How do you trust the machine?
Minds made for reinventing financial services

Using artificial intelligence to combat money laundering
By Patrick Craig, EMEIA FSO Partner and Financial Crime Lead, and Dr Mark Gregory, EMEIA FSO Senior Manager
Introduction

Combating money laundering is a key challenge for the financial services industry. Current anti-money laundering (AML) compliance processes are dominated by high levels of manual, repetitive, data-intensive tasks that are inefficient and failing to disrupt money laundering activity.

Given the low impact of current AML efforts combined with the increasing complexity of threats and growing volume of data to analyze, now is the time to explore the capabilities of artificial intelligence (AI). This technology has the potential to enable a step change in AML capability and provide a means to scale and adapt to the modern threat of money laundering.

Despite this potential, the increasing awareness and number of AI applications has ignited debate on the effectiveness of these solutions and the extent to which AI could and should be trusted and, ultimately, replace human analysis and decision making. Although caution towards wider AI adoption is easy to understand, the human brain is arguably the most opaque and unpredictable system in existence. Indeed, there is growing sentiment that combining human insight and processes with AI can drive better outcomes and new ways of working that are more effective than deploying humans or AI in isolation.

In order to realize the potential of AI, the financial services industry needs to continue building its understanding of the capabilities, risk and limitations of this technology. Furthermore, it must establish an ethical framework through which the development and use of AI can be governed, and the efficacy and impact of these emerging models can be proven and, ultimately, trusted.

"The application of AI to AML can provide compelling economic and risk management benefits. However, these rewards need to be balanced with the need for data and model governance. Explainable results and transparency are critical success factors for all AI applications."

Peyman Mestchian, Advisory Board Member, The AI Initiative @ The Future Society

1 AI spans a breadth of fields, techniques and technologies and, as such, can be hard to define. For the purposes of this paper, we adopt the Financial Stability Board definition of AI as "the theory and development of computer systems able to perform tasks that traditionally have required human intelligence." Machine learning is a sub-field of AI and it is developments in machine learning that have powered many of the recent successes of AI.
There is both need and opportunity for change in AML

At present, both the industry approach and regulatory framework are failing in the fight against money laundering. The financial services industry has evolved significantly since the Financial Action Task Force on Money Laundering published its first recommendations in 1990. Over the past two decades, an increasingly varied set of products and services, globally connected markets and digitally enabled channels have inadvertently provided a platform for highly organized and sophisticated money laundering activity to proliferate and diversify.

Money laundering enables organized crime and terrorism to operate globally and at scale, with money laundering activity estimated to be between 2% to 5% of global GDP3. In the UK alone, the social and economic cost is estimated to be least £24b a year4.

Despite the vast resources deployed by financial institutions to combat money laundering, the current approach is not delivering results. According to a report by Europol4, just around 10% of the suspicious activity reports (SARs) filed by financial services institutions lead to further investigation by competent authorities. Worse still, Europol estimates just 1% of criminal proceeds in the European Union end up being confiscated by the authorities. Yet, this inefficient system of AML accounts for an estimated 4% of annual financial services revenue, and tallied up a global industry spend of around $8b in 20175.

While financial services companies struggle to contain compliance costs, the threat of money laundering continues to evolve. There is increasing recognition of the need for change and innovation in AML. The requirement for greater and more effective alignment between regulatory compliance activities, risk management and prevention measures is a common concern among financial crime professionals6.

As the industry explores and demonstrates more effective ways to identify and disrupt money laundering activity through initiatives such as financial information-sharing partnerships, the industry can expect data volumes and the sophistication of threats to continue to increase. Leveraging the latest technology to develop and act on this data-rich intelligence is an increasing necessity in the next generation of AML controls.

The capability and impact of AI is growing rapidly

Interest in AI has risen significantly, driven by greater awareness of the capabilities and applications of AI such as virtual assistants and robotics across industries as diverse as health care, government and manufacturing. AI has been a field of research since the 1950s, however its capability has grown rapidly in recent years. This progress is underpinned by advances in computing, greater availability and quantity of data, and increased AI research and development.

---

2 “Understanding organised crime: estimating the scale and the social and economic costs,” UK Home Office, 7 October 2013.
3 “From suspicion to action: Converting financial intelligence into greater operational impact,” Europol, 2017.

---

Figure 1 Annually published AI papers
The recent successes of AI are making news headlines and challenging traditional operating models. In the UK, the Home Office funded an AI project to detect ISIS videos which, they claim, can detect 94% of videos posted online. It makes so few mistakes that a single person could moderate borderline cases for the whole of YouTube. The Home Office is making this capability available to industry to promote more effective and efficient methods of identifying and removing harmful terrorism propaganda posted online.

The transformative potential of AI has caught the imagination of businesses that are seeking to reduce cost, more effectively manage risk and increase productivity. It is estimated that annual venture capital investment into US AI start-ups has increased sixfold since 2000. Similarly, CB Insights reported that in 2017 investors poured in over $15.2b in funding to AI start-ups, a 141% jump in funding from 2016.

Governments have also recognized the strategic importance of AI to the future economy as well as national security. They have identified the need for investment in skills, and better understanding of the role, impact and ways to develop and harness this technology safely. Media outlets are calling the competing national investments in AI a modern day arms race, with China recently announcing plans to build a ¥13.8b ($2.12b) AI development park in Beijing as it pushes ahead to fulfil its ambition to become a world leader in AI by 2025. Clearly, developments in AI and its transformative potential cannot be ignored.

Is it time to transform AML with AI?

Current compliance processes are dominated by high levels of manual, repetitive, data-intensive tasks that are both inefficient and error prone. The AML technology that supports these processes relies heavily on expert systems that, in general, have not advanced since their introduction more than a decade ago. Although these systems and processes can be, and have been, effective, the growing volume of data, increasing complexity of risks, changing nature of financial activity and the rigid rules-based nature of these systems have driven maintenance and operational cost levels to unsustainable limits and the potential for missing new risks is high.

Many of AI’s capabilities are highly applicable to AML. The strengths of AI to enhance current capabilities include its ability to:

- Drive insight and value from large volumes of complex data that are often involved in due diligence, risk assessment and monitoring activities.
- Learn from, and adapt to, changing environment and inputs, helping firms to keep up with the rapidly changing financial landscape and risk profile.
- Automate human tasks, operate at scale and take decisions at speed to reduce cost and focus human engagement where there is the highest value add.
- Reduce error and improve consistency in processes and decision making.

The potential for AI to aid regulatory compliance has not been missed by technology providers. More than £238m of venture capital was invested in RegTech firms in the first quarter of 2017. We see clear signs that the appetite for leveraging AI is increasing and with an increasing number of case studies in the public domain. For example, HSBC recently announced a partnership with an AI vendor to harness technology and data better as part of its financial crime controls. Regulators and industry bodies such as the Financial Conduct Authority (FCA) and the Financial Stability Board (FSB) have also recognized the growing prevalence of AI in financial services and its applications to regulatory compliance.

---

8 “Isis videos targeted by artificial intelligence that can detect propaganda before it’s uploaded,” The Independent, 13 February 2018.
11 “Preparing for the future of artificial intelligence,” Executive Office of the President, National Science and Technology Council, Committee on Technology, October 2017.
12 “Preparing for the future of artificial intelligence,” Executive Office of the President, National Science and Technology Council, Committee on Technology, October 2016.
15 “Putting AI to work,” Fintech Australia, August 2017.
Addressing the AML efficiency issue and cost of compliance with AI

Addressing inefficiencies in AML and the cost of compliance is a key priority, but it requires banks to innovate and better harness technology and AI. Common pain points for organizations are typically the high caseloads and human effort involved in customer due diligence, screening and transaction monitoring controls. AML transaction monitoring has been a particular pain point for many banks and has come under significant criticism in recent years. Incumbent transaction monitoring controls typically generate high levels of false positive alerts and significant operational workloads.

The cost issue is often further amplified by inefficiencies in the investigation process, which create a low return on the effort employed versus the impact of transaction monitoring controls. There are immediate opportunities to significantly reduce operational cost with no detriment to effectiveness by introducing machine learning techniques at different stages of transaction monitoring process.

Some of the key enhancements to typical transaction monitoring controls that can be deployed are:

- **Improved data quality and richer set of holistic behavioral features** to model money laundering activity using entity resolution and network analytics.

- **Enhanced segmentation** using machine learning techniques such as unsupervised learning to enhance top-down, expert-led segmentation models and provide a more effective basis for outlier analysis and rule-based detection.

- **Enrichment, rollup and prioritization of rules-based output** opening up opportunities to auto-escalate or deprioritize rule based output.

- **Greater automation in investigations** can significantly reduce the level of human-led analysis required. In this area alone, there are significant opportunities to collate and analyse data before presentation to investigators.

- **Enhanced detection using challenger models** developed using machine learning techniques can provide data-driven insight into usual activity. This can be deployed in tandem with traditional processes and rules to enhance or validate risk coverage.

Similar opportunities exist in other control areas with AI being successfully applied to customer due diligence and screening controls using natural language processing and text mining techniques.

---

**Figure 2** Trust: an enhanced AML transaction monitoring model

---

*How do you trust the machine? Using AI to combat money laundering*
**Integrated KYC involves bringing context back into AML with AI**

While AI capability is growing rapidly, experience is showing that combining AI with human insight and processes can drive more effective solutions that are better than deploying humans or AI in isolation. We are already starting to see examples of this in manufacturing and engineering industries. This insight points to the continued importance of human expertise in the next generation of AML, but also the way in which humans will interface, interact and work with machines in the future.

This increasing use and understanding of how AI could be applied and integrated with human activity in AML is driving new thinking and opening up opportunities that could lead to a fundamental shift in the approach to know your customer (KYC) controls.

Perhaps, in the next generation of controls, we will see closer integration of risk assessment, monitoring, investigative and due diligence processes, with AI helping to break down silos and provide a more contextual basis for determining risk and detecting suspicious activity.

In this vision for the future, AI could bring increased breadth, scale and frequency to holistic KYC reviews in a way that better integrates ongoing screening and monitoring analysis. Risk and detection models would assess and learn from a richer set of inputs and produce outcomes in the context of both the customer’s profile and behavior. By leveraging AI’s dynamic learning capability coupled with skilled investigators, this model could be used to augment operations, provide quality control and even to train new resources.

**Figure 3** The integrated know your customer framework AML transaction monitoring model

---


Barriers to adoption
For many working in AML it is well known that there have been previous attempts to leverage more advanced analytical techniques, so it begs the question why those previous attempts failed and what aspects of AI are hindering greater adoption and realization of benefits. Root causes may be the perceived barriers and new risks associated with AI. We outline some of these considerations below:

► Low levels of maturity, industry adoption and regulatory guidance on AI
► The organization’s current compliance maturity, roadmap and appetite for innovation
► The increased technical complexity and reduced transparency of AI solutions
► Sensitivity to data quality and the specificity and consistency of intelligence used to train AI
► New and potential unknown and unquantified risks with AI
► The level of change and disruption to operating models and business processes
► New infrastructure, technology and people demands

For AI to make the leap into the AML mainstream and win trust from financial institutions, it will need to face these challenges. This clearly requires investment, with the emphasis on banks to explain the workings and ultimately prove the effectiveness of such techniques. This investment may be prohibitive for some institutions until there is greater adoption and trust in the industry.
How do we build trust in AI applications?

Financial institutions are in a key position to explore opportunities and build trust in AI applications for AML. Many organizations are, however, at the outset of their AI journey and hence may not be aware or well equipped to manage the new risks and challenges of deploying these new technologies. So what are the key dimensions of building trust in AI AML solutions?

Institute strong governance

Establishing strong governance and controls over the design, development and deployment of AI is critical to the safe and effective use in AML compliance and will go a long way to building trust in AI solutions. Good governance provides the means to assess and manage risk, promotes effective challenge and drives the necessary levels of understanding and documentation to inform effective decision making across the lifecycle of an AI solution. Better assessment of the end-to-end AI lifecycle can also help to inform the required skills to develop and provide effective risk management of AI-enabled solutions.

A good starting point for developing AI governance and controls may be to leverage and adapt existing model risk management approaches. The practice of model risk management has been increasingly applied to AML in recent years and many of the core principles were included in New York Department of Financial Services Superintendent’s Regulations for AML monitoring and filtering solutions. Firms can use these and other similar regulatory pronouncements as a foundation from which to build a reasonable approach to AI adoption which addresses stakeholder expectations of risk management and oversight.

Define scope, objectives and success criteria at the outset

The basis for developing AI-enabled AML solutions must start with a clear statement of purpose and objectives to ensure that the design and implementation is aligned with the intended use and integrates effectively into business processes.

Defining what success looks like is key to assessing the performance and impact of an AI solution. This can be very difficult in AML, as the outcomes and data sets can be highly subjective. The quality and specificity of intelligence used to train and assess the performance is an important consideration, and institutions may find that, without enhancing investigative and intelligence capabilities, AI will not yield significant benefits beyond incumbent controls. Establishing clear performance indicators and parameters, which link to a well-defined risk appetite statement, will be critical to tracking whether the outputs from the AI are meeting objectives at an acceptable level of risk. For example, in the context of AML transaction monitoring, one of the criteria may be that the model ensures coverage of activity that historically led to SARs.

Defining the scope of the AI solution comes next. The choice of data sources used to train and operate the model is a critical consideration. With many expert systems the risk factors and rules are based on expert judgment and anecdotal evidence, but AI has the ability to analyze broader and more specific customer and counterparty data points – from account activity on the one hand, to social media accounts and risk intelligence on the other.

---

19 “Banking division transaction monitoring and filtering program requirements and certifications,” Department of financial services Superintendent’s regulations, 30 June 2016.
This capability presents stakeholders with new risks and considerations such as adherence to data protection policies, fair use of personal data and the legal right to explanation\textsuperscript{20}.

The scope of data also has implications for the intended usage and scope of model output. Organizations need to consider the degree to which sensitive intelligence and specific personal information can and should be obscured from downstream consumers without impacting the usability or ability to explain model outcomes. For example, if SAR intelligence is used to train AI, the organization needs to consider the risk of tipping off, if it is feeding, for example, customer risk assessment models or transaction monitoring solutions.

**Make the design transparent**

The ability to demonstrate and audit compliance is a cornerstone of the current AML framework and, for that reason alone, the transparency of AI and the underlying algorithms is one of the key areas of debate\textsuperscript{21}. AI is inherently statistical in approach and hence can often be found to perform well in aggregate. However, this is often at the cost of greater complexity in the model and reduced ability to extract rationale and reasoning for outcomes\textsuperscript{22}. AI capability continues to develop and the next wave of AI may enhance the reasoning capabilities. Correspondingly, organizations will have to balance carefully the benefits in performance with the loss of reasoning and transparency of AI-driven models through effective governance and risk management.

AI is a broad field with varying levels of complexity and transparency. At the more complex end of the spectrum, neural networks and deep learning may prove more difficult to build trust in, if we compare them with more traditional techniques, as their logic can be opaque even to their developers. Because of these challenges, so far we have seen very few current AML solutions trialed in banks that have advanced beyond regression, decision trees and clustering.

\textbf{Figure 4} Varying levels of interpretability transparency across common machine learning techniques

\textsuperscript{20}“Accountability of AI under the law: the role of explanation,” Doshi-Velez and Mason Kortz at the Berkman Klein Center for Internet and Society at Harvard University, 27 November 2017.

\textsuperscript{21}“The dark secret at the heart of AI,” MIT Technology Review, 11 April 2017.

\textsuperscript{22}“Explainable artificial intelligence (XAI),” David Gunning for DARPA, October 2018.
The design process should therefore consider the different choices of AI capabilities and algorithms and how appropriate they are for their intended purpose and the usage of the model, as well as the features of the input data. This activity should document the technical specification in detail along with known limitations and constraints of the proposed design for governance and stakeholder review.

This need for transparency and auditability has implications for more advanced AI vendor solutions and the RegTech market. Organizations will have to balance carefully the benefits in performance AI can bring with the loss of reasoning and transparency of AI-driven models through effective governance and risk management. Vendors may need to open up details of their offerings, and institutions may need to enhance their in-house capabilities to replicate and validate third-party solutions and AI results. That will go a long way towards enabling companies to gain confidence and to trust the technical soundness of the vendor offering, as well as understand any limitations, constraints and potential risks.

**Collaborate to define best practice**

Successfully embedding AI in the compliance ecosystem requires commitment and collaboration across multiple stakeholders: firms, vendors, regulators and government. Collaborative efforts can underpin wider adoption, and identification of further benefits, but also set standards for appropriate governance and controls to manage the safe development and deployment of AI-enabled solutions.

Greater adoption, collaboration and increased guidance can help drive AI innovation and deployment. Broader adoption, underpinned by regulatory convergence, will also help avoid asymmetries in control effectiveness that could otherwise push illicit activity away from more innovative institutions and further under the radar.

Perhaps, for this reason, governments in many regions are leading the way. The UK has made significant steps, including the creation of the Turing Institute to bring academia and industry together, and Project Innovate, led by the FCA, providing a platform for greater debate and experimentation with innovative technologies in financial services. Similar initiatives are underway in other jurisdictions. Through these avenues of collaboration, perhaps we will begin to see the emergence of common principles and standards for the safe and successful development of AI solutions for AML. But, not all risks can be easily addressed or anticipated.

**Focus on data inputs and ethical implications**

The input data used to train and operate AI is critical and, therefore, one of the common concerns with AI applications is that it may increase the control sensitivity to poor data quality. Data quality is a major challenge for many financial institutions, often impacting the effectiveness and efficiency of current AML controls. AI projects should therefore assess data quality and its appropriateness for AI use as part of the design and development phase but also implement data management controls to monitor the ongoing data quality during operation.

Many institutions are actively looking to remediate and improve their data quality. The industry has seen an increase in the use of external third-party data sources to enrich and validate internal data sets. In addition, banks have embarked on big data projects aimed at centralizing and building a single view of customers and counterparties using entity resolution and network analytics techniques. These developments may go some way to improve the data quality available for AI applications and improve control effectiveness.

Data bias and AI ethics are hot topics in this narrative. High profile examples such as the Tay chatbot\(^23\) have highlighted the potential unintended consequences when trained on uncontrolled data inputs. Bias in AI-enabled AML processes

---

could stem from many areas such as variations in risk appetite, differences in regulatory guidance and poor operational processes. Institutions will need to consider carefully the choice of training datasets and implement controls to manage the ongoing quality and appropriateness of intelligence used to train a machine, as well as the overall performance and outcomes. For example, in the case of AML transaction monitoring, where investigation feedback is often used to optimize monitoring, quality controls should be implemented to ensure the intelligence produced meets the bank’s investigative standards and is of sufficient quality and specificity to train an AML solution.

Apply robust testing and validation

The greater the level of testing and independent challenge, the more effective the solution is likely to be and the less operational risk it will present. Many of the more successful AI applications have focused on specific tasks that rely on immediate, categorical feedback and, as such, are often easier to simulate and perform scenario-based testing.

A common component of model risk management frameworks is model validation and independent model review functions. Leveraging such an approach with AI solutions can greatly improve the level of effective challenge and reveal additional risks that were not identified during the design and development stages. Model validation and independent model review teams can assess all aspects of the AI solution, including governance and documentation, clarity of objectives, technical design and ongoing performance of the solution.

Other common techniques used in model risk management are stress and sensitivity testing, which are also applicable to AI solutions. Stress testing could be adapted to look at how AI performs in scenarios that are outside the bounds of training data sets, and hence can be used to assess and understand AI’s ability to adapt to changing environments and to identify unintended consequences. Similarly, sensitivity testing could be used to assess the importance of design assumptions or sensitivity to specific features of input data.

The champion/challenger approach runs alternative models alongside existing models on the same data to allow the outputs and performance to be compared and contrasted. This, too, should be part of the implementation toolbox, providing relevant information for “what-if” type analysis and impact assessment when transitioning between solutions.

More novel techniques for validating AI applications could be drawn for other domains such as the use of red teams, bug bounties and secret shopper type approaches that are leveraged in testing and ongoing enhancements to cyber controls.

Engage early, deploy incrementally, review regularly

AI can bring significant disruption to compliance processes and the institution’s operating model. Engaging stakeholders early, building a common vision and deploying incrementally can help to drive more effective change, constructive feedback and, ultimately, trust in business stakeholders.

When moving AI into production, organizations should consider the operational risks that require ongoing monitoring controls. An increasing concern with promoting AI into everyday use is the possibility of malicious manipulation or unintended misuse. Such risks were brought to life by analysis of an image recognition system which demonstrated the possibility of fooling deep learning AI by changing a few pixels that are invisible to the human eye. Periodic validation activities including review of business use and sensitivity testing will help to mitigate risk of post-deployment manipulation, along with regular review of AI decisions. Expert-rules-based systems can also be used to provide an ongoing baseline to compare with and help to identify where AI decisions significantly deviate from expected norms.

Conclusion: Act now

The current AML approach is struggling to keep pace with modern money laundering activity. There is a real opportunity for AI not only to drive efficiencies but, more importantly, to identify new and creative ways to tackle money laundering.

Although AI continues to pose challenges and test our appetite for risk, the question all financial institutions should be asking is: can we afford not to embrace AI in our AML?

Ultimately, when integrated with the right strategy and with the right focus on building trust, innovating with AI must be seen as a risk worth taking.
How do you trust the machine? Using AI to combat money laundering
Learn more about EY offerings and services around
Financial Crime at ey.com/financialcrime.
Find more EY insights from across financial services on
our thought leadership hub, fsinsights.ey.com.
About EY
EY is a global leader in assurance, tax, transaction and advisory services. The insights and quality services we deliver help build trust and confidence in the capital markets and in economies the world over. We develop outstanding leaders who team to deliver on our promises to all of our stakeholders. In so doing, we play a critical role in building a better working world for our people, for our clients and for our communities.

EY refers to the global organization, and may refer to one or more, of the member firms of Ernst & Young Global Limited, each of which is a separate legal entity. Ernst & Young Global Limited, a UK company limited by guarantee, does not provide services to clients. For more information about our organization, please visit ey.com.

EY is a leader in shaping the financial services industry
Over 30,000 of our people are dedicated to financial services, serving the banking and capital markets, insurance, and wealth and asset management sectors. At EY Financial Services, we share a single focus — to build a better financial services industry, not just for now, but for the future.

© 2018 EYGM Limited.
All Rights Reserved.

EYG No. 03012-184Gbl
EY-000063578.indd (UK) 05/18.
Artwork by Creative Services Group London.
ED None

In line with EY’s commitment to minimize its impact on the environment, this document has been printed on paper with a high recycled content.

This material has been prepared for general informational purposes only and is not intended to be relied upon as accounting, tax or other professional advice. Please refer to your advisors for specific advice.

ey.com/fincrime