporal patterns and anomalies over time, Naïve Bayes for real-time classification and decision trees for interpretable detection. The culmination of this paper is the presentation of a state-of-the-art end-to-end AI-driven solution that integrates AI technology to offer a holistic and dynamically adaptable approach to financial crime detection and prevention. By implementing this framework, financial institutions can significantly enhance their capabilities to identify, mitigate, and prevent financial crimes, ensuring a more secure financial ecosystem.

Table of Contents

1. Introduction

It is no secret that financial crime, such as money laundering, fraud and scams are not only a significant current problem for both firms and consumers, but one that is due to grow rapidly in the coming years. Fraud represented 40% of all crime committed in 2023 with an estimated £6.8 billion cost to society in England and Wales in 2019-20 [1].

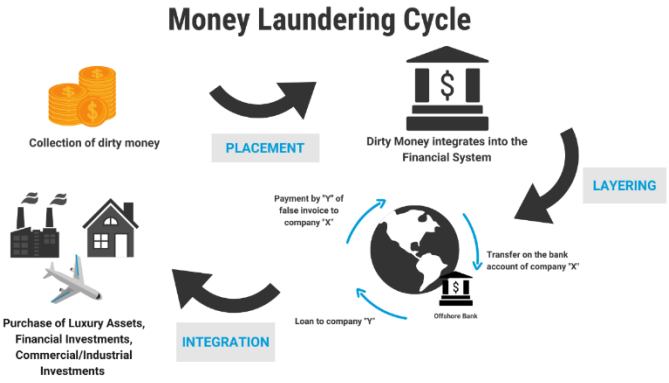
This situation is only being made worse due to the cost-of-living crisis, with consumers more willing to take risks, whether that be making 'too good to be true' purchases online, accepting opportunities that offer quick payouts, or romance scams resulting from individuals feeling alone and isolated.

Mix this with the rapid advancement and accessibility of technology, in particular Generative AI, and scams are becoming more realistic and security layers becoming easier to breach when in the hands of bad actors. For example, it may be exciting to create fake images of yourself with interesting backgrounds using AI, but in eyes of the fraudsters, that is fake IDs, synthetic documents and an opportunity to create fake bank accounts.

Whilst all of this presents significant challenges for financial institutions, it is more important than ever to give consumers the best user experience possible with a smooth customer journey. So, how do we strike the best balance between these two drivers?

2. Fraud, Scams and Money Laundering

Two of the main types of financial crime, fraud and scams, usually occur as isolated incidents, through individual transactions. Fraud is a type of crime when the payment in question is not authorised, usually processed as a result of ID theft or compromised personal information from plastic cards. A particularly concerning issue in the digital payment landscape is the way fraudsters use digital wallets contactless card payments, driven by technologies like near-field communications (NFC). With nearly 1bn people using contactless payments today, the total amount of transactions of such type is expected to generate approximately $10 trillion by 2027 [2]. According to UK Finance's 2024 annual fraud report, around £1.2bn has been stolen by fraudsters in each of 2022 and 2023 [3], [4].



Typical Money Laundering Cycle
Source: UN Office on Drugs and Crime

Scams occur when the customer is tricked into transferring money to the criminal's account, or has provided their account details, trusting that these will be used for genuine purposes [5]. Some of the most common types of scams are imposter (e.g. romance) scams, blackmail, charity scams, online shopping, prizes and lotteries, investment-related, mobile services, travel and others [6], [7].

Financial crimes like money laundering, evolve gradually through multiple transactions. According to Europol, 86% of the EU's most threatening criminal networks employ money laundering techniques and use legal business structures, to carry out their operations [8]. According to the United Nations' Office on Drugs and Crime, money laundering is estimated between 2% and 5% of global GDP every year [9].

Financial institutions are expected to collaborate with customers, experts and regulators to protect customers, market security and their own reputation. We have

seen several fines imposed on major banks in recent years, resulting from outdated or inefficient AML practices, such as Santander UK (£108M in 2022) [10], NatWest (£265M in 2021) [11], and HSBC (£64M in 2021) [12].

3. Global rise of AI-driven financial crime

Several global factors have significantly accelerated the use of AI by fraudsters and scammers:

COVID-19 pandemic, geopolitical conflicts, and economic uncertainty

The pandemic led to a substantial increase in online activity, as more people work from home and rely increasingly on digital services. This shift has created new opportunities for fraudsters to exploit vulnerabilities in online platforms and remote work environments. This has contributed to a significant rise in phishing and other online scams since the pandemic [34, 35].

Economic downturns and financial instability often result in an increase in fraud as individuals and businesses become more desperate for financial gain. The global economic impact of COVID-19, combined with other factors like inflation and the resulting cost of living crisis, has provided prolific ground for fraudsters to exploit economic fears and uncertainties. With the massive post-COVID jump in online transaction volumes, some banks are having trouble managing the volume of data required for machine learning models to learn behavioural patterns. Subsequently, the rise in false positives has opened a new set of challenges as with banks investigate transactions as suspicious. The operational costs and available resources cannot catch up with the new levels of manual investigation resource needed [31].

Geopolitical tensions and conflicts can disrupt global economic stability, leading to increased cyber activities, including state-sponsored hacking and cyber espionage. Fraudsters exploit these uncertain times by launching attacks, taking advantage of the chaos and the increased focus of nations on security over cybersecurity.

Advancements in AI technology

The rapid development and accessibility of AI technologies have made it easier for fraudsters to create sophisticated scams. Generating deepfakes, automating phishing attacks, conducting credential stuffing etc. has become more accessible, lowering the barrier for entry into high-tech fraud.

Digital transformation, increasing connectivity and IoT devices.

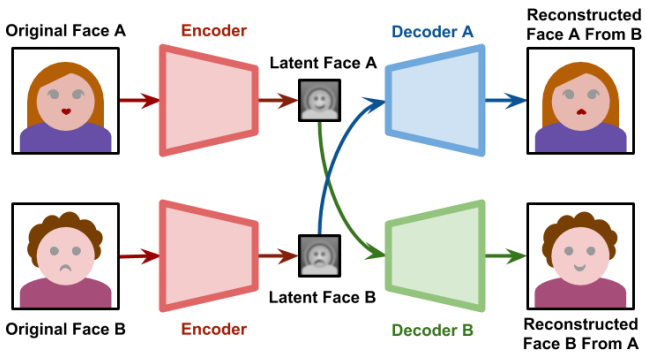
As businesses increasingly move their operations online and adopt digital transformation strategies, the attack surface for criminals expands. This includes more digital financial transactions, remote work infrastructure, and online customer interactions and others, which can be targeted by AI-driven fraud techniques.

The growth of Internet of Things (IoT) devices has created new avenues for attacks. Many IoT devices should adopt more robust security measures, making them less vulnerable to being used as entry points for larger network intrusions.

4. Common AI applications used by fraudsters

4.1. Deepfakes

AI-generated synthetic media where a person in an existing image or video is replaced with someone else's likeness are called ‘Deepfakes’. Falsifying biometric data enables impersonation for unauthorised access to accounts, spreading misinformation, and creating fake identities for fraudulent activities. Machine Learning frameworks, such as generative adversarial networks (GANs) and diffusion models are amongst the common methodologies used to generate deepfakes [13].

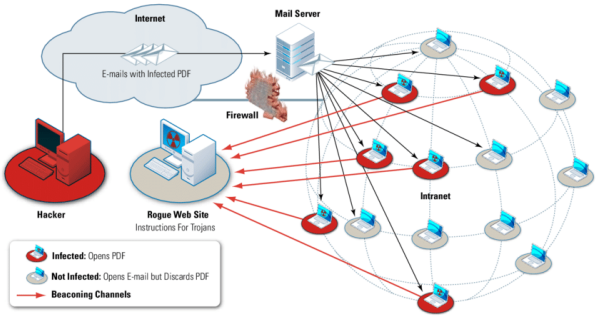


Generating Deepfakes Process Source: alanzucconi.com

4.2. Phishing and spear phishing

AI tools are used to craft highly personalised and convincing phishing emails or messages, harvesting sensitive information like login credentials, financial information, and personal details by mimicking legitimate communications.

Whilst phishing is a generic automated scam message, targeting a large audience and usually containing links to malicious websites, spear phishing is a personalised cyberattack toward individual or organisations. These emails or texts contain highly convincing personalised messages, attempting to gain your trust [14], [15], [16].



Visualisation of spear phishing attack Source: ResearchGate "Security Through Understanding… and Emulating…the Advanced Persistent Threat"

Generative AI enhances the criminals' ability to generate phishing emails and vishing (voice phishing) calls and voicemails. Large Language Models (LLMs) are used to consume vast amounts of real-time information and AI chatbots target corporate environments for communication campaigns. These tools are becoming more advanced and harder to spot, with the expectation of a drastic increase in both quality and quantity [17], [18]. This emerging thread amongst all other financial crimes, outlines the importance of the responsible use of AI, as it is expected that criminals may soon exploit real-time technologies for phishing and spear phishing attacks [19].

4.3. Automated social engineering

Social engineering is effectively manipulation of people to feel a sense of urgency in taking an action [20]. AI-driven chatbots and voice assistants are often used to convincingly interact with victims and use their vulnerabilities to make them open scam links, install malware, share credentials and others. There are known cybercriminal forums where hackers share tips and even tools which can be exploited for criminal activities. One of the biggest known cyber-attacks of the century, which happened on Yahoo! in 2014, was a result of advanced automated social engineering, as confirmed by the FBI [21].

Fraudsters can extract personal information through automated conversations, often mimicking trusted individuals or entities. The usual lifecycle of social engineering contains four phases: 'Investigation', 'Hook', 'Play' and 'Exit' [21]. In simple terms, these represent victim selection, building of a trusted relationship, manipulation to obtain information, and moving on to the next victim.

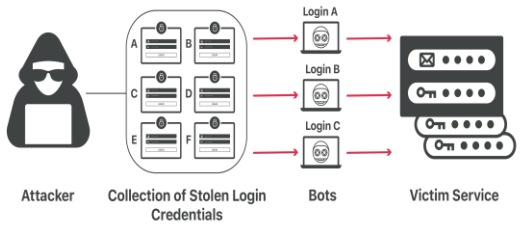
Cyber-attacks on social and professional networks use AI chatbots for automated social engineering, acting as fake accounts and simulating human behaviour, bypassing security mechanisms [22]. This form of criminal activity is mainly used as an engine for stealing sensitive personal or corporate data.

4.4. Credential stuffing

Using AI to automate the process of testing large sets of stolen credentials across various sites is called credential stuffing. Gaining unauthorised access to multiple accounts if the same credentials are reused, is a validation approach used by criminals.

Despite the regular reminders and corporate requirements imposed by regulators, the

human tendency of using the same credentials across multiple accounts is still a significant vulnerability used by hackers through the 'dark web'. Opposed to the 'brute force attacks' where hackers use automated software to generate a huge number of potential passwords until the log-in is successful, the 'credential stuffing' approach uses valid credentials from compromised accounts and targets other logins of the same individual [23].



Credential stuffing approach
Source: cloudflare.com

Credential stuffing is a gateway for a variety of criminal activities, such as ransomware, identity theft, fraudulent transactions and others. In addition to the financial loss, the impact on reputational damages and user frustrations are not to be underestimated [24]. There is a variety of best practices to use technology for detection of credential stuffing. The most common techniques are monitoring login patterns, multi-factor authentication (MFA), rate limiting (CAPTCHA), custom security rules and device fingerprinting [25].

4.5. Synthetic identity fraud

Opening new accounts, securing loans, and making fraudulent transactions that are hard to detect is often done using synthetic identities. Other examples are setting up mule accounts for money laundering and financing terrorism. Fraudsters create fictitious identities by combining real and fake information using (generative) AI and often sell these as fraud-as-a-service (FaaS).

Synthetic identity fraud involves creating a new identity of a person who doesn't exist legally, by mixing real, stolen and synthetic information. These scalable and automated techniques require more sophisticated biometric verification systems, combining forensic and non-forensic inspection of multiple ID documents [26] (estimations show that 95% of synthetic identities are not detected [27]), comparing with credit bureau databases, associated accounts and know-your-customer (KYC) checks [28].

Elements of Synthetic Identity Fraud
Source: fedpaymentsimprovement.org

Other use cases of AI applications for financial crime include AI-driven malicious software (malware) and ransomware (the most common malware). These can adapt to avoid detection and select targets based on their ability to pay, by stealing data, encrypting systems, and demanding ransom with sophisticated evasion techniques or benefiting from poor cycler hygiene [29]. Another example is automated financial trading fraud - using AI algorithms to conduct fraudulent trading activities, engaging in pump-and-dump schemes, insider trading, and market manipulation [30].

5. Leveraging (AI) technology to fight financial crime

With the increasing sophistication of AI-driven fraudulent activities, traditional methods of detection and prevention are often inefficient. AI technologies present a promising solution, offering advanced analytics and automation to enhance detection accuracy and efficiency, revolutionising the financial crime landscape. In effect, the key exam question is how AI can confront AI in a long-term battle.

This can be illustrated as a game theory setup where AI technologies adopted by financial

institutions and criminals are the primary players, each with opposing objectives. The institutions aim to maximise security and minimise risk by deploying strategies such as enhanced monitoring, AI-driven anomaly detection, and strict compliance procedures. Criminals, on the other hand, seek to maximise their illicit gains while avoiding detection. This setup can be viewed as a non-cooperative game where each player continuously adapts their strategies in response to the other's actions. The equilibrium in this game occurs when neither side can unilaterally improve their outcome—financial institutions optimise their defences within regulatory constraints, while criminals adjust their tactics to evade these defences. Understanding this dynamic through game theory helps in designing more resilient and adaptive financial crime prevention systems.

The adoption of AI and Machine Learning (ML) within fraud detection and prevention systems has meant large improvements in the battle against fraud. The use of anomaly detection algorithms or classification models that provide banks with a probability score are prevalent within firms, providing them with a tool to reduce the number of fraudulent transactions that occur.

AI solutions can identify underlying trends that are simply too difficult for a human to see, mainly due to the vast quantities of data available to fraud prevention analysts, along with the imbalance of fraudulent versus genuine transactions.

Although AI solutions are key enablers in the fight against fraud, they are not always fully adaptable and transparent, making it difficult to react to emerging fraud threats or understand why a high-risk score has been produced. This is why rulesets are still fundamental to the operation of fraud prevention.

Rulesets give the organisation ultimate control over their risk appetite, alert volume and end user experience. They are easily interpreted, meaning they are easier to audit, but they can also be adjusted quickly when required.

While AI offers immense potential in combating financial crime, its implementation is not without challenges. Ensuring the ethical and responsible use of AI, mitigating algorithmic biases, and addressing data privacy concerns are key goals. Additionally, the evolving nature of financial crime demands continuous innovation and adaptation of AI solutions. AI represents a game-changer in the fight against financial crime, empowering institutions with innovative capabilities to detect and prevent unlawful activities. By harnessing the power of AI technologies and collaborating with regulatory bodies, the financial sector can safeguard the integrity of global financial systems.

6. Examples of AI techniques for financial crime prevention

Neural networks:

Neural networks can be used to analyse vast amounts of financial transactional data, identifying patterns indicative of fraudulent behaviour. By training neural networks on historical data containing both legitimate and fraudulent transactions, the models learn to detect anomalies and flag suspicious activities in real-time.

Neural networks enable financial institutions to enhance fraud detection capabilities by automatically identifying unusual patterns or behaviours in transactions.

Gradient boosting algorithms:

Gradient Boosting Algorithms (such as XGBoost) can be utilised to develop predictive models that assess the risk associated with different financial transactions or customer profiles. By analysing various features and historical data, they can assign a risk score to each transaction, enabling the institution to prioritise investigations and allocate resources effectively.

It allows financial institutions to build advanced risk assessment models that accurately predict the likelihood of fraudulent activities. By leveraging gradient boosting

algorithms, banks and other financial entities can mitigate risks associated with money laundering, terrorist financing, and other criminal activities, ensuring compliance with regulatory requirements and protecting their reputation.

Reinforcement learning:

Reinforcement learning can be applied to optimise decision-making processes in fraud detection and prevention. By simulating different scenarios and learning from feedback, reinforcement learning algorithms can autonomously adapt and improve fraud detection strategies over time, staying ahead of evolving threats. These models empower financial institutions to continuously enhance their fraud detection capabilities by learning from past experiences and adapting to new challenges.

Natural Language Processing (NLP):

NLP techniques can be used to analyse textual data from various sources, such as emails, chat logs, and social media, to uncover clues related to financial crimes. NLP algorithms can detect suspicious communication patterns, identify key entities or keywords associated with fraud, and extract actionable insights to support investigations.

NLP models enable financial institutions to enhance their monitoring and surveillance capabilities by analysing unstructured text data for signs of fraudulent behaviour. By leveraging NLP, banks can detect and prevent fraud schemes such as phishing scams, insider trading, and money laundering, to support protecting the integrity of the financial system and preserving customer trust.

Markov chains

Markov chains are stochastic models that describe a sequence of possible events where the probability of each event depends only on the state attained in the previous event. Markov chains can model the sequence of transactions or activities to detect unusual transitions that may suggest fraudulent behaviour. They are effective in identifying temporal patterns and anomalies over time.

Naïve Bayes:

Naïve Bayes is a probabilistic classifier based on Bayes' theorem, assuming independence between features. It’s particularly effective for large datasets and works well with categorical data.

These models can be used for fraud detection by classifying transactions as fraudulent or legitimate based on features such as transaction amount, location, time, and customer behaviour patterns. Naïve Bayes is fast, works well with large and high-dimensional data, good for real-time fraud detection.

Decision trees

Decision trees are a type of supervised learning algorithm that splits data into branches to form a tree-like structure, where each node represents a feature, each branch represents a decision rule, and each leaf represents an outcome.

Implementing decision trees can help identify complex decision patterns and anomalies in transaction data that are indicative of fraudulent activities. They are interpretable, allowing investigators to understand the reasoning behind a flagged transaction.

Cost-Benefit summary of the presented AI techniques

AI Technique	Cost	Benefit
Neural Networks	High computational resources and complexity, requiring significant data and expertise.	Highly effective for detecting complex patterns and anomalies in large datasets, ideal for identifying sophisticated financial crimes like fraud or money laundering.
Gradient Boosting Algorithms	Moderate to high computational resources with longer training times, though less intensive than neural networks.	Excellent at handling imbalanced datasets and boosting model accuracy, useful for detecting less obvious financial crimes with fewer false positives.
Reinforcement Learning	Usually, extensive training time and the need for a well-defined reward system, which can be challenging to design. The complexity can vary significantly depending on the specific problem domain.	Ideal for adaptive systems that learn and improve over time, especially useful in evolving threat landscapes where criminal tactics frequently change.
Natural Language Processing (NLP)	Requires large amounts of text data and complex preprocessing. Modern NLP models, particularly transformer-based models, can be computationally intensive, and require significant resources, especially for tasks like language modelling or sentiment analysis	Highly effective for analysing unstructured data like emails, transaction notes, or social media, to detect fraudulent activities and other financial crimes based on language.
Markov Chains	Simpler models with lower computational costs, but assumptions of the Markov property might not hold in more complex scenarios.	Useful for modelling sequential events and detecting anomalies in transaction sequences, such as suspicious account behaviour over time.
Naïve Bayes	Computationally efficient and easy to implement, but assumes independence among features, which may not be realistic.	Good for quick, initial screening of potential financial crimes, especially in situations with clear, probabilistic relationships.
Decision Trees	Prone to overfitting without careful tuning, though computationally less demanding.	Easy to interpret and explain, making them useful in regulatory contexts where transparency of AI decisions in detecting financial crimes is crucial.

While such AI-enabled systems are effective at identifying potentially criminal transactions, they often generate large sets of false positives – instances where legitimate transactions are incorrectly flagged as suspicious. False positives can result in delays, inconvenience, and additional scrutiny for customers. Moreover, investigating false alarms consumes resources, including manpower and time, leading to operational inefficiencies, increased compliance costs and sometimes reputational damages for the financial firms.

7. Regulatory approach to fighting financial crime

An example of a state-driven regulatory framework is the new UK regulation, PS23/3: 'Fighting Authorised Push Payment Fraud: A New Reimbursement Requirement', which will be implemented by the Financial Conduct Authority (FCA) to combat authorised push payment (APP) fraud. This regulation mandates financial institutions to reimburse victims of APP fraud in certain circumstances, aiming to enhance consumer protection and trust in the banking system. It sets out criteria for reimbursement eligibility and emphasises the responsibility of banks to safeguard customers against fraudulent transactions.

It will [32]:

- Require UK payment service providers (PSPs) to reimburse all in-scope customers who fall victim to APP fraud, unless the consumer is involved in the fraud themselves, or has acted with gross negligence.
- Share the cost of reimbursing victims 50:50 between sending and receiving PSPs, to provide incentives for both to detect and prevent fraud.
- Provide additional protections for vulnerable customers.

Another example is PS22/9 - the new Consumer Duty regulation refers to the ethical and legal obligation of financial institutions to prioritise the best interests of their customers [33]. This Duty encompasses ensuring transparency, fair treatment, and adequate protection of consumers from fraudulent activities such as scams, identity theft, and unauthorised transactions. Upholding Consumer Duty not only builds trust and confidence among customers but also contributes to the overall integrity and stability of the financial system.

Finally, the AI Act and broader digital ethics frameworks play a crucial role in guiding the responsible use of AI technologies. These regulations promote transparency, accountability, and fairness in AI systems, addressing concerns such as algorithmic bias, data privacy, and ethical considerations. One way to enhance regulatory compliance is Explainable AI (XAI). Regulators require that financial institutions not only detect suspicious activities but also clearly justify and document their findings. XAI enables institutions to provide interpretable insights into how AI models flag potential criminal activities, making it easier for regulators to assess compliance with legal standards and for institutions to defend their decisions during audits or investigations. By fostering trust in AI systems, XAI also helps mitigate the risk of regulatory penalties and strengthens the overall effectiveness of financial crime prevention efforts.

Compliance with the AI Act and adherence to digital ethics principles are essential for ensuring that AI-powered solutions in financial crime mitigation are effective, explainable, trustworthy and aligned with societal values and regulatory requirements.

8. What can financial services firms do to better protect their customers?

Organisations can create a hybrid approach to combat fraud and scams. By creating rulesets that factor in AI and ML based risk scores, a solution that is both transparent, adaptable and accurate can be implemented. This

methodology is already being used across different organisations and is seen to be incredibly effective when compared to either technique used in isolation. The white paper *"Using Automation and AI to Combat Money Laundering" (Devraj Basu, Godsway Korku Tetteh)* in the current White Paper Series articulates the nature of conventional financial crime purpose-built detection solutions.

However, there is a problem with this methodology. Rulesets combined with AI become very complex, with millions of possible combinations and permutations of rulesets available. In order to adjust rulesets to changes in the fraud environment or the business drivers, thresholds need to be changed. Data Science communities are already addressing this problem with methods such as those discussed earlier.

This then presents a further issue. Rulesets get tuned, adjusted and updated over time, moving them further away from the very reason they were created. Organisations then find themselves updating legacy rulesets that are out of date, ineffective and far too complex to manage. We can indeed continue to tune the ruleset, but we are better off redesigning the ruleset for the intended purpose at that moment in time.

By using AI to automate the design and construction of these rulesets, the benefits of hybrid rules are maintained, but with the added value of complete confidence that the rule design cannot be improved. An added benefit is that due to frequent and complete rebuild of the designs, they are no longer static, with gaps in the detection layer that fraudsters can expose.

A new technology built and patented by Sopra Steria provides a complete end-to-end optimised fraud management process that allows financial services organisations to stay in control, whilst having complete trust that they are providing the very best service for their customers. It allows financial services firms to be fully optimal in fraud prevention, delivering higher fraud detection and lowering false positive alerts.

What is it and what does it do?

This is not a point solution. It is an innovative tool that constructs optimal hybrid business rules with AI at the core, sitting as a layer on top of existing fraud solutions. The rules delivered by the tool daily allow firms to be in full control of their fraud management environment by alerting only the transactions that need to be, balancing their risk appetite with resource management, whilst ensuring their customers are protected, all in a way they have not been able to before.

Fundamentally, the solution takes in historical transaction data and outputs a set of 'rulesets', optimised for three objectives, minimising false positives, maximising true positives and maximising detected fraud value. There is always a trade-off between the three objectives, which means if you decrease one objective, you will also decrease another.

The algorithm will optimise the use of existing fraud detection models used by the firms today, as well as transaction data such as transaction amount, merchant ID and time/day. This solution does not replace existing fraud models, it enhances them, and as such, is not a fraud detection model in itself.

The rulesets produced offer an option for the firm in which one can choose the ruleset that adheres to the given risk appetite at that moment in time. As an example, the user could choose a ruleset that detects the most fraud cases possible, but at the cost of a higher number of false positives. Alternatively, they could choose a ruleset that focuses on high value payments, in turn preventing more loss at the expense of not detecting as many fraud cases.

The chosen ruleset will need to be implemented in the firm's existing decision engine platform, which will then utilise the ruleset with live transactions going forward. Without the frequent adjustment of rulesets, various negative situations can occur, such as not capturing the behaviour and patterns of new fraud typologies, not fluctuating according

to seasonal human behaviour changes or struggling to adapt to business environment changes like lower operational capacity.

By generating new rulesets with a rolling window of data and by focusing on the three objectives discussed previously, the scenarios above can be mitigated.

What does it deliver?

The solution will create a number of rulesets that combine the available parameters (i.e. transaction amount, time of day, fraud detection model 1 output, etc) along with optimal thresholds for each parameter. The combinations of parameters and thresholds will vary according to the trade-off being made. For example, for a low number of false positives, it could set more demanding thresholds for model scores which will be met less often.

The model/solution offers complete flexibility to cater to operational demands/requirements each time it is run by giving the client complete choice over which ruleset is implemented in the ruleset platform currently in place.

Due to being fully automated and self-learning, the model is a hands-off approach until the resulting rulesets are output. This means the only time required from the Data Scientists or Fraud Analysts is for reviewing and selecting the appropriate ruleset.

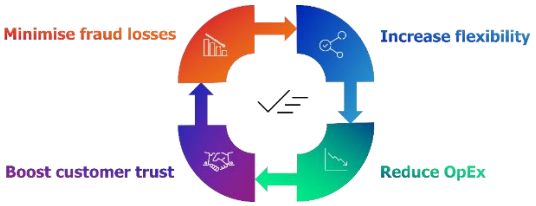
Finally, the number of false positives, true positives and fraud value detected when generating rulesets will be based on historic data, so the numbers may not be reproduced when running on future data. However, procedures have been put in place when the model is 'learning' which helps prevent the model from learning only the historic fraud patterns rather than being able to detect future fraud.

How can the model and results be used by financial services firms?

The model can be run as frequently as the user requires, matching the current schedule of multiple ruleset adjustments a day, or less frequently such as daily or weekly adjustments.

Our solution challenges traditional approaches by replacing previously defined business rules with an optimised set of AI generated business rules which the organisation chooses from; each offering a different approach depending on the risk appetite of the organisation at any given time.

Our rigorous analysis and testing performed to date supports the case that our optimised models are highly efficient, require little input from the analyst community and once deployed, will offer fraud analysts optimal options for balancing reduction of false positives, increase in fraud detection and increase of prevented loss.



As part of the end-to-end system design, it is crucial to have a human-in-the-loop approach, particularly when human behaviour is being captured by an AI solution. As well as the importance of interpretable and explainable solutions in terms of regulatory compliance, maintaining the use of rulesets, as opposed to a black box solution, allows the firms to understand the type of fraud that is being detected, an important aspect of continuous fraud management development.

9. Conclusion

The rapid advancement of AI technologies presents both significant challenges and remarkable opportunities in the realm of financial crime detection. As criminals become increasingly proficient at exploiting these technologies, the imperative for financial institutions and consultancy firms to adopt advanced AI-driven solutions becomes ever more critical. This white paper has highlighted the diverse range of AI approaches currently employed by criminals and the corresponding AI techniques that can effectively counteract these threats. By leveraging Machine Learning for anomaly detection, financial institutions can build a resilient defence against financial crimes. The proposed end-to-end AI

framework represents a comprehensive solution that not only addresses current threats but is also adaptable to future challenges. Implementing such a framework will enable financial institutions to stay ahead of criminal tactics, ensuring a robust and secure financial environment. In conclusion, the integration of advanced AI technologies is not just a strategic advantage but a necessity for the sustainable protection of financial assets and customers.

References

[1] “Fraud Strategy: stopping scams and protecting the public” – UK Government Updated 01/06/2023, last accessed 02/09/2024

https://www.gov.uk/government/publications/fraud-strategy/fraud-strategy-stopping-scams-and-protecting-the-public

[2] “Top 5 fraud trends in 2024 and how to mitigate them” – Comply Advantage Updated 18/04/2024, last accessed 02/09/2024

https://complyadvantage.com/insights/top-fraud-trends/

[3] “Annual Fraud Report 2023” – UK Finance Published 10/05/2023

https://www.ukfinance.org.uk/policy-and-guidance/reports-and-publications/annual-fraud-report-2023

[4] “Annual Fraud Report 2024” – UK Finance Published 03/06/2023

https://www.ukfinance.org.uk/policy-and-guidance/reports-and-publications/annual-fraud-report-2024

[5] “Fraud and scams” – Financial Ombudsman Service Updated 18/12/2023, last accessed 02/09/2024

https://www.financial-ombudsman.org.uk/businesses/complaints-deal/fraud-scams

[6] “The 10 Most Common Types of Fraud” - Louis DeNicola, Experian Published 17/04/2024

https://www.experian.com/blogs/ask-experian/most-common-types-of-fraud/

[7] “What are some common types of scams?” – Consumer Financial Protection Bureau, US Government Updated 13/03/2024, last accessed 02/09/2024

https://www.consumerfinance.gov/ask-cfpb/what-are-some-common-types-of-scams-en-2092/

[8] “Decoding the EU’s most threatening criminal networks” – Europol, Publications Office of the European Union, Luxembourg. ISBN 978-92-95236-25-7 | DOI: 10.2813/811566
Updated 29/05/2024, last accessed 02/09/2024

https://www.europol.europa.eu/publication-events/main-reports/decoding-eus-most-threatening-criminal-networks

[9] “Money Laundering” – Europol Last accessed 02/09/2024

https://www.europol.europa.eu/crime-areas/economic-crime/money-laundering

[10] “Santander UK fined £108mn for anti-money laundering failures” - Owen Walker and Oliver Ralph, Financial Times Published 09/12/2022

https://www.ft.com/content/fc78858a-5bfa-41f7-9fca-d9bfa6321ef6

[11] “NatWest fined £265m for money laundering failures” - Jane Croft and Robert Wright, Financial Times Published 13/12/2021

https://www.ft.com/content/f080cc09-62bc-4898-9814-ee7759d80cd7

[12] “HSBC fined £64m for failures on anti-money laundering” - Owen Walker and Laura Noonan, Financial Times Published 17/12/2021

https://www.ft.com/content/304f7abb-981d-47c1-bf89-4168597b9443

[13] “Future Cyber Threats 2021" – Accenture
Published: 2021

https://bankingblog.accenture.com/wp-content/uploads/2021/05/2021-Future-Cyber-Threats-for-Financial-Services_Accenture_Report.pdf

[14] “Phishing attacks: defending your organisation” – National Cyber Security Centre
Updated: 13/02/2024

https://www.ncsc.gov.uk/guidance/phishing

[15] “What is spear phishing?” – Cisco
Last accessed: 02/09/2024

https://www.cisco.com/site/uk/en/learn/topics/security/what-is-spear-phishing.html

[16] “Spear phishing: A definition plus differences between phishing and spear phishing” – Norton
Published 01/06/2022

https://uk.norton.com/blog/malware/what-spear-phishing

[17] “Generative AI is making phishing attacks more dangerous” – Ashwin Krishnan, techtarget.com
Published 18/12/2023

https://www.techtarget.com/searchsecurity/tip/Generative-AI-is-making-phishing-attacks-more-dangerous

[18] “AI Will Increase the Quantity — and Quality — of Phishing Scams” - Fredrik Heiding, Bruce Schneier and Arun Vishwanath, Harvard Business Review
Published 30/05/2024

https://hbr.org/2024/05/ai-will-increase-the-quantity-and-quality-of-phishing-scams

[19] “How AI is changing phishing scams” – Microsoft
Published: 14/07/2023

https://www.microsoft.com/en-us/microsoft-365-life-hacks/privacy-and-safety/how-ai-changing-phishing-scams

[20] “Advanced Automated Social Engineering Bots: The High Tide of Social Engineering Bots and the Scammers Riding Them” – CloudSEK blog
Updated: 03/02/2024

https://www.cloudsek.com/blog/advanced-automated-social-engineering-bots-the-high-tide-of-social-engineering-bots-and-the-scammers-riding-them

[21] “Overview of Social Engineering Attacks on Social Networks” - Kaouthar Chetioui, Birom Bah, Abderrahim Ouali Alami, Ayoub Bahnasse – Procedia Computer Science, Volume 198, Pages 656-661, ISSN 1877-0509
Published: 2022

https://doi.org/10.1016/j.procs.2021.12.302

[22] “Automated Social Engineering Attacks using ChatBots on Professional Social Networks” - Ariza, Maurício & Azambuja, Antonio & Nobre, Jéferson & Granville, Lisandro
Published: 05/2023

http://dx.doi.org/10.5753/wgrs.2023.747

[23] “Advisory: Use of credential stuffing tools” – National Cyber Security Centre
Published: 19/11/2018

https://www.ncsc.gov.uk/files/Credential%20stuffing%20advisory.pdf

[24] “What Is Credential Stuffing?” – ProofPoint.com
Last accessed: 02/09/2024

https://www.proofpoint.com/uk/threat-reference/credential-stuffing

[25] “Credential Stuffing: Examples, Detection and Impact” – Bret Settle, ThreatX
Updated: 05/07/2023

https://www.threatx.com/blog/credential-stuffing-examples-and-keys-to-detection/

[26] “Synthetic Identities: The Darker Side Of Generative AI” - Muhammad Shahid Hanif, Forbes
Published: 29/05/2024

https://www.forbes.com/sites/forbestechcouncil/2024/05/29/synthetic-identities-the-darker-side-of-generative-ai/

[27] “Trends in synthetic identity fraud” – Tad Simons, Thomson Reuters
Published: 21/04/2023

https://legal.thomsonreuters.com/en/insights/articles/trends-in-synthetic-identity-fraud

[28] "Beating synthetic identity fraud and building trust" – Chris Farmer, GBG
Last accessed: 02/09/2024

https://www.gbgplc.com/en/blog/beating-synthetic-identity-fraud-and-building-trust/

[29] "Learning from the mistakes of others – A retrospective review: Malware and ransomware" – Information Commissioner's Office
Last accessed: 02/09/2024

https://ico.org.uk/about-the-ico/research-reports-impact-and-evaluation/research-and-reports/learning-from-the-mistakes-of-others-a-retrospective-review/malware-and-ransomware/

[30] "AI-driven Market Manipulation and Limits of the EU law enforcement regime to credible deterrence" – Alessio Azzutti – ILE Working Paper Series, No. 54 (This version) Computer Law & Security Review Volume 45
Last updated: 12/08/2022

https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4026468

[31] "Covid-19 frazzles AI fraud systems" – Steve Marlin, Risk.net
Published: 06/04/2020

https://www.risk.net/risk-management/7520706/covid-19-frazzles-ai-fraud-systems

[32] "Anti-fraud controls and complaint handling in firms (with a focus on APP Fraud)" – Financial Conduct Authority
Updated: 23/04/2024

https://www.fca.org.uk/publications/multi-firm-reviews/anti-fraud-controls-complaint-handling-firms-focus-app-fraud

[33] "PS22/9: A new Consumer Duty" – Financial Conduct Authority
Updated: 27/07/2022

https://www.fca.org.uk/publications/policy-statements/ps22-9-new-consumer-duty

[34] "Criminals exploit Covid-19 pandemic with rise in scams targeting victims online" – UK Finance
Last accessed: 02/09/2024

https://www.ukfinance.org.uk/press/press-releases/criminals-exploit-covid-19-pandemic-rise-scams-targeting-victims-online

[35] "Learning from the mistakes of others – A retrospective review: Phishing" – Information Commissioner's Office
Last accessed: 02/09/2024

https://ico.org.uk/about-the-ico/research-reports-impact-and-evaluation/research-and-reports/learning-from-the-mistakes-of-others-a-retrospective-review/phishing/

ABOUT THE AUTHORS

Kal Bukovski is Consulting Senior Manager and Director of Academia & Research at Sopra Steria. He specialises in the financial services domain, driving transformative projects and data-driven excellence. With expertise in analytics, data science, business intelligence and data visualisation, he supports clients in making strategic decisions and gaining a competitive edge in this dynamic, regulated domain.

Kal leads business projects and collaborations with Academia, fostering innovation, compliance and data-driven storytelling. His main areas of expertise are regulatory modelling, credit risk, consumers' financial health, scorecards, pricing and others, enhancing risk management and customer experience for sustained success.

Email: kal.bukovski@soprasteria.com

Jonny Cooper is the AI Lead for Presales and Propositions at Sopra Steria, bringing 8 years of deep expertise in data science. Throughout his career, Jonny has been at the forefront of AI innovation, successfully leading the development and deployment of cutting-edge AI-driven solutions across a range of high-impact sectors, including aerospace and financial services.

Email: jonny.cooper@soprasteria.com

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

Get in touch

FRIL@FinTechscotland.com

FinTech Scotland®

University of Glasgow

University of Strathclyde Glasgow