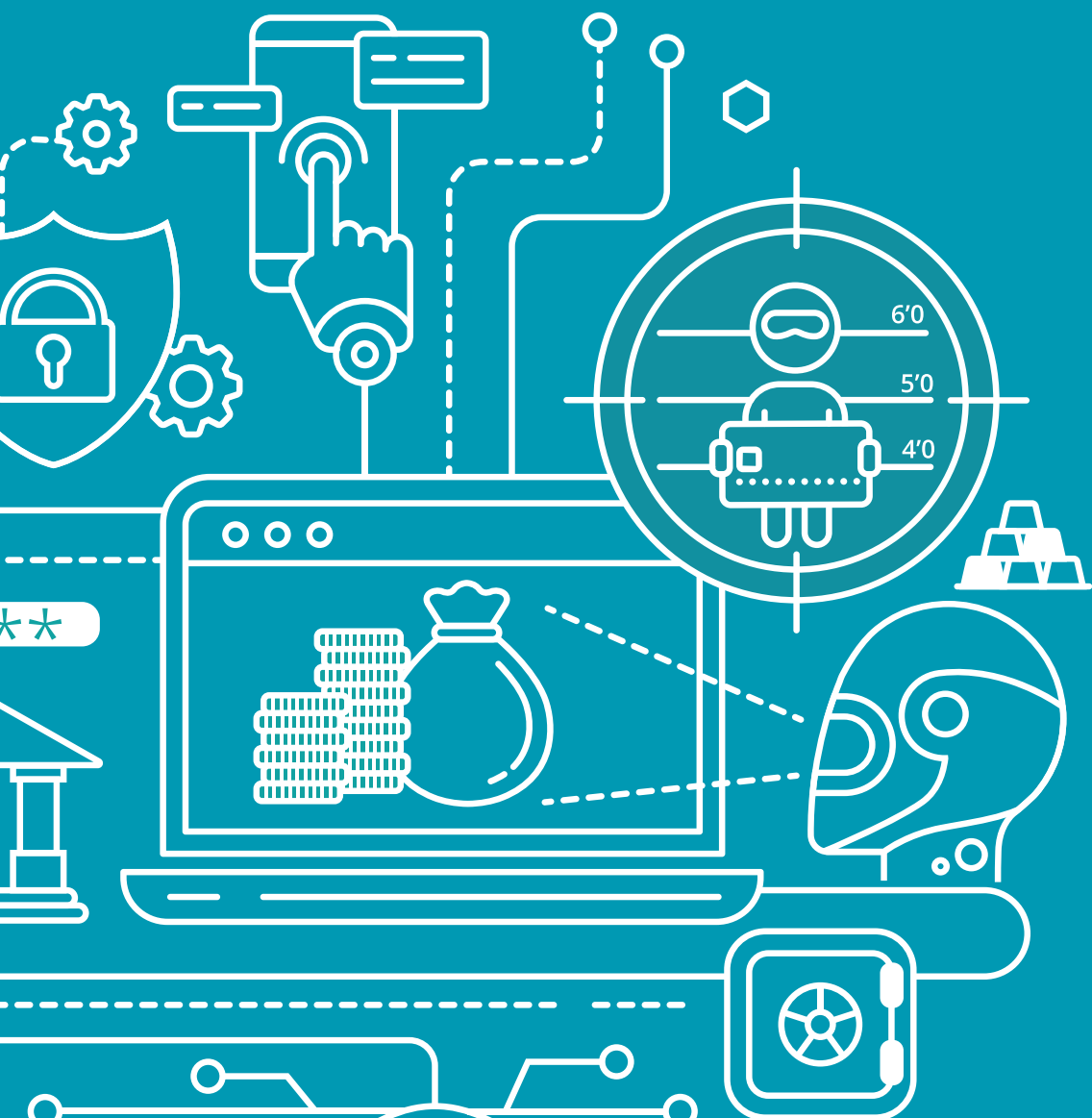


Deloitte.



Transforming Financial
Crime Management
Through Technology

**MAKING AN
IMPACT THAT
MATTERS**
since 1845



Content

Introduction	1
Overview of Recent Developments in the Landscape	3
Use of Technology to Combat Financial Crime	15
Selected Case Studies of Technology Solutions	19
Key Takeaways from our Case Studies	29
Managing Technology Through the Customer Lifecycle	33
Looking to the Future	38
Conclusion	41
Glossary	43
Contacts	45
Endnotes	47

Introduction

Financial crime remains a trillion dollar issue and one of the key risks faced by both the financial services industry (FSI) and society today despite significant investment in detection, prevention, and deterrence capabilities.

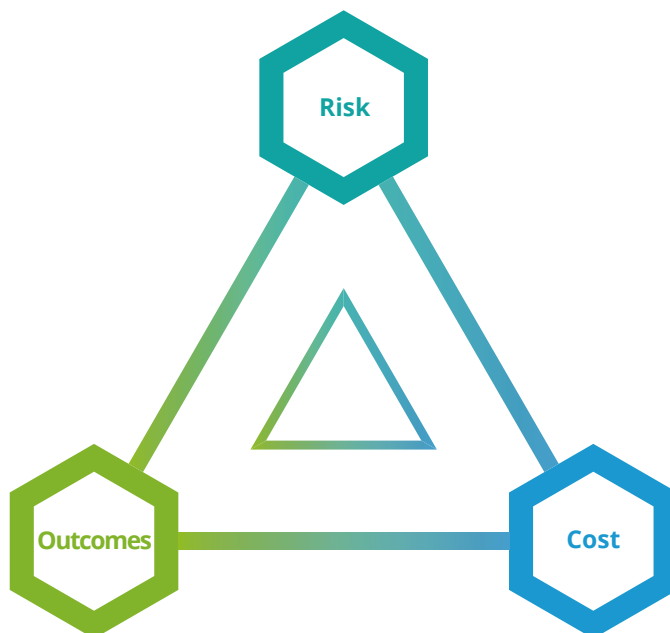
Criminals are becoming increasingly sophisticated in their use of technology to perpetrate financial crime, finding and exploiting loopholes in our financial system and leveraging emerging technologies such as new payment platforms and cryptocurrencies to conduct complex, multi-layered transactions that are increasingly difficult to detect and trace.

Meanwhile, money laundering (ML) and terrorist financing (TF) activities continue to threaten social order and undermine global efforts to tackle important social and ethical issues such as crimes against the environment, and human, wildlife, and drug trafficking.

However, the impact of technology isn't limited to criminals. The trend of digitisation, which has been accelerated by the impacts of COVID-19, is changing the typology of financial crime and the way in which law enforcement and regulated entities seek to detect it. For example, traditional cash-heavy indicators and physical document verification controls are becoming less relevant in the face of digital transactions.

Against this backdrop, firms have been investing significantly in capabilities to uplift their financial crime management programs. However, despite considerable time and money committed to addressing financial crime risk, there is still more work to be done, as evidenced by significant enforcement actions from regulators and high-profile scandals linked to the proliferation of financial crime.

Therefore, there is a need to bring updated thinking on the use of technology to efficiently balance risk, outcomes, and cost.



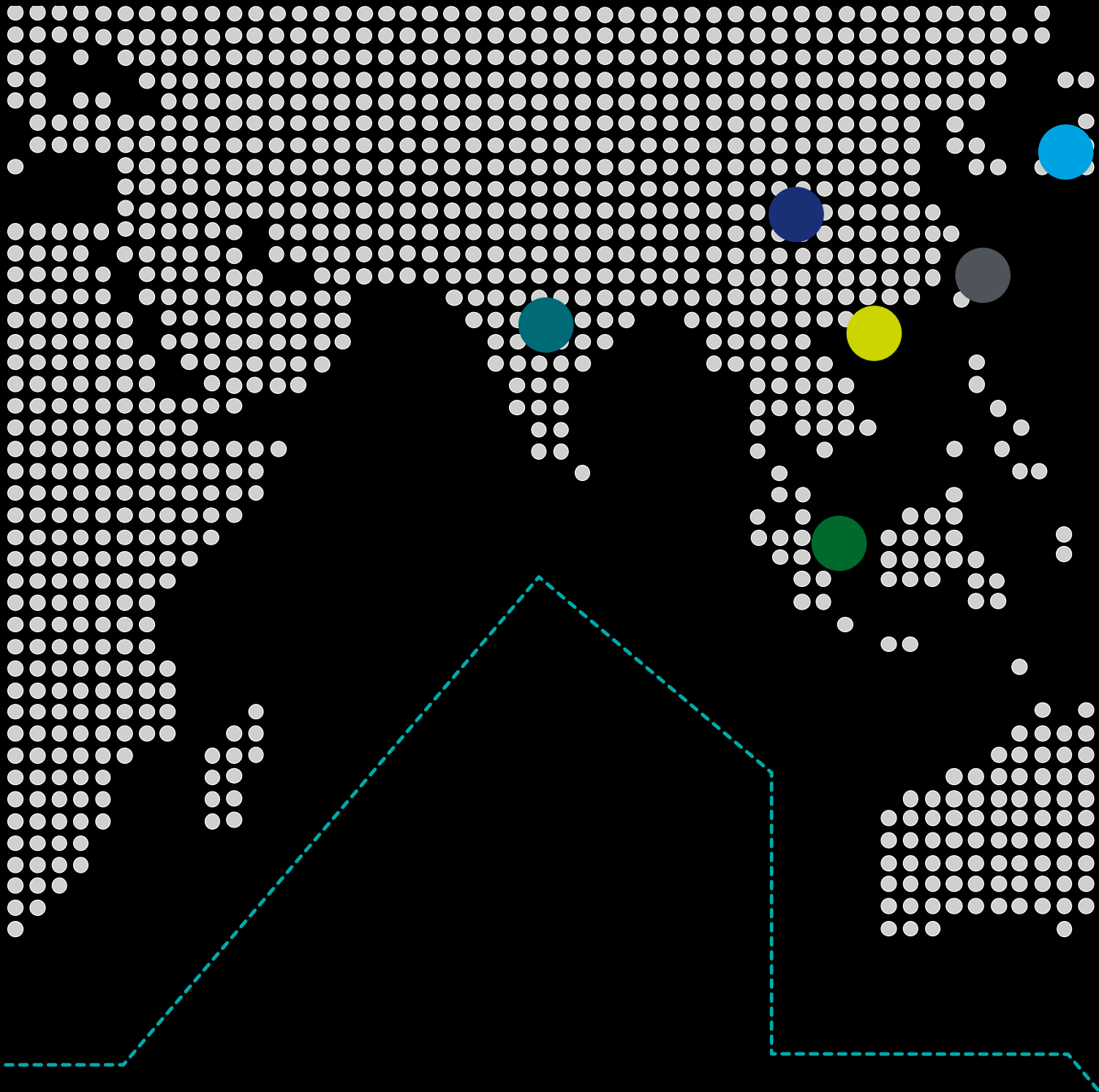
For firms to see the biggest benefits of technology in combatting financial crime, they will need to embrace its use across the customer lifecycle in an integrated manner.

However, different organisations are at different stages of technological adoption and have varying appetite and budget to take on such projects, especially as technology solutions are often heavily dependent on the ability to effectively integrate with existing systems and require complete and accurate data.

Moreover, there is a natural tension, when selecting technology solutions, between safety and confidence in established solutions with strong performance histories, as compared to cutting-edge solutions using the latest, but untested, technologies. Therefore, organisations often start with a proof-of-concept to demonstrate the benefits of 'RegTech^[1]' before investing more heavily in solutions. Further, firms often have to 'parallel run' new solutions alongside existing processes, while efficacy is proven internally and to regulators. This in turn has cost implications and so will require organisations to commit to investing in change over the medium-to-long-term.

This report considers how firms can deploy technology in the fight against financial crime to lift efficacy and improve the quality of outcomes, while increasing efficiency and reducing costs in the long-term. We showcase five case studies from across the Asia Pacific (AP) region, providing industry practices and insights into how technology is being used to prevent and detect financial crime.

^[1]RegTech' is used in reference to technology solutions that are designed to enhance processes in place to meet regulatory requirements and expectations. Specifically, those related to financial crime laws, rules and regulations.



Overview of Recent Developments in the Landscape





Jurisdiction: Australia



Key Regulatory Updates

Following record fines to two of Australia's major banks for breaches of anti-money laundering (AML) and counter-terrorism financing (CTF) laws, the Australian regulator, Australian Transaction Reports and Analysis Centre (AUSTRAC), has momentum and political support to continue its focus on how players in Australia's financial services and payments landscape are managing financial crime risk.

This has seen AUSTRAC perform a number of detailed reviews into not only key players in the Australian financial industry, but also global companies and emerging players in the payments space, with the results of these reviews highlighting a number of systemic failures in the management of financial crime risk.

In addition, there has also been continued pressure on the Government and regulators such as AUSTRAC to continue its reform agenda with respect to both

financial crime risk and risk management. This has seen a number of reforms introduced in response to industry-wide reviews, such as the Royal Commission into Misconduct in the Financial Services Industry and the Financial Action Task Force's (FATF) Mutual Evaluation recommendations, including:

- The extension of the *Banking Executive Accountability Regime* (BEAR) to other FSI firms, which will result in a larger cohort of FSI firms and other entities (such as wealth managers and payments providers) expected to comply with increased responsibilities and end-to-end product accountabilities relating to conduct, culture and risk management (including financial crime risk management). The proposed extension of BEAR to a larger group of FSI firms will see the existing regime renamed to the *Financial Accountability Regime* (FAR).¹

- Passage of the *Anti-Money Laundering and Counter-Terrorism Financing and Other Legislation Amendment Bill 2020* (the Amendment) in December 2020, which will give effect to the recommendations from the FATF 2015 report, and introduces changes to key elements of Australia’s AML/CTF framework around customer identification procedures, correspondent banking relationships, tipping-off offences, access to information, and cross-border movements of money. These changes are due to come into force on 18 June 2021.²
- The prudential regulator, the Australian Prudential Regulation Authority (APRA), updating its standards and guidance relating to risk management (*Prudential Standard CPS 220 Risk Management* and *Prudential Practice Guide CPG 220 Risk Management*, effective 1 July 2019),³ and information security (*Prudential Standard CPS 234 Information Security*, effective 1

July 2019).⁴ These updates came with an increased expectation that FSI firms and Boards have in place appropriate reporting mechanisms to allow greater visibility on how they are complying with financial crime obligations and managing risks.

In addition to the above, AUSTRAC worked with a number of industry and community organisations on changes to the *AML/CTF Customer ID and Verification Rule*⁵ (effective 28 May 2020) to help Australians fleeing family and domestic violence gain financial independence. Under the rule, if a customer cannot produce their driver’s license or birth certificate, or show a different address, banks and other regulated businesses can use alternative ways to verify their customer’s identity. Guidance on how reporting entities can apply the rule is available through an updated Guideline from AUSTRAC.⁶



Enforcement Actions

AUSTRAC handed out a record AU \$1.3 billion fine to one of Australia’s major banks in September 2020 for AML/CTF breaches, partly resulting from failures relating to the monitoring of transactions that were connected to child sexual exploitation. The investigation by AUSTRAC identified over 23 million occasions where the Bank contravened the *Anti-Money Laundering and Counter-Terrorism Financing Act 2006* (the AML/CTF Act), exposing Australia’s financial system to criminal exploitation.

In 2019, AUSTRAC also ordered the appointment of external auditors to two large payments/technology companies to examine their compliance with obligations under the AML/CTF Act, following ongoing concerns.

In addition, AUSTRAC issued fines and infringement notices to two reporting entities in 2019 for failures to report international fund transfers in line with obligations under the AML/CTF Act.



Jurisdiction: New Zealand



Key Regulatory Updates

In September 2020, New Zealand's AML and countering financing of terrorism (CFT) supervisors jointly updated the *Enhanced Customer Due Diligence (CDD) Guideline*⁷ to assist reporting entities to understand when enhanced CDD is required or should be applied based on the reporting entities' AML/CFT risk assessment.

In March 2020, AML/CFT supervisors published urgent guidance relating to verifying a person's identity during COVID-19 alert levels. The Guidance⁸ outlines how reporting entities may continue to meet their AML/CFT obligations relating to CDD and account monitoring in a way that limits the risk of the spread and transmission of COVID-19, with limited interactions with customers.

In November 2019, New Zealand's AML/CFT regulators, the Department of Internal Affairs (DIA), the Financial Markets Authority (FMA), and the Reserve Bank of New Zealand (RBNZ) jointly updated and published two

new guidance notes outlining the revised *AML/CFT Supervisory Framework*⁹ (describing the functions and powers of the three AML/CFT supervisors), and the territorial scope of the AML/CFT Act.¹⁰

The final stages of the 'Phase 2 amendments' of New Zealand's AML/CFT laws¹¹ (enacted in 2017 under the *Anti-Money Laundering and Countering Financing of Terrorism (AML/CFT) Amendment Act 2017*), came into effect on 1 August 2019. This means that from 1 August 2019, the New Zealand Racing Board (which administers all racing and sports betting in New Zealand) must have put AML/CFT measures in place. In addition, accountants, lawyers, real estate agent as well as businesses trading in high value goods (such as jewellery, precious metals, precious stones, watches, motor vehicles, boats, art or antiquities) are required to comply with the AML/CFT Act if certain operating criteria apply.



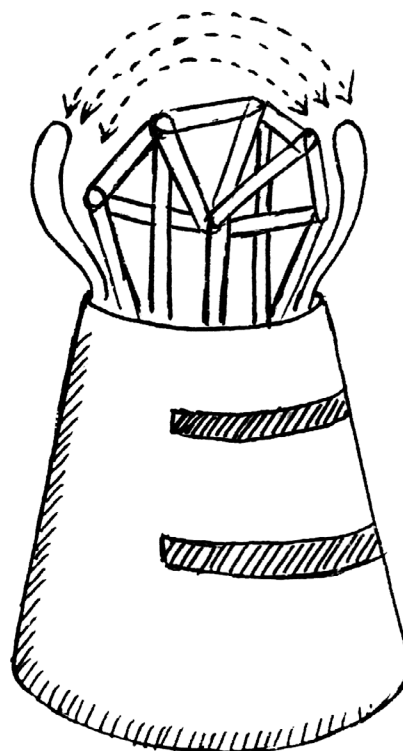
Enforcement Actions

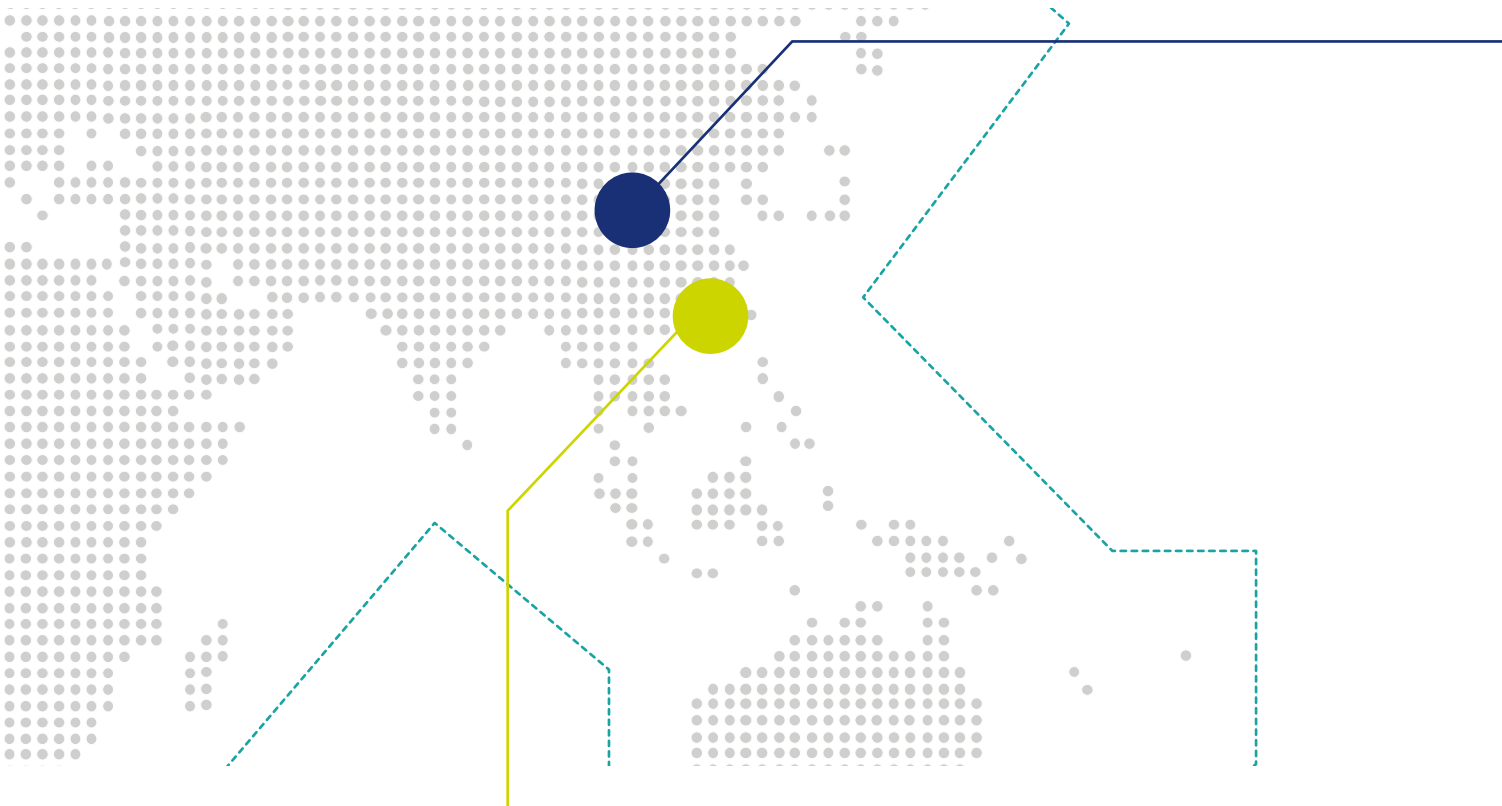
In July 2020, the DIA fined two money remitters over NZ \$7.5 million for violations of the 2009 *Anti-Money Laundering and Countering Financing of Terrorism Act* between 2014 and 2019. The violations specifically relate to behaviours reflecting aggravated conduct, including failing to cooperate with the Department in its investigation and attempts to mislead the Department, and trying to disguise the status of one of the money remitters under investigation as a reporting entity.

In August 2019, the New Zealand Police arrested six people and seized millions in assets following a significant money laundering investigation in Auckland.

In July 2019, the DIA issued a formal warning under the AML/CFT Act to seven reporting entities within a leading New Zealand workplace provider for failing to meet AML/CFT Act requirements that include failing to conduct customer and enhanced due diligence, failing to keep records and failing to establish, implement and maintain a current risk assessment and AML/CFT programme.

In June 2019, the DIA issued a formal warning to a major safe deposit provider in New Zealand for failures to meet AML/CFT obligations, including failing to conduct CDD, failing to adequately monitor accounts and transactions, failing to keep records, and failing to establish, implement or maintain an AML/CFT programme.





Jurisdiction: Hong Kong Special Administrative Region (SAR)



Key Regulatory Updates

The Hong Kong Monetary Authority (HKMA) continues to work on “*promoting responsible innovation in AML work*”¹² with a key focus on:

1. Making sure new and emerging sectors can develop in a responsible way, with adequate safeguards built in so they are not exploited by bad actors;
2. Ensuring requirements are up-to-date and enabling firms to take full advantage of the opportunities offered by new technology; and
3. Enabling change that is consistent with the HKMA’s objectives, “*so that we can continue to supervise*

effectively; in our supervision we need to think and act in a way that is consistent with the changes occurring in the sectors we supervise”.

In support of this ‘innovation in AML focus’, the HKMA has updated key literature^{13,14} to provide clearer guidance on how technology can be used in the fight against financial crime, and how new market entrants (such as those providing stored value facilities and virtual banks) can ensure they have adequate safeguards and a robust framework to manage financial crime risk.



Enforcement Actions

The Hong Kong Securities and Futures Commission (SFC) fined several financial institutions (FI) more than

HK \$25 million for AML violations, including internal control failures relating to AML risk.



Jurisdiction: Mainland China



Key Regulatory Updates

In January 2021, the People's Bank of China (PBOC) released an updated Guideline¹⁵ outlining how regulated FIs should complete their Institutional Risk Assessment (IRA) for ML/TF risks. Under the Guideline, regulated FIs must finalise their IRA Framework by 31 December 2021, and complete their first IRA by 31 December 2022. The IRA Framework implemented by FIs must be:

- Comprehensive
 - Capturing geographical, client, product and services, transactional and channel perspectives;
 - Covering all branches and subsidiaries;
 - Considering all risk factors; and
 - Covering all decision making, execution and oversight aspects of management;
- Objective;
- Appropriate and applicable to the bank's own business model; and
- Flexible.

On 30 December 2020, the PBOC published for consultation an amended draft version of the *Financial Institution Anti-money Laundering Anti-terrorist Financing Supervisory Administrative Measures*.¹⁶ The proposed measures will seek to overhaul China's AML framework, following completion of the FATF's assessment in 2019. Upon conclusion of the consultation and approval, these new measures will supersede the existing AML regime established by PBOC in 2014.



Enforcement Actions

In the past few years, AML law enforcement inspections have continued to intensify, with more frequent and larger penalties being imposed. In 2019, for example, the PBOC carried out AML enforcement inspections on 1,744 organisations, and imposed penalties for violations of anti-money laundering regulations. The total fines amounted to CN ¥215 million, a year-on-year increase of 13.7%. 525 institutions that violated regulations were penalised and fined a total of ¥202

million; while 838 individuals were fined a total ¥13.41 million. In 2020, the PBOC and its branches performed inspections on 614 organisations and levied fines amounting to ¥525 million. Up to 1000 people were punished, with fines totalling CN ¥25 million. It is anticipated that inspections and penalties will continue to rise in the coming years, given the priority placed on the topic by the PBOC and other government agencies.



Jurisdiction: Singapore



Key Regulatory Updates

Singapore's continued focus on RegTech has seen the introduction of regulations designed to capture new and growing sectors in financial services such as payments, digital banks, and crypto-assets. One of the most significant of these regulations is the introduction of the *Payment Services Act (2020)* (PSA),¹⁷ which came into effect in January 2020, and consolidates the regulation of payments providers in Singapore's regulatory landscape.

Outside of the regulatory sphere, Singapore has also seen FinTech^[2] associations such as the Association of Cryptocurrency Enterprises and Start-Ups Singapore (ACCESS) working together to develop a voluntary Code of Practice^{18,19} in order to expand Singapore's AML/CFT regulations to crypto-firms.



Enforcement Actions

The Monetary Authority of Singapore (MAS) has revoked the licences of Singapore-based asset management firms and trust companies for breaching AML regulatory requirements, and internal control failures relating to AML/CFT risks.

In addition to the above, MAS imposed penalties of more than SG \$2 million for failures to comply with AML/CFT obligations relating to implementation of adequate AML/CFT policies and procedures, failure to subject AML/CFT controls to independent audits, and failures to verify information relating to sources of wealth or relationships between customers.

[2] 'FinTech' is used in reference to technology solutions that are designed to support, enhance or enable banking and financial services.



Jurisdiction: Japan



Key Regulatory Updates

The Japan Financial Services Agency (JFSA) released the results of its consultative proposals for partial amendments to the *Guidelines on Measures against Money Laundering and the Financing of Terrorism* and published the revised Guideline.²⁰ The key updates are as follows:

1. The establishment of an effective control environment for FIs is considered critical given the fact that the threat of terrorism is spreading across borders;
2. Risk assessment and mitigation measures should be taken for all customers as appropriate by conducting a risk assessment for each common customer type; and
3. As points to be noted when making overseas remittances, there is a risk that import/export

transactions may be used for the transfer of criminal proceeds, and for the transaction of illegal drugs and goods diverted for military use.

The JFSA is also considering the possibility of developing a joint system that local banks can use to combat ML which will use artificial intelligence (AI) to assess customers' risks and check against sanctions lists.²¹

Further, the JFSA announced its request for *notification of source and destination information when transferring cryptographic assets (Travel Rules)*.²² It requested that the Japan Virtual and Crypto Assets Exchange Association (JVCEA) thoroughly disseminate the necessary system.



Enforcement Actions

The JFSA took administrative action (known as a 'business improvement order') against a crypto payment platform provider for violating a number of acts including:

- *The Order for Collection of Reports*;
- Articles 4 and 6 of *the Act on Prevention of Transfer of Criminal Proceeds* (Act No. 22 of 2007); and
- Insufficient measures pertaining to the guidelines on measures against money laundering and terrorist financing.

Under the order, the firm was required to submit a business improvement plan to the JFSA as well as set up an AML/CFT risk management system that ensures that exchanges are confirmed and documented within the hour of a transaction.



Jurisdiction: Taiwan



Key Regulatory Updates

Taiwan's move from the 'enhanced follow up' category to the 'regular follow up' category places it within the same supervisory category as Hong Kong SAR, Macau, Indonesia and the Cook Islands, and reduces the level and frequency of reporting required to be provided to the Asia Pacific Group on Money Laundering (APG).²³

Key to this change in rating is the raft of amendments made by the Legislative Yuan of Taiwan to the *Money Laundering Control Act* (MLCA),²⁴ which brought the

'business operations of virtual currency platforms and currency trading' under its scope in 2018, and laid the groundwork for Taiwan's *Virtual Bank Licensing Framework*, and introduction of virtual banks from the latter half of 2020.²⁵

Taiwan has taken steps to significantly strengthen its AML regime in recent years, resulting in an improvement in its ranking by key regional watchdog (the APG) in late 2019.



Enforcement Actions

In the past months, Taiwan's Financial Supervisory Commission (FSI) has fined some local banks more than NT \$72 million for conduct risk and internal fraud.



Jurisdiction: India



Key Regulatory Updates

In response to rapid developments in the payment system landscape with the increased adoption of technology, availability of payment products, and increase in more non-FI players, the Reserve Bank of India (RBI) introduced a number of changes to strengthen the regulatory framework governing cybersecurity and financial crime, including:

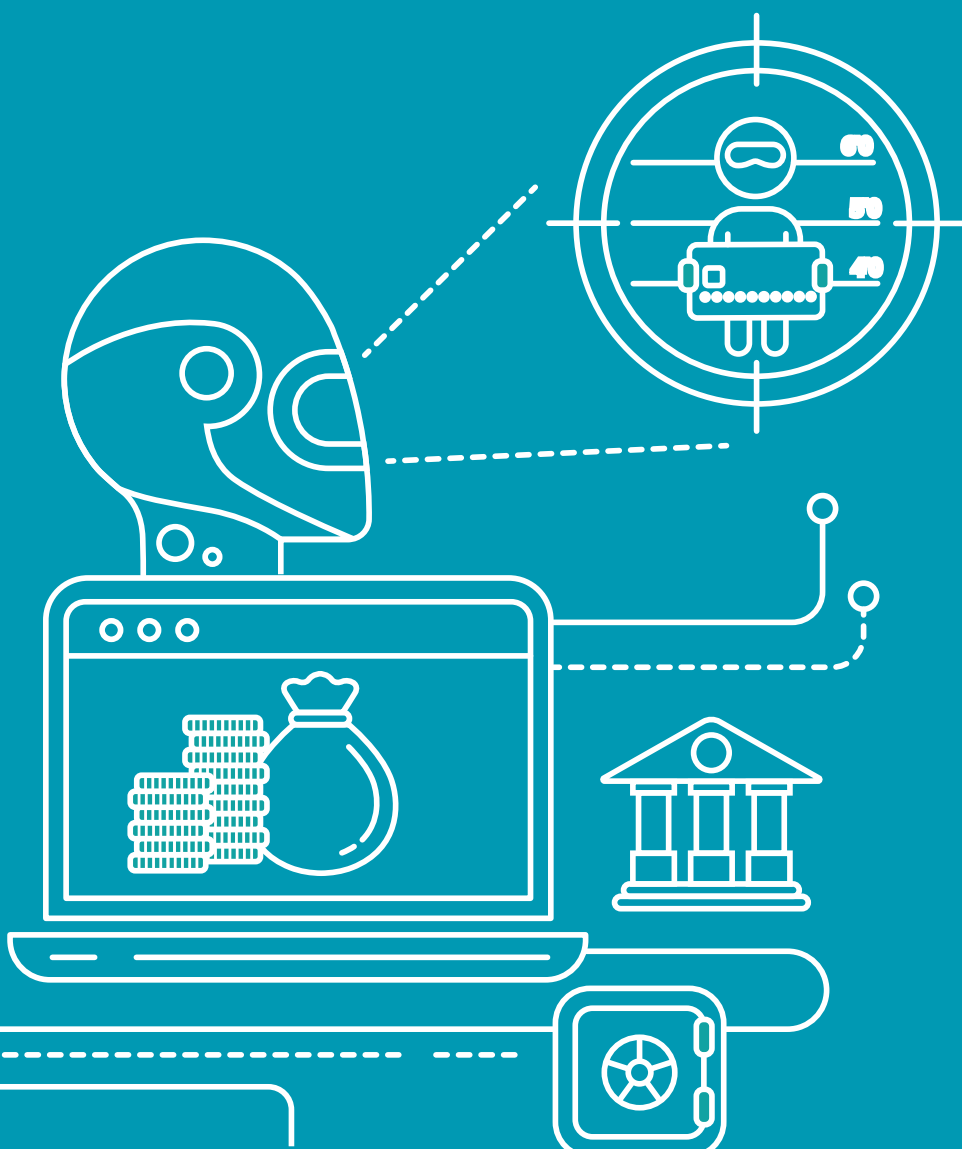
- An update to the *Master Direction on Digital Payments Security Controls*²⁶ which will come into effect in August 2021. The Master Directive (MD) includes guidelines for regulated entities (REs) to establish robust governance structures and implement common minimum standards of security controls for digital payment products and services.
- An extension of the *Master Direction – Know Your Customer (KYC) Direction*²⁷ issued in 2016 to all Housing Finance Companies (effective 19 May 2020), following transfer of regulation of Housing Finance Companies to the RBI. The MD on KYC is a consolidation of directions on KYC, AML and CFT, and is applicable to all REs of the RBI. Additionally, in December 2020, the MD was amended²⁸ to include legal entity templates and REs are now required to upload KYC data on legal entities opened on or after 1 April 2021, onto the Centralized KYC Registry. In a further Amendment²⁹ dated 10 May 2021, the RBI laid down revised minimum standards to be adhered to by REs in respect of infrastructure, procedure, records and data management of the Video based Customer Identification Process. The Amendment also restricted the use of one-time password-based verification in (non-face-to-face) e-KYC.
- An update to the *Guidelines on Regulation of Payment Aggregators and Payment Gateways*³⁰ in March 2020 (effective 1 April 2020), which revised the 'directions for opening and operation of accounts and settlements of payments for electronic payments involving intermediaries' originally issued as part of *Circular DPSS.CO.PD.No.1102/02.14.08/2009-10* (dated November 24, 2009). The revised Guidelines contained updated guidance from the RBI on KYC requirements under AML/CFT regulations, fraud prevention and risk management frameworks, and security-related recommendations in respect of information technology (IT) systems, information security governance, and data security requirements.
- Revisions to the framework for the imposition of monetary penalty and compounding of contraventions/offences under Sections 30 and 31, respectively of the *Payment and Settlement Systems (PSS) Act, 2007*. The revised framework³¹ outlined in the January 2020 updates to the PSS continues to centre around objectivity and transparency in the decision-making process.



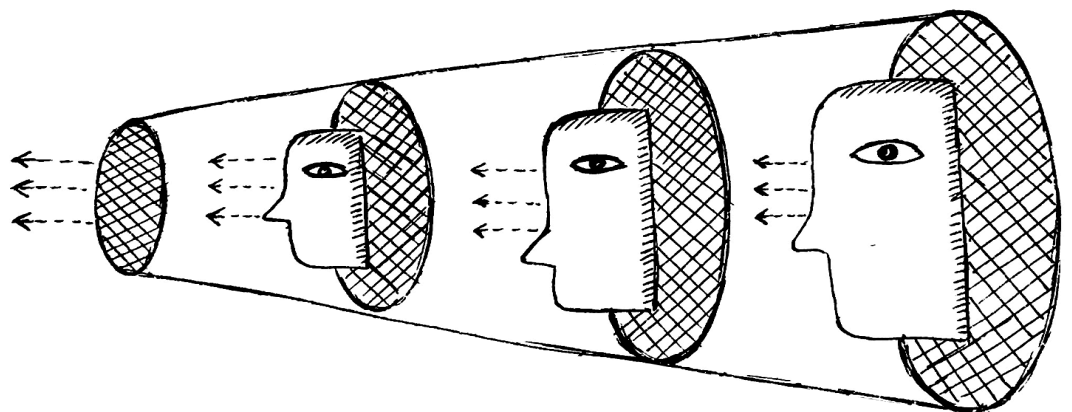
Enforcement Actions

Over the last 12-18 months, the RBI's Enforcement Department fined several bank and non-bank FIs over ₹23 million for breaches of AML/CFT regulatory requirements.

Use of Technology to Combat Financial Crime



On the following pages we have summarised some of the current and emerging key technologies employed in the fight against financial crime. There is a degree of overlap between some of the technologies, while others complement and bolster the effectiveness of each other. Firms can, in some instances, 'supercharge' their financial crime risk management processes by implementing a portfolio of RegTech solutions to reap the most significant benefits.





Machine Learning

Machine learning is a subset of AI which enables continuous improvement of a model, allowing the effective capture of subtleties and dynamism around criminal behaviours which are almost impossible to code effectively under a rules-based approach. Through continued exposure to data points, the machine 'learns' to grasp patterns in data or tasks beyond its pre-defined coding, therefore facilitating more accurate and predictive analytics from large, complex data sets. This is embodied by the capability to adapt quickly to new threats and methodologies. Machine learning is particularly relevant for ML/TF transaction monitoring, due to its ability to 'make judgements' about criminal behaviour, increasing the accuracy of its risk assessments and thus reducing the risk of 'false positive' alerts (falsely alerting teams of suspected improper behaviour).



Artificial Intelligence

AI refers to machines that can mimic human cognition and take on tasks that require relatively complex reasoning and decision making. AI can help to automate business processes, detect patterns in criminal behaviour, generate insights, and engage customers and employees through routine communications. This technology is being used to enhance CDD and enable KYC processes by making them faster and producing more accurate AML data, which allows an organisation to conduct thorough risk assessments.



Natural Language Processing

Natural Language Processing (NLP) is another subset of AI that allows systems to recognise and interpret meaning from human languages. NLP enables machines to process and 'understand' large volumes of unstructured data such as news articles, emails, and social media posts. From an AML/CFT perspective, the machine is able to read and compile information written about an individual or organisation, consider the context of the information, and form 'judgements' as to whether or not the individual or organisation is suspicious. Therefore, NLP can also support Suspicious Activity Report (SAR) and Suspicious Transaction Report (STR) processes through the automatic generation of reports with standardised terminology and language, reducing a firm's administrative burden and ensuring a consistent approach. Furthermore, NLP can provide more robust screening solutions that assists organisations in uncovering politically exposed persons (PEP) and sanctioned persons.



Robotic Process Automation

Robotic Process Automation (RPA) uses logic and structured inputs to automate (previously) manual business processes. RPA software can capture, interpret, and manipulate data, carrying out actions such as moving folders and files, copying and pasting data into different systems, and filling out forms. There are a number of historically manual financial crime risk management processes which could benefit from RPA use, including name screening, transaction monitoring and SAR/STR reporting due to their repeatable, routine, and rules-based nature. RPA is particularly effective when combined with AI capabilities, such as machine learning and NLP, by facilitating the automation of more sophisticated tasks that require more 'complex reasoning'.



Big Data/Data analytics

Big data analytics uses advanced diagnostics to digest large volumes of diverse data from a wide range of sources, including structured and unstructured data sets. The need for big data analytics has become increasingly important, given the sheer volume of information now being generated globally. As part of their analysis, machines can uncover patterns and relationships in consumer behaviour, which could indicate instances of ML or TF.



Cloud Computing

Cloud computing facilitates access to and the consolidation and enrichment of data and processing, enabling FIs greater flexibility of approach and significantly lower operating costs. RegTech solutions are often underpinned by cloud technology. From an AML perspective, cloud computing can facilitate the consolidation of vast amounts of data from disparate sources without compromising accessibility or quality and is particularly helpful for KYC analysis through, for example, identifying the beneficial owner of assets.

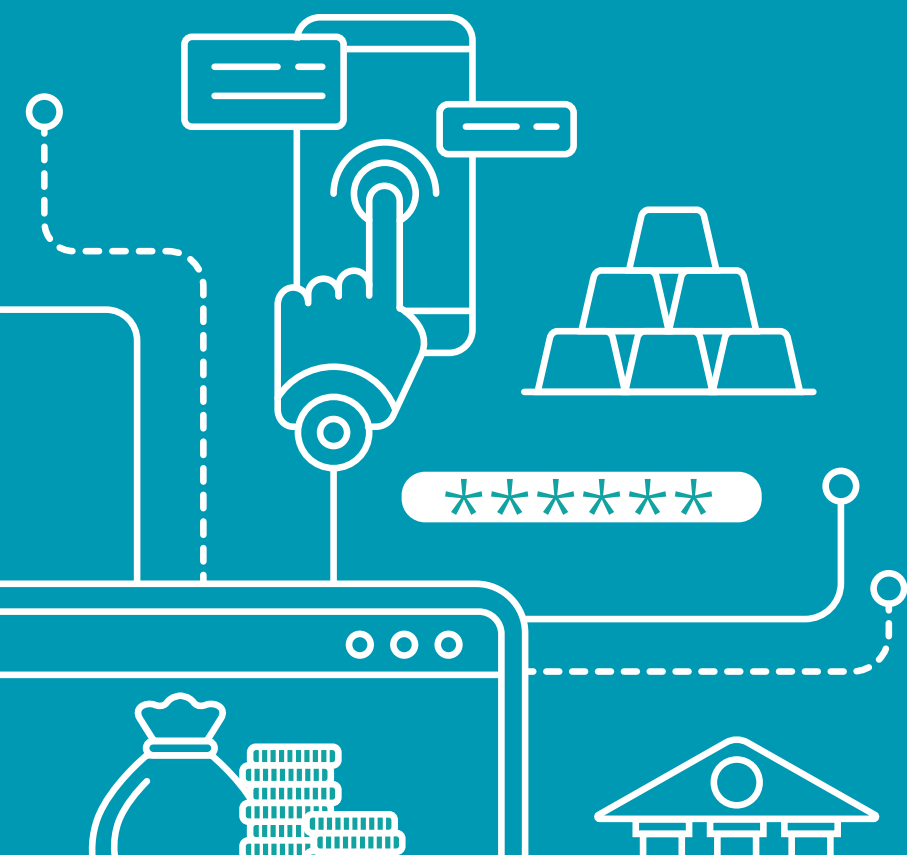


Privacy Enhancing Technologies

Privacy enhancing technology (PET) allows users to analyse data held within a secure environment and produce reports and analysis that do not disclose any sensitive information. While some companies use this technology intra-group to enable information sharing between corporate entities, it also has the potential to significantly enhance the effectiveness of information sharing more broadly. PET can improve information sharing between FIs (private-to-private); FIs and AML/CFT regulators (private-to-public); and supervisory regimes at a national, international and supra-national level (public-to-public), thereby facilitating greater access to information and supporting collaboration on financial crime risk intelligence.

Selected Case Studies of Technology Solutions

In the following section, we present five case studies showcasing how RegTech solutions have been deployed to improve financial crime risk management programs across the region. These case studies are a curated selection from the various initiatives that Deloitte has supported to highlight how technology can add value regardless of an organisation's size, complexity, resourcing and appetite for exploratory solutions.



Case Study A



Case Study A^[3] is a Hong Kong SAR subsidiary of a large international bank, which operates in multiple AP jurisdictions, and offers a broad range of services, including retail products. The bank is an early adopter of technology, and has been at the forefront of the development and application of AML and CFT technology-driven solutions for over a decade. This case study explores the application of an AI-aided machine learning and NLP tool in the bank's name screening process, which is used when performing due diligence for new customer account openings and for periodic checks on existing customers.



The Challenge

Prior to the adoption of its RegTech solution, the bank's name screening process was labour intensive, requiring manual intervention from over 300 analysts. As watchlists and customer volumes continued to increase year-on-year, processes were becoming increasingly overburdened, leading to rising operational costs and a growing risk of errors in the screening process. Under the traditional rules-based name screening systems, high volumes of alerts were being generated (many of which were later deemed to be 'false positives'), making it difficult for overstretched analysts to thoroughly review and clear alerts. This, in turn, increased the risk of overlooking a key data point, or failing to document investigations in a full or appropriate manner.

The bank sought to significantly reduce the amount of human intervention required to clear alerts, whilst maintaining its rigorous control standards. An ambitious target was set to develop a fully automated solution, which would not only assign a probabilistic 'score' to alerts (based on the likelihood of possible criminal behaviour), but also issue well-reasoned, AI-generated recommendations to either escalate or close each case.



The Solution

After securing senior management buy-in, the bank formed a diverse cross-functional team to work on the RegTech solution. The team included subject matter experts (SME) in financial crime, compliance, risk, and technology, as well as representatives from the bank's business and product operations functions. Following careful consideration of available technology and technology providers, the bank decided to partner with a third-party vendor that specialises in machine learning based AML/CFT applications to develop the solution. Data from previous name screening alerts, including the decisions made by analysts in the review process was used to 'train' the machine learning model. This 'training' was repeated a number of times, until the model began to produce promising results, and an internal proof-of-concept could be conducted to validate the solution.

The proof-of-concept was a success, with the AI solving more than 25% of alerts without needing manual intervention, and more impressively, providing adequate 'explanations' on its decision-making process. One year after securing the third-party vendor, the bank was able to move into the production phase, further developing and rebuilding internal systems and controls to support the RegTech solution, and conducting thorough testing across a number of complex markets.



Artificial Intelligence



Machine Learning



Natural Language Processing



Robotic Process Automation

^[3]This case study is also covered in the Hong Kong Monetary Authority paper on "AML/CFT RegTech: Case Studies and Insights", January 2021, written in collaboration with Deloitte.



Speed Bumps

While the bank did not encounter any significant setbacks during the process, there were a number of challenges. Given the scale of the ask, the bank could not find a ready-made solution in the market that met all of its criteria. Therefore, the bank spent a significant amount of time finding the right third-party vendor to co-develop its solution, and also invested a significant amount of time and resource in developing and testing its model.

The lack of 'track record' for the solution coupled with the complexity of legacy systems also resulted in a significant amount of time spent updating internal systems and controls and conducting rigorous testing. In total, the project took around 12 months from partnering with the third-party vendor, to roll-out of the production phase.



Strategic Impact

Despite the lengthy implementation process, the bank's thorough approach and rigorous testing helped build confidence with internal stakeholders across the bank, as well as external stakeholders, including regulators.

The key benefit of the bank's machine learning-powered name screening solution was a significant increase in the efficiency of the investigation process, reducing the number of alerts that required human intervention by an average of 35% (and as much as 50% in some jurisdictions). This in turn streamlined the review process, increasing the amount of time analysts could dedicate to reviewing flagged alerts.

Case Study B



Case study B is a Singapore-based bank with a large presence in Asia offering a broad range of services covering banking, investments, and asset management. The bank is a strong advocate of technology, as demonstrated by its efforts to foster, accelerate, and promote promising FinTech start-ups across the region. This case study focuses on upgrading the bank's transaction monitoring and name screening alert processes, utilising technologies including RPA, and AI-aided machine learning and NLP within the bank's end-to-end 'Anti-Money Laundering Suite' (AMLS) integrated solution. From its inception to the 'business live' phase, the project took almost three years to complete.



The Challenge

The bank has in place rules-based AML and CFT legacy systems for name screening and transaction monitoring. As is the case with all rule-based systems, given the volume and velocity of transactions that flow through the bank, a large number of 'false positives' were being generated despite optimisation efforts.

An ambitious goal was set to improve efficiency and effectiveness by being innovative and forward looking. This also presented opportunities to simplify the relevant AML processes, and focus on material and meaningful risks through the use of AI, machine learning and RPA.



The Solution

Following a strategic review of possible options, the bank decided to partner with a Singapore-based specialist RegTech company to develop an AI-driven, single integrated platform to host AML technologies, tools, and systems. The bank and the technology vendor co-created a bespoke RPA machine learning solution to supplement and enhance the bank's existing systems. A RegTech model risk management and governance framework was also developed to underpin risk management of the technology, ensure its responsible use, and to validate the developed models.

The bank's compliance team worked closely with its data management office and FinTech data scientists from the technology vendor to design, develop, analyse and deploy modules for the four key processes in the bank's AML framework (KYC, transaction monitoring, name screening, and payments screening). The result was the AMLS integrated solution, prioritising transaction monitoring and name screening – an end-to-end-system that combines supervised and unsupervised machine learning techniques to facilitate the detection of suspicious activities and high-risk clients faster, and more accurately.

For its transaction monitoring module, the bank focused on optimising the detection of new, unknown suspicious patterns, while the name screening process module was designed to handle a wider range of complex name permutations, and to reduce the number of undetermined hits through enriched 'inference' features and the inclusion of additional customer profile identifiers. The new specifications, coupled with advanced machine learning technology, significantly improved the accuracy of flagged alerts.

The bank also utilised RPA and NLP to facilitate the automatic generation of SAR reports. For every alert, RPA extracted customer profile information and transaction data from various systems which was then enriched with additional NLP-generated data points and a visual representation of the customer's flow of funds.



Artificial Intelligence



Machine Learning



Natural Language Processing



Big Data/Data Analytics



Robotic Process Automation



Cloud Computing

In 2018, the bank undertook a proof-of-concept to validate the solution. The results achieved were a significant step forward, with a 5% increase in true positives, and a 40% drop in ‘false positives’ for transaction monitoring, a 60% reduction for individuals, and a 50% reduction for corporates in the name screening process.

Following the success of the pilot, in 2019, the bank was able to move into the ‘technical live’ phase, where the model was deployed alongside business as usual (BAU) functions. During the technical live phase, the bank continued to test and develop the model, resulting in an increased reduction in false positives to 50% (up from 40%) for transaction monitoring, 70% (up from 60%) for individuals, and 60% (up from 50%) for corporates in the name screening process.

Finally, following rigorous testing, validation and the establishment of a robust governance framework and low value alert management framework, the solution went ‘business live’ in October 2020.



Speed Bumps

Given the size, scope and ambition of its vision and the bank’s commitment to developing a high quality, durable and scalable product, a significant amount of time (close to three years) and resources were dedicated to developing, testing and validating the tool at every stage of its development.

During the proof-of-concept phase, rigorous internal validation was performed by the bank’s data management office. This was further verified by an independent assessment of the pilot program and its approach to confirm that it was ‘fit-for-purpose’. The assessment included a detailed comparison with the pre-existing rules-based monitoring process, and stress testing the machine learning model and AMLS solution to ensure that they were capable of dealing with a variety of AML compliance typologies.

This stringent validation was then repeated in the ‘technical live’ phase of the project, with additional independent assessment and model validation undertaken prior to going ‘business live’.

The bank also invested a significant amount of time developing a RegTech-specific AI and machine learning model management framework to guide key aspects of the governance and model architecture, which in turn ensured the model’s veracity and stability.



Strategic Impact

The bank was able to manage transaction monitoring and name screening alerts more effectively and efficiently, following the implementation of the AI machine-learning models. After the ‘business live’ phase, the name screening models continued to perform within the predictive boundaries established during the ‘technical live’ phase, producing significantly fewer ‘false positive’ results. Additional benefits included:

- Significant decrease in error rates due to automation of previously manual inputs;
- Reduction in analyst man-hours required for inputs, reviewing alerts and producing reports which could be reallocated to higher value work;
- Improved compliance and increased auditability; and
- Standardisation of transaction monitoring processes across the bank.

The bank intends to continue optimising its AMLS machine learning algorithms by adding new transactional data into the database, with the aim of implementing the solution across its entire AML framework in the future.

Case Study C



Case Study C is a large lender in Vietnam. The bank's current AML, fraud detection, and transaction monitoring processes are run using a rules-based approach, with differing levels of integration into systems across business lines. Moreover, the rules themselves bear the risk of higher error rates, as they are manually derived based on SME knowledge. Hence, a more holistic and integrated solution is planned, which focuses on improvement of rules-based monitoring and the incorporation of machine learning models and scenario analysis. The initiative is currently ongoing at the time of publication.



The Challenge

At present, there are multiple challenges within the bank's AML and fraud detection control frameworks, and a number of areas for improvement within the control environment were identified. For example, manual controls or controls which are not embedded into a systemic solution (i.e. end-to-end view) can be bypassed by employees. Further, a lack of data and in-depth models has led to 'false positive' results.



The Solution

The project has been divided into two phases. The first phase is currently under way, with a gap analysis being conducted to compare the bank's current capabilities with international standards and practices for AML and fraud risk, such as those set out in the Committee of Sponsoring Organisations of the Treadway Commission's (COSO's) fraud risk management guidelines,³² and the Australian Fraud and Corruption Control Standards AS 8001-2008.³³ Based on the results of the gap analysis, an action plan will be developed, which will be implemented in the second phase of the project.

Following a preliminary assessment, the bank is currently considering using machine learning and scenario analysis to support its rules-based analysis, as well as updating its AML and fraud detection platforms. The new platforms will offer advanced technology which can provide a holistic view of all transactions and activities pertaining to fraud risk detection (in both real-time and batch), and is customisable to the bank's needs. The use of machine learning models designed with precise and tested parameters will provide a more robust statistical basis to tackle the risk of high error rates.



Machine Learning



Speed Bumps

Presently, the bank is assertive, innovative and eager to apply the new technology. No significant speed bumps have been observed to date; however, the initiative is still ongoing.

The timeframe for the project and expected resource requirements will largely depend on the outcome of the gap analysis currently under way. However, some headwinds are expected when liaising with various system providers in order to achieve a solution most compatible with the bank's requirements. The undertaking is likely to impact various parts of the bank and involve numerous stakeholders, both internal and external. Hence, the bank is preparing for a multi-disciplinary approach to governance and execution to enable the initiative's success.



Strategic Impact

The technology is intended to be implemented as an enhancement to existing methodologies. The implemented solution is expected to provide the benefits of increased accuracy, reduced costs for staff and efficiency in fraud detection. The end-to-end solution should also ensure a comprehensive view of financial activity and customer risk to inform decision making, as well as transparency in detecting and investigating potential ML behaviour.

Case Study D



Case Study D is a global, top tier bank based in China, with almost 20 business units across 37 top-level branches (i.e. branches in key cities). This case study showcases the possibilities of adapting and combining existing technologies including modelling, data analytics and visualisation to develop an Enterprise Wide Risk Assessment (EWRA) for ML and TF risk. The bank used a combination of visualisation technologies at the front-end, and a server at the back-end to support its EWRA solution.



The Challenge

The RegTech project was driven by a specific regulatory expectation set by the PBOC AML Bureau. The PBOC required FIs to perform ML and TF EWRAs or IRAs (depending on the size of the institution) covering all branches and subsidiaries, clients, products and services. All ML and TF risk factors must be considered, and the firm's decision-making process and governance framework, as well as underpinning methodologies, must be clearly documented. The PBOC also set out its expectation for firms to continue to improve their EWRA/IRA processes over time.

After performing a thorough assessment, a number of gaps were identified in the pre-existing data and processes. While the bank already had processes in place to detect ML and TF risks, it was unclear how to implement EWRAs/IRAs, including what data should be fed into the new system to run the models properly, and how to demonstrate a scientific and reasonable calculation algorithm in order to gain the regulator's approval. Furthermore, the bank needed to not only improve the quantity and quality of existing data to enhance its capabilities to accurately tag customers and transactions, but also develop the capacity to locate outliers and residual ML and TF risks across the organisation. Additionally, in order to fully meet the PBOC's expectations, the bank also wanted the EWRA solution to support continuous improvement of its methodology and processes.



The Solution

A bespoke system was developed over a period of 1.5 years to enable the bank to carry out EWRAs. The overall solution is composed of a number of analytics tools at the front-end to provide visualisation of both individual components and a consolidated view, and a server at the back-end to support data warehousing and processing. The solution is underpinned by a methodology that comprises risk indicators and analytics based on several factors, including customer sector, geography, product, channel, calculation logic for inherent risk, controls effectiveness, and residual risk.

The new system has been designed to facilitate refinement of the methodology on an ongoing basis by continually 'feeding' the EWRA engine. This is made possible through the use of an index technology that tracks the iterative data extraction process of hundreds of evaluation units, while keeping change records and making use of horizontal and vertical verifications of data to gradually improve data accuracy. Moreover, the availability and update of data in near real-time enables rapid management assessment and response.

The solution has enabled the bank to understand and hence manage ML and TF risks more efficiently and effectively across the organisation. Furthermore, the system provides users with a complete and accurate audit trail of analysis and the decision-making process.



Speed Bumps

The scale of the project resulted in the involvement of more than 1,000 participants and took over 1.5 years to complete. Due to the complexity of the comprehensive model and back-end logic to the engine, a significant amount of time and effort was dedicated to ensuring that the bank's personnel understood the nuances of the model, and that appropriate parameters and data inputs were selected. This issue was proactively detected and remediated throughout the project through ongoing training and awareness programs across the bank in line with PBOC's expectations.



Strategic Impact

The solution has been in place since 2019, and has significantly improved the efficiency and effectiveness of the bank's ML and TF assessments, as well as ensuring the most appropriate allocation of financial resources. The bank now has the ability to run EWRAs in over 600 evaluation units (business units of top-level branches). Further, over 20,000 inherent risk data points and over 20,000 control self-assessment scores have been collected as of March 2020. Given the success of the rollout, the bank is planning to extend implementation of its EWRA solution to its local subsidiaries, as well as its overseas subsidiaries and branches.

The regulator expressed great interest in the project, and was kept informed throughout the development and implementation phases, providing input where relevant. As a result, only minimal updates were required to the bank's methodology and systems to reflect the final regulatory guidance on EWRAs/IRAs issued on January 15, 2021.

Case Study E



Case Study E^[4] is a Hong Kong SAR subsidiary of a large foreign bank which offers a number of services including asset management, wealth management, and investment banking. This case study explores a large-scale two-year project to upgrade the bank's financial crime data infrastructure using cloud computing, data analytics, and data storage capabilities. In total, the bank has been adopting RegTech solutions for over five years and continues to do so in order to modernise and standardise its technology infrastructure.



The Challenge

The bank's data infrastructure was largely disparate and siloed. AML and CFT processes such as adverse media searching, transaction monitoring and name screening were dependent on customer information, transaction, and trade level data sourced from numerous systems. This led to significant operational inefficiencies, consolidation and data quality issues, and increasingly high costs as customer and transaction volumes grew, alongside increased expectations around financial crime investigations and reporting. Furthermore, the bank was receiving a growing number of ad-hoc and standalone requests for data, which required significant manual processing. For example, it often took two weeks or longer for a dedicated ad-hoc reporting team to produce reports for the Hong Kong SAR Financial Intelligence Unit (FIU).

Therefore, the bank set out to consolidate, standardise and enhance the way that AML and CFT related data was captured and stored. The bank also wanted to improve data extraction efficiency, by enabling analysts to directly access the data in order to streamline the production of ad-hoc reports. Further, the bank aimed to use the consolidated data set to develop the capability to proactively investigate suspicious client groups.



The Solution

The bank decided to fully upgrade its data infrastructure by focusing on data aggregation, data completeness, and data access. The solution involved the creation of a single intermediate data repository source. The data repository not only aggregated over eight billion data points and fed them directly into the bank's AML/CFT control systems, but also provide end users direct, near real-time access to the data. This was no small task and in total, the project took two years to complete.

However, the RegTech solution allowed AML/CFT and FIU analytics teams to efficiently produce both ongoing and ad-hoc reports. Further, it enabled AML/CFT specialists to directly extract data from the repository and perform proactive data analytics reviews, referred to as 'look across' exercises. In such exercises, AML/CFT specialists analyse the data using risk patterns identified by FIU investigations to see whether there are any similar patterns that could indicate possible criminal activities across other client groups.



Big Data/Data Analytics



Cloud Computing

^[4]This case study is also covered in the Hong Kong Monetary Authority paper on "AML/CFT RegTech: Case Studies and Insights", January 2021, written in collaboration with Deloitte.



Speed Bumps

The bank's biggest challenge was locating and aggregating data from several systems into its aggregated data repository. In fact, data sourcing, cleansing and consolidation was the largest driver of the two-year development timeframe.



Strategic Impact

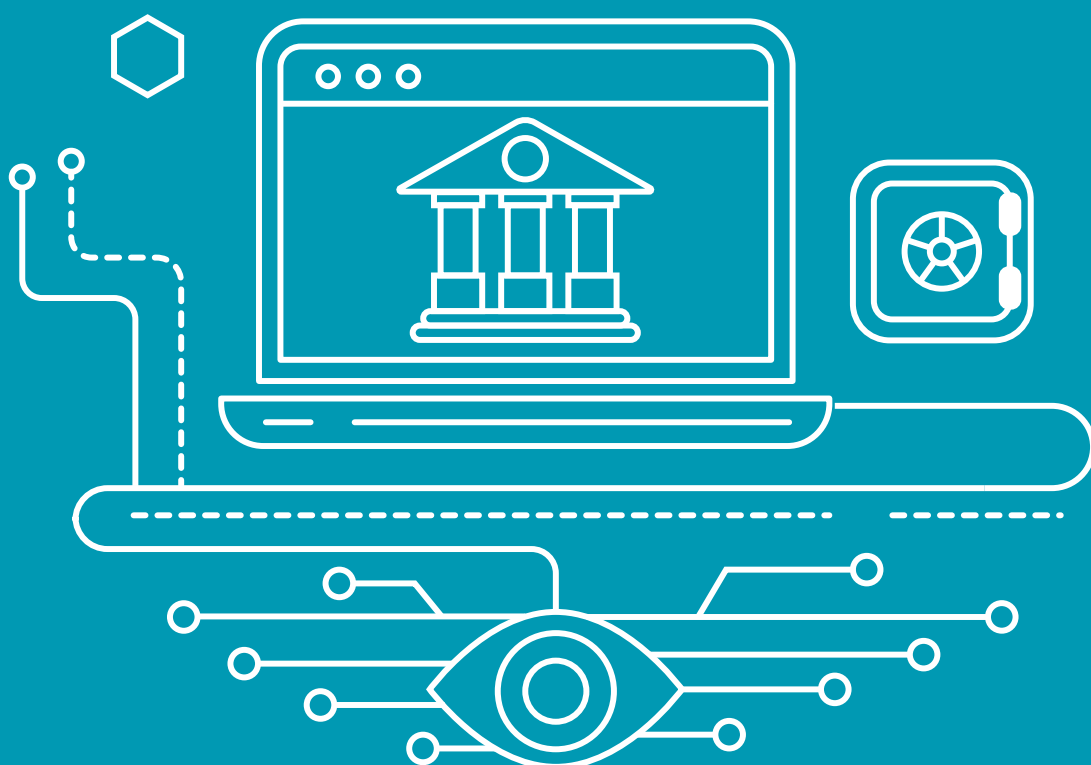
The creation of a single aggregated data repository with near real-time access to data vastly increased the efficiency of data reporting, reducing the amount of time it took to produce certain ad-hoc reports from a few weeks, to a few days.

Additionally, it allowed analysts to perform proactive and detailed analysis of the data to identify potential criminal activities across different client groups. For example, after the repository went live, the bank undertook three 'look across' exercises, and within 18 months of the go-live date, 10 detailed reviews of customer and transaction data had been conducted. The results of these assessments led to a number of escalations to the FIU and STR filings to law enforcement.

The bank's highly aggregated data storage has also provided a solid foundation on which the bank can develop more advanced AI-driven technologies. For example, the bank is currently developing a machine learning driven media and name screening application, as well as a network analytics tool, which it hopes will facilitate the assessment of undisclosed or less obvious relationships between client entities, therefore enhancing FIU investigations.

Key Takeaways from our Case Studies

There are a number of key takeaways from the selected case studies and from our combined experience supporting FIs on their RegTech journeys throughout the AP region.



Assess data quality and readiness

Data can often be a significant - or even the most significant - roadblock when developing and implementing RegTech tools. Organisations should not underestimate the amount of time and effort required to identify, source, process, transform, and interpret data. FIs are often plagued with issues around data quality, and concerns around the completeness and validity of data are often major hurdles in RegTech adoption. Moreover, RegTech solutions sometimes demand data that is not readily available and will therefore require time-intensive and costly remediation

work. Organisations must take the time to fully understand the data requirements and potential data impediments of any RegTech solution before they begin working on implementation. The saying 'garbage in, garbage out' is extremely apt, and firms must ensure that the data is complete, relevant, sufficiently diverse and any biases in the data have been fully addressed. Nevertheless, perfection in data is not what FIs should be striving for - instead, management should look to understand and recognise limitations as part of starting their RegTech transformation journey.

Know your systems

Operating systems and data quality issues go hand-in-hand for many organisations. Indeed, untangling the web of legacy systems and processes is, in particular, a challenge for large FIs with a legacy of acquisitions. However, all institutions will need to consider how their systems currently operate and the impact this will have on the application of RegTech. Organisations will have to decide whether to replace, integrate, or work around

pre-existing systems when designing their RegTech solutions. This decision will depend on the scale of the project, and the firm's vision on short, medium and long-term goals. Investing in changes to technology infrastructure or systems could potentially lead to pervasive benefits for the organisation, but will also involve significant upfront costs, resource, and time commitments.

Ensure compliance through design

Acknowledging market fragmentation and divergence between regulatory requirements around data sharing, localisation, processing, and privacy will need to be a core tenet of any program. Larger initiatives that cut across multiple jurisdictions will face related challenges earlier than specialised, specific deployments. Firms will need to consider their long-term aspirations in order to set themselves up for success when scaling

and/or expanding, and organisations will have to thread the needle to keep sufficient flexibility and agility, whilst navigating the web of applicable regulatory requirements. For instance, management should consider regular assurance and reviews of outcomes to ensure any unintended consequences are identified and actioned.

Form a robust governance framework

It is paramount that firms set clear roles and responsibilities for managing RegTech solutions and associated risks from inception, all the way through to implementation, as well as post implementation review. Appropriate governance and sponsorship of the initiative is critical to success, as the solution is likely to interface with numerous stakeholders and existing processes, systems and data. Tight management will ensure that the organisation understands its solution

and the 'explainability' of underlying models, which in turn, is critical when engaging with stakeholders such as the Board or regulators. Lastly, model outcomes should be continuously monitored to ensure they are still operating within the required parameters and remain fit for purpose. All changes to models should also be documented, stored, and recoverable for audit purposes.

Ensure stakeholder buy-in

Securing senior management buy-in early on and throughout the design, testing and implementation of any AML/CFT RegTech solution is crucial for building credibility, preventing a siloed approach, and ensuring that expectations are aligned with the project approach and expected outcomes.

This is likely to be more of a challenge for FIs at the beginning of their technology journeys than for early adopters of RegTech. It is vital to cultivate relationships with business sponsors, and to arm them with sufficient knowledge of the organisation's AML/CFT processes and controls, and the potential benefits of RegTech adoption. This will allow sponsors to act as advocates of technology when discussing its

application to AML/CFT with senior executives within the organisation.

There is also a need to ensure external stakeholders and in particular, regulators understand and support the use of RegTech solutions. Working collaboratively with regulators can also reap extra benefits, as they may be able to pass on invaluable insights based on their conversations with other institutions and/or regulatory bodies.

Bringing all this together, it is integral to have a clear vision, yet remain flexible and agile as the technology landscape continues to evolve.

Establish diverse cross-functional, cross-regional teams

When embarking on RegTech implementation, it is also important to form diverse cross-functional and cross-regional teams which includes SMEs in financial crime, compliance, risk, technology and data scientists, as well as representatives from the bank's business lines and operational functions. Diversity will enhance the effectiveness of project scoping in terms of timeframe and costs, facilitate the identification and remediation of potential hurdles, support the comprehensive evaluation of third-party providers, and secure buy-

in for the project. A diverse team will also be better positioned to identify intersectional opportunities to deploy technology more broadly in other areas of the organisation.

In particular, large global firms can benefit from setting up platforms in which AML/CFT RegTech adoption ideas, knowledge, and experience can be shared across businesses and regions.

Thoroughly scrutinise third-party vendors

Securing the right third-party vendor can bring a wealth of experience and technical expertise when developing a RegTech solution, but it is not without risk. Firms will need to carefully consider the long-term viability of the vendor, especially if their continued support on the maintenance of or updates to the solution is required. Firms should also consider the size and scale of the vendor's operations and its product offerings, specifically whether they are compatible with the organisation, its systems and structure, and

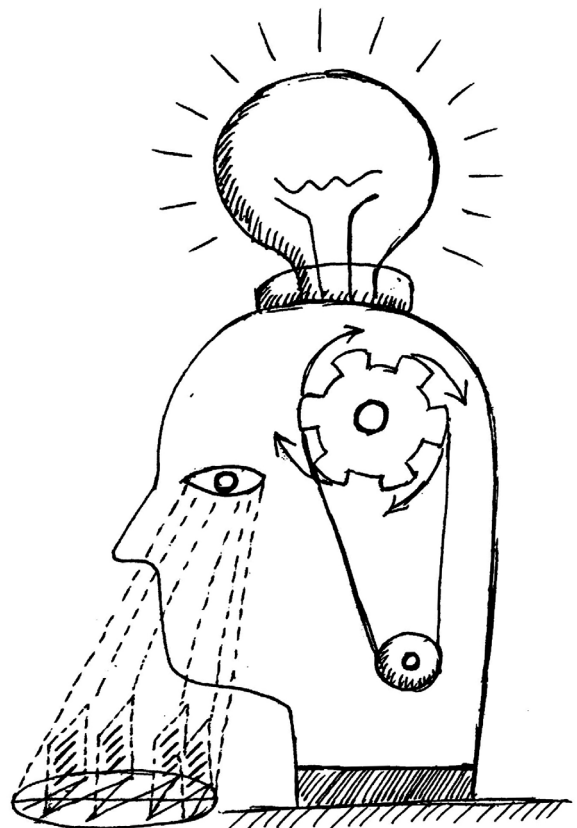
the size and scale of the project both presently and aspirationally.

Firms will also need to carefully consider any implications relating to intellectual property ownership before on-boarding or co-developing solutions with third-party vendors, as well as ensure that, where required, vendors manage data in accordance with the applicable regulatory requirements across various jurisdictions.

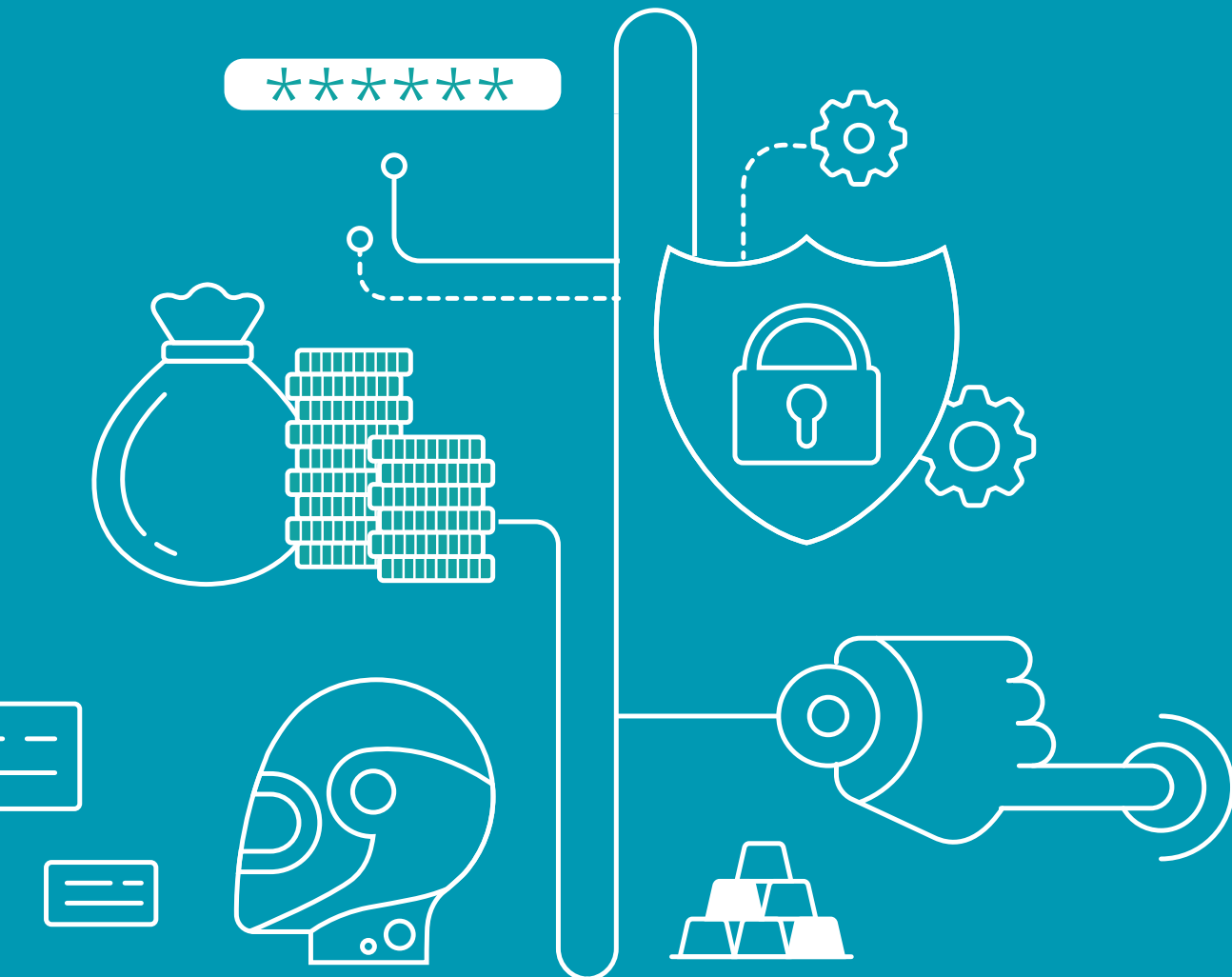
Arm the organisation with knowledge

Once a RegTech solution has been developed, it is vital that there is sufficient knowledge within the organisation to enable its effective use and further development. Good quality documentation to explain the technology, its functionality, business requirements, outcome, risk mitigation approaches,

testing and assurance, and disaster recovery is a necessity. Firms should also ensure that staff receive suitable training on how to best utilise the new solution, whilst management should understand the solution in order to provide effective review and challenge.



Managing Technology Through the Customer Lifecycle



Using Technologies Across the Customer Lifecycle

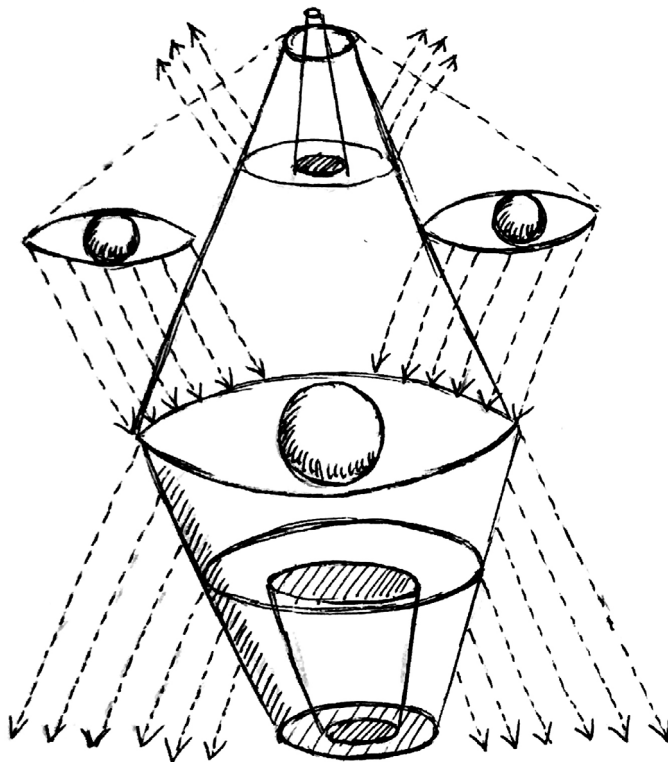
Key opportunities for innovation and the use of technology and analytics to curb financial crime at every step

A new approach

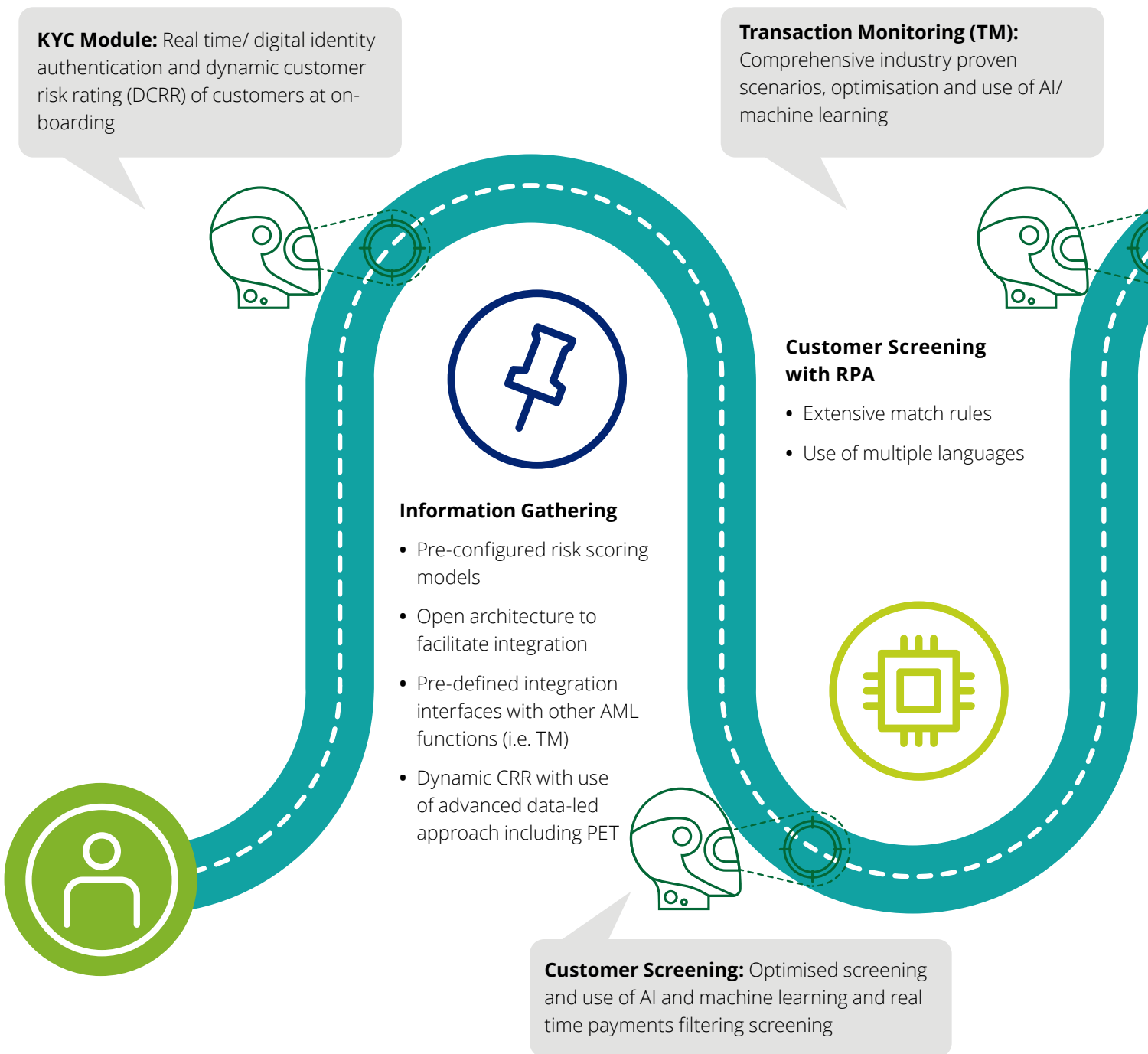
In order to fight financial crime in the most effective and efficient manner, financial institutions should embrace the use of technology throughout the customer lifecycle.

While no two financial institutions will adopt technologies in the same way due to differing business models, infrastructure and budgets, certain RegTech solutions have a proven track record at being particularly effective when combined (such as AI and RPA), and for targeting specific aspects of the customer lifecycle.

Technology such as cloud computing and big data/ data analytics can be used to form a solid foundation upon which data can be aggregated, consolidated and enriched to support every aspect of the customer lifecycle. Further, emerging technologies such as privacy enhancing technologies have the potential to significantly increase a firm's access to data.

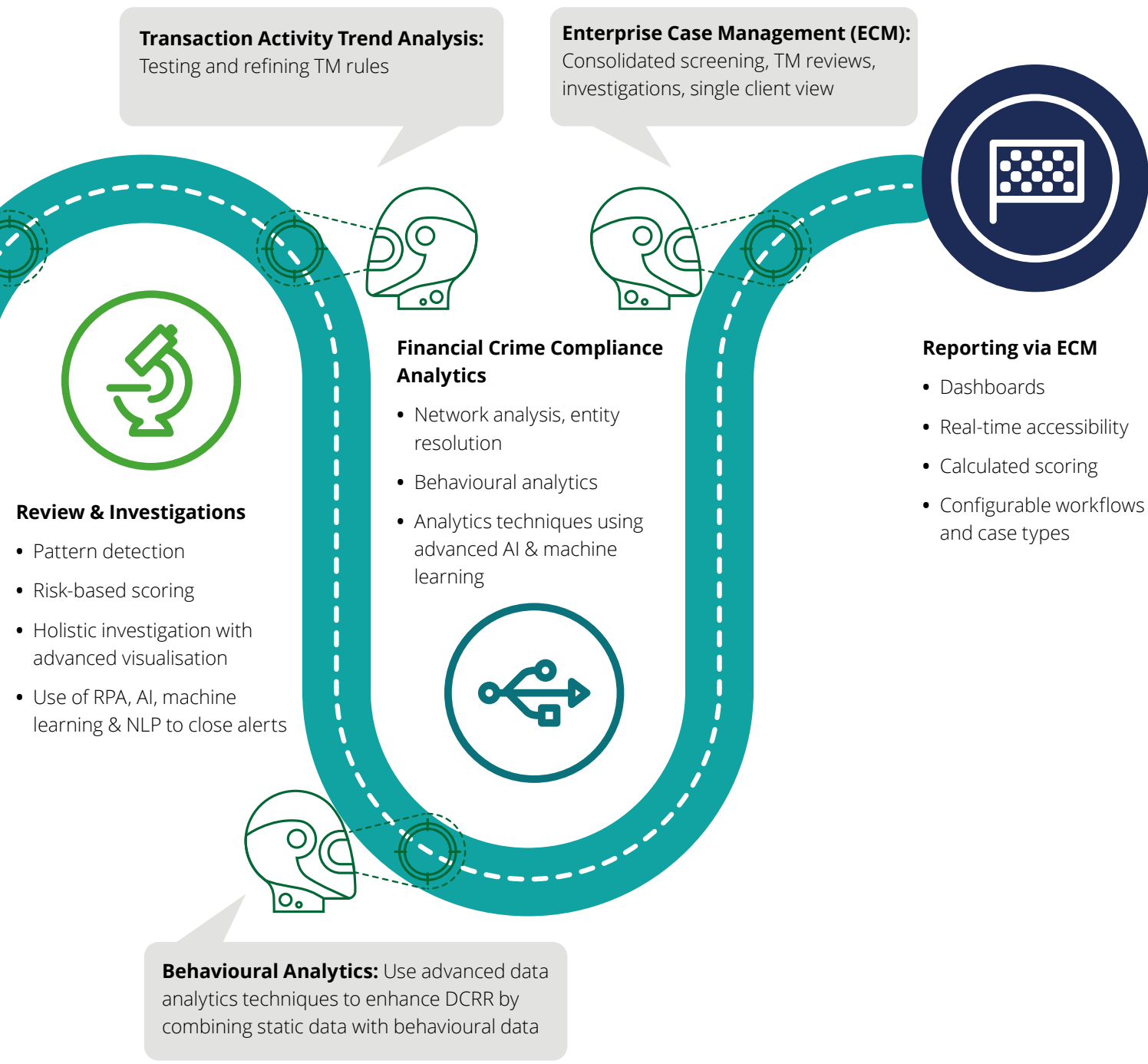


A holistic view is important



An aggregated data repository/integrated solution forms the















to manage customer risk

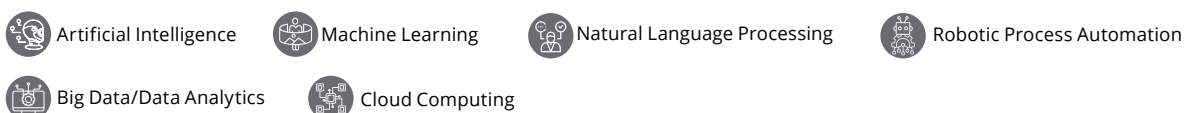


foundation for all aspects of financial crime risk management

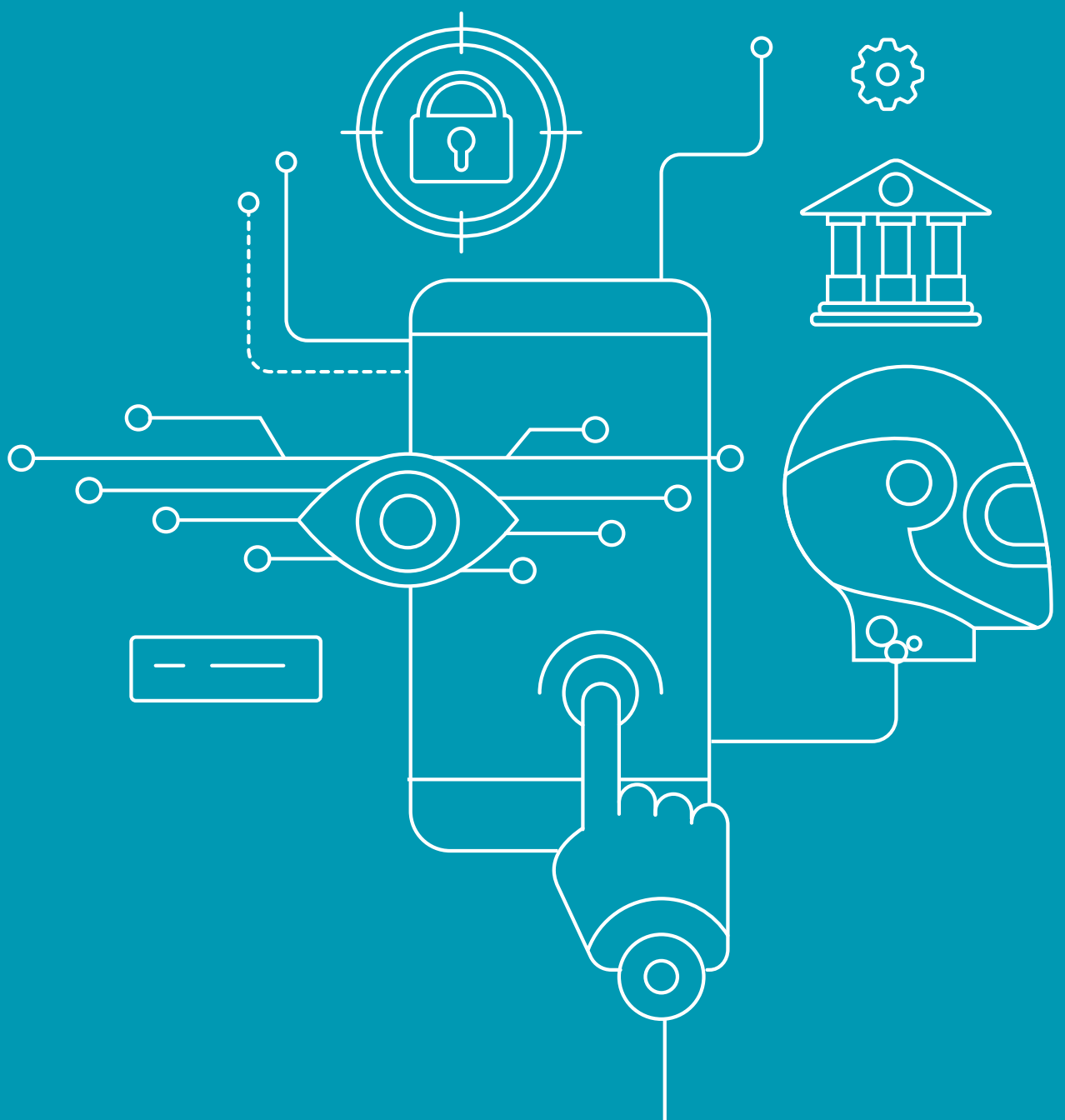
Deployment of Technology Solutions

Below is a summary of our case studies showcasing how technology solutions have been deployed to improve financial crime risk management programs

Case Study	Overview	Key Benefits	Type(s) of Technology Employed
A	Enhancements to the bank's name screening process due diligence	35% reduction in alerts requiring human intervention	   
B	Upgrade of the bank's transaction monitoring and name screening alert processes, and development of an end-to-end 'Anti-Money Laundering Suite'	50% reduction in 'false positive' alerts for transaction monitoring, and 70%/60% reduction in 'false positive' alerts for individuals/corporates in the name screening process	     
C	Transformation of fraud detection, and transaction monitoring processes	Increased accuracy, reduced costs for staff and efficiency in fraud detection	
D	Development of an Enterprise-Wide Risk Assessment	Collection of over 20,000 inherent risk data points and 20,000 control self-assessment scores	
E	Upgrade of the bank's financial crime data infrastructure	Creation of a single aggregated data repository with near real-time access to data. Significant reduction in time spent producing ad-hoc reports	 



Looking to the Future



01 **Global Partnerships and Cross-Organisational Collaboration**

ML and TF is a global business being run by increasingly sophisticated and technology savvy criminals. Therefore, it is vital that organisations work collaboratively to enhance visibility and ensure a coordinated strategy on data and technology sharing, while carefully managing the risks, regulations and rules around data privacy. There are promising advances in technology which may help to facilitate this goal, such as through the development and improvement of PETs, which allow users to analyse data from within a secure environment and extract data without disclosing sensitive information. Cross-organisational and cross-regional knowledge exchange events, forums and committees also help to support information sharing on data, and the tools and techniques needed to successfully implement RegTech solutions. Sharing can arm the industry with better expertise and intelligence, as well as increased effectiveness and efficiencies in the fight against financial crime. Here, regulators and international bodies have a role to play as facilitators and enablers of information sharing.

02 **Proactive Financial Crime Prevention in the New Digital Era**

The growth of digital platforms and digital banks (which found tailwinds in 2020/2021) brought a wealth of benefits for customers; however, it also enabled criminals to exploit the anonymity and lightning fast transaction speed of technologies such as cryptocurrencies, online banking and electronic payments. Often, by the time a suspicious transaction

has been identified, the illicit funds have already been transferred across borders and cannot be recovered. However, proactive prevention is becoming increasingly viable through the use of advanced AI predictive analytics techniques. For example, scenario analysis and threat modelling can enable firms to assess weaknesses in their AML/CFT processes and systems, and pre-emptively address high risk areas. Intertwining with this, technology can also be used in behavioural analysis to help predict future criminal activity, allowing FIs to stay one step ahead of the criminals.

03 **Focus on the Customer Lifecycle**

As FIs become more mature in their adoption of technology, they should start to view and manage AML and CFT risk holistically across the entire customer lifecycle. Firms can then consider how best to employ technology at every step of the process – from onboarding, to data collection and verification, client data management, transaction monitoring, investigations, and reporting. By focusing on the customer lifecycle, not only can firms close potential vulnerabilities for criminal activity, but they can also ensure a seamless customer experience.

Privacy Enhancing Technologies

Helping FS firms fight financial crime, whilst protecting customer information

Balancing the need to protect personal customer information with the need to access meaningful data has been a major hurdle in financial crime compliance and management. However, emerging PET can help FIs meet these needs by supporting the analysis of large swathes of data, whilst maintaining security and encryption over personal identifiable information. For example, a leading provider of PETs has recently partnered with a prominent technology provider to FIs to integrate its PET offerings with the technology provider’s existing Financial Crime and Compliance Management product suite available to the Australian market.

The partnership supplies participating FIs with the PET tools to securely collaborate on sensitive data insights (such as transaction data) whilst meeting their global privacy and secrecy regulations. Users of this PET suite will be able to securely share insights (across institutional and country boundaries), while maintaining privacy and the sensitivity of the underlying customer’s personally identifiable information. Further, this ability to easily share encrypted and de-identified customer data will also help to enable open banking and other financial crime management purposes such as CDD, behaviour monitoring, and collaborative financial crime investigations, without compromising risk and regulatory compliance management. For example, the encrypted querying process provides answers in seconds, helping FIs effectively weed out ‘false positives’ and expose financial crime.

Other Applications of Privacy Enhancing Technologies

KYC	Transaction Monitoring	Investigations
Participating FIs can collaborate on potential persons or entities that they are considering onboarding. As a result, FIs have a greater understanding of their customer and robust identity verification without intrusion. In turn, customers have a better experience as they are onboarded swiftly.	Collaboration between FIs means that FIs can access a wider range of customer related information, such as the source of funds, related accounts and transaction history. More relevant and current data would significantly reduce the rate of ‘false positives’ in transaction monitoring and improve customer insights.	Broad information sharing streamlines the gathering of data and evidence for suspicious matter reports. This enables quick validation of ‘false positives’ and can help overcome dead ends in investigations. Further, it empowers institutions to write more robust and comprehensive report narratives, without compromising on the privacy of subjects under investigation. Cross-institutional collaboration mitigates risk by allowing FIs to see blind spots in their financial crime and compliance processes. Greater collaboration, information sharing, and visibility can create a safe financial crime compliance environment.

Conclusion

While there are significant differences in technological capabilities employed in the fight against financial crime across FIs, as demonstrated by our case studies, all firms can benefit from increased efficiency and effectiveness in identifying and mitigating financial crime risks through the adoption of RegTech solutions. Moreover, the benefits of RegTech can be bolstered by embracing their use holistically across the entire customer lifecycle.

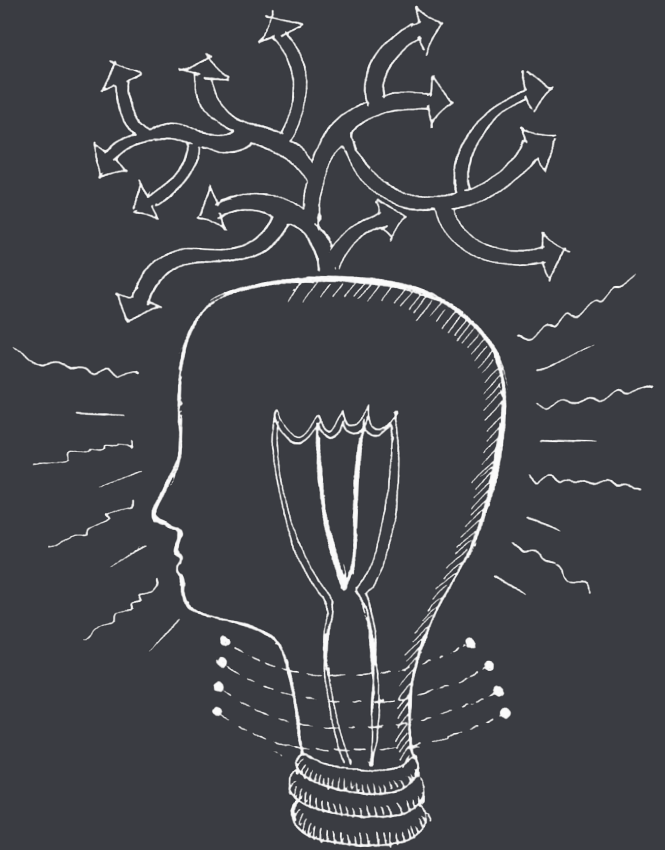
In order to gain the biggest return on their investment, firms will need to ensure that their RegTech solutions are designed with consideration to data quality and access, systems, processes and organisational structure, and available technologies and technology providers. Establishing diverse cross-functional and cross-regional teams, and ensuring stakeholder buy-in will also be paramount to ensuring a successful outcome. Robust governance frameworks, the establishment of ongoing training on financial crime risk management, and ongoing development of RegTech solutions will also ensure their continued success.

For FIs to remain resilient and reduce the risk of financial and reputational damage resulting from regulatory enforcement actions, it is important to employ new approaches to tackle the evolving challenges around financial crime (e.g. digitisation of FSI, increasingly tech-savvy criminals etc.)

Pulling all this together, senior management and Boards would benefit from reflecting on a few questions to better understand their own appetite for RegTech, in conjunction with available opportunities and strategic objectives, both current and aspirational.

- What is the supervisory comfort level with the use of technology for risk management and regulatory compliance?
- What are the supervisory priorities, especially with respect to recent updates to mandates and inspections/reviews?
- What is the existing relationship with the regulator? Does the regulator have confidence in the organisation's financial crime management capabilities?
- What is the organisation's technology landscape and architecture? And how is it envisioned to change over the next few years?
- What is the firm's financial crime risk exposure and profile? How does it compare to that of the wider industry? Are there relevant technology solutions available in the market?
- What is the effectiveness of the financial crime risk management program? Are there identifiable enhancement and development areas within the financial crime risk management program?

These, among other questions, can help organisations assess how best to implement RegTech solutions. Moreover, as the technology landscape evolves, and firms start to move away from single platform solutions to a more agile, multi-solution approach targeting specific technologies/approaches to specific risk types, value can emerge in creating a portfolio of RegTech solutions to support existing financial crime risk management programs.



Glossary

ECM	Enterprise Case Management
ACCESS	Association of Cryptocurrency Enterprises and Start-Ups Singapore
AI	Artificial Intelligence
AML	Anti-Money Laundering
AMLS	Anti-Money Laundering Suite
AP	Asia Pacific
APG	Asia Pacific Group on Money Laundering
APRA	Australian Prudential Regulation Authority
AU	Australia
AUSTRAC	Australia Transaction Reports and Analysis Centre
BAU	Business as Usual
BEAR	Banking Executive Accountability Regime
CDD	Customer Due Diligence
CFT	Countering Financing of Terrorism/ Combating Financing of Terrorism
CN	Mainland China
CTF	Counter-Terrorist Financing
COSCO	Committee of Sponsoring Organizations of the Treadway Commission
COVID-19	Coronavirus Disease 2019
DIA	Department of Internal Affairs
EWRA	Enterprise Wide Risk Assessment
FAR	Financial Accountability Regime
FATF	Financial Action Task Force
FI	Financial Institution
FIU	Financial Intelligence Unit
FMA	Financial Markets Authority
FSC	Financial Supervisory Committee
FSI	Financial Services Industry
HK SAR	Hong Kong Special Administrative Region

HKMA	Hong Kong Monetary Authority
IRA	Institutional Risk Assessment
IT	Information Technology
JFSA	Japan Financial Services Agency
JVCEA	Japan Virtual and Crypto Assets Exchange Association
KYC	Know Your Customer
MAS	Monetary Authority of Singapore
MD	Master Directive
ML	Money Laundering
MLCA	Money Laundering Control Act
NLP	Natural Language Processing
NZ	New Zealand
PBOC	People's Bank of China
PEP	Politically Exposed Person
PET	Privacy Enhancing Technology
PSA	Payment Services Act (2020)
PSS	Payment and Settlement Systems
RBI	Reserve Bank of India
RBNZ	Reserve Bank of New Zealand
RE	Regulated Entity
RPA	Robotic Process Automation
SAR	(Hong Kong) Special Administrative Region
SFC	(Hong Kong) Securities and Futures Commission
SG	Singapore
SME	Subject Matter Expert
STR	Suspicious Transaction Report
TF	Terrorist Financing

Contacts



Akihiro Matsuyama

**ACRS Executive Sponsor
Partner, RA FSI**

amatsuyama@deloitte.com.hk
+852 28521287



Nai Seng Wong

**SEA ACRS Co-lead
Executive Director
SEA Regulatory Strategy Leader**

nawong@deloitte.com
+65 6800 2025



Mike Ritchie

**Australia ACRS Co-lead
Partner, RA FSI**

miritchie@deloitte.com.au
+612 9322 3219



Jessica Namad

**China ACRS Co-lead
Director, RA FSI**

jnamad@deloitte.com.hk
+852 2238 7892



Shiro Katsufuji

**Japan ACRS Co-lead
Director, RA FSI**

shiro.katsufuji@tohmatcu.co.jp
+81 70 6473 7748

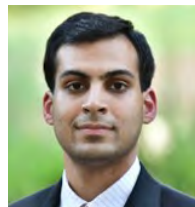
Contributors



Nicola Sergeant

**Senior Manager
Coordinator**

nicola.sergeant@tohmatcu.co.jp



Siddharth Agarwala

**Senior Consultant
Contributor**

siagarwala@deloitte.com



Jaramie Nejal

**Senior Manager
Contributor**

jnejal@deloitte.com.au

Acknowledgements

Lisa Dobbin

Partner
Australia

Amanda Lui

Partner
Australia

Radish Singh

Partner
SEA

Marc Anley

Partner
SEA

Mark Woodley

Partner
SEA

Chris Cheung

Partner
China

Thao Nguyễn Hoàng

Senior Manager
SEA

Celeste Lu Wang

Director
China

Sally Watson

Senior Analyst
Australia

Endnotes

1. The Treasury, Australian Government, "Consultation: Financial Accountability Regime (FAR)", 22 January 2020, <https://treasury.gov.au/consultation/c2020-24974>
2. Australian Government, "Anti-Money Laundering and Counter-Terrorism Financing and Other Legislation Amendment Act 2020", 17 December 2020, <https://www.legislation.gov.au/Details/C2020A00133>
3. Australian Prudential Regulation Authority, "Risk Management", 1 July 2019, <https://www.apra.gov.au/risk-management>
4. Australian Prudential Regulation Authority, "Prudential Standard CPS 234 Information Security", 1 July 2019, https://www.apra.gov.au/sites/default/files/cps_234_july_2019_for_public_release.pdf
5. Australian Transaction Reports and Analysis Centre, "New Rule will help Australians fleeing family and domestic violence gain financial independence", 28 May 2020, <https://www.austrac.gov.au/about-us/media-release/new-rule-will-help-australians-fleeing-family-and-domestic-violence-gain-financial-independence>
6. Australian Transaction Reports and Analysis Centre, "Identifying customers who don't have conventional forms of ID", Aug 2020, <https://www.austrac.gov.au/business/how-comply-and-report-guidance-and-resources/customer-identification-and-verification/identifying-customers-who-dont-have-conventional-forms-id>
7. Financial Markets Authority & Reserve Bank of New Zealand, "Enhanced Customer Due Diligence Guidelines", September 2020, <https://www.rbnz.govt.nz/-/media/ReserveBank/Files/regulation-and-supervision/anti-money-laundering/guidance-and-publications/Enhanced%20Customer%20Due%20Diligence%20Guideline%202020.pdf>
8. Financial Markets Authority & Reserve Bank of New Zealand, "Guidance: Complying with AML/CFT verification requirements during COVID-19 Alert Levels", 26 March 2020, <https://www.rbnz.govt.nz/-/media/ReserveBank/Files/regulation-and-supervision/anti-money-laundering/AMLCFT-Supervisor-Guidance-COVID-19-Alert.pdf>
9. Financial Markets Authority, "AML/CFT Supervisory Framework", 22 November 2019, <https://www.fma.govt.nz/compliance/guidance-library/amlcft-supervisory-framework/>
10. Financial Markets Authority, "AML/CFT – territorial scope of the AML/CFT Act 2019", 22 November 2019 <https://www.fma.govt.nz/compliance/guidance-library/amlcft-territorial-scope-of-the-amlcft-act-2019/>
11. Ministry of Justice "Tackling money laundering and terrorist financing", 2019, <https://www.justice.govt.nz/justice-sector-policy/key-initiatives/aml-cft/>
12. Stewart McGlynn (Hong Kong Monetary Authority) "Moving the Needle: Improving Outcomes in Anti-Money Laundering", 26 September 2019, https://www.hkma.gov.hk/media/eng/doc/key-functions/banking-stability/aml-cft/Speech_Stewart_McGlynn_201909.pdf
13. Hong Kong Monetary Authority, "Guideline on Anti-Money Laundering and Counter Financing of Terrorism", September 2020, https://www.hkma.gov.hk/media/eng/doc/key-functions/financial-infrastructure/infrastructure/svf/Guideline_on_AMLCFT_for_SVF_eng_Sep2020.pdf
14. The Hong Kong Association of Banks, "Frequently Asked Questions in relation to Anti-Money Laundering and Counter-Financing of Terrorism", February 2021, https://www.hkma.gov.hk/media/eng/doc/key-functions/banking-stability/aml-cft/FAQ_amlcft_feb_2021.pdf
15. The People's Bank of China Anti-Money Laundering Bureau, Regulations and Policies webpage, <http://www.pbc.gov.cn/fanxiqianju/135153/135173/index.html>
16. The People's Bank of China, "Measures for the Supervision and Administration of Anti-Money Laundering and Anti-terrorist Financing of Financial Institutions", 17 April 2021, http://www.gov.cn/xinwen/2021-04/17/content_5600258.htm

17. Monetary Authority of Singapore, "Payment Services Act", 15 April 2019, <https://www.mas.gov.sg/regulation/acts/payment-services-act>
18. Association of Crypto Currency Enterprises and Start-ups Singapore, "Code of Practice" (for members), August 2019, <https://www.access.org.sg/products/code-of-practice-members>
19. Association of Crypto Currency Enterprises and Start-ups Singapore, "Code of Practice" (for non-members), August 2019, <https://www.access.org.sg/products/code-of-practice>
20. Japan Financial Services Agency, "Results on Public Comments on partial Revisions to the Guidelines on Measures against Money Laundering and the Financing of Terrorism", 11 December 2020, https://www.fsa.go.jp/news/r2/202102_amlcft/202102amlcft.html
21. Japan Financial Services Agency, "Financial Services Agency considers system development jointly with regional banks", 31 October 2020, <https://www.nikkei.com/article/DGXMZO51644020R31C19A0EE9000/>
22. Japan Financial Services Agency, "Notification of Originator and Beneficiary Information Upon Crypto Asset Transfer (i.e. the travel rule)", 31 March 2021, <https://www.fsa.go.jp/news/r2/sonota/20210331.html>
23. Taiwan Business TOPICS, "Enhanced Anti-Money Laundering Controls Pay-off For Taiwan", 27 May 2020, <https://topics.amcham.com.tw/2020/05/antimoney-laundering-controls-pay-off/>
24. Taiwan Ministry of Justice, "Money Laundering Control Act", 7 November 2018, <https://law.moj.gov.tw/ENG/LawClass/LawAll.aspx?pcode=G0380131>
25. Fintech Hong Kong, "Taiwan's First Virtual Banks: The Progress So Far", 7 October 2020, <https://fintechnews.hk/13536/fintechtaiwan/taiwans-first-virtual-banks-the-progresses-so-far/>
26. Reserve Bank of India, "Master Direction on Digital Payment Security", 18 February 2021, <https://rbidocs.rbi.org.in/rdocs/notification/PDFs/MD7493544C24B5FC47D0AB12798C61CDB56F.PDF>
27. Reserve Bank of India, "Extending Master Direction – Know Your Customer (KYC) Direction, 2016 to Housing Finance Companies", 19 May 2020, <https://rbi.org.in/scripts/NotificationUser.aspx?Mode=0&Id=11892>
28. Reserve Bank of India, "Amendment to Master Direction (MD) on KYC – Centralized KYC Registry – Roll out of Legal Entity Template & other changes", 18 December 2020, <https://www.rbi.org.in/Scripts/NotificationUser.aspx?id=12008&Mode=0>
29. Reserve Bank of India, "Amendment to the Master Direction (MD) on KYC", 10 May 2021, <https://www.rbi.org.in/scripts/NotificationUser.aspx?id=12089&Mode=0>
30. Reserve Bank of India, "Guidelines on Regulation of Payment Aggregators and Payment Gateways", 17 March 2020, <https://rbi.org.in/scripts/NotificationUser.aspx?Mode=0&Id=11822>
31. Reserve Bank of India, "Framework for imposing monetary penalty on authorised payment system operators / banks under the Payment and Settlement Systems Act, 2007", 10 January 2020, <https://rbi.org.in/scripts/NotificationUser.aspx?Mode=0&Id=11785>
32. Committee of Sponsoring Organizations of the Treadway Commission & Association of Certified Fraud Examiners, "Fraud Risk Management Guide", September 2016, <https://www.acfe.com/fraudrisktools/guide.aspx>
33. Standards Australia, "Fraud and Corruption Control Standards" (AS 8001-2008), 2008, <https://www.standards.org.au/standards-catalogue/sa-snz/other/qf-017/as--8001-2008>



Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited (“DTTL”), its global network of member firms, and their related entities (collectively, the “Deloitte organization”). DTTL (also referred to as “Deloitte Global”) and each of its member firms and related entities are legally separate and independent entities, which cannot obligate or bind each other in respect of third parties. DTTL and each DTTL member firm and related entity is liable only for its own acts and omissions, and not those of each other. DTTL does not provide services to clients. Please see www.deloitte.com/about to learn more.

Deloitte Asia Pacific Limited is a company limited by guarantee and a member firm of DTTL. Members of Deloitte Asia Pacific Limited and their related entities, each of which are separate and independent legal entities, provide services from more than 100 cities across the region, including Auckland, Bangkok, Beijing, Hanoi, Hong Kong, Jakarta, Kuala Lumpur, Manila, Melbourne, Osaka, Seoul, Shanghai, Singapore, Sydney, Taipei and Tokyo.

This communication contains general information only, and none of Deloitte Touche Tohmatsu Limited (“DTTL”), its global network of member firms or their related entities (collectively, the “Deloitte organization”) 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 representations, warranties or undertakings (express or implied) are given as to the accuracy or completeness of the information in this communication, and none of DTTL, its member firms, related entities, employees or agents shall be liable or responsible for any loss or damage whatsoever arising directly or indirectly in connection with any person relying on this communication. DTTL and each of its member firms, and their related entities, are legally separate and independent entities.

© 2021 Deloitte Asia Pacific Services Limited
Designed by CoRe Creative Services. RITM0678744



This is printed on environmentally friendly paper