Risk and Regulatory Outlook 2021

Impact of RegTech on anti-money laundering/terrorist financing with a focus on transaction monitoring and fraud detection

pwc

Impact of RegTech on anti-money laundering, terrorism financing transaction monitoring and fraud detection

Overview

Financial institutions (FIs) are facing an increasingly complex regulatory landscape with new challenges associated with compliance, risk management and reporting. Perhaps the proliferation of technology-driven financial solutions over the last decade have raised more concerns, as more institutions deploy them in different ways.

Increased adoption of mobile banking, innovations in payments and acceptability of cryptocurrency globally have resulted in a significant growth in transaction volumes. This increase in opportunities to do cashless and anonymous transactions has led to an increase in the overall volume of financial crime. Card fraud volume increased by 20% globally since 2017 to USD28.65 billion in 2019, as card transactions surged by 22% to USD420 billion during the same period [1].

Global losses from payment fraud tripled from USD9.84 billion in 2011 to USD32.39 billion in 2020 [2]. COVID-19 further exacerbated fraud, money laundering (ML) and terrorist financing (TF) activities amid:

- Surge in online payments during nationwide lockdowns led to a spike in Card Not Present “CNP” fraud.
- Increase in online real-time payments allowing fraudsters to have a level of anonymity, whilst perpetuating fraud.
- Job losses or financial desperation turning some individuals into money mules.
- Rise in wholesale banking fraud, as fake companies took advantage of supply chain and other operational disruptions caused by COVID-19 (e.g. Personal Protective Equipment, PPE, fraud)[3].
- Increased social media adoption leading to surge in social engineering and other cyber-criminal activities as people started working from home[4].
- Certain transactions flagged for suspicious activities missed being thoroughly investigated for clearance of doubt amidst added pressure of remote working.

To capitalise on this opportunity and assist FIs in keeping pace with the growing complexity of compliance and regulations, there are many solution providers in the RegTech space today, each with their own unique spin on the proposition they advocate. Moreover, the industry has made use of advanced technologies, like machine learning, blockchain, Natural Language Processing (NLP) to list a few. As a result, RegTech now sits at the core of future of compliance, and FIs are increasingly becoming heavily reliant on it.

In this article, we aim to provide a perspective and raise awareness around selection and deployment of RegTech solutions safely by FIs to deal with anti-money laundering (AML), countering the financing of terrorism (CFT) transaction monitoring and fraud detection in the financial services industry.

1 The Nilson report December 2020/Issue 1187
2 https://www.merchantsavvy.co.uk/payment-fraud-statistics/
3 https://www.natlawreview.com/article/ppe-fraud-rise-during-coronavirus-pandemic
4 https://www.aarp.org/money/scams-fraud/info-2020/social-media-scams-spike-pandemic.html

Regulatory developments

Acknowledging that technology and AI-driven RegTech will be a core component of compliance in the near future, regulators are working towards creating a conducive adoption environment. Regulators are also incentivising the adoption and advancements within RegTech, albeit slowly.

Global scenario

Globally, regulatory mandates have evolved with the emergence of RegTech and the proliferation of fintech solutions among other developments. Examples are:

Hong Kong Monetary Authority (HKMA) launched the Fintech Supervisory Sandbox in 2016[5]. It allow banks and their partnering technology firms to conduct pilot trials of their fintech initiatives involving a limited number of participating customers without the need to achieve full compliance with the HKMA's supervisory requirements.

Dubai Financial Services Authority launched the Hive accelerator initiative in 2017, which aims to assist Fintech and RegTech solution providers with a testing sandbox for innovations[6].

Similarly the Financial Conduct Authority (FCA) in the United Kingdom and Swiss Financial Market Supervisory Authority (FINMA) in Switzerland have set up sandboxes for testing innovations in a protected environment[7].

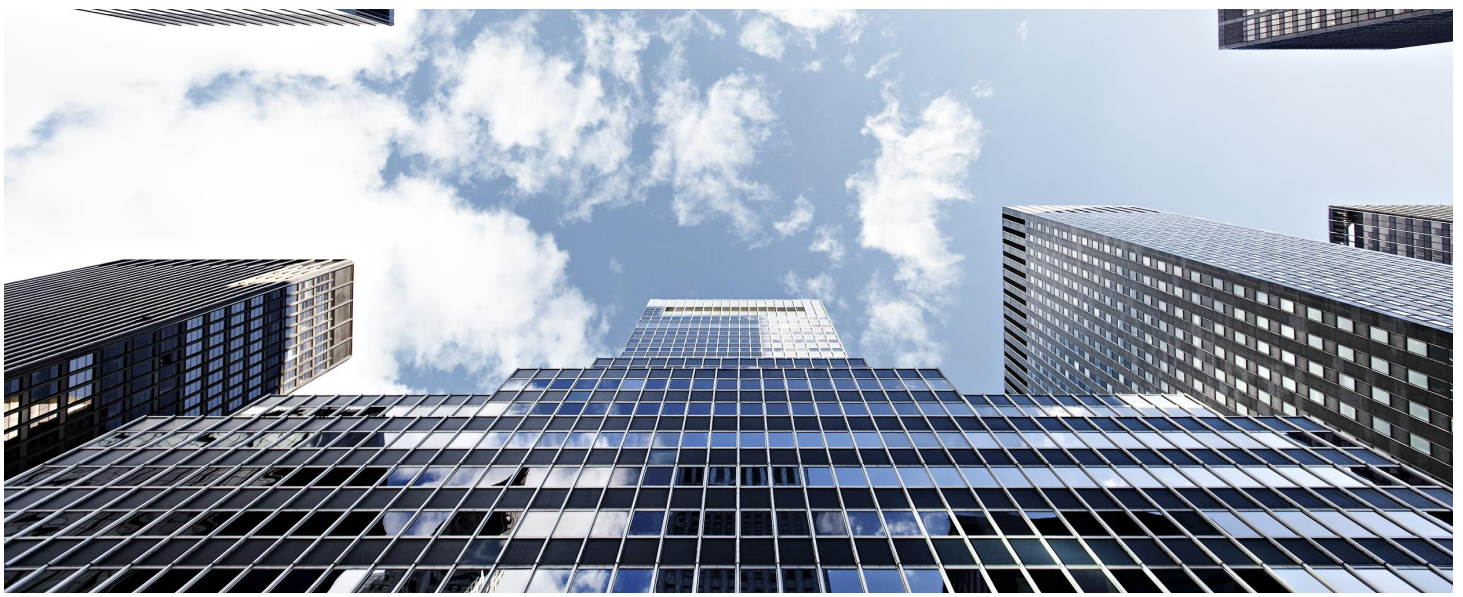
In the midst of the current lack of global coordination towards the issue, the Financial Action Task Force (FATF) has expressed its strong support for responsible financial innovation. This is in line with the FATF Standards, and exploration of opportunities that new financial and regulatory technologies present for improving the effective implementation of AML/CFT measures.

It is worth noting that this support in its current form is non-binding and needs mutual cooperation amongst different countries to effectively deter financial crime. Also, these incipient regulatory mandates in their current form and view do not capture all the complexities of financial crimes and the application of new AI solutions to tackle the complexities.

Southeast Asia

Most regulators in Southeast Asia have not yet fully grasped these complexities to provide guidelines or regulations to govern the RegTech space. Only the Monetary Authority of Singapore (MAS) has been making some headway in this regard.

Since 2016, MAS has been proactively employing fintech to streamline and enhance its regulatory capacity. MAS launched an accelerator scheme Sandbox Express in August 2019, for enhanced market testing of innovative financial products and services. Under this scheme, applicants can commence market testing within 21 days of applying and approval by MAS[8].



5 https://www.hkma.gov.hk/eng/key-functions/international-financial-centre/fintech/fintech-supervisory-sandbox-fss/
6 https://www.theasianbanker.com/updates-and-articles/regulators-have-%E2%80%98upped-their-game%E2%80%99-in-ways-that-would-have-been-considered-to-be-very-%E2%80%98un-regulator-like
7 https://www.juliusbaer.com/de/intermediaries/business-navigator/regulation/how-the-financial-industry-is-using-regtech-to-its-advantage/
8 https://www.mas.gov.sg/news/media-releases/2019/mas-launches-sandbox-express-for-faster-market-testing-of-innovative-financial-services

Key industry observations

FIs have been conducting proof of concepts to test the efficacy of adopting AI/machine learning-based and blockchain RegTech solutions for their compliance needs and in certain cases, replacing their existing detection and monitoring systems with these RegTech solutions. Nonetheless, we observe:

1. Lack of reg in RegTech

FIs perform risk assessments to assess their exposure via their customers, channels they operate through and the services they offer. Our observations on over 100 solutions in the market indicate that very few of these solutions have regulatory intellectual property in two forms i.e. risk assessment-based typologies and direct correlations to applicable regulatory requirements within the detection solution. For an FI to address all the risks it is exposed to and all typologies it needs to monitor, the majority of solutions available are toolboxes which need a fair amount of trial and error and significant time to deliver tangible results. Apart from getting rid of false positives by legacy solutions, which is the first improvement seen, on-going incremental improvements are slow.

Along with the need to be regulatory-driven and incorporate domain expertise within the RegTech space, there is a glaring gap due to the absence of inter-bank and intra-bank intelligence sharing. It limits the FIs ability to deter ML/FT and fraudulent transactions. The implementation of an AI solution without proper planning and regulatory direction only adds to challenges faced by compliance and is actually a step back from incumbent solutions in the long run.

2. Unaligned expectations and lack of clarity in the use of AI

FIs are not discerning of the solutions they are investing in and continue to invest without extensive research or knowledge of the solution to meet their goals. Without understanding of the business goals and the return on investment from AI solutions, the investment in AI is futile and in some cases underperforming compared to the traditional rule-based solutions.

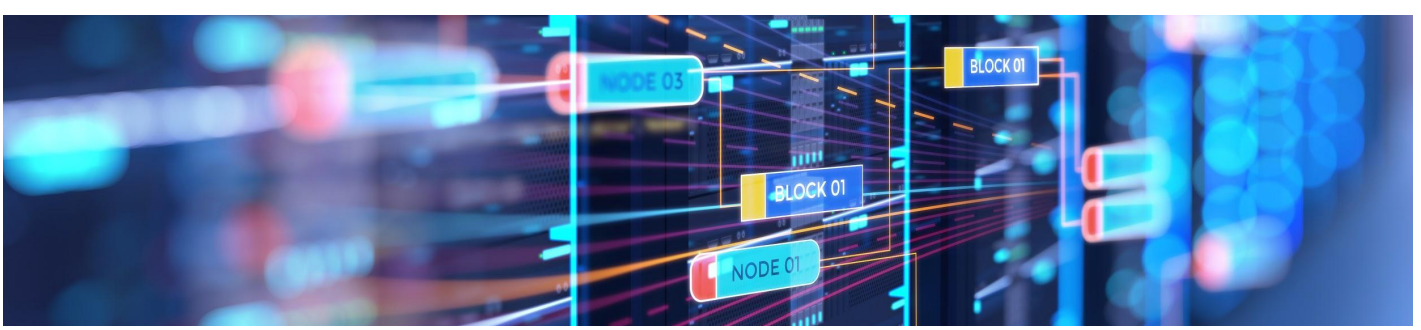
FIs have now turned their attention to buying AI-based solutions to top their traditional rule-based systems, primarily to optimise all alerts raised by their traditional systems. However, if the goal of the solution is short term such as alert optimisation, it can be achieved through open source and cloud based technology and can be built in-house without spending money on procuring expensive software from vendors. If the goal is beyond alert optimisation, then knowing how to assess further capabilities is critical.

With the growth of real-time payments and increasing complexity of customer behaviour, traditional rule-based systems are increasingly becoming obsolete due to their inability towards identifying ‘unknown unknowns’ and detect complex patterns. The high volume of false positive alerts generated by rules-based systems is also contributing to compliance overload within banks. But despite the flaws, most banks continue to use rule-based systems due to their high degree of familiarity with such systems. There is a better use of AI than just alert optimisation that can be done in other more cost effective ways.

3. Lack of adequate transparency and explainability

RegTech solutions are being plagued by the lack of interpretability and explainability in their results/ outcomes. Interpretability is the extent to which a cause and effect can be observed within a system, to which one can predict what is going to happen, given a change in input or algorithmic parameters. Explainability is the extent to which the internal mechanics of a machine or algorithm can be explained in human terms. Both interpretability and explainability of results are equally important to ensure transparency in a solution.

Most solutions are either sufficiently interpretable or explainable but not both. This poses a challenge to FIs since the alerts and predictions generated by such solutions are either not interpretable or explainable or both to the business users and investigators who interact with these alerts. Hence, it does not supplement the current information available to alert investigators to adequately investigate and dispose of an alert raised by the FI's detection solution. AI solutions based on blackbox models without clear transparency will not withstand the scrutiny of regulatory compliance.



Outlook for 2021 and recommendations

Outlook #1: Growing need for domain expertise and shared learnings in RegTech

Despite advances in technology and machine learning, it would take some time before regulators are able to establish the regulatory framework or even provide recommended guidelines. Hence, RegTech solutions will continue to be limited by the lack of regulatory direction and domain expertise within AML/CFT and fraud, impacting the ability of RegTech solutions to maximise the potential of AI and technology for efficient monitoring.

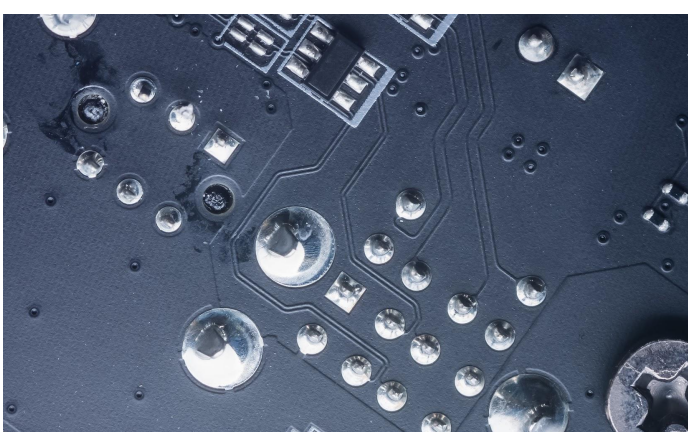
Recommendations: To help banks mitigate all known financial crime risks, new solutions must be developed with regulatory requirements in mind and supplemented with extensive typology libraries aligned to regulatory requirements. FIs need to identify and think through:

- How much verticalisation they need to build into 'toolbox' solutions?
- How does the application of artificial intelligence solve their business problem?
- How to set adequate coverage within the solution?
- Explainability and interpretability metrics from day one of implementation.

For FIs to readily identify typologies as they evolve across regions and other FIs, there is a need for:

- Shared learnings and improvements across all implementations of a RegTech solution.
- Respect confidentiality of the shared information and adhere to applicable data sharing laws.

FIs should also seek expert and independent help from consultants who see the industry as a whole and have wider RegTech experience.

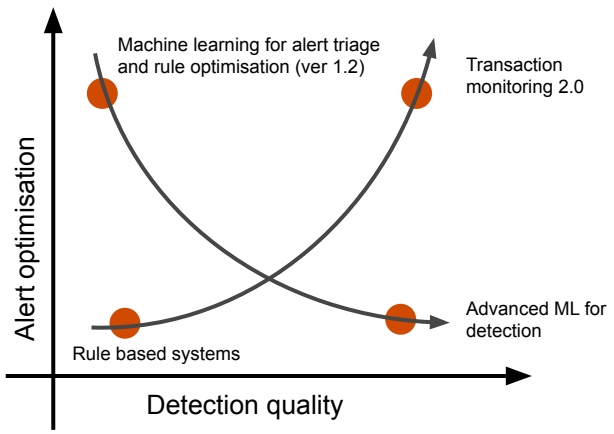


Outlook #2: Banks need to move to transaction monitoring 2.0

Banks will continue to augment their existing rule-based systems (to a 1.2 version) with machine learning to optimise alerts generated by the rules and Robotic Process Automation (RPA) for the disposition of low-quality alerts as it is a low hanging fruit.

But these measures are short-term and will not address the underlying issues of inefficient detection in monitoring systems. Transaction monitoring 2.0 must address the issue of high false positive rates and complex pattern detection at its roots by improving detection through machine learning. Hence, while banks may think they are moving to 2.0 version of transaction monitoring systems, they are just upgrading to version 1.2 (Exhibit 2).

Exhibit 2: Transaction monitoring 2.0 provides the highest alert optimisation as well as detection quality



Recommendations: While augmenting rule-based systems with RegTech may help in reducing some operational overhead associated with addressing alerts, banks need to expand the currently limited use of machine learning to improve detection. As purchasing a vendor solution to just optimise alerts is expensive, FIs can consider more cost effective options such as in-house solutions built using open source technology.

By improving the detection capability of AML/CFT transaction monitoring systems, FIs can identify complex patterns, generate better alerts and improve overall alert productivity which will benefit them in the long run. Thus, FIs must focus on adoption of transaction monitoring 2.0 as means to achieve the long term goal of improving detection and scaling up the level of anomaly detection instead of limiting the use of machine learning to optimise alerts generated by legacy systems.

Outlook #3: Growing misalignment between expectations from AI and its ability to deliver

As the AI-based solutions get popular, there will be a growing misalignment between expectations from AI solutions and compliance needs. This confusion may further exacerbate if banks rely only on RegTech vendors and treat AI-based solutions as the silver bullet to tackle all their compliance issue.

Recommendations: FIs need to establish certain foundational structures to enable use of AI solutions e.g. development of data lakes to store information for the function.

FIs should also consult the experts on the process of developing an AI/machine learning solution for the organisation and seek guidance on steps to be taken in order to meet the desired objectives.

RegTech solutions need to dispense and debunk the confusion surrounding AI and machine learning and help FIs understand the process of incorporating machine learning/AI based advanced solutions into their monitoring and detection operations.

AI is transformational, so FIs need to think of how to move towards next generation transaction monitoring, fraud, sanctions or KYC, and not try to fit AI on top of an outdated and obsolete operating financial crime model.

Outlook #4: Adoption of RegTech implementations will be required to be followed with changes in operating models

While FIs are moving towards the use of technology and AI to improve their monitoring and surveillance functions, traditional systems will get replaced by newer RegTech solutions. This inclination towards new RegTech solutions will only increase in the future as payments get complex and real time.

Recommendations: As FIs move towards new RegTech solutions and replace traditional systems, they must also supplement this change with changes in operating models. Implementations of RegTech solutions must be followed by changes in the operating model. These solutions should not be plugged into the traditional operating models to maximise efficiency gains.

Outlook #5: Responsible use of AI will become more pertinent

With the need for interpretability and explainability within RegTech solutions being mandated by both regulators and industry experts, the responsible use of AI is to increasingly take centre stage. This responsible use of AI which is also being encouraged by regulators can be thought across three pillars: ethics and regulations; robustness and security; and bias and fairness.

Towards ethics and regulations, RegTech vendors and FIs will take strides towards AI solutions that are morally responsible while also legal and ethically defensible. While we see a general awareness of responsible use of AI, the confusion around explainability of AI models and interpretability of results still persists. Any implementation of AI should be transparent enough to stand the test of regulatory compliance.

Recommendations: For the principles of responsible use of AI to become actionable, FIs need to:

- Contextualise principles into specific guidelines for front-line staff, and
- Monitor regulatory environment and understand how emerging regulations will shape future business practices.

To be effective and reliable, the implemented AI systems should be:

- Self-aware - with a built-in ability to detect and correct faults and inaccurate or unethical decisions.
- Secure - with security protocols built into the AI development process from the start and encompassing all AI systems, data, and communications to prevent catastrophic outcomes of AI data or systems being compromised or “hijacked”.
- Safe - AI systems must be safe for the people whose lives they affect, whether they are users of AI or the subjects of AI-enabled decisions.

Significant strides need to be made towards robustness and security and bias and fairness in order to drive transparency within AI solutions to the desired and required levels for meaningful adoption of such solutions towards fighting financial crime.

Solutions will also need to address the issues of bias and fairness by recognising that while there is no such thing as a decision that is fair to all parties, it is possible to mitigate unwanted bias and achieve decisions that are fair under a specific and clearly communicated definition in the design.

#RiskandRegs

Contact

Nitin Parmar
Partner
South East Asia Consulting
PwC Singapore
nitin.parmar@pwc.com