Deloitte.

UOB

The case for artificial intelligence in combating money laundering and terrorist financing

A deep dive into the application of machine learning technology

Forensic

Contents

Glossary of Terms

AI	–	Artificial Intelligence
AML	–	Anti-Money Laundering
CFT	–	Counter Terrorist Financing
FCC	–	Financial Crime Compliance
LIME	–	Local Interpretable Model-Agnostic Explanations
MAS	–	Monetary Authority of Singapore
ML	–	Machine Learning
PEP	–	Politically Exposed Person
POC	–	Proof of Concept
PPP	–	Public-private Partnerships
SLA	–	Service Level Agreement
SAR	–	Suspicious Activity Report
STR	–	Suspicious Transaction Report
SHAP	–	SHapley Additive exPlanation

Introduction

Combating money laundering is an enormous task, and it comes with substantial costs and risks, including but not limited to regulatory, reputational and financial crime risks.

Managing these risks rest with the guardians of the financial system. Moreover, criminals continue to evolve in their laundering techniques, finding and exploiting loopholes in the system to move money.

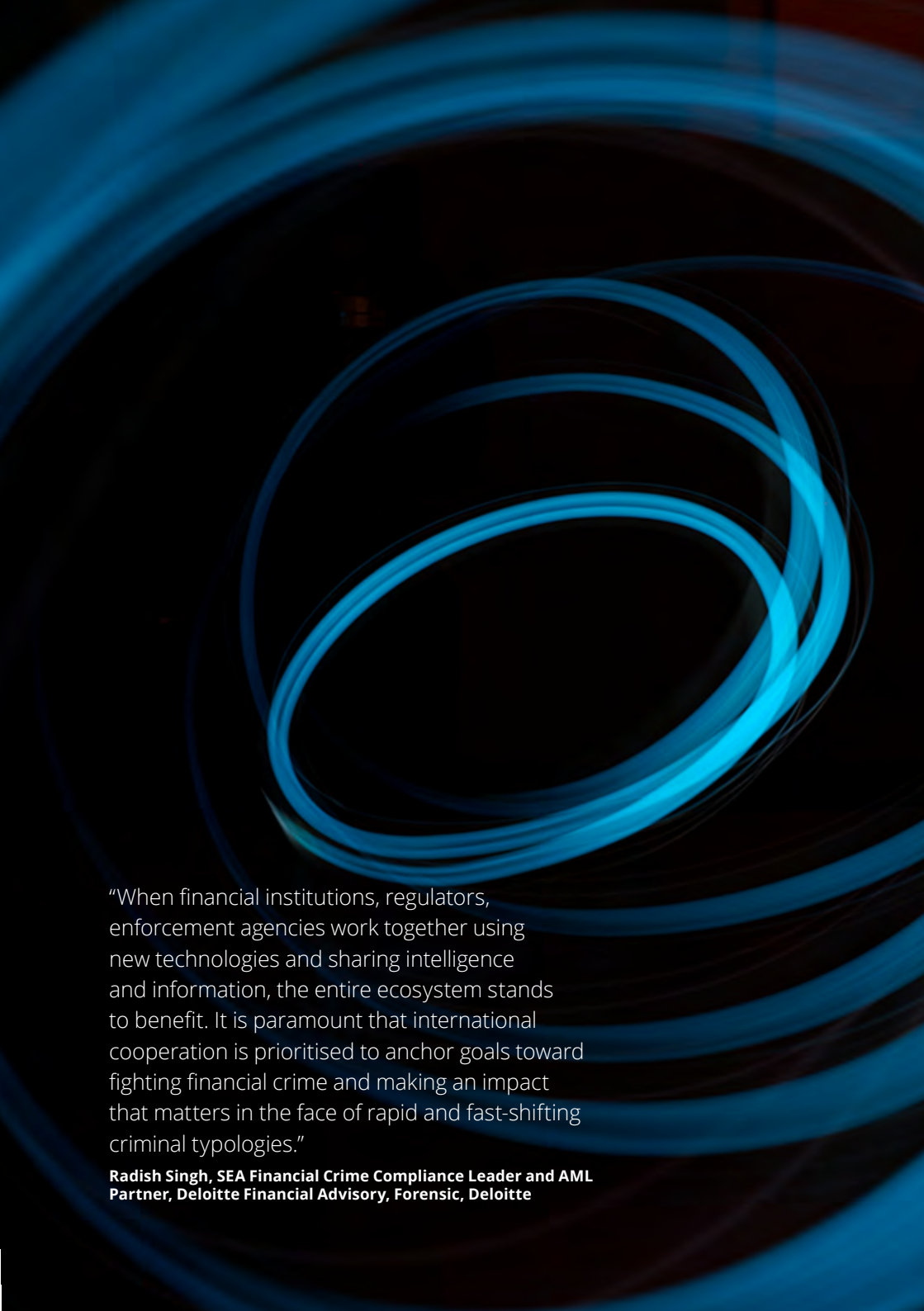
These criminal minds are also capable of using new technologies such as online banking, electronic payments, and cryptocurrencies to move illicit funds across borders at breakneck speed. This creates complex and layered transactions that are increasingly real-time, making it difficult to monitor and to detect with traditional approaches.

At the heart of criminal activity are sophisticated money launderers with the ability to move illicit funds seamlessly through the formal financial system. These money launderers are sophisticated and pose a serious threat to financial institutions across the globe, and their activities have a devastating consequence for society as well. As a result, societal ills such as terrorism, drug and human trafficking challenge social structures and order, societal governance, as well as open and fair commerce. For these reasons, the importance of continuous improvement of an organisation's financial transaction monitoring and name screening effectiveness has never been more critical in the digital age.

Singapore, as a top-4[1] global financial centre has a front row seat to these money laundering threats. As a nation, Singapore is not immune to new laundering threats that emerge expediently. In fact, the country has taken the lead in addressing these evolving 'threatscape' through innovative initiatives, solutions and forums, as seen in the continued run of the Singapore Fintech Festival by the Monetary Authority of Singapore (MAS).

More than ever, there is a need for the industry and regulators to sharpen surveillance on an ongoing basis, or risk being at the wrong end of the threatscape. With the potential of public-private partnerships (PPP), an ecosystem driven strategy will be a key step forward to combat money laundering and terrorist financing risks in the future. In fact, banks such as UOB have taken steps to work with different players in the ecosystem to combat money laundering, as seen in a case study on their journey of co-creating a machine learning solution that is discussed in this Whitepaper.

In the interim, forging closer links to realising the benefits and the full potential of PPP, innovation and new technologies are the best bet to better manage regulatory risks.



"When financial institutions, regulators, enforcement agencies work together using new technologies and sharing intelligence and information, the entire ecosystem stands to benefit. It is paramount that international cooperation is prioritised to anchor goals toward fighting financial crime and making an impact that matters in the face of rapid and fast-shifting criminal typologies."

Radish Singh, SEA Financial Crime Compliance Leader and AML Partner, Deloitte Financial Advisory, Forensic, Deloitte

The promise of machine learning in compliance

Today, banks have invested and continue to invest billions of dollars to prevent money laundering.

However, traditional technological approaches to combat these evolving threats are meeting with less success resulting in large numbers of "false positives" (95[2] per cent of false positives in some organisations where 98 per cent do not result in a SAR or STR) and an army of resources to tediously dispose of these. Undoubtedly, using limited resources to close off non-material and unimportant alerts is manual and onerous.

Furthermore, the ballooning costs of Anti-Money Laundering ("AML") compliance (of more than US$25 billion[3] in the United States alone) coupled with the high volume of backlog alerts swamp compliance teams and potentially distract them from 'true' high risk events and customer circumstances.

Needless to say, this demands a more efficient and effective approach to strengthen AML efforts. Ultimately, compliance teams ought to be focused on higher value work such as issues resolution and also to ensure that policies and procedures are continuously reviewed and updated to reflect the typologies detected across the bank.

In response, banks need to embrace the opportunity to apply technological innovations – these include robotics, cognitive automation, machine learning ("ML"), data analytics and artificial intelligence ("AI") to their AML compliance framework. As a result, the banking and finance industry has been exploring opportunities to use AI and ML to alleviate some of the compliance burden.

In fact, a report released by the World Economic Forum and Deloitte in August 2018 entitled "How AI is transforming the financial ecosystem"[4] showed that the continued development of AI will radically transform the front and back office operations of financial institutions. The report goes on to state that the AI expansion will require adjustments to long-standing regulations and major changes to the current structure of global financial markets. This shift is an opportunity for compliance teams to strategically invest in new technologies in order to enable banks to become more future ready.

Technology companies and banks are actively designing AI solutions and tools to better assess high risk jurisdictions, to identify potentially problematic or suspicious funds movements, and to refine the screening of Politically Exposed Persons (PEP) and sanctioned individuals and/or organisations. Regulators are also in agreement that such advanced technologies can and should be leveraged by banks to improve risk identification and mitigation.

"As financial institutions and FinTechs increase the experimentation and use of AI and data analytics to improve their services, government agencies need to ensure that our support, policies and regulations are attuned to developments and remain supportive of these new technologies[5]."

Dr David Hardoon, Chief Data Officer, Monetary Authority of Singapore

As some of the main advancements in technology and analytics are relatively recent, there is often confusion when it comes to understanding what AI and ML actually entail and the differences between the two. To be clear, ML is a subset of AI, and within AI, there exist further subsets such as natural language processing, robotics, image recognition, speech recognition, deep learning, and virtual agents.

Until very recently, banks have relied on traditional, rules-based AML transaction monitoring and name screening systems, which generate high numbers of false positives due to rules thresholds (this will be discussed in the next section). Accordingly, ML has served as the first port of call for many banks beginning their journey to advance their compliance innovation programmes.

Innovation in compliance is needed both to reduce false positives and to bring about greater effectiveness in the manner in which AML and/or Counter Terrorist Financing ("CFT") risks are monitored and addressed by banks. As Alan Turing famously said, "What we want is a machine that can learn from experience." Turing's thinking can be applied to banks and AML compliance as these institutions face increasing threats and risks.

As the industry forges ahead with ML, these advancements present opportunities for banks to consider the strategic creation of an AI ecosystem in this wave of innovation. The learnings from the traditional approach to transactions monitoring reflect that operating in a silo environment has its pitfalls of, amongst others, creating inconsistencies across the industry.

With an AI ecosystem, it will mean more sharing and transparency of standards, which can be advantageous to the industry in achieving greater expertise, effectiveness, and efficiencies when considering the adoption and integration of machines into the mainstream.

AI involves machines that can perform tasks that are characteristic of human intelligence – anything that can be described by a human being can be mimicked through AI applications. ML is a branch or subset of AI, encompassing those actions where a machine learns to understand patterns in data or tasks without having pre-defined coding. ML promises to be particularly relevant and impactful for transaction monitoring platforms within banks.

Uses and potential applications of machine learning in fighting money laundering

The unintended consequences of regulatory expectations on AML compliance has spurred banks to ensure that they are on the right side of the regulatory fence and consider the use of machines to learn and to detect suspicious activity and behaviour more critically and effectively.

Banks are therefore keen to leverage the rise in computing power to analyse large volumes of data assets and to "learn" from the results.

In the compliance realm, there is a real sense of opportunity where ML can assist in enhancing effectiveness, efficiency and accuracy of processes within a bank's core money laundering and terrorist financing risks detection and reporting system. For example:

1. ML algorithms can be taught to detect and to recognise suspicious behaviour and risk rate them accordingly. For instance, machines will learn and focus on "bigger" risks whilst knowing when to omit non-anomalous transactions that do not present any risks as dictated by customers' profile and behavior.

The greatest opportunity for application is in the money laundering and terrorist financing transaction monitoring process. Traditional systems detect very specific typologies that can be circumvented. Furthermore, the results from these models contain more noise than 'signals of risk' as the net is often cast wide in order to not miss a potentially suspicious activity.

By relaxing rule thresholds to capture suspicious transactions that are closer to 'normal' activity, there will inevitably be larger numbers of alerts requiring costly manual reviews to resolve. However, only a very small number of these alerts will result in suspicious behaviours requiring escalation.

2. Combining outputs of existing systems, ML models can be trained to identify the behavioural characteristics or indicators that highlight when activity is truly suspicious. ML techniques such as anomaly detection can be used to identify previously undetected transactional patterns, data anomalies and relationships amongst suspicious individuals and entities.

Such ML techniques no longer require static rules, and are based on known and trending patterns or threats that make it harder for criminals to hide within the bank's environment.

3. ML can be applied to name screening where systems are required to screen customer names against global lists of known criminals and black-listed and sanctioned organisations and individuals.

The challenge faced by many banks is balancing 'fuzziness' with accuracy. In other words, current text matching algorithms are not an effective tool to track potential data capture nuances such as the order of names, titles, salutations, abbreviations, name variants, common misspellings, etc. In addition, the task becomes complicated further when dealing with common names where it is difficult to pinpoint the exact individual. The prevailing rules-based approach is both onerous and manual, resulting in increased workload for compliance, as well as potential gaps in surveillance and monitoring.

4. Applying ML to improve the matching criteria as well as predicting the likelihood of a name match can lead to significant efficiency gains while also increasing efficacy by identifying hidden links (conducting link analysis from available) or relationships.

Enriching the data with more contextual information about the entity such as demographic, network and behavioural data is where the true enhancements to the accuracy of screening processes lie.

Some other areas that are gaining traction include Fraud Detection, Automated Reporting, Enhanced Surveillance including voice, video, text, pattern based transaction monitoring.

When determining where to apply ML, it is important to understand the opportunities in terms of the bank's innovation strategy, key priorities, unique financial crime compliance risks, existing operational challenges, and long-term feasibility.

A smart approach to compliance will also be of strategic commercial value. Aside from having better known risks that can be escalated and investigated by compliance teams, optimising historically compliance driven methods such as the "Know-Your-Customer" process offers another opportunity for the banks' business portfolio of clients to be enriched.

In the long term, the bank will have a fuller and more robust profile of their clients that can be used to enhance ongoing client management to delight customers and to build loyalty. In this regard, ML models can modernise compliance by removing needless interruptions to services while achieving deeper and more customised insights to improve customer experience.

In terms of business efficiency, using ML techniques in compliance has immense potential to reduce manual processes, and even streamline repetitive tasks that often weigh compliance teams down. Such improvements can also alleviate cost and make compliance a more meaningful exercise.

The first steps to success include:

- maturity assessment or model validation of the existing technology in place and identification of opportunities for enhancement;
- understanding of the key risks, threats and complexities of the business including the bank's correspondent banks, customers and known transaction risks;
- effective governance framework for AI and ML in the bank – clear focus on AML/CFT controls it will be deployed to address data quality issues, project management, stakeholder expectation management and engagement;
- strategy, framework and intended outcome of deploying AI and ML;
- approach for operationalising and documenting the AI process with particular focus on deployment into production and an in-depth understanding of the models and algorithms used;
- appropriate structure for monitoring and validating the approach for operationalisation as well as the outcome of deployment that it meets regulatory objectives and addresses risks appropriately; and
- robust due-diligence of vendors selected to provide the technology know-how and infrastructure.

Navigating and adopting machine learning

Even with the potential to be harnessed from ML and its promise of increased efficacy, there are considerations that should be addressed before commencing on this journey.

A UOB case study presented in this Whitepaper details many of these considerations.

The key considerations are as follows:

Ensuring model results are consistent and reproducible

In the case of AML/CFT transactions monitoring, ML models dealing with high risk processes, will become an integral part of the control framework and it is imperative that:

- there is the ability to reproduce a bank's results within the production settings for the purposes of, inter alia, providing assurance from a regulatory standpoint and for maintaining a good quality audit trail; and
- the model is designed and trained to produce a specific and consistent set of results by learning behaviours and patterns within data sets.

There is recognition that due to variable factors such as random initialisation of parameters, different chip architectures that perform calculations differently, changes to data and changes to underlying statistical libraries, it is often a challenge to reproduce a set of results in a consistent fashion.

To address this inherent challenge, banks must put in place a robust and continual process to evaluate and to validate the performance of their models. This includes a governing framework that measures performance, documents the training process, and ensures that steps can be replicated with the same results. The framework should test the performance impact of any changes to production prior to release, and should also execute unit testing algorithms, in order to understand the impact of specific components and parameters on performance.

Flexibility and customisation

Much of the shift and speed in the adoption of ML has led to the increased demand for "off-the-shelf" models that use pre-built data sets that are easy to implement. The flip side is inaccuracy when using different data sets.

Off-the-shelf models are trained using data that are not specific to the bank and do not reflect learnings from underlying data and transactions, key customer segments and profiles, as well as products and services offered by the bank. The machines are also not trained with data that contain other risk nuances, existing trends or typologies such as high risk cross-border transactions or simply those that do not correspond to the customers' behavior.

In most cases, banks will increasingly require scalable and deployable ML models, which may require customisation to suit a bank's needs and one that has the ability to scale with a sustained impact. In such circumstances, the long term benefits and scalability should be recognised rather than the focus on its relatively higher initial cost due to customisation.

While limitations do exist, off-the-shelf ML models may still be used, but only when they are calibrated according to the bank's unique data sets, profile and requirements.

In addition, transfer learning (which is the ability to customise a pre-trained model using new and relevant data), image recognition in name screening (an existing off-the-shelf ML image recognition model could be modified to perform facial recognition) or natural language processing, as applicable, are additional enhancements that could be looked into.

Sustainability, scalability and industrialisation of the machine learning model – from POC to Production

The process to move models from Proofs of Concepts ("POC") into a live setting needs to be industrialised to the point that all the necessary considerations such as sustainability, scalability and industrialisation as well as controls are embedded.

The model should be scalable to handle in production:

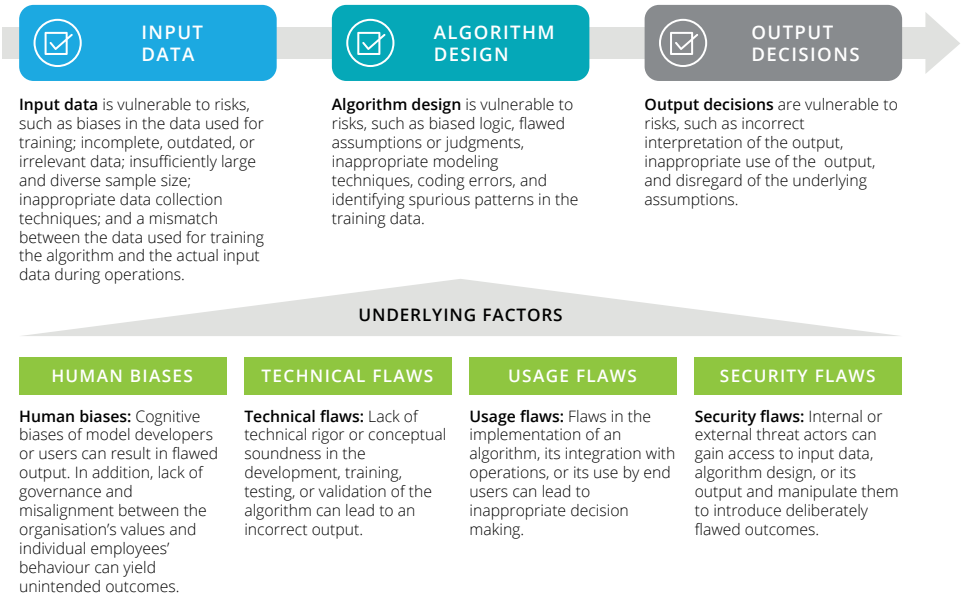
- new data volumes being pumped through for prediction;
- use feedback from live data to adjust parameters and help the model re-learn;
- business requirements that impact the production design;and
- appropriate and resilient technical and performance failovers

To industralise ML within a bank, there has to be proper governance to ensure consistency in the design, use and maintenance of the models. An enterprise-wide strategy, framework and platform is critical for the deployment of multiple ML models (that could be a mix of both Off-the-shelf and bespoke ML models) to effectively use resources and manage risks across the bank.

Moving into production also requires working towards the creation of a centralised platform embedded with data controls to attain accuracy, completeness, privacy and regulatory compliance that will go the distance to ensure data standardisation and reliability across the organisation. Cleansed data is a dire need for the success of ML model and we will expand on this point further in a subsequent section.

Recognising and addressing risks associated with machine learning

Figure 1: The associated risks with using ML models



Source: Managing algorithm risks: Safeguarding the use of complex algorithms and machine learning, Deloitte[6]

To effectively manage the risks of cutting edge technology such as ML, banks will need to establish a solid framework; to restructure and to modernise traditional risk-management framework and capabilities. This goes back to the key success factors discussed under the section on "Uses and potential applications of machine learning in fighting money laundering."

Readiness for a machine learning pilot

Different organisations have different levels of readiness for integration and usage. Ahead of any ML pilot programmes, the following considerations should be weighed:

Figure 2: Readiness for a machine learning pilot

Data management

The ML model is only as good as the data it receives. It is simple to conclude that bad quality data will produce bad results. As such, selecting data sets to train the model may cause unintended biases. To mitigate this risk, it is important to consider:

Figure 3: Considerations for data management

Having good and clean data sets is a critical component for any bank venturing into designing ML models. The foundation of data management is acquisition, preparation and maintenance, upon which ML models are embedded. In turn, the benefits of a well-managed data infrastructure will enable multiple ML models to leverage richer datasets and deliver valuable insights and patterns to help with complex analyses, especially in countering money laundering and terrorist financing.

Explaining the inner workings of machine learning models

As models become increasingly complex to uplift performance outcomes, the inner workings of the algorithms becomes more opaque. Banks are often faced with the tricky issue of balancing between decoding the algorithms and maintaining accuracy.

With the adoption of ML technology, banks are expected to understand and defend the algorithms used by the machine that may bring about better predictive capabilities but are significantly more complex. In order to understand if the model is picking up valid patterns and that it is not overfitting the training data, the outputs must be transparent and auditable.

While ML models may pick up associations within the data, it is not necessarily a proof of causation and this may result in false hypotheses. When left undetected and not remedied, the opposite effect will cause greater risks and lack of precision in monitoring AML/CFT risk, resulting in a lack of accurate regulatory assurance.

Practitioners using the model will need to understand decisions made by the machine and be able to explain how the related data points shape the outcomes. Decisions need to be transparent to determine if they were fair, ethical and in line with legal and regulatory requirements.

Interpretability is the degree to which a human can understand the cause of a decision. This is critical in understanding model weaknesses as well as being able to defend any decisions made to the regulator as well as to other stakeholders.

One way to understand why models make decisions is to appreciate the important features that drive the model. This allows for determination of the core decision criteria for the model but does not help with understanding why specific predictions were made.

Additionally, if predictions impact customers, they may want the right to understand the manner in which their data is being used and reasoning behind the decision that impact their banking experience.

Ultimately, any technology deployed in the AML/CFT framework is a control in itself. Therefore, its explanability and transparency is critical in providing ongoing regulatory assurance that the risk is managed adequately as with managing customer experience.

There has been a lot of research in this space on how to make model outcomes more explainable. Some examples of this are SHapley Additive exPlanation (SHAP) and Local Interpretable Model-Agnostic Explanations (LIME) which attempt to determine the impact of specific features on localised predictions. SHAP is filling the gap to provide the link between accuracy and human interpretation of models using game theory[7]. While LIME aids the predictions of ML classificaters[8]. Research in this space is ongoing.

Choosing the right vendor partner

ML involves changes in strategy, culture, technological landscape and how banks address regulatory risks and their modes of operation. Innovation occurs rapidly and it is common for large institutions to partner with technology companies to address such challenges.

Managing vendor risk is crucial to maintain business sustainability. Aside from the technical capabilities of a technology vendor, it is also key to choose a partner that has the right established experience and financial sustainability. Essentially, smart technology is needed alongside the right experience, expertise and track record to be successful.

When transitioning a vendor to the data environment, banks need to perform due diligence to ensure that legal reviews and Intellectual Property ("IP") ownership before on-boarding are appropriately governed and secured, to ensure that deployments are not only robust, legally sound and operationally possible. Based on our experience, these are some common obstacles raised by both vendors and banks alike when onboarding new technologies:

- handling of data in line with regulatory requirements and respectful of local jurisdictional boundaries (General Data Protection Regulation, unstructured data, non-English languages etc.);
- sustainability of a technology solution;
- clear list of onboarding requirements;
- ownership of IP and co-created solutions as part of the journey for on-boarding; and
- measuring success with mutually beneficial expectations.

Summary

ML in AML/CFT is not yet a silver bullet.

All ML techniques have strengths and weaknesses and understanding what these are together with clever application could create something greater than the sum of their parts. There are limitations and increased requirements for useful available data. Other non-machine learning approaches such as analytics, data enrichment, statistical analysis and robotics should also be considered as better solutions to some problems in this space.

Time should be spent understanding the problem and then determining a solution that is the best fit for the specific use case and business context. Even when applying ML to business processes, keeping humans in the loop is always beneficial to enhance the performance of these models - humans are far better at judgement-based tasks than machines.

Humans can perform additional tasks such as providing new labelled training data to the model, assessing false hypotheses and correcting the same, providing necessary assurances as required by regulators, boards and senior management, evaluating the performance of the model, and making decisions on complex cases using predicted outputs.

A way of embedding ML into existing processes to enrich these models with intelligence is to break them down into component parts and create 'narrow' models for each component. This allows for the creation of focused models that can enhance specific process steps. These outputs can then be fed into other models to enhance their performance or into a controller that would make an overall decision based on the individual parts.

While this could potentially be beneficial there are increased risks involved with introducing this level of complexity such as compounding errors propagating through the system. Having a robust management framework for models and ensuring human oversight would go a long way in mitigating these.

Case Study

UOB, Tookitaki and Deloitte readies machine learning pilot to accelerate the fight against money laundering

Company Business Overview

United Overseas Bank (UOB or the Bank) is a leading bank in Asia with a global network of more than 500 offices and territories in Asia Pacific, Europe and North America. In Asia, UOB operates through its head office in Singapore and banking subsidiaries in China, Indonesia, Malaysia, Thailand and Vietnam, as well as branches and representative offices across the region.

As a consistent market leader, the Bank set up The FinLab, an accelerator to promote and to accelerate the growth of the best and brightest financial technology start-ups and innovators in the region. Through the support of The FinLab, Tookitaki, a Singapore-based regulatory technology start-up, was able to collaborate with UOB to roll out a co-created machine learning solution that enables its compliance team to conduct deeper and broader analyses as part of its anti-money laundering efforts.

With the commitment to enhance its AML surveillance, UOB saw a significant opportunity in tapping on machine learning to augment and to enhance its existing systems to spot and prevent illicit money flows.

The Bank made a strategic decision to prioritise co-creation by working with Tookitaki to develop a fit-for purpose AI-driven AML technologies, tools, and systems in a single integrated platform.

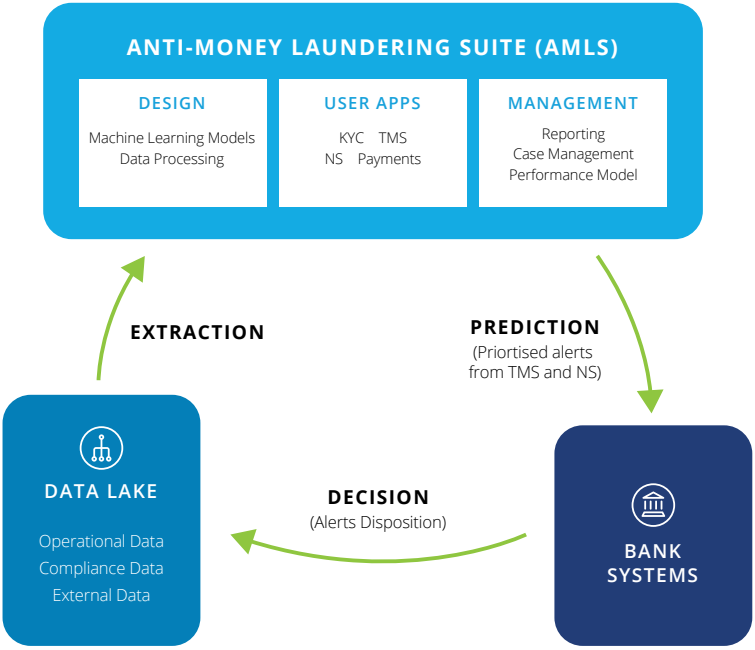
The Anti-Money Laundering Suite

UOB recognised the importance of creating a scalable 'sandbox' production environment to rapidly move a model from a Proof of Concept to Development.

Following a strategic review of the various options available, UOB chose to implement a customised model as it was more fitting for its compliance requirements. A customised model enables UOB to address specific needs such as the reduction of cost, greater efficiencies and simplified processes, allowing it to be faster in its production and operationalisation.

Entitled the '**Anti-Money Laundering Suite**' (AMLS), the integrated solution[9] is designed around the Bank's AML framework that features Know Your Customer, Transaction Monitoring, Name Screening, and Payments Screening processes. For UOB, the AMLS acts as a seamless and easy platform that is interoperable with a variety of modules.

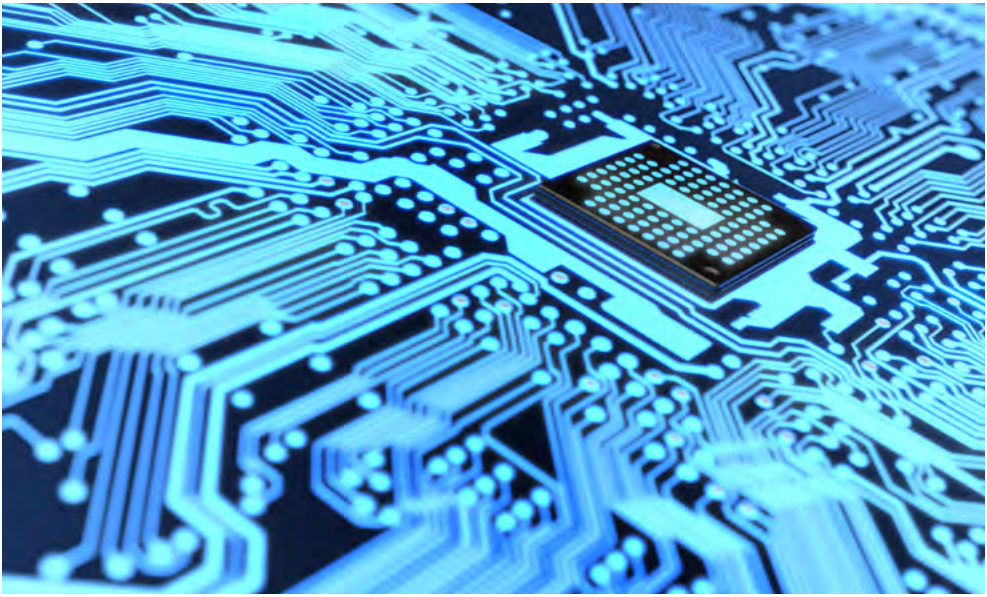
Figure 4: An integrated ML platform for rapid development and deployment of models.



Given the volume and velocity of transactions that flow through the Bank, it is crucial for UOB to optimise its alerts management, mainly to reduce the "false positives" and close alerts more efficiently.

As key objectives, the AMLS will be an additional layer leveraging ML models and techniques over and above their existing rules-based transaction monitoring systems. Central to that is UOB's keenness to acquire better insights from the transactions and activities of high-risk individuals and companies and suspicious activities to remain vigilant against any potential money laundering activities. Accordingly, it is also a means to compare performances of such new ML models to its existing rules-based systems.

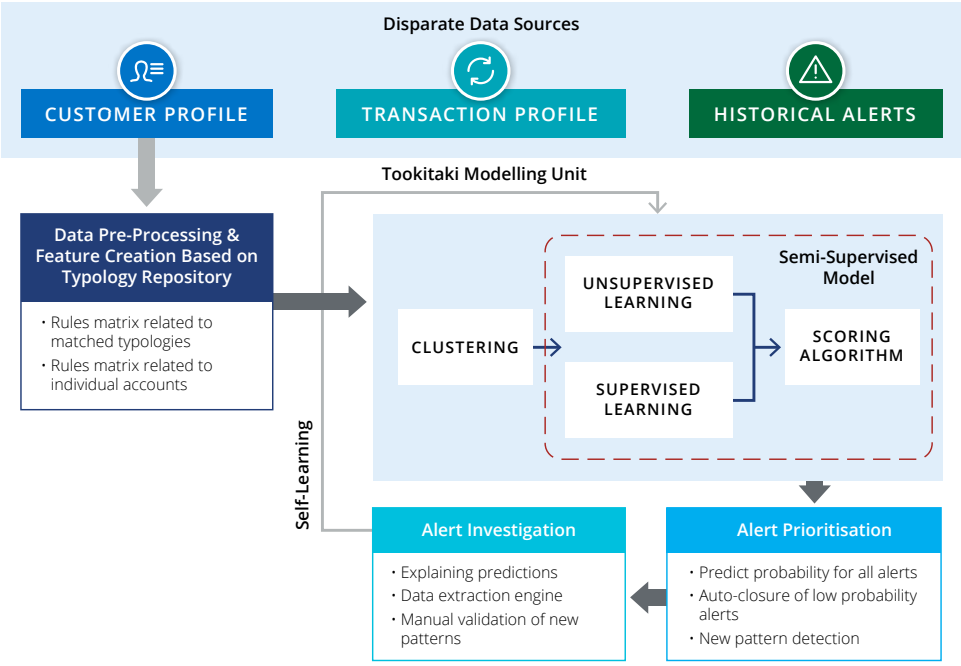
As part of the process to launch the AMLS, the Bank's compliance team worked closely with its Data Management Office and the fintech data scientists from Tookitaki to assess, to review and to deploy separate modules for the four key processes within its AML framework.



Machine learning a key accelerator

Prioritising transaction monitoring and name screening, the AMLS has completed pilots with its ML models and will roll out tests on the two other AML processes, namely customer risk assessment and sanctions screening progressively. In addition to reducing false positives for both the transaction monitoring and name screening modules, capabilities such as a self-learning mechanism for automatic, continuous learning, 'explainability' for thorough understanding and the ability to conduct quality investigations were deemed critical for achieving the desired business benefits.

Figure 5: Applying Machine Learning to alert prioritisation



"Multiple AI solutions need to come together to build a sophisticated, integrated AI framework in banking and financial services world. Tookitaki AMLS follows the same guiding principle and allows seamless integration with existing frameworks, while being scalable and explainable. Our motto is to help financial institutions be compliant, without any complications and further enable integrated, sustainable compliance management."

Mr Abhishek Chatterjee, Founder & CEO, Tookitaki

Nonetheless, ML goes beyond mere technicalities. Here are three key learnings from UOB when it comes to the co-creation process:

1. Models require a lot of data that may be housed in different places and not readily available. But, ML models are hugely reliant on data. The better the data, the more successful the model. To fast-track the development process, an audit of data information is essential to fine tune the extraction process. This then allows a robust environment for a model to be tested, developed and deployed.

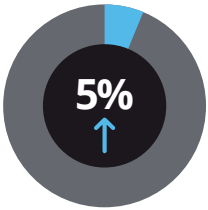
2. Keep building confidence in the pilots. Regular updates, guided principles and close working relationships with various departments within the Bank help create an informed and strong environment to discuss and refine the project.

3. To further collaborate and co-create, engaging the regulator in the early stages also facilitates greater transparency and accountability on the inner workings of new ML models.

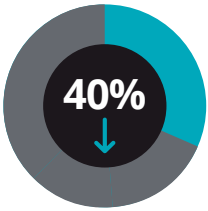
Driving new levels of efficiency and effectiveness

For its transaction monitoring module, UOB focused on the optimisation of detecting new, unknown suspicious patterns and to prioritise known alerts. The results achieved proved to be a significant step forward with a five per cent increase in true positives and 40 per cent drop in false positives.

TRANSACTION MONITORING



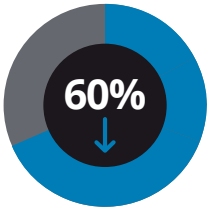
increase in
true positives



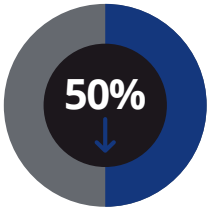
reduction in
false positives

The name screening module also saw similar positive results. To enhance the name screening process and to improve detection, the module was designed to handle a wider range of complex name permutations. At the same time, the module was also designed to reduce the number of undetermined hits through enriched "inference" features and the inclusion of additional customer profile identifiers. For its name screening alerts, there was a 60 per cent and 50 per cent reduction in false positives for individual names and corporate names respectively.

NAME SCREENING



reduction in false
positives for
individual names

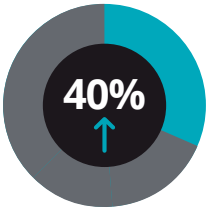


reduction in false
positives for
corporate names

The results demonstrated what was achievable through ML to reduce false positives in the AML process. It signals more opportunities to invest in ML to prioritise alerts management progressively. And, equally important is to uplift the capabilities in case management and confidence scoring.

The investment in the ML pilot attained 40 per cent in operational efficiency, reinforcing the vision to do things differently with practical results that address money laundering risks effectively.

OPERATIONAL EFFICIENCY



increase in
operational efficiency

With positive steps forward, UOB will continue to optimise AMLS' ML algorithms by adding new transactional data into the database with the goal to implement the solution across the entire AML framework over time. The Bank will also continue to adopt a "glass box" versus "black box" approach when applying ML, ensuring that the decisions made by the ML model can be explained and translated in understandable business terms that will result in the increase of trust with end users and regulators.

To further boost confidence in the model, UOB has engaged Deloitte to perform an independent assessment of the pilot programme and its approach.

In working with Deloitte for the first ongoing independent assessment of the ML model, UOB's AMLS solution went through a series of stress tests to ensure that it was capable of dealing with a variety of AML compliance typologies. Starting the assessment in August 2018, the key priority was for Deloitte to validate the conceptual soundness of UOB's AMLS model, confirm that it was 'fit-for-purpose', and compare the performance of the model with the existing rule-based monitoring process.

"UOB is committed to upholding a strong risk-focused culture in which regulatory compliance is a key pillar to maintaining the trust our stakeholders place in us. The area of AML requires constant vigilance and continual enhancement to ensure that we stay on top of preventive, detective and enforcement measures. The use of RegTech such as Tookitaki's AMLS enables us to augment our ability to identify actionable alerts and to minimise false positives. These sharpen the accuracy and effectiveness of our AML risk management."

Victor Ngo, Head of Group Compliance, UOB

From POC to Production:

The **key success factors** discussed under the chapter on "Uses and potential applications of machine learning in fighting money laundering" should be considered, as applicable at this juncture.

Start with a detailed blueprint for model deployment.

Banks should ensure that the model architecture is able to operate within the business process and contain all the necessary controls. The model should be gradually phased into operation to ensure that the performance is in line with expectations and that employees gain confidence with the outputs.

Relevant talents and resources need to be adequately enabled to use the model outcomes.

The benefits of the application of ML within this space will only be realised if the end users buy in to the process, know how to use the outputs and trust the predictions made. Key to achieving this is to provide training for the review team as well as providing comprehensible explanations to the reviewers why specific predictions were made.

Governance needs to be embedded into the model lifecycle.

The critical aspects of the solution need to be fully understood and documented. There should be clear roles and responsibilities established for managing the models as well as the associated risk. The model outcomes should be continuously monitored to ensure that they are still operating within. All changes to the models should also be stored and recoverable for audit purposes.

Documentation of the ML model and algorithms.

The importance of good quality documentation cannot be under estimated. Any model validation conducted starts with the review of documentation. The documentation should cover key elements – which to name a few are, explanation of the technology and its functionality, business requirements, its outcome, risk mitigation approaches, testing and assurance and disaster recovery.

What lies ahead?

In order to extract benefit from the capabilities of AI it is necessary to have a robust ecosystem to tap into. There are multiple parties that are critical to ensuring successful adoption and growth ranging from internal and external.

In preparation for the design and development of an "AI Management Framework", UOB will continue to solidify and develop the AI ecosystem for AML compliance in the next few years. As part of this journey, Deloitte will work with UOB to develop a blueprint for managing an AI AML ecosystem including and not limited to the design pillars of a robust goverance process, the governance operating model, the acquisition of AI solutions (working across the selection and on-boarding of technology providers), and the mechanisms for implementation.

Internally technology, data and business functions need to work together to develop a cohesive strategy and leverage enterprise capabilities while tapping into domain expertise of the users. Externally, the technology and hardware providers need to develop solutions that meet business needs as well as address the legal and regulatory requirements imposed on Banks.

As such, regulators should play an active role in this discussion and assist with the measured application of such technologies. All of these parties need to work together and learn from each other on key learnings and success factors as well as effective and sustainable approaches and models, in order to fully tap into the potential benefits of these technologies.

Conclusion

Ultimately, it is not about tools, technologies but rather an effective financial crime compliance framework with an embedded innovation strategy.

Ultimately, it is not about tools or technologies but rather an effective financial crime compliance framework with an embedded innovation strategy. Innovation certainly has presented a good "business case" for creating better ways of monitoring AML/CFT risks.

Banks however, cannot afford to undertake a piecemeal or reactive approach to innovation in compliance. The risk and costs involved are too high. For this reason, banks must first explore and design a clear innovation and technology enhancement strategy that spans their organisation's compliance framework, their unique control and risk environment, and their desired 'customer experience'.

More critically, is for banks to take active steps to identify complex activity patterns and anticipate "rare events" to ensure that there are well-designed safeguards and controls and move towards proactive measures to detect and prevent any suspicious activity or respond to evolving regulatory requests. To do so, this will also require a single view of an entire business' portfolio, transactions and operations.

Knitting together business, operations, compliance and technology divisions into one team is a strategic response to recognise the new realities of fighting against coordinated and sophisticated criminals.

There is a strong call from customers, regulators, shareholders and society at large for C-suite leaders and boards of directors to proactively seek out effective strategies to protect their organisations now and in the future.

For AI, what was once a mere concept and debated promise is now an inflection point in the fight against financial crime, and banks progressing forward in this new terrain of machines and humans working together are all the better for it. This also signals that all relevant parties should come together to create the much needed ecosystem to cement the road and building-blocks to success.

"Seeing the progress made by UOB in their pilot programme to use machine learning is proof positive that a holistic company strategy which encompasses technology, new approaches and collaboration will accelerate the response to financial crime and its corresponding complications. The ASEAN region with its diverse businesses and trade will benefit greatly from financial technology and the continued adoption of innovative solutions."

Ho Kok Yong, SEA Financial Services Leader, Deloitte

End notes

[1] Long Finance, China Development Institute, Financial Centre Futures, Z/Yen, The Global Financial Centres Index 24, September 2018, https://www.longfinance.net/media/documents/GFCI_24_final_Report_7kGxEKS.pdf, accessed October 24, 2018.

[2] Joshua Fruth, "Anti-money laundering controls failing to detect terrorists, cartels, and sanctioned states", Reuters, March 2018,https://www.reuters.com/article/bc-finreg-laundering-detecting/anti-money-laundering-controls-failing-to-detect-terrorists-cartels-and-sanctioned-states-idUSKCN1GP2NV, accessed October 24, 2018.

[3] Brian Monroe, "Financial Crime Wave – U.S. Compliance Costs surpass $25 Billion, EU, U.K. AML Fines, and More", Association of Certified Financial Crime Specialists, October 2018, https://www.acfcs.org/news/422560/Financial-Crime-Wave--U.S.-compliance-costs-surpass-25-billion-EU-U.K.-AML-fines-and-more.htm, accessed October 24, 2018.

[4] Bob Contri, Rob Galaski, "How artificial intelligence is transforming the financial ecosystem", Deloitte, August 2018, https://www2.deloitte.com/global/en/pages/financial-services/articles/artificial-intelligence-transforming-financial-ecosystem-deloitte-fsi.html, accessed October 24, 2018.

[5] Monetary Authority of Singapore, "Strengthening the AI ecosystem in Singapore's financial sector", Media Release, 7 May 2018 http://www.mas.gov.sg/News-and-Publications/Media-Releases/2018/Strengthening-the-AI-ecosystem-in-Singapore-financial-sector.aspx

[6] Dilip Krishna, Nancy Albinson, Yang Chu, "Managing algorithmic risks: Safeguarding the use of complex algorithms and machine learning", Deloitte, 2017, https://www2.deloitte.com/us/en/pages/risk/articles/algorithmic-machine-learning-risk-management.html, accessed October 24, 2018.

[7] Peter Cooman, "Demystifying Black-Box Models with SHAP Value Analysis", Medium, May 2018, https://medium.com/civis-analytics/demystifying-black-box-models-with-shap-value-analysis-3e20b536fc80, accessed October 24, 2018.

[8] Eric Brown, "Local Interpretable Model-agnostic Explanations – LIME in Python", Python Data, January 2018, https://pythondata.com/local-interpretable-model-agnostic-explanations-lime-python/, accessed October 24, 2018.

[9] UOB, "UOB and Tookitaki strengthen combat against money laundering through co-created machine learning solution", News Release, 24 August 2018, https://www.uobgroup.com/web-resources/uobgroup/pdf/newsroom/2018/UOB-and-Tookitaki-strengthen-combat-against-money-laundering.pdf

Contact us

Radish Singh
SEA Financial Crime Compliance Leader and AML Partner, Deloitte Financial Advisory, Forensic, Deloitte & Touche LLP
radishsingh@deloitte.com

Miguel Fernandes
Director, Analytics, Deloitte Financial Advisory, Forensic, Deloitte & Touche LLP
fmiguel@deloitte.com

Nick Lim
Head of AI, Analytics & Automation Group Compliance, United Overseas Bank
Nick.LimYC@UOBgroup.com

Eric Ang
Senior Vice President, AML Compliance Analytics & Insights Group Compliance, United Overseas Bank
Ang.BoonHin@UOBgroup.com

Deloitte.

Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited (“DTTL”), its global network of member firms, and their related entities. DTTL (also referred to as “Deloitte Global”) and each of its member firms are legally separate and independent entities. DTTL does not provide services to clients. Please see www.deloitte.com/about to learn more.

Deloitte is a leading global provider of audit and assurance, consulting, financial advisory, risk advisory, tax and related services. Our network of member firms in more than 150 countries and territories serves four out of five Fortune Global 500® companies. Learn how Deloitte’s approximately 264,000 people make an impact that matters at www.deloitte.com.

This communication contains general information only, and none of Deloitte Touche Tohmatsu Limited, its member firms or their related entities (collectively, the “Deloitte network”) is, by means of this communication, rendering professional advice or services. Before making any decision or taking any action that may affect your finances or your business, you should consult a qualified professional adviser. No entity in the Deloitte network shall be responsible for any loss whatsoever sustained by any person who relies on this communication.

© 2018. For information, contact Deloitte Touche Tohmatsu Limited.