axis
TRUSTED FIRST.

Compliance Automation: A new dawn in the financial services sector

by **Mohammud Nabeel Khodabux**
Compliance Executive

There is a new dawn in human civilisation: humankind and robots have joined hands in bringing down Covid-19. The contribution of robots in the context of the pandemic is widely acclaimed. They have literally been at the epicentre of enemy territory by serving food to sick patients, disinfecting contaminated areas and monitoring sanitary protocols. Technology has indeed radically changed our lives and the way business is conducted. Consequently, it seems that failure to innovate is akin to guaranteed failure. As criminals find new ingenious ways to launder money or finance terrorists, compliance professionals have the duty to outsmart them. Fortunately, with the help of robots and intelligent automation, a possible state-of-the art solution has been proposed, to the potential satisfaction of all the relevant stakeholders.

In the Mauritian landscape, laws are becoming more and more stringent on financial institutions especially in terms of transactions monitoring. For instance, when carrying out any transaction, it is paramount to watch out for 'Designated and Listed Parties' under the United Nations (Financial Prohibitions, Arms Embargo and Travel Ban) Sanctions Act 2019. In addition to this, regulators have considerably increased their inspections. Hence, compliance practitioners are not allowed to fail in their day-to-day operations. Failing which, the Board, the Compliance Officer and Money Laundering Reporting Officer may be held liable, with terrible consequences. In practice, to be flawless, this requires a massive workforce in the compliance department to carry out daily screenings, risk assessments, verification of KYC documents, whilst adopting a risk-based approach, in view of avoiding the unintended consequences of de-risking and financial exclusion. This, therefore, begs the question: what could be a more efficient and effective solution to enhance compliance functions in a way that could meet the expectations of the financial institution, regulator and client?

The answer could be in the setting up of a digitalised AML-CFT infrastructure. In an interesting document entitled "Opportunities and challenges of new technologies for AML/CFT" published in July 2021, the international AML-CFT standard setter, the Financial Action Task Force (FATF) has raised awareness on the vast potentialities and benefits of investing in digital solutions. Accordingly, Artificial Intelligence and its different subsets (machine learning, natural language processing) can be of

great help both to the regulator and to the private sector. For the regulator, investing in cutting-edge RegTech and SupTech would result in more live (real-time) monitoring and facilitate flow of information between key actors, thereby improving supervision of licensees. As for a financial institution, by operating its systems, this could result in more efficacious risk assessments, onboarding of customers and promote overall good governance practices. In relation to clients, at onboarding stage, digital identity mechanisms could cater for non-face-to-face verification of customers' identity with greater accuracy. Additionally, eliminating the trouble of having to carry multiple customer due diligence documents. As a cautionary note, the FATF has advised against over-reliance on technological systems. Instead, human input is a sine qua non to assess any possible residual risks and apply mitigating measures.

However, compliance automation may still pose security and privacy concerns for technophobes. On this point, it can be argued that Mauritius as an international financial centre has the appropriate ecosystem to enable compliance automation to bloom in a safe and conducive environment for three reasons:

01 AML-CFT laws act as a safety valve in the digitalisation of compliance services

There are many impressive benefits in using digital products for everyday compliance functions. To begin with, compliance automation produces more results than a whole compliance team altogether could. For example, automated ongoing screening enables substantially more daily monitoring to be conducted on a 24/7 basis. Such technological prowess makes it difficult for human beings to compete with. This would prove highly beneficial for a financial institution to save more money than having to recruit an enormous number of employees to carry out screenings on a 24/7 basis.

Recently, during lockdowns, financial institutions and clients have experienced considerable difficulties to manually verify the authenticity of customer due diligence documents because of mobility restrictions. In this regard, using software to electronically verify documents has proved particularly helpful instead of having had to physically go to a lawyer's office for this purpose.

Furthermore, it is an undeniable fact that human beings are bound to commit mistakes. However, since compliance practitioners cannot afford to make mistakes, technology offers a viable option. This is because technology does not have tough choices to make based on subjective criteria. Nor is technology ever affected by any emotional charge to cloud its judgment. Technology thus limits human error.

Yet, is technology always faultless? It is worth highlighting that before using any FinTech product, a financial institution should scrutinize it to become aware of any lacuna. By virtue of section 17(3) of the FIAMLA and Regulation 19(1) of the FIAML Regulations 2018, a financial institution should identify and assess the money laundering and terrorism financing risks that may arise regarding the use of new or developing technologies for both new and pre-existing products, as well as manage and mitigate such risks. The choice of technological product to be used should also go through an assessment that takes into account the operational, reputational and legal risks. This assessment exercise should provide comfort to technophobes by enabling the financial institution to become aware of the strengths and limitations of the digital product; and eventually to take mitigating steps to resolve these deficiencies. This means that despite placing reliance on technology, human alertness is still essential.

02 The Cybersecurity and Cybercrime Act 2021 (CCA) guards the Mauritian cyberspace from cyberthreats

This Act has repealed the former Computer Misuse and Cybercrime Act 2003. The differences between the former Act and the CCA is that the latter has criminalised additional offences in order to comply with the latest provisions of the Budapest Convention on Cybercrime. This means that based on the latest trends and patterns of cybercrime, the CCA is an up-to-date legislation that should be resilient against any prevailing form of cybercrime. Moreover, under section 22 of the CCA, any perpetrator engaged in criminal activity involving a Critical Information Infrastructure would be subject to increased penalty for greater deterrence.

03 The privacy rights of data subjects would be protected under the Data Protection Act 2017 (DPA)

Insofar as data subjects' personal data are being processed, financial institutions, in their capacity as data controllers should ensure that any compliance automation product complies with the provisions of the DPA and the General Data Protection Regulation (where applicable). Some of the relevant statutory provisions include but are not limited to the lawful basis of processing their personal data, the security of processing, whether there will be any automated individual decision making or transfer of data abroad, the processing of special categories of personal data and all the sections related to the rights of data subjects. Under section 28 of the DPA, one of the lawful conditions behind the processing of personal data is that the data subject 'consents to the processing for one or more specified purposes'. In this light, the rights of data subjects are adequately safeguarded since the latter can also withdraw their consent whenever they want, under section 24(2) of the DPA.

> "In conclusion, failing to innovate, is planning to fail."

A more sustainable future for compliance services is digital compliance. This new dawn appears to be more promising for the regulator, the client and the financial institution. Besides, Mauritius has the right climate for it to blossom considering its current legislation in place. All that is required is a little bit of trust in technology and striking the right balance between human input and technology. Steve Jobs has well put it: "Innovation distinguishes between a leader and a follower". There is no doubt that, in order to remain competitive in the financial services sector, innovation is a must.

by **Mohammud Nabeel Khodabux**
Compliance Executive