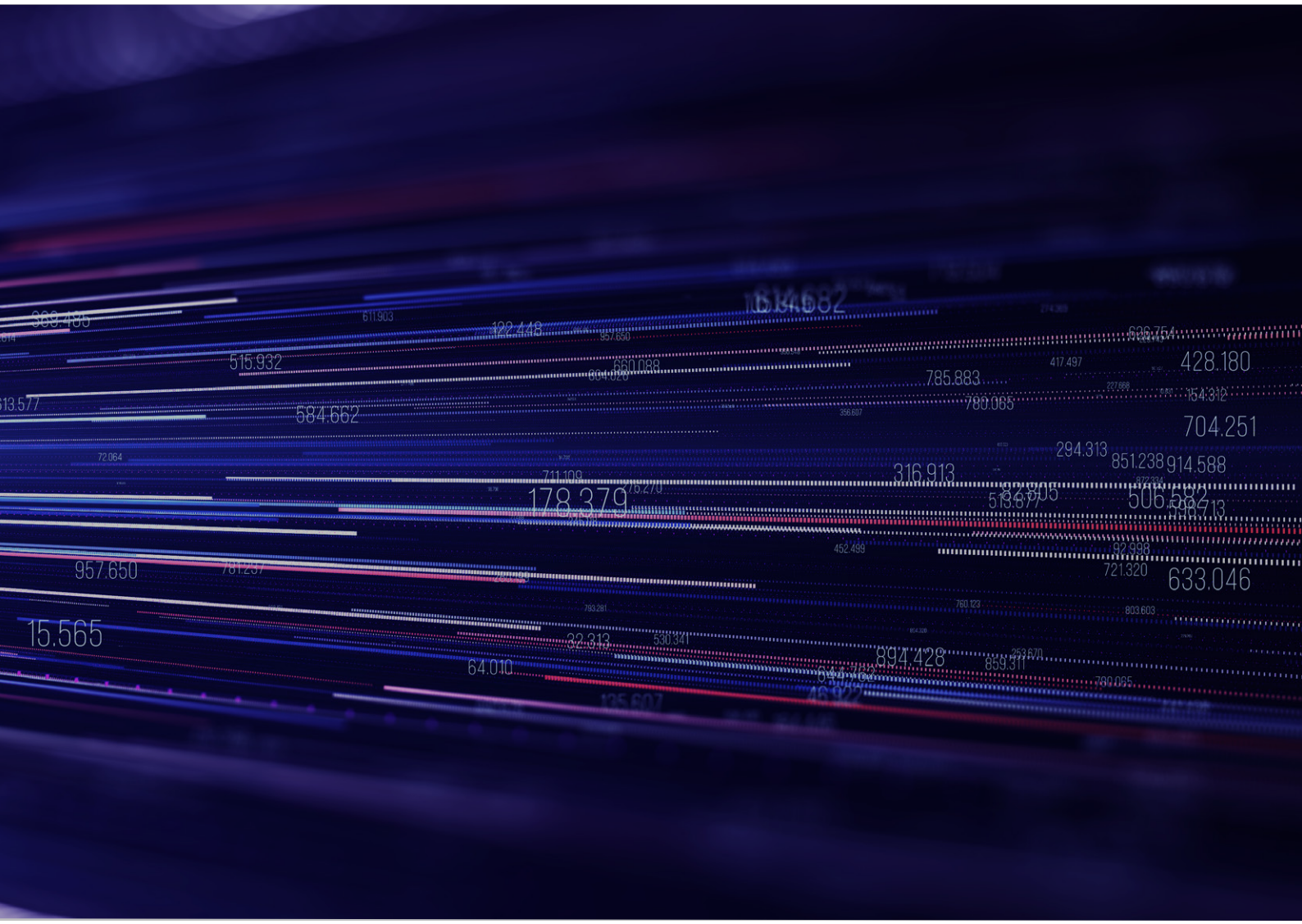
HONG KONG MONETARY AUTHORITY
香港金融管理局

AML/CFT Regtech: Case Studies and Insights Volume 2

September 2023

Deloitte.

Contents


515.932
584.662
785.883
428.180
704.251
294.313
851.238
914.588
316.913
178.379
957.650
633.046
15.565
64.010

Foreword

When I spoke at the HKMA's AML/CFT Regtech Forum in 2019, I asked a number of questions, the most important of which was whether Hong Kong's AML/CFT system was working as well as it needed to be. There seemed to be general agreement that we could do better, and that collective actions were required to deliver a more effective response.

Our response was developed around two main areas of focus: modernising supervisory activities, or *Suptech*, and promoting responsible innovation by the industry, or *Regtech*. Four challenging years have passed since then, during which balancing the threats and opportunities from the transformation of the digital economy has become a central theme in how the HKMA delivers its mandate to ensure the stability of one of the most efficient banking systems in the world.

In the same period, our AML Digitalisation Programme has progressed, enabling us to significantly improve the breadth and scope of the engagement we provide as part of our regulatory toolbox. But still, we stick to our vision and the roadmap which recognises that no two institutions are at the same stage in their development and use of AML Regtech. The rapid development of digital fraud has undoubtedly sharpened our sense of purpose in fully deploying that roadmap, but fraud is by no means the only financial crime threat we face as a well-connected international financial centre.

We have achieved much. In terms of Suptech, the HKMA has automated AML data processing and optimised its AML data management. We have developed data-driven capabilities that enable us to continuously monitor financial crime risks, and developed a Suptech environment that supports the analysis of larger data sets and enhanced risk profiling. These help in actively identifying new or evolving risks and control vulnerabilities, allowing us and the banks concerned to take proactive measures to mitigate.

But we were also clear four years ago that the modernisation of supervisory activities should go hand-in-hand with the adoption of AML Regtech by the private sector, in order to fully leverage the increased volume and maturity of data available to banks.

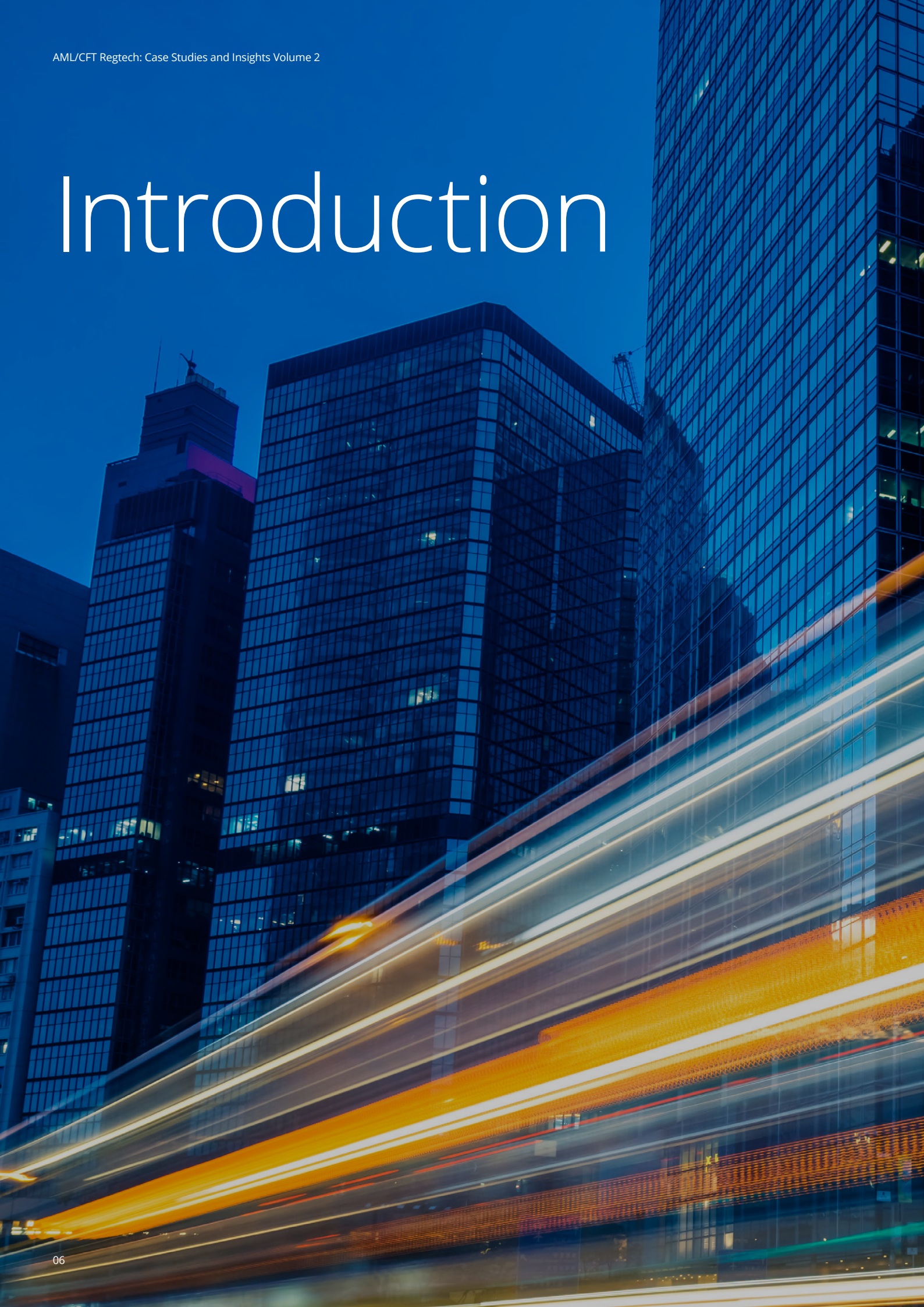
Today it is pleasing to see that in most banks, AML functions are already well past the early stage of Regtech adoption, while some have reached an advanced stage.

However, much remains to be done in bringing together the advances we have made in Suptech, Regtech and Data to turn the tables on fraud and other financial crime. We must not lose sight of the need to be dynamic and creative, revamping outdated processes where there is a better way to do things.

These latest case studies, some of which have a particular focus on the response to digital fraud, embody those principles and further demonstrate the value of forums to share views and experience. I am confident that the collective will exists to sustain the pace we are achieving in materialising our vision to reduce harm from financial crime.

Arthur Yuen
Deputy Chief Executive
Hong Kong Monetary Authority

Introduction



In 2019[1], the HKMA partnered with Deloitte in a series of industry engagements to explore how banks were deploying technology-enabled solutions to enhance their AML/CFT programmes, and to support the banking sector's further adoption of Regtech.

As part of this, we published our inaugural Case Studies and Insights paper[2], sharing perspectives of Hong Kong banks that were in the process of incorporating Regtech in their AML/CFT processes. The objective is to share with the industry practical insights and lessons learned on Regtech adoption, encourage broader adoption of Regtech solutions and ultimately uplift the collective AML/CFT effectiveness of our ecosystem.

Since the release of Case Studies and Insights, our industry engagement on AML Regtech has continued to evolve, including a series of AML Regtech Lab (AMLab) events – in collaboration with Cyberport – and a further publication[3] that shares deep-dive case studies on the use of Network Analytics within AML.

Despite the progress being made, there is more to be done: the capability of Regtech solutions continues to evolve and, as part of HKMA's Fintech 2025 strategy, all Hong Kong banks are encouraged to keep pace with change by fully digitalising their operations. In that light, this paper seeks to build on the first one, by sharing case studies on more advanced Regtech solutions that have been deployed within AML. Recognising that no 'one-size-fits-all', the case studies are organised by use case – or problem statement – rather than by institution, allowing us to highlight the perspectives of multiple banks in tackling similar Regtech initiatives.

The case studies shared cover four broad areas of Regtech implementation:

- **Real-time Fraud Monitoring**
- **Machine Learning for Transaction Monitoring Alerts Handling**
- **Natural Language Processing for News Monitoring**
- **Analytics with a 'Single View of the Customer'**

Banks may refer to the case studies shared in this paper, along with other resources made available by the HKMA, to facilitate internal discussions on what more can be achieved in further raising AML/CFT effectiveness through Regtech adoption.

1. The Hong Kong Monetary Authority (HKMA) fosters a diversified ecosystem for Anti-Money Laundering and Counter-Financing of Terrorism (AML/CFT) Regulatory Technology (RegTech), November 2019. https://www.hkma.gov.hk/eng/news-and-media/press-releases/2019/11/20191122-4/
2. The Hong Kong Monetary Authority, AML/CFT Regtech: Case Studies and Insights, January 2021 https://www.hkma.gov.hk/media/eng/doc/key-information/guidelines-and-circular/2021/20210121e1a1.pdf
3. The Hong Kong Monetary Authority, AML Regtech: Network Analytics, May 2023 https://www.hkma.gov.hk/media/eng/doc/key-functions/banking-stability/aml-cft/AML_Regtech-Network_Analytics.pdf

Case Studies in AML Regtech Adoption

The case studies shared in this paper are based on the adoption journeys of six Hong Kong Banks:

1

Bank A
A bank that serves retail and corporate customers with full range of financial products and services.

2

Bank B
A bank that provides consumer, SME, and corporate banking services.

3

Bank C
A bank that provides banking, wholesale banking, and wealth management services.

4

Bank D
A bank engaging in commercial and retail banking services.

5

Bank E
A private bank that offers private, corporate, and investment banking services.

6

Bank F
An international bank, based in Hong Kong, that serves corporate and retail banking customers with a range of products and services.

Case Study 1: Real-time Fraud Monitoring

BACKGROUND AND CONTEXT

Against a backdrop of increasing fraud and scams, often enabled by criminal exploitation of new and emerging technology, it is imperative that banks continue to deploy innovative solutions to enhance their anti-fraud efforts. In that light, the first case study focuses on Bank A and Bank B – which are both working to enhance their fraud monitoring and detection capabilities through the application of advanced analytics.

MONITORING PAYMENTS FOR SUSPECTED FRAUD

As part of a joint initiative by the HKMA, the banking industry and Hong Kong Police Force ("HKPF"), all Hong Kong retail banks have committed to implementing real-time fraud monitoring capabilities. The HKMA surveyed the retail banks that had a dedicated fraud monitoring platform in June 2023, and found that:

Over 80% analyse 'non-traditional' data[4], such as digital footprint and biometric information, as part of their fraud monitoring.

Around 40% have already implemented advanced analytics, such as machine learning, to enhance their fraud monitoring capabilities.

4. The Hong Kong Monetary Authority: Feedback from Thematic Review of the Use of External Information and Data in Anti-Money Laundering and Counter-Financing of Terrorism (AML/CFT) Systems, April 2021
https://www.hkma.gov.hk/media/eng/doc/key-information/guidelines-and-circular/2021/20210426e1.pdf
https://www.hkma.gov.hk/media/eng/doc/key-information/guidelines-and-circular/2021/20210426e1a1.pdf

RULES-BASED FRAUD MONITORING

Bank A acquired an off-the-shelf fraud monitoring solution in 2018, and has tailored this extensively through developing a library of bespoke monitoring rules based on intelligence (e.g. from the Fraud and Money Laundering Intelligence Taskforce (FMLIT[5]) and law enforcement) and evolving typologies. Bank A's monitoring solution has since been developed into a more comprehensive anti-fraud platform that includes reporting and network analytics functionalities.

Echoing case studies shared in our recent Network Analytics publication, Bank A emphasised the benefits of using network analytics in post-event or intelligence-led reviews. Through its anti-fraud platform, Bank A shares information on confirmed fraud cases with an investigations team for further follow-up. Using network analysis, investigators can identify additional suspicious accounts or potential scam victims. In 2022 alone, Bank A's anti-fraud platform enabled it to safeguard around 200 customers from being victimised by scams, preventing around HKD35 million in losses.

Bank A conducts ongoing enhancements of its fraud monitoring solution to ensure that monitoring keeps pace with the evolving modus operandi of fraudsters, and seek operational efficiencies such as optimised alert volumes and reduced false-positive rates.

When implementing new or updated monitoring rules, Bank A conducts 'back-testing' to assess system performance in a development environment. This approach allows the Bank to identify any potential issues – such as a sudden uptick in alert volumes – before operationalising new rules. Having a 'safe' environment allows the Bank to test a range of ideas and be more radical in their innovation.

5. Established in May 2017, the FMLIT is a public-private partnership for information sharing among the HKPF, the HKMA and 28 banks

Reflecting on the evolution of its fraud monitoring solution – now comprising around 100 rules and scenarios covering 11 product channels – Bank A shared that one critical success factor of its ongoing development work is having a dedicated, interdisciplinary team that brings together fraud domain expertise with analytics specialists. This collaboration enabled Bank A to customise an off-the-shelf tool to its own products and services and helped it to keep pace with evolving threats. Working collaboratively, Bank A's fraud team is now able to readily develop new monitoring rules in response to new insight or intelligence.

Bank A recognises that new and emerging technology offers further opportunity to enhance its anti-fraud capability, and are currently working to deploy an in-house developed Machine Learning (ML) solution to improve the performance of rules-based monitoring. The objectives are to: i) prioritise high-risk alerts from the rules-based engine based on a 'feedback loop'; and ii) develop additional monitoring scenarios based on dynamic thresholds and behavioural analytics.

Bank A plans to roll out its ML capability on a product-by-product basis, and is currently developing ML for credit card payments as a pilot exercise, due to the product nature and availability of training data. As part of this, Bank A will conduct a parallel run of the ML against existing anti-fraud operations to assess model performance before committing to implementation.

Despite its ongoing enhancement efforts, Bank A acknowledges that real-time fraud monitoring will not be a 'silver bullet' in reversing any rise in fraud or deception scams , and is committed to collaborating more closely with the wider banking sector and law enforcement agencies (LEAs) to support a range of anti-fraud efforts such as consumer education and enhanced training of front-line Bank staff.

TAKING ACTION TO TACKLE FRAUD AND DECEPTION

On 21 April, the HKMA and HKPF jointly hosted a high-level sharing session on anti-deception efforts[6], where participants committed to continuing to support innovation in the fight against fraud.

"Our common task has got harder. In the last few years, financial crime, especially digital fraud, has become a more serious concern"

Carmen Chu
Executive Director (Enforcement and AML), Hong Kong Monetary Authority, Regulation Asia Fraud & Financial Crime Summit[7], 13 July 2023

The HKMA encourages banks to be pragmatic and dynamic in their allocation of resources across AML/CFT. Bank A's deployment of a fraud monitoring solution is a solid example of value-driven resource allocation, where time and talent are directed towards activities that yield real outcomes – in this case protecting customers from fraud – rather than less productive activities.

The HKMA will further assess how the policy and regulatory framework can enable resources across the ecosystem to be released from low-value activities, and refocused to have the greatest impact against imminent and emerging threats.

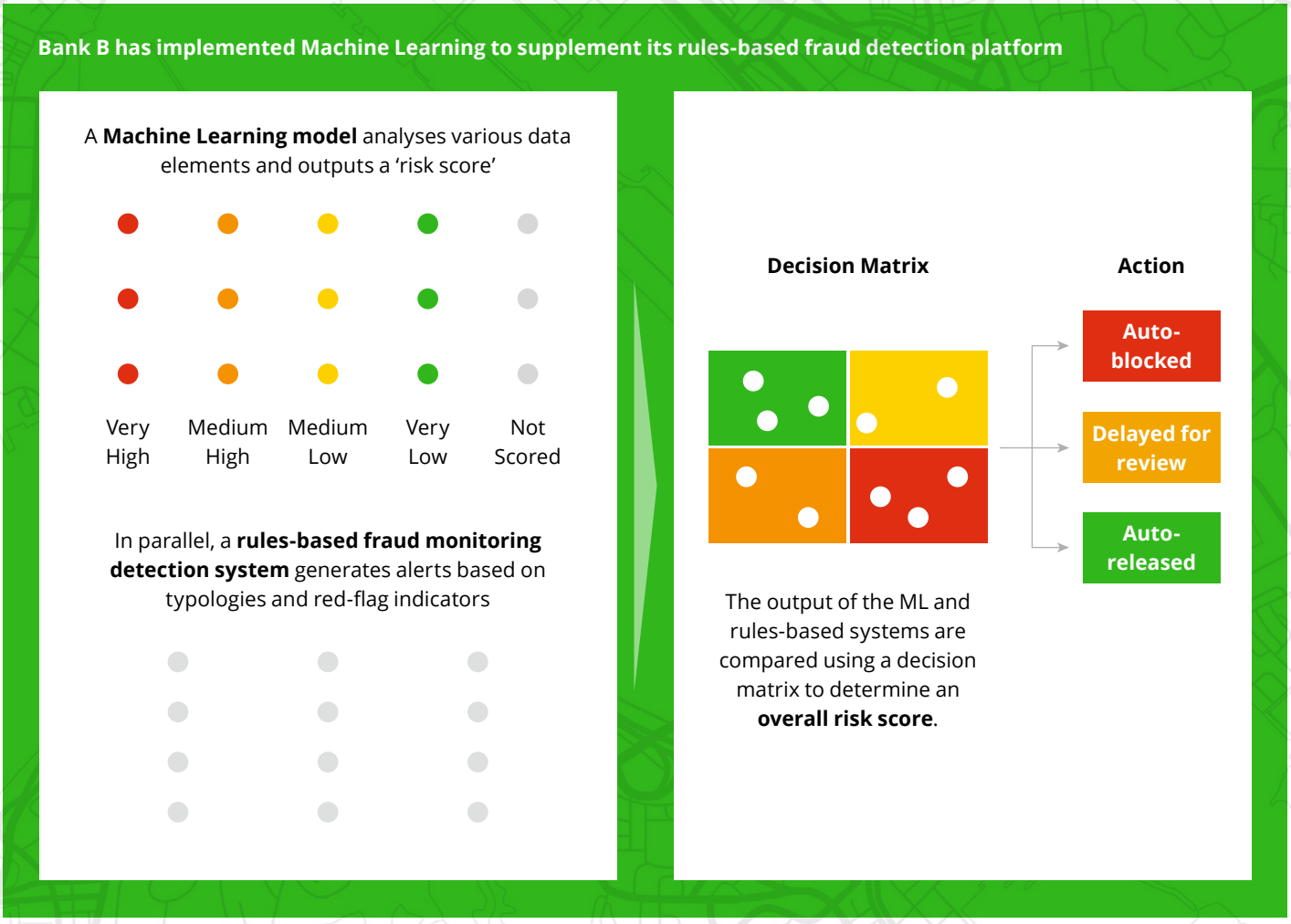
6. Hong Kong Monetary Authority and Hong Kong Police Force co-host sharing session with banking industry on anti-deception efforts, April 2023 https://www.hkma.gov.hk/eng/news-and-media/press-releases/2023/04/20230421-7/
7. Opening Keynote Speech at Fraud and Financial Crime Asia Summit 2023, July 2023 https://www.hkma.gov.hk/eng/news-and-media/speeches/2023/07/20230713-1/

FRAUD DETECTION WITH MACHINE LEARNING

Like Bank A, Bank B operates a rules-based fraud monitoring solution. Bank B has implemented ML to supplement its rules-based fraud detection, to improve the false-positive alert rate – reducing friction in the customer experience, and improving operational efficiency. Bank B's ML ingests around 300 data elements and considers a range of suspicious event indicators including flow-of-funds, beneficiary account behaviour, and customer demographics.

Bank B's ML runs against payments data in parallel to the rules-based fraud detection system, and the outputs of both are compared against a decision matrix to determine an overall risk score. Based on the risk score, payments can be auto-blocked, delayed for review, or auto-released. Through this approach, Bank B has not only reduced its false-positive alert rate, but has also been able to identify confirmed fraud cases that would have earlier gone undetected. Around 20% of Bank B's low-risk alerts are now auto-released.

Although Bank B set out to improve KPIs such as false-positive rates and overall alert volumes, Bank B stated that having management and other key stakeholders aligned to the mission of combatting fraud and protecting customer funds enabled fast decision-making and an outcome-driven approach. Thanks to this buy-in, and the oversight and support offered by a Project Steering Committee, Bank B was able to develop working a ML solution in six months.



AMLAB 4 – AN AGILE, COORDINATED, AND STRATEGIC RESPONSE TO DIGITAL FRAUD AND FINANCIAL CRIME

AMLab – a series of AML Regtech Labs – was launched by the HKMA in November 2021 as an interactive and collaborative platform for banks, industry experts, and technology companies to share knowledge, experience, and new ideas on AML Regtech adoption and implementation.

The HKMA's fourth AMLab event[8], held on 7 June 2023 in partnership with Cyberport and supported by Deloitte, sought to explore innovative fraud monitoring and detection solutions aligned to the HKMA and HKPF joint initiative. In this session, the HKMA shared with the participants the joint initiative requirements for real-time fraud monitoring and how the discussions can support further technology adoption within their banks.

All retail banks and major Stored Value Facility (SVF) licensees , alongside Regtech vendors and international experts, shared their perspectives on the future of Hong Kong's anti-fraud regime – focusing on the critical role that technology will play in helping banks on the front line of defence.

Following AMLab 4, a 'Regtech Connect' networking session was held, where vendors offering fraud detection and analytics solutions met with local banks to explore further collaboration opportunities.

8. The fourth Anti-Money Laundering Regtech Lab: supporting an agile, coordinated, and strategic response to digital fraud and financial crime, June 2023 https://www.hkma.gov.hk/eng/news-and-media/press-releases/2023/06/20230607-5/

BALANCING FRAUD PROTECTION WITH A FRICTIONLESS CUSTOMER EXPERIENCE

A key theme explored at AMLab 4 was the balance between anti-fraud processes and providing customers with a seamless banking experience. Bank A shared its perspective: the growing library of fraud detection rules has led to an increase in alert volumes and therefore the likelihood of customer payments being interrupted. To address this, Bank A closely monitors the performance of its fraud monitoring platform using quantitative (false-positive and false-negative rates) and qualitative (customer feedback) measures. This allows the Bank to readily identify pain points and inefficiencies.

Multiple banks cited the importance of implementing 'customer profiling' within fraud detection, where rules and thresholds are based on the customer demographic. By tailoring the detection rules in this way, banks can more accurately identify behaviours and events that are non-typical for any given customer. Bank A's fraud monitoring platform consumes various customer attributes – both static (e.g. demographic information) and dynamic (e.g. customer behaviour) – to reduce false-positives and enhance detection accuracy.

COMBINING RULES-BASED AND MACHINE LEARNING CAPABILITIES

Banks A and B adopt a hybrid approach to fraud detection – with ML working alongside rules-based engines to identify suspicious activity. Both Banks shared that this allows them to benefit from the positive outcome of ML in identifying complex fraud patterns whilst maintaining the ability to implement new and explainable rules readily, in response to new or well-known typologies.

WHAT LIES AHEAD?

Banks A and B acknowledge that more work is required to further improve their anti-fraud capability and, ultimately, better protect their customers. The methods of fraudsters and scammers continue to evolve, including the rapid exploitation of new technology. To combat this, the entire banking sector will need to continue to invest and innovate. Banks A and B, although already leveraging advanced analytics in fraud detection, are both driven to continue to raise the operational efficiency of their fraud programmes, better-protecting their businesses from fraud-related losses, and ensuring that resources and talent are efficiently managed.

Case Study 2: Machine Learning for Transaction Monitoring Alerts Handling

BACKGROUND AND CONTEXT

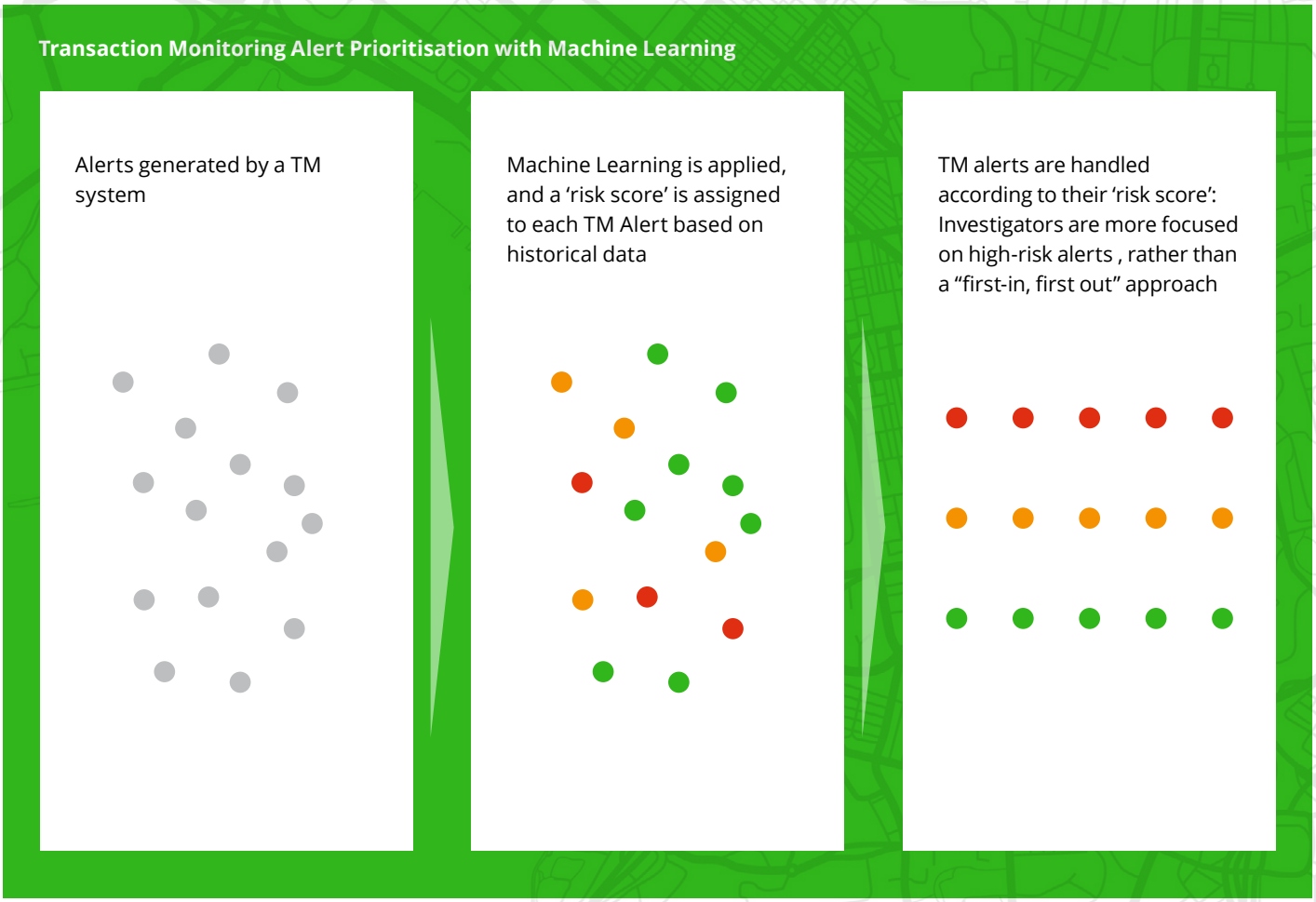
In the 2019 AML/CFT Regtech Forum, there was a focus on machine learning and the perennial challenge of excessive false-positive alerts. While a few mature adopter banks have subsequently deployed ML with some success, in recent engagement with the banking sector on AML Regtech case studies, transaction monitoring (TM) alerts handling has continued to be cited as an area with operational pain points, where some banks find the adoption of technology-enabled solutions challenging for a number of reasons. In this Case Study, we share perspectives from Banks B, C, and D, which are in the process of implementing ML to enhance their TM operations.

MACHINE LEARNING FOR ALERT PRIORITISATION

Referring to the high volume of false-positive alerts generated by off-the-shelf TM systems, Banks C and D are both exploring ML-enabled solutions to improve the efficiency and productivity of TM alerts handling. Both Banks are developing a 'feedback loop', whereby an ML model is 'trained' using historical TM alert data, including review outcomes. When future TM alerts are raised, the ML model assigns a score, based on the likelihood that they will be true-positive. Based on the assigned score, TM alerts can be prioritised so that investigators direct their attention on the highest-risk alerts, rather than dealing with them chronologically.

In consultation with its Head Office, Bank D engaged a well-known vendor with expertise in deploying ML-enabled solutions for AML. Bank D trained an initial ML model by providing the vendor with one year of historical TM alerts data. Over a six-month period, a trial run was conducted to assess initial outcomes and agree refinements to the ML model based on user feedback. Bank D's long-term goal is to develop an 'auto-clear' mechanism, whereby TM alerts that are classified as low-risk are automatically discounted, without the need for manual intervention. For more detailed guidance on how to define and measure the value of the AML Regtech initiatives, please refer to Performance Metrics & Indicators in the first Case Studies and Insight Paper.

Bank C opted to develop an ML solution in-house, having decided based on an initial vendor assessment process that it had the capability and bandwidth do to so. Bank C already had a team of experienced data scientists, and recognised the importance of leveraging institution-specific knowledge during the innovation process. Bank C launched a Proof-of-Concept (PoC) exercise in early 2023, and is working through an iterative development process to enhance its initial ML solution. Like Bank D, Bank C defined an initial Key Performance Indicator to assess the performance of its ML solution, focusing on ensuring that at least a specific proportion of TM alerts are assigned a high-risk rating in the first instance. After working through several model iterations, Bank C's PoC exercise has yielded promising results. Investigators confirmed that the 80% of alerts scored as high-risk lead to a Suspicious Transaction Report (STR) being filed.

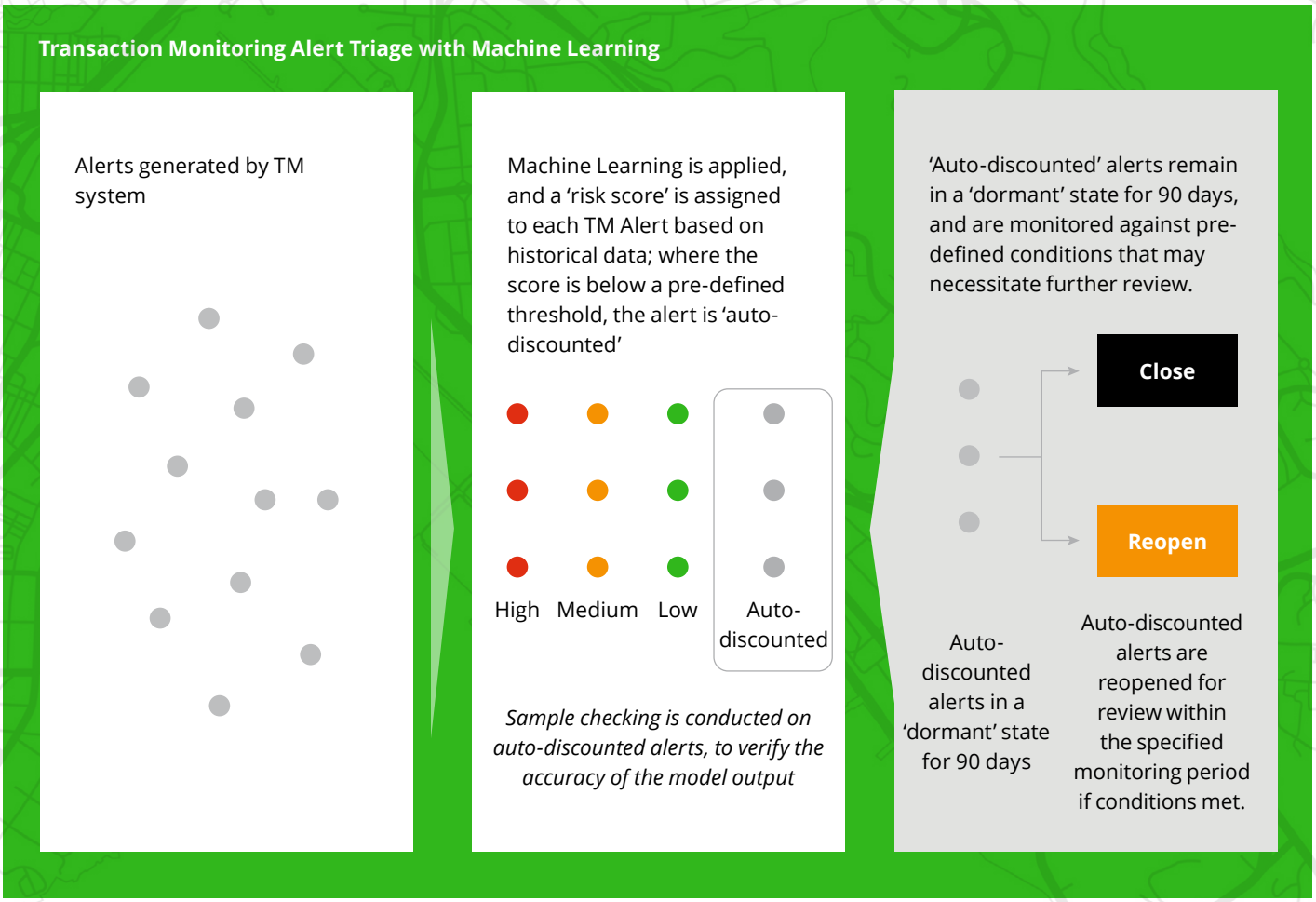


MACHINE LEARNING FOR ALERT TRIAGE

As part of a programme to enhance its TM alert review process, Bank B has developed ML to prioritise and auto-clear TM alerts. Bank B was driven to launch this programme by high false-positive alert rates, and a lengthy post-alert review process.

Like Banks C and D, Bank B's ML solution leverages historical TM alert review data to assign a risk score to TM alerts. The solution, developed in-house, also includes further features to enhance the scoring mechanism through automatically contextualising the alert. These features include customer data, account attributes, and other red flag indicators. Customers that are PEP, accounts that have recently been opened, and whether an STR has previously been filed are all factors that would further impact the score, in addition to historical alert data.

Bank B's TM alerts are reviewed using a purpose-built case management tool that consolidates data from multiple sources to facilitate the review process. Investigators can view alert information – generated by the TM system – alongside ML output and supplementary data such as customer profile and any previous review cases. The case management tool is also used for management reporting, and to view and monitor operational metrics. This centralised, interactive platform provides the investigators with an increased situational awareness, and has enabled an uptick in TM operation productivity: 7% of TM alerts are auto-closed, subject to sample checking for quality assurance, and the daily workload for an investigator is reduced by 1 to 3 hours.



GETTING STARTED: MACHINE LEARNING MODEL IMPLEMENTATION

When sharing perspectives on 'getting started' with developing ML, Banks B, C, and D all referred to the relatively large datasets required to train an initial ML model – ranging from 6 months' to 2 years' of historical data comprising TM alerts, review results, and payment information.

For Bank B in particular, this exercise involved a one-off data cleansing exercise to standardise the format of legacy data so that it was readily consumable by its ML solution. The scale of this exercise was managed by agreeing to focus on 'critical data elements' – those deemed most relevant to the ML solution.

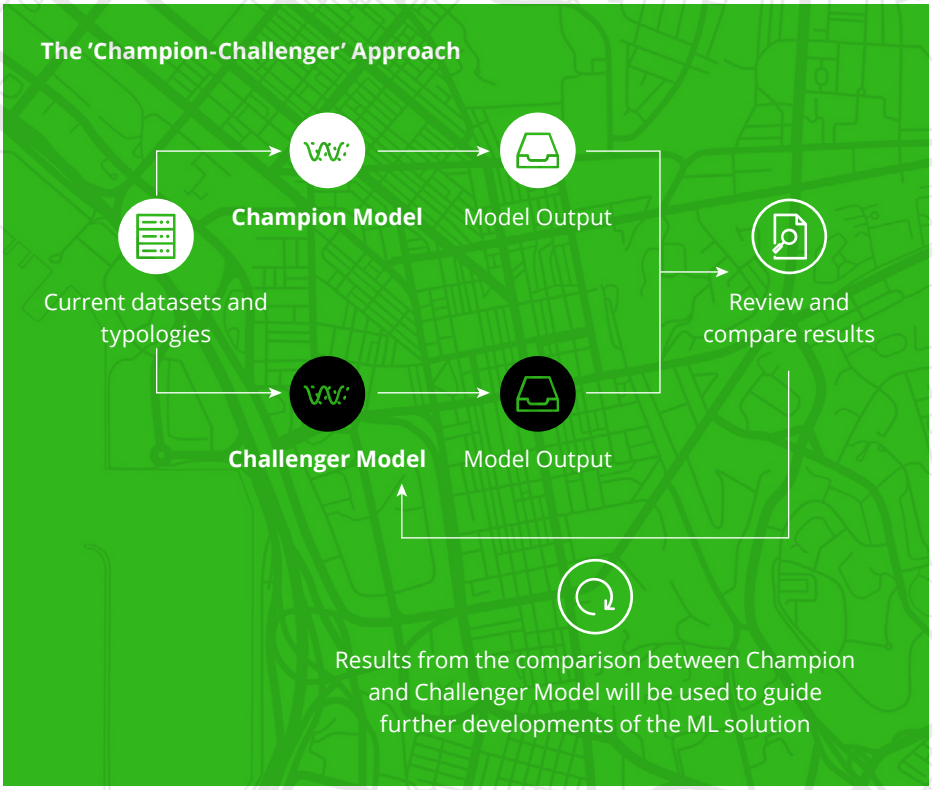
Bank C also made reference to the underlying infrastructure required to host and process the data required to implement and operate its ML solution. Bank C relied on cloud infrastructure, as it could be scaled to its requirements relatively quickly.

MEASURING SUCCESS: MACHINE LEARNING MODEL PERFORMANCE

Bank C follows a 'Champion-Challenger' approach when assessing the potential impact of updates to its ML models. 'Champion' refers to the current, operational version of the ML, and 'Challenger' to an updated version. Both models are run in parallel on the same dataset, allowing for analysis and comparison of the outputs to assess the limitations and strengths of each, and inform decision making on next steps. During the parallel run, model performance is measured using business-specific KPIs such as false-positive rates, and technical metrics such as performance efficiency. By iterating through many 'Champion-Challenger' tests, Bank C can continuously develop its ML solution with no risk of impacting business-as-usual processes. This enables the team to be more innovative and creative when attempting to develop better-performing solutions.

Bank B – whose ML solution auto-closes alerts when the assigned risk score falls below a certain level – conducts manual sample checks of its ML solution output as part of its ML performance assessment process. Where required, risk scores are manually adjusted and fed back to the model to retrain the ML and achieve more optimal results. Bank B stated that low re-opening rates of auto-closed alerts, among other performance metrics, have inspired confidence in the robustness of its ML solution.

Where 'model drift' occurs – that is, the ML output deviates from what is observed to be 'normal' or 'expected' performance – Bank B has established a protocol that requires investigations to be performed to determine the cause of performance degradation, and will initiate the model retraining process.

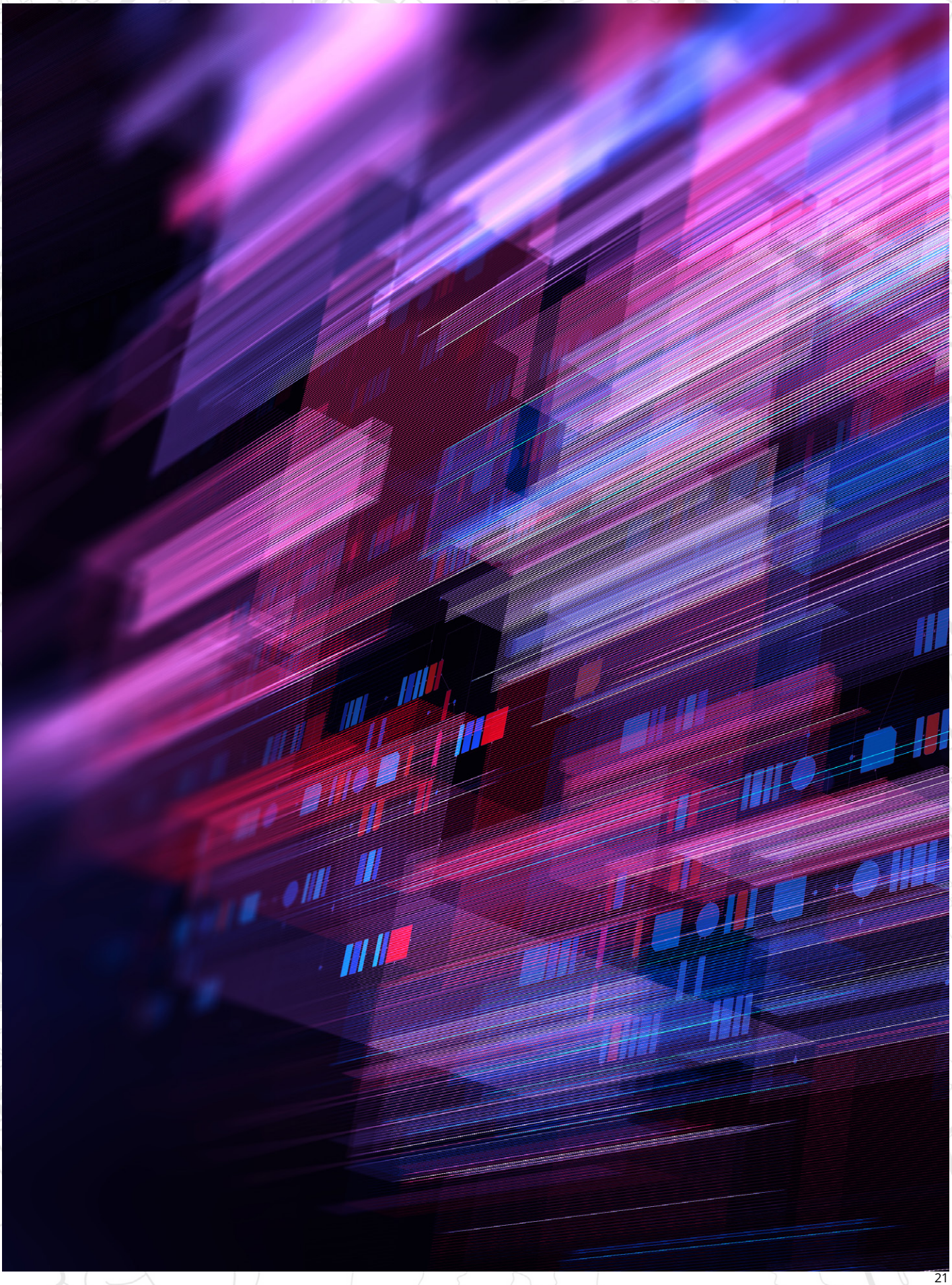


EXPLAINABILITY AND INTERPRETATION

ML, and the outputs generated by ML solutions, can be difficult to explain in simple or layman language. The application of ML requires robust safeguards that include building-in model explainability from the start, and performing regular model evaluation and retraining. To support this, Bank B developed a visualisation tool to present the interactions between various risk factors that contribute to the scoring of a TM alert, and Bank C requires its data scientists to provide a high-level summary that explains the ML outputs. Bank C referred to the importance of closely involving key AML stakeholders with any technical ML development activities.

TALENT CONSIDERATIONS FOR MACHINE LEARNING OPERATION

Banks B, C, and D all shared that the availability and capability of in-house technical resources was a key factor when assessing whether to develop ML solutions in-house, or engage a third-party vendor. Although in-house data scientists may seem to be a critical element, banks that do not have the necessary resources or expertise can still deploy third-party solutions that are customised to the bank's specific needs. The key is to have business users and other technical expertise within the bank who can effectively communicate their requirements and expectations of the model.



Case Study 3: Natural Language Processing for News Monitoring

BACKGROUND AND CONTEXT

Bank E has implemented a third-party platform to enhance its global news monitoring processes. The platform combines entity resolution with Natural Language Processing (NLP) capabilities to identify specific individuals alongside relevant topics and themes in open-source media information.

Many banks adopt a keyword search approach to news monitoring where articles are scanned for specific terms that relate to topics of interest, such as "crime" or "fraud" or "bribery". While often combined with matching of customer information to article contents, this approach is generally cumbersome, requiring manual effort to search for and review information. By using an NLP-enabled platform, Bank E set-out to more accurately identify risk exposures in media data, and focus the attention of its investigators on articles that are most likely to contain relevant information on its customers.

Bank E shared that the platform has significantly improved its risk detection timelines, and citing cases identifying previously unknown risks associated with customers, leading to some being subject to more enhanced monitoring (e.g. refined transaction monitoring thresholds).

"JOHN SMITH" – USING ENTITY RESOLUTION AND NLP TO ENHANCE NEWS MONITORING

To search for adverse media associated with a customer, an investigator would typically use a search engine to identify articles containing a combination of keywords and the subject's name or alias. Particularly for customers with common names (e.g. "John Smith"), and terms that carry ambiguity (e.g. "convict"), investigators are likely to be faced with largely irrelevant or misleading material.

Through entity resolution and NLP, unique entities can be identified across huge volumes of unstructured data – where information such as age, occupation, or nationality is used to identify different individuals. This capability can be leveraged to assess the likelihood that an article containing the term "John Smith" relates to "John Smith", the target. This enables banks to cast a wider net, and at the same time be more targeted in the information that is relevant to their customers.

DEPLOYMENT APPROACH

Bank E described its relationship with the vendor as a 'journey of co-creation' – where many features have been developed collaboratively since an initial PoC in 2017. This echoes the insights shared by early adopter banks in the 'Third-Party Vendor Relationships' section of the first Case Studies and Insights Paper: that banks should consider what a vendor relationship could look like across a multi-year time horizon. The co-creation relationship has not only allowed Bank E to ensure that the platform is tailored to its specific needs, but also helped the vendor to refine its product so that it can be more usefully deployed for others in the industry. This cross-industry sharing was also referenced by Bank D as a factor in its decision to engage a third-party vendor.

A key success factor cited by Bank E was that the vendor had physical presence in the region where its PoC was conducted, allowing the Bank to work closely with the vendor's technical support team, and identify and resolve issues at an early stage. Bank E shared that the PoC locations were selected on a risk-based approach – as they managed the Bank's highest-risk client portfolios – and to ensure that the Bank could assess the solution's adaptability to multiple languages and other local nuances.

DEFINING AND MEASURING SUCCESS

When discussing limitations and hesitations around adopting analytics-enabled media screening, rather than relying on more traditional processes, Bank E and its vendor shared that many decision makers often associate technology with offering 'zero-risk' solutions, and are discouraged when vendors acknowledge that products cannot possibly detect every single potential risk. Instead, focus should be placed on the extent to which existing processes are effective, particularly those that rely on manual trawling through vast quantities of information.

In an effort to objectively measure the impact of the vendor solution, Bank E and its vendor worked together to assess solution performance using both qualitative and quantitative metrics across large samples – rather than just focusing on false-positive rate or missed hit numbers.

Case Study 4: Analytics with a 'Single View of the Customer'

BACKGROUND AND CONTEXT

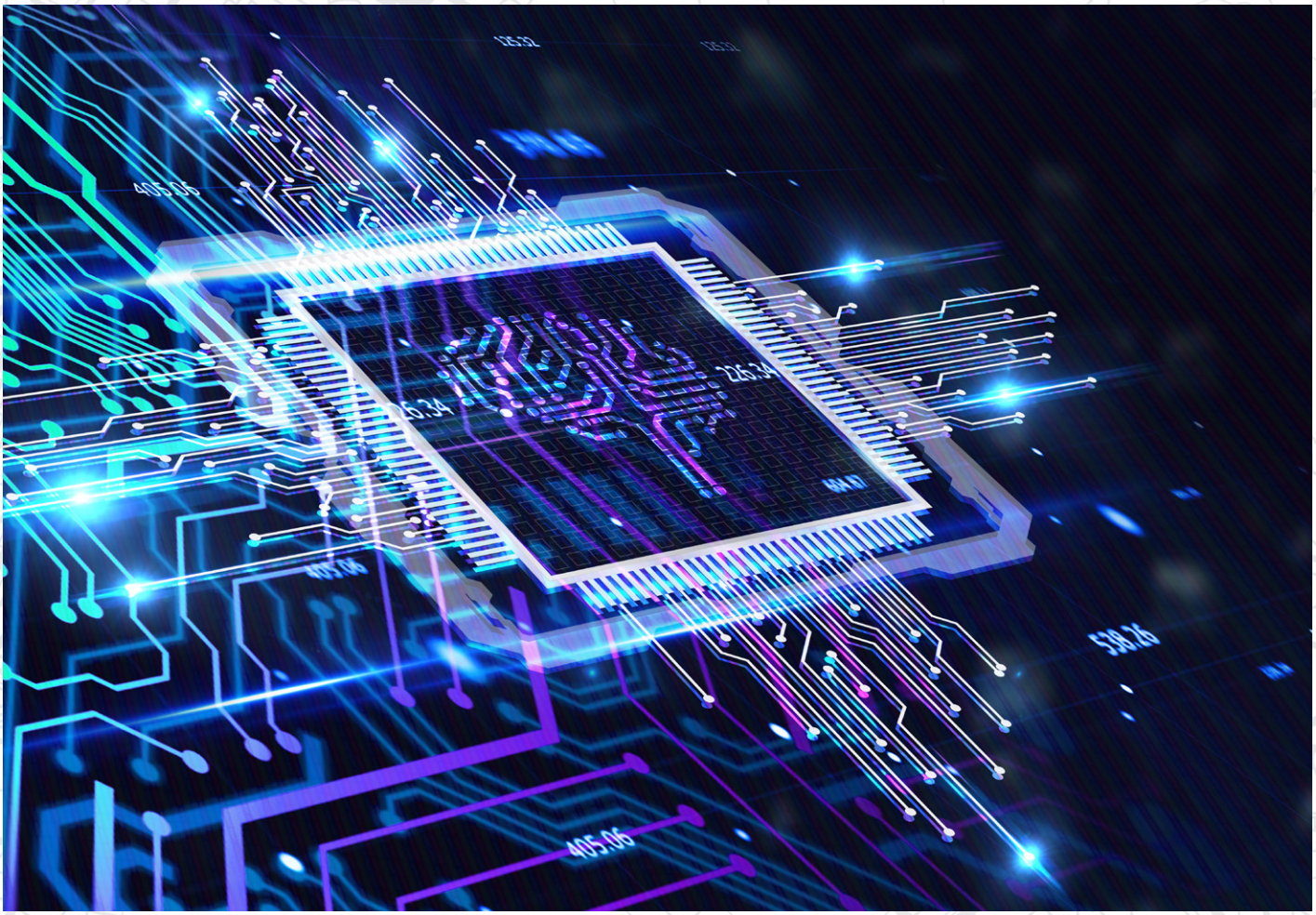
In the first Case Studies and Insights paper, one case study focused on the development of a centralised data repository, by a bank seeking to address inefficiencies in its downstream AML/CFT processes. Since then, many banks have indicated that they are pursuing the ability to form a 'single customer view' to uplift AML/CFT capabilities. And, as explored in this paper, banks looking to adopt solutions like ML will need to ensure that data is in a sufficient state of readiness in terms of quality and accessibility.

This case study builds on the theme of 'single customer view' by sharing how Banks D, E, and F are all leveraging their single customer view to enhance their AML/CFT capabilities.

THEMATIC AND INTELLIGENCE LED ANALYTICS

Bank E has a regional working group that conducts proactive and intelligence-led analysis to explore the impact of new and emerging threats. The working group regularly brings together representatives from the Bank's Financial Intelligence Unit and AML compliance team with data analytics specialists. Through developing a centralised data warehouse, the team has ready access to granular data on which thematic and deep-dive analysis can be conducted. Recently, in response to an urgent management request, the team performed analysis of payments and digital footprint information to assess the Bank's exposure to specific jurisdictions, and was able to provide an early response within 30 minutes. As part of a thematic review, the team also analysed payments data to identify potential connections between high-risk customers (including global PEPs) and other, non-high-risk individuals. This data-driven approach has proven to be an effective early risk indicator as part of Bank E's proactive risk management efforts.

Bank D has also developed a single customer view by implementing a centralised data lake that provides multiple end-users with ready access to data. Bank D's financial crime team retrieve granular data from the data lake to support their investigations work and thematic analysis. In the development journey, Bank D shared that a key challenge was the development of a single set of data definitions and standards as it migrated from siloed platforms to a single warehouse. To manage this process, Bank D set up a centralised data management committee that brings together representatives from different departments, including AML and compliance, as part of the Bank's ongoing data governance.



DATA-DRIVEN RISK PROFILING

Bank E developed a standardised Customer Risk Rating (CRR) framework to address the issue of inconsistent CRRs across its various global locations. During the development process, dynamic risk factors, including changes in customer behaviour and transactional patterns, were also included. Bank E shared that it was able to readily implement new dynamic risk factors as part of its CRR – and consider updates to these in future – thanks to its centralised data warehouse. Further, Bank E has been able to resolve disparate customer risk ratings across business divisions and booking centres through having a centralised and consistent dataset on which CRR is applied.

Bank F's ability to form a single customer view has underpinned their development of more precise customer segmentation, as part of TM. Various factors are taken into consideration including customer demographics, customer profile, and CRR. The segmentation of individual customers, for example, considers information such as the assets under management; for corporate customers, annual turnover is used to segment customers by size. Centralised access to customer data facilitates refinements to segmentation, leading to more optimal TM operations.

LEVERAGING CLOUD TECHNOLOGY

While Bank E has developed a centralised data warehouse for real-time data access, it is now considering migration to cloud-based infrastructure because of increased computational capacity, improved accessibility, and more flexible scalability compared with traditional storage solutions. Acknowledging that migration is a long-term effort, Bank E is looking to make progress through incremental efforts – including the deployment of 'micro-services' on cloud infrastructure, to support specific use cases.

What next? The convergence of Suptech and Regtech...

In 2019 we set out to develop a more effective AML/CFT approach for Hong Kong through modernising the HKMA's Suptech capability, and supporting the industry with Regtech innovation through various industry engagements, lowering adoption barriers and fostering stronger industry collaboration.

Looking back on the past four years, there are clear signs of progress. Further to Regtech adoption statistics shared in previous Case Studies publications, this paper demonstrates that more banks in Hong Kong are progressing well beyond the early stages of maturity and are – in some cases self-sufficiently – starting to deploy more sophisticated AML solutions such as ML.

That progress is in part thanks to collaboration by many stakeholders across the AML/CFT ecosystem. The work of FMLIT further proves the value of collaboration and information sharing with over 21,000 previously unknown mule accounts identified in 2022, followed by proactive actions by LEAs and banks.

Such collaboration will only become more central in future, as public-private partnerships and information sharing initiatives[9] are increasingly explored as we collectively aim to tackle the financial-crime challenges of tomorrow.

Despite the progress made, we must continue to improve our collective response to fraud and other financial crimes. The HKMA will continue to collaborate with the industry on information sharing initiatives, and transforming its own supervisory approach to better assess sector-level threats and share insights with the industry. At the same time, we expect all banks to commit to speeding up improvements to the capability of our AML/CFT ecosystem. These combined efforts will see greater convergence of Regtech and Suptech, and unlock greater potential for our collective response to financial crime.

Digital transformation is a continuous journey that requires ambition, collaboration, and new ways of working with talent and technology in the face of constantly evolving landscapes. The HKMA is committed to continuing its promotion and facilitation of AML Regtech to maintain the safety and stability of the financial system that we should all be proud to serve.

9. The HKMA supports the launch of bank-to-bank information sharing platform, June 2023 https://www.hkma.gov.hk/eng/news-and-media/press-releases/2023/06/20230620-5/

References

1. The Hong Kong Monetary Authority (HKMA) fosters a diversified ecosystem for Anti-Money Laundering and Counter-Financing of Terrorism (AML/CFT) Regulatory Technology (RegTech), November 2019.
   https://www.hkma.gov.hk/eng/news-and-media/press-releases/2019/11/20191122-4/
2. The Hong Kong Monetary Authority, AML/CFT Regtech: Case Studies and Insights, January 2021
   https://www.hkma.gov.hk/media/eng/doc/key-information/guidelines-and-circular/2021/20210121e1a1.pdf
3. The Hong Kong Monetary Authority, AML Regtech: Network Analytics, May 2023
   https://www.hkma.gov.hk/media/eng/doc/key-functions/banking-stability/aml-cft/AML_Regtech-Network_Analytics.pdf
4. The Hong Kong Monetary Authority: Feedback from Thematic Review of the Use of External Information and Data in Anti-Money Laundering and Counter-Financing of Terrorism (AML/CFT) Systems, April 2021
   https://www.hkma.gov.hk/media/eng/doc/key-information/guidelines-and-circular/2021/20210426e1.pdf
   https://www.hkma.gov.hk/media/eng/doc/key-information/guidelines-and-circular/2021/20210426e1a1.pdf
5. Established in May 2017, the FMLIT is a public-private partnership for information sharing among the HKPF, the HKMA and 28 banks
6. Hong Kong Monetary Authority and Hong Kong Police Force co-host sharing session with banking industry on anti-deception efforts, April 2023
   https://www.hkma.gov.hk/eng/news-and-media/press-releases/2023/04/20230421-7/
7. Opening Keynote Speech at Fraud and Financial Crime Asia Summit 2023, July 2023
   https://www.hkma.gov.hk/eng/news-and-media/speeches/2023/07/20230713-1/
8. The fourth Anti-Money Laundering Regtech Lab: supporting an agile, coordinated, and strategic response to digital fraud and financial crime, June 2023
   https://www.hkma.gov.hk/eng/news-and-media/press-releases/2023/06/20230607-5/
9. The HKMA supports the launch of bank-to-bank information sharing platform, June 2023
   https://www.hkma.gov.hk/eng/news-and-media/press-releases/2023/06/20230620-5/

Acknowledgements

This report was made possible thanks to the active participation of banks, Regtech vendors, and subject matter experts on AML Regtech. Their time, energy and invaluable insights are greatly appreciated.

Terms and Abbreviations

Term / Abbreviation	Disambiguation
AML	Anti-Money Laundering
CFT	Counter-Financing of Terrorism
CRR	Customer Risk Rating
FMLIT	Fraud and Money Laundering Intelligence Taskforce
HKMA	Hong Kong Monetary Authority
HKPF	Hong Kong Police Force
LEAs	Law Enforcement Agencies
ML	Machine Learning
NLP	Natural Language Processing
PEP	Politically Exposed Person
PoC	Proof-of-Concept
Regtech	Regulatory Technology
SVF	Stored Value Facility
STR	Suspicious Transaction Report
Suptech	Supervisory Technology
TM	Transaction Monitoring

HONG KONG MONETARY AUTHORITY
香港金融管理局

Hong Kong Monetary Authority

55/F Two International Finance Centre,
8 Finance Street, Central, Hong Kong

Telephone: (852) 2878 8196
Fax: (852) 2878 8197
E-mail: hkma@hkma.gov.hk

www.hkma.gov.hk

For more information, please contact us at aml@hkma.iclnet.hk

Deloitte.