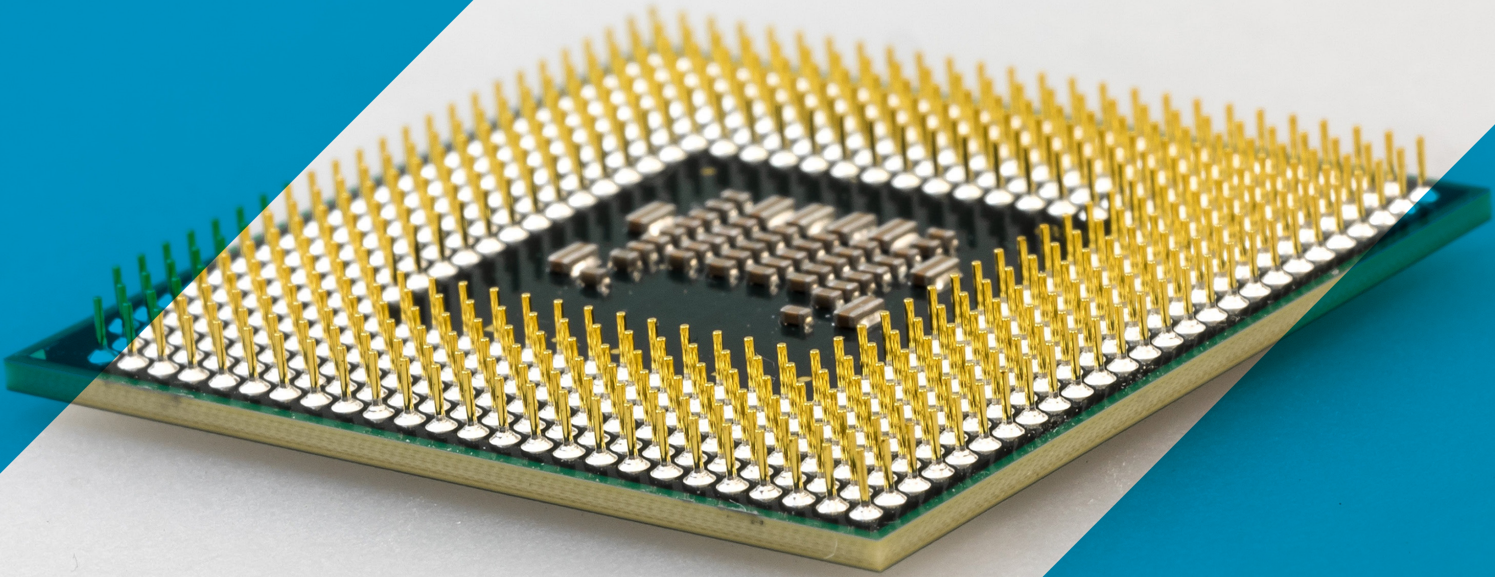
AI and FinTech: An intelligent choice or artificial hype?

An FFE and RDC White Paper

July 2019



FINTECH FINCRIME EXCHANGE

powered by:

rdc Smarter Screening

FINTRAIL

FINTECH FINCRIME EXCHANGE

The FFE brings together a global network of FinTechs to collaborate on best practices in financial crime risk management. By sharing information on criminal typologies and controls, members help to strengthen the sector's ability to detect and counter the global threat of financial crime.

The FFE was established in January 2017 by FINTRAIL and the Royal United Services Institute (RUSI), and its members meet monthly to discuss these topics and share information and insight on an ongoing basis. The FFE produces quarterly white papers on financial crime topics relevant to its members and stakeholders in law enforcement, the government and the financial services sector.

The global scope of financial crime and the shared threats faced by all major FinTech hubs particularly underscore the need for a global FFE network, which will give its members not only a trusted place to exchange information, but also access to an increasingly far-reaching network of resources and perspectives.

www.fintrail.co.uk/ffe

RDC is proud sponsor of the FFE as part of efforts to help improve collaboration within the FinTech community and anti-financial crime space.

www.rdc.com

Introduction

The pace of technological change continues to advance significantly, bringing with it a host of new technologies with promise for AML compliance. Artificial intelligence (AI) and machine learning are being rapidly adopted for a range of applications in the financial services industry.

Machine learning programmes - equations that can 'learn' by testing for patterns in data - are amongst the most exciting of modern technological advances. Machine learning evangelists see them revolutionising modern life, allowing computers to solve problems that have previously eluded human brains. Machine learning appeals to FinTechs for an obvious reason - technological innovation is at the heart of why the sector exists. And it particularly appeals to the sector's financial crime risk professionals, because - if the evangelists are correct - it might provide a faster and cheaper way to identity financial crime than the 'baseline compliance model' that FinTechs have inherited from the legacy banks.

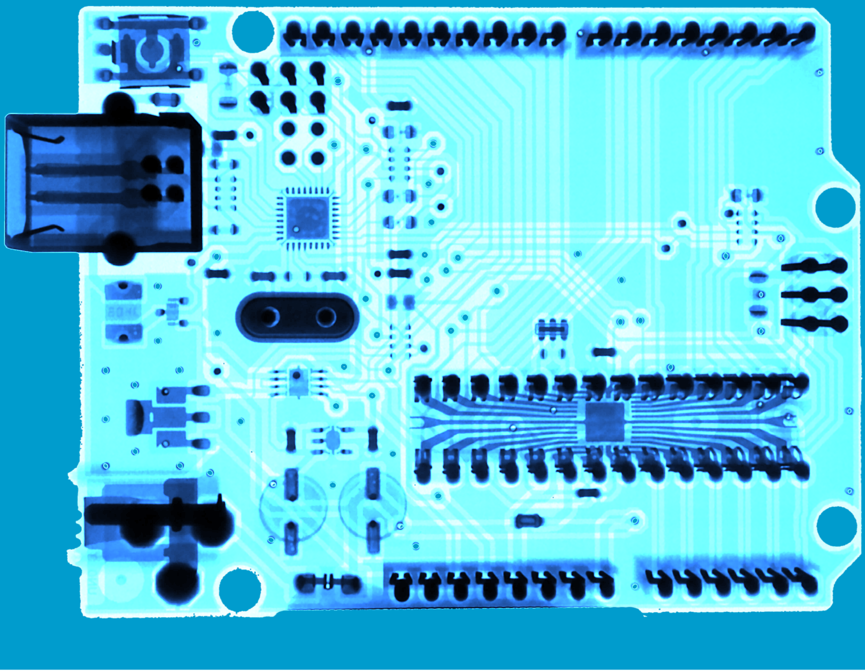
Nonetheless, despite its potential to make a difference in the long term, machine learning is still in its relative infancy. So, while it's great for FinTechs to explore the field, as with any new product or service, there are important issues around appropriate risk management and oversight.

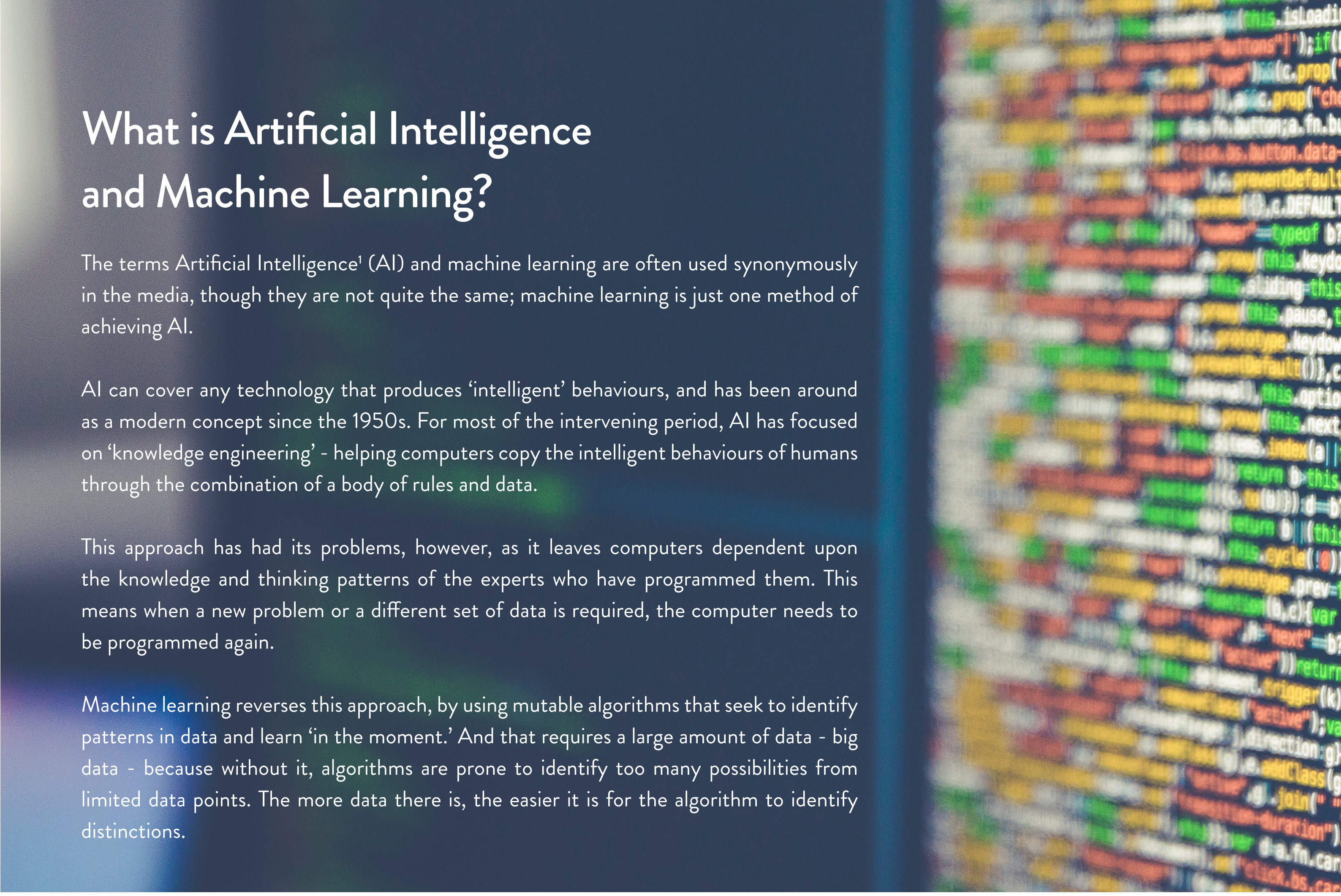
We surveyed 18 of the FinTech FinCrime Exchange's (FFE) UK membership to understand their approach to AI, their outlook on its potential, and their views on the most impactful ways to deploy the tool. The results have been further enriched with information gained from follow up interviews with some participants.

Based on the results, we found that 61% of surveyed FinTechs are currently either in the process of developing in house AI solutions or reviewing third party options for their fraud or AML programmes. 33% of surveyed FinTechs currently employ AI solutions developed in-house against 11% that use third party AI solutions.

Cost and data deficiencies, followed by human resources, were reported as the main barriers in implementing AI solutions by FinTechs. The lack of sufficient knowledge or understanding also appeared prominently as one of the top risks highlighted by respondents.

FinTechs, who had managed to overcome the barriers and challenges, reported a number of benefits already observed after deploying their in-house built AI solutions. These included better accuracy and fewer false positives, faster turnaround on onboarding and some improvements in fraud detection.





What is Artificial Intelligence and Machine Learning?

The terms Artificial Intelligence[1] (AI) and machine learning are often used synonymously in the media, though they are not quite the same; machine learning is just one method of achieving AI.

AI can cover any technology that produces 'intelligent' behaviours, and has been around as a modern concept since the 1950s. For most of the intervening period, AI has focused on 'knowledge engineering' - helping computers copy the intelligent behaviours of humans through the combination of a body of rules and data.

This approach has had its problems, however, as it leaves computers dependent upon the knowledge and thinking patterns of the experts who have programmed them. This means when a new problem or a different set of data is required, the computer needs to be programmed again.

Machine learning reverses this approach, by using mutable algorithms that seek to identify patterns in data and learn 'in the moment.' And that requires a large amount of data - big data - because without it, algorithms are prone to identify too many possibilities from limited data points. The more data there is, the easier it is for the algorithm to identify distinctions.

Tackling Financial Crime

The use of machine learning has become increasingly common in 'data heavy' sectors. On a day-to-day level, learning algorithms are behind the recommendations of many online retailers and the filtering tools that sift out spam from emails. But their capacity to identify patterns - and potential outliers - with greater accuracy than either humans or previously applied forms of data analytics, has an obvious potential for financial crime risk mitigation.

Back in 2017, the Financial Conduct Authority commissioned a study[2] into new technologies in Anti-Money Laundering (AML) compliance. There were several areas mentioned, where machine learning is in the early stages of making a difference in the sector:

Onboarding: Facial identification technology driven by mutable algorithms can be used for online or automated Identification and Verification (ID&V), comparing and contrasting key data points between the faces of customers as they present, with their photographic identification.

Screening: There are now RegTechs who claim that a combination of machine learning and Natural Language Processing (NLP), a further field of AI focused on computer recognition of human languages, has the potential to massively reduce false positives when screening against risk information such as sanctions lists, PEPs and adverse media.

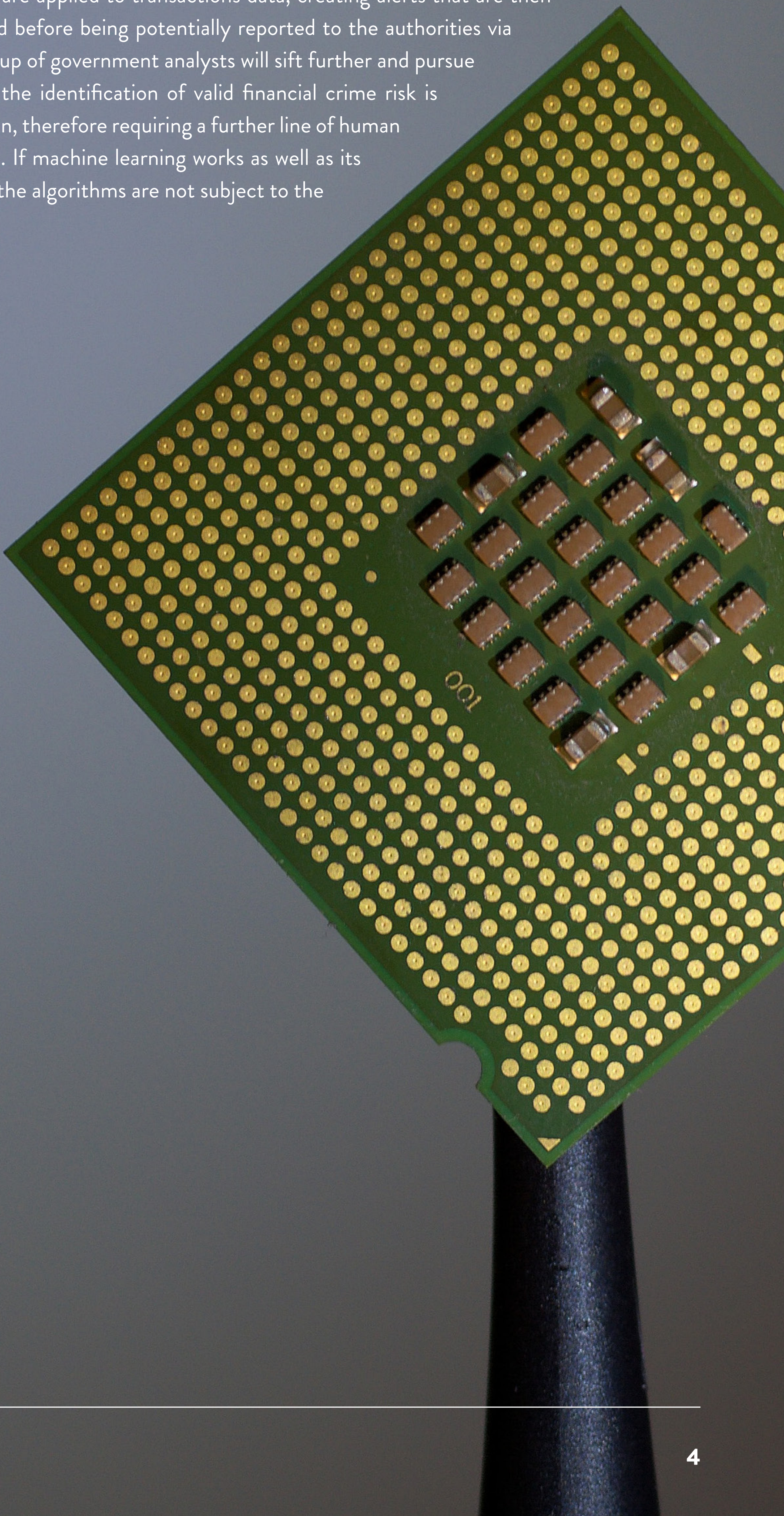
Transaction Monitoring: In principle, machine learning can clarify patterns of 'normal' behaviour for clients of different types, creating dynamic profiles that do not require the imposition of static rules that are only revised on a scheduled basis. These profiles should allow the systems to see when a given client is moving outside the pattern of what is 'typical' and also offers the possibility of identifying new typological outliers of financial crime behaviour.

[1] The term artificial intelligence was coined in 1955 by John McCarthy, a mathematics professor at Dartmouth College.
[2] PA Consulting Group on behalf of the Financial Conduct Authority, New Technologies and Anti-Money Laundering Compliance, 31 March 2017

Views on AI as a tool for financial crime risk management

AI tools offer the potential to achieve something of a 'holy grail' for financial services providers - both legacy banks and FinTechs alike. On one side, machine learning's promise of a massive reduction of false positives (and false negatives - the ones that currently get away) suggests that it will become easier to prevent and detect financial crime.

On the other, such a reduction could have the added benefit of bringing down the modern behemoth of the 'compliance spend.' A large proportion of compliance expenditure is currently dedicated to paying for analysts to review alerts and sift out the false positives - of which there are many. This is most acutely a problem in transaction monitoring. Under the current conventions, static rules based on known money laundering 'red flags' are applied to transactions data, creating alerts that are then queued for review. These alerts then need to be reviewed before being potentially reported to the authorities via Suspicious Activity Reporting (SAR), where a further group of government analysts will sift further and pursue the cases that appear most concerning. At every step, the identification of valid financial crime risk is subject to the vagaries of human judgement and perception, therefore requiring a further line of human judgement to assess the performance of its predecessors. If machine learning works as well as its supporters say, this system becomes redundant, because the algorithms are not subject to the failings of human judgement and perception.



FFE view

It should not come as a surprise that 33% of surveyed FinTechs currently employ AI solutions developed in-house. Many FinTech firms chose built, over buy, option because their needs may not be easily catered for by current vendors. Although, it is also changing with the rise of the RegTech sector.

One interviewed MLRO stated that he has a team of three data scientists working for him. This trend, of embedding IT resources directly within the broader AML team structure, rather than a traditional model of sharing IT resources with other business areas, seems to be on the rise.

Among the reasons, which prompted firms to build AI solutions in-house, respondents also mentioned:

- a better control over development and implementation processes;
- an (almost) unlimited time to train models in parallel with other controls acting as a safety net;
- an opportunity to expand in-house knowledge, which could be then extended to cover other business areas;
- more efficient and effective; they can tailor it to their specific customer behaviour.

Skill sets for data scientists[3]:

What does a data scientist's profile look like?
While there's no official accreditation for the domain, the people needed to work in this field will typically have a similar set of qualifications, experience and attributes:

- Degree-level education, often to Master or PhD level – and strong quantitative skills
- Experience of programming languages (especially R and Python), good coding and database design skills
- Familiarity with disciplines such as statistical analysis, predictive modelling and hypothesis testing
- Insatiable curiosity

In general, areas, where these solutions have been deployed by respondents, include:

Onboarding - improving customer risk assessment or in conjunction with digital onboarding vendors to look for hidden patterns among selfies submitted by clients; and

Transaction Monitoring - mostly fraud detections aimed at reducing exposure to common fraud typologies.

Out of 6 firms which deployed their in-house built AI solutions already, more than 80% of them rated their understanding of employed AI techniques as very good.

11% of respondents stated that they use third party solutions that utilise AI, which may indicate that FinTechs put more trust in solutions developed in-house. These in-house developments mostly focus on transaction monitoring and customer risk assessment. No FinTech reported developing any in-house screening tools.

Overall, 61% of surveyed FinTechs are currently either in the process of developing an in-house (39%) or reviewing third party (22%) AI solutions for their fraud or AML programmes. It seems to confirm the observed trend that FinTechs prefer to build rather than buy. The 61% figure is in line with 57%, quoted in a speech[4] by James Proudman (Executive Director of UK Deposit Takers Supervision), as a percentage of the firms regulated by the Bank of England, that responded to its survey, using AI applications in risk management and compliance areas, including anti-fraud and anti-money laundering applications.

[3] RDC, The Science that's Transforming the World, 3 April 2018
[4] James Proudman, Managing Machines: the governance of artificial intelligence, Speech given at FCA Conference on Governance in Banking, 4 June 2019 2018

Regardless whether a FinTech decides to build, or employ a third party's AI solution the European Banking Authority highlighted in its opinion[5] a need to assess:

- whether or not firms have appropriate technical skills to oversee the development and proper implementation of innovative solutions, particularly where these solutions are developed or used by a third party or an external provider;
- whether or not the senior management and the compliance officer have appropriate understanding of the innovative solution; and
- whether or not firms have proper contingency plans in place.

The importance of clearly communicating AI methodology to internal teams and external regulators

With increasing use of machine learning, statistical models are used to make decisions that were previously made by people. In many cases, those decisions are subject both to internal policy and to regulatory scrutiny. The characteristics of the statistical models – and particularly a clear description of the limits of their abilities – need to be communicated to ensure that their use does not unintentionally violate policy or the law[6].

[5] The Joint Committee of the three European Supervisory Authorities, Opinion on the Use of Innovative Solutions by Credit and Financial Institutions in the Customer Due Diligence Process, JC 2017 81, 23 January 2018

[6] Comments provided by Jeff Sidell (Chief Technology Officer, RDC).

Barriers & challenges

This prospect described at the beginning of the previous section is exciting. But we should take care - for now at least - not to get carried away by a utopian vision of financial crime risk management. There are still significant challenges for the use of machine learning in this field, especially when it comes to matters such as transaction monitoring and screening.

From a practical perspective, machine learning is dependent on large amounts of data. In theory, the quality of that data can be variable, the thinking being that errors, anomalies and variations are effectively 'tuned out' by the sheer volume of material. But what if there are systemic and large-scale errors, replications etc. in a given data set? How well will a machine learning driven transaction monitoring system deal with such issues? At this point, we do not have enough public information on the implementation of such systems to know.

There is also the regulatory challenge. It is a key requirement for regulators to understand how monitoring and screening systems work. They need to be able to look inside the 'black box' and understand what rules are applied, when, and how, to make a judgement on how effective and equitable the system is. How easy that will be with a mutable algorithm, which is constantly adjusting and re-adjusting to variations in customer behaviour, is also uncertain at present.

FFE view

Cost and data deficiencies, followed by human resources, were reported as the main barriers in implementing AI solutions by FinTechs. Expanding further on the perceived cost barrier, one of the respondents stated that "generally AI solutions are more expensive than we can justify at our scale" with another highlighting that "justification of costs involving implementation versus spend improving customer experience and UI" adds the traditional view of compliance as a cost centre.

Large amounts of data are required for training AI models, however as reported by one of the respondents:

> ***"in many cases there might not be enough data to do supervised learning efficiently. This is especially relevant for younger companies. Also the data quality can vary depending on how the cases are annotated by operational teams etc.".***

The data deficiency does not just relate to limited sample size for 'training' AI, but also on issues with legacy data already experienced by some longer established FinTechs.

The importance of data to feed machine learning capabilities & what signs to look for when assessing AI claims from RegTech providers

Machine learning is nothing more than statistical analysis over large amounts of data, powered by computers. The power and accuracy of machine learning is entirely dependent on the data used to train and test a statistical model. With any software or service provider claiming to use machine learning in their solution, including RegTech providers, it is important to understand not only their technology, but their access to data. The analysis and modeling, while important, are useless without adequate training data[7].

In addition to barriers, FinTechs were also asked about what they believe are the biggest risks of building an AI solution in-house. The lack of sufficient knowledge or understanding appeared prominently as one of the top risks highlighted by respondents. It included the lack of understanding by a compliance function of how an AI model operates as well as the lack of compliance understanding from engineers and the tech teams which might lead to not identifying critical links or risks and typologies.

One respondent also mentioned a risk resulting from information and capabilities not being shared among team members as creating a personnel risk "where only few people deeply understand the technical details. If these people decide to leave the company, then it'll be very difficult to hand things over".

This risk was also mentioned in relation to a level of understanding by external auditors or regulators as well as a lack of regulatory guidance. The GDPR[8] was specifically mentioned, as it applies to all automated individual decision-making and profiling. Especially relevant with respect to the use of AI and machine learning is Article 11, which provides a right to "an explanation of the decision reached after [algorithmic] assessment," and allied articles providing for similar disclosures. Other key articles relating to AI and machine learning are Article 9, which prohibits the processing of "special [sensitive] categories of personal data" as defined; Article 22, which provides for a data subject's qualified right not to be subject to a decision with legal or significant consequences based solely on automated processing; and Article 24, which provides that decisions shall not be based on special categories of personal data.

Finally, a risk of mistakenly incorporating bias and managing the AI through effective governance was also mentioned.

Some of the risks described above reappeared in answers when FinTechs were asked about the biggest risks related to using third party AI solutions with the lack of understanding what's "under the hood" being the most prominent again. This perceived risk is further aggregated by concerns regarding the extent to which FinTechs could influence and control the development, maintenance and audit of AI models.

[7] Comments provided by Jeff Sidell (Chief Technology Officer, RDC).

[8] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)

Overcoming challenges and reaping rewards

Many applications, or "use cases" of AI and machine learning in the financial sector already exist and the Financial Stability Board[9] report probably offers one of the most comprehensive lists of these use cases. Until very recently, financial institutions have relied on traditional, rules-based AML transaction monitoring and name screening systems, which generate high numbers of false positives due to rules thresholds.

FinTechs, who had managed to overcome the barriers and challenges described in the previous section, reported a number of benefits already observed after deploying their in-house built AI solutions. These included better accuracy and fewer false positives, faster turnaround on onboarding and some improvements in fraud detection. For example, one interviewed FinTech reported 80% increase in accuracy in identifying funds linked to authorised push payment[10] fraud. The same FinTech also described how models built using Benford's law[11] are successful at flagging suspicious transfers or card transactions. However, FinTechs continue to use traditional threshold based transaction monitoring in conjunction with machine learning models.

Another FinTech praised the flexibility offered by building the AI solution in-house as it is able to continuously tune settings to increase the tool's accuracy.

140 year old law helping to fight financial crime

Benford's law, also called the Newcomb–Benford law, is an observation about the frequency distribution of leading digits in many real-life sets of numerical data. The law states that in many naturally occurring collections of numbers, the leading significant digit is likely to be small. If the data doesn't look anything like the distribution predicted by Benford's Law, it may mean the numbers have been manipulated.

A look ahead

Although the adoption of AI technologies in the FinTech sector has been slower than some anticipated, an overwhelming 78% of respondents reported that they anticipate implementing a proprietary AI solution as part of their fraud or AML programmes in the future. 57% of these FinTechs are looking to implement it within the next 12 months.

Separately, 44% of surveyed FinTechs are anticipating implementing a third-party AI solution as part of their fraud or AML programme in the future with 63% looking to do it within the next 12 months.

Overall, on a 1 to 10 scale, FinTechs rate the potential for AI techniques in allowing fraud or AML teams to be more proactive when combating financial crime as very high with an average score of 9. However, AI techniques are not sufficiently tested or matured yet to provide the financial services with a silver bullet.

[9] Financial Stability Board, Artificial Intelligence and Machine Learning in Financial Services. Market Developments and Financial Stability Implications, 1 November 2017.

[10] Authorised push payment fraud happens when fraudsters deceive consumers or individuals at a business to send them a payment under false pretences to a bank account controlled by the fraudster.

[11] This law is named after physicist Frank Benford, who published it in 1938 in a paper titled "The Law of Anomalous Numbers", although it had been previously stated by Simon Newcomb in 1881.

Conclusions

In conclusion, it may be beneficial to quote the final remarks from a speech[12] by Rob Gruppetta (Head of the Financial Crime Department at the FCA) delivered not long ago:

> *"Artificial intelligence has the capability to greatly amplify the effectiveness of the machine's human counterparts, but it will be a constant work in progress. Any firm hoping for a black box in the corner that will sniff out the launderers will be disappointed, but the technology has the capability to better achieve what we all want: keeping finance clean."*

While there are risks associated with implementing AI solutions, and these were clearly articulated by the respondents, there are also benefits to be gained, including a potential opportunity to move away from traditional reactive ways of dealing with financial crime to a more proactive approach of stopping crime before it occurs.

FinTechs are founded on the premise of the value of technological innovation, and therefore machine learning is an inherently attractive possibility. The "move fast and break things" motto could also be applied to fighting financial crime as long as FinTechs move fast and break the right things for this to work.

Are we seeing a shift from AI overpromise towards delivering real value?

The hype cycle around AI and machine learning resembles that around the world-wide web in the early 2000s. The empty promises of vast benefits with little to no effort (remember "The web changes everything!"?) have been sifted out like chaff from wheat, and the kernels of value are beginning to emerge: Gradually, machine-learned models are beginning to enhance human productivity. Machine learning still requires people in white lab coats (data scientists – kind of like the Java engineers of the early 90s) but as the sophistication of the tooling and infrastructure improves, increasingly powerful machine learning solutions will be created with greater ease. Finally, expect to see consolidation among the pure-AI technology players in the next 5 years[13].

No technology should be applied unthinkingly, or out of context. More to the point, there is much FinTechs can do in their financial crime risk management that requires human judgement and decision making, such as risk assessing their product, their customer base, and where they are operating; from all of this flows decision making about risk appetite, policies, procedures, controls - and eventually - systems and platforms. In other words, the choice of which platform to invest in for a given task should follow from that thinking - rather than the other way around.

Further, when it comes to actually introducing new AI tools, the best way forward, as described by some of the respondents who successfully employ them, appears to be to deploy them alongside traditional systems: monitor and audit both old and new tools until you are satisfied, and then you are able to rely on the new tool.

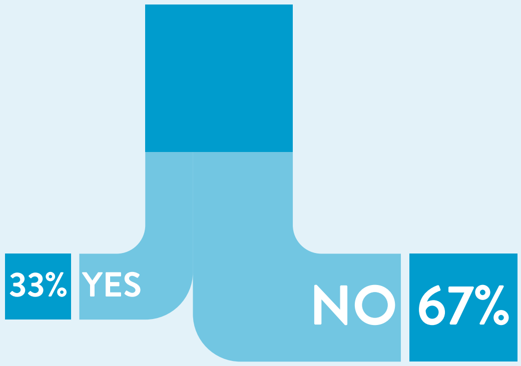
Clearly as outlined there are risks and challenges with AI, but anything that enhances the ability for the sector to combat financial crime should be explored for the overall positive benefits it will bring to the companies involved and the people it affects. As highlighted by the survey results, FinTechs are not only well placed but are actively seeking opportunities to integrate AI to enhance their AML framework.

[12] Rob Gruppetta, Using Artificial Intelligence to Keep Criminal Funds out of the Financial System, Speech given at FinTech Innovation in AML and Digital ID regional event, London, 6 December 2017 https://www.fca.org.uk/news/speeches/using-artificial-intelligence-keep-criminal-funds-out-financial-system Accessed on 20 June 2019

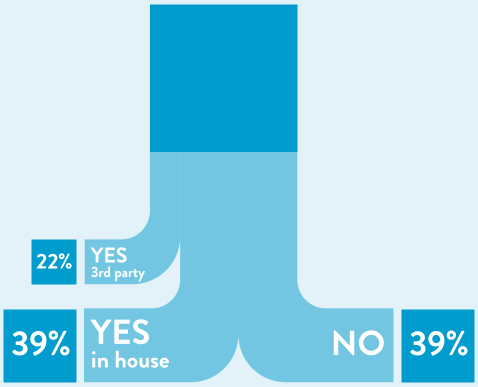
[13] Comments provided by Jeff Sidell (Chief Technology Officer, RDC).

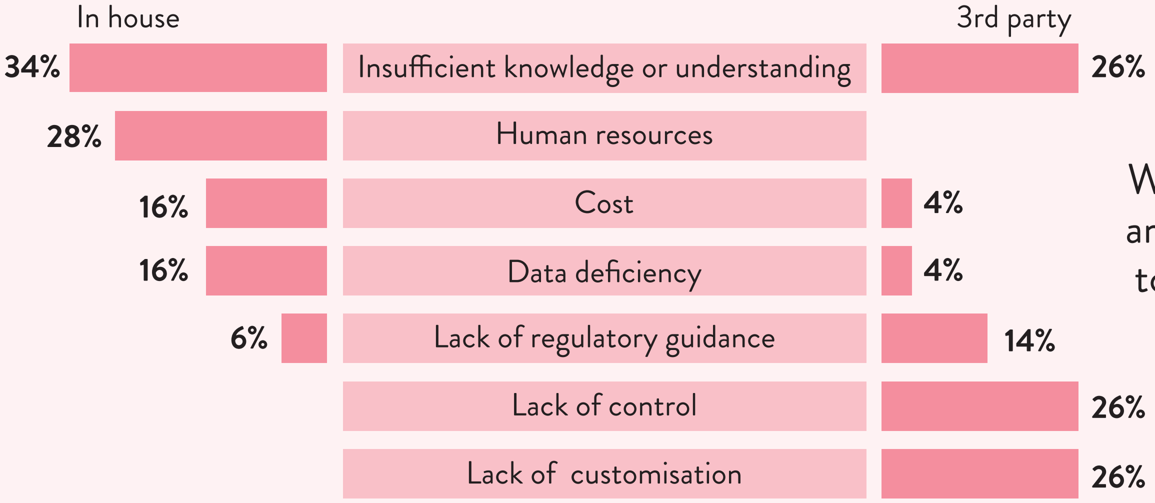
Results from AI questionnaire of FFE members

Do you currently employ any proprietary AI solutions as part of your fraud or AML programme?



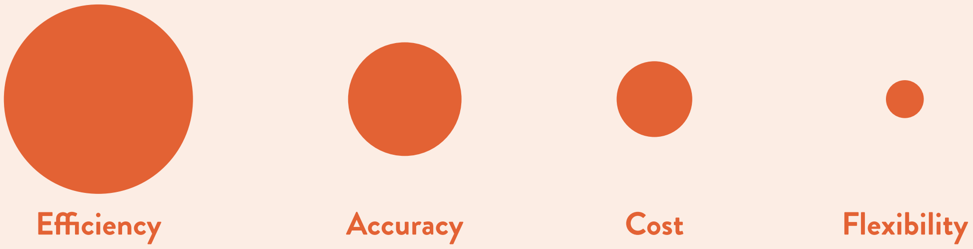
Are you in the process of developing any in-house AI solutions or reviewing third-party AI solutions for your fraud or AML programme?

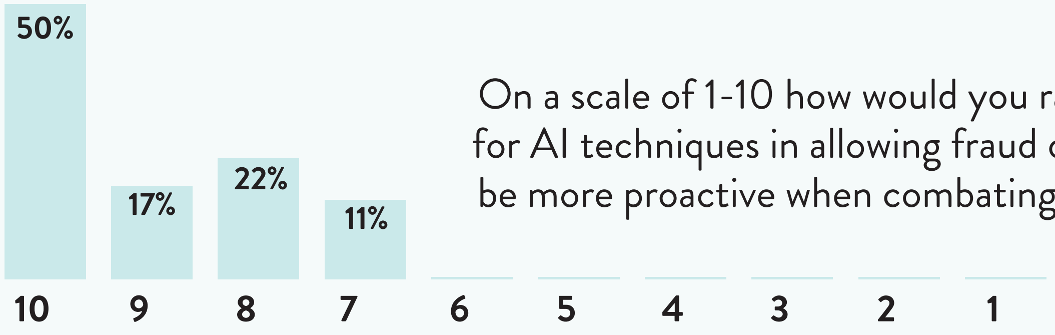




What do you believe are the main barriers to implementing AI techniques?

Benefits reported by members who successfully implemented AI solutions





On a scale of 1-10 how would you rate the potential for AI techniques in allowing fraud or AML teams to be more proactive when combating financial crime?

Brought to you by the FinTech FinCrime Exchange & RDC

FINTECH
FINCRIME
EXCHANGE

FINTRAIL

RUSI
www.rusi.org

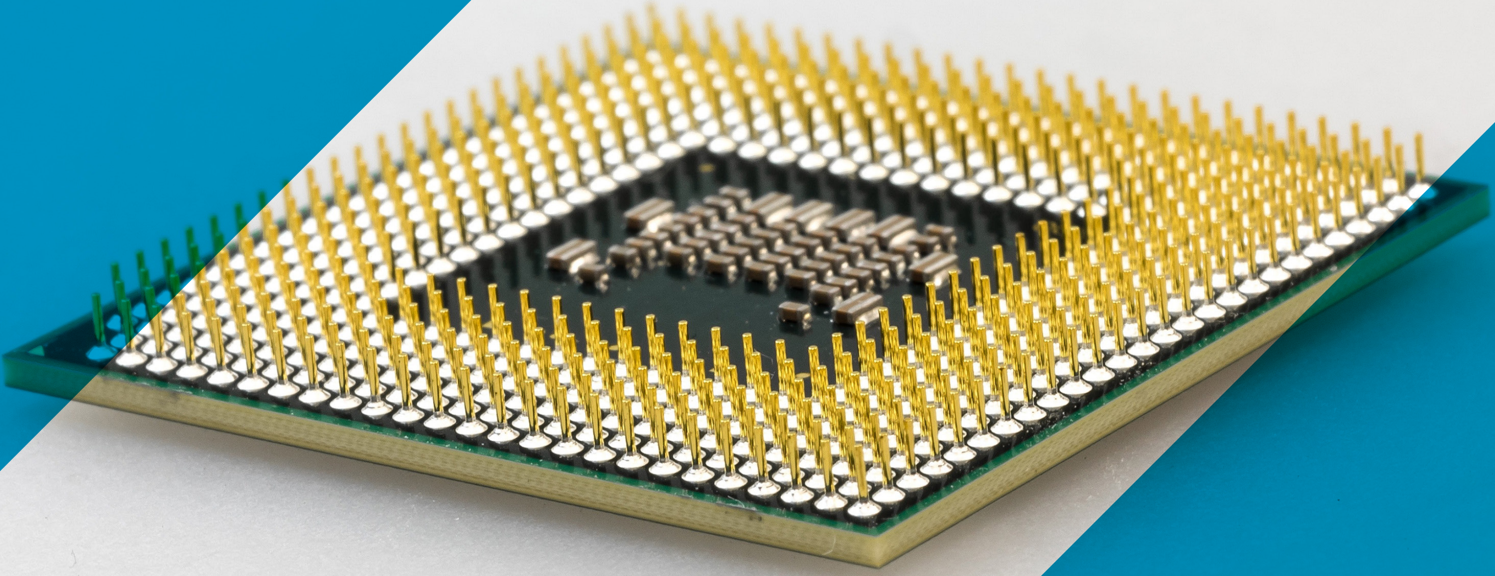
rdc
Smarter Screening

RDC prevents criminal infiltration of the world's financial systems by providing intelligent, automated customer screening solutions to more than 1,000 financial institutions and FinTech companies around the world.

The rapid growth and evolution of the FinTech industry requires innovative technologies and protocols for fighting financial crime. RDC's partnership alongside the FFE is the result of the two organisations' shared commitment to the FinTech community and the belief that effectively fighting financial crime requires a cohesive and collaborative response.

www.rdc.com

rdc
Smarter Screening



FINTECH FINCRIME EXCHANGE

powered by:

rdc Smarter Screening

FINTRAIL