Ongoing due diligence and why it is important for regulated businesses in Australia and New Zealand

illion

The compliance landscape has evolved significantly during the past decade. Regulations in major financial centres across the globe were amended and their scope was expanded to include new reporting organisations and more persons and businesses that are subjected to anti-money laundering (AML) and counter-terrorist financing (CTF) checks.

Criminals "are keeping the pace" by devising complex schemes in their attempts to disguise the unlawful activities they engage in. This is why, know your customer (KYC) processes have become extremely important for money-processing organisations. They must take appropriate steps to ensure that offenders are not using their systems to launder illegitimate funds or finance offences like terrorism or proliferation of weapons of mass destruction. Regulators are aware of the present risks and show no lenience towards reporting businesses that have weak compliance controls, particularly those that demonstrate "wilful blindness" and deliberately violate their obligations.

The notion that financial institutions are required to perform customer due diligence (CDD) is not new. It is incorporated in the Financial Action Task Force (FATF) Recommendation 10 which stipulates that this principle should be set out in law. CDD measures consist of the following elements: identifying the customer and verifying their identity; identifying the beneficial owner and the corporate structure of legal entities; understanding the purpose and nature of the customer's business relationship; and conducting ongoing due diligence on the relationship to ensure that the customer information is up to date, especially for high-risk clients.[1]

FATF recommendations are not mandatory, however, they are considered the golden standard for AML/CTF compliance and many countries have integrated them in their national legislation either fully, or partially. Lawmakers and enforcers have emphasised on the importance of ongoing monitoring because reporting organisations tend to overlook it. This is not surprising because it is a time- and resource-consuming effort that requires knowledge in multiple areas and overcoming state-endorsed non-transparency in many jurisdictions whose economy is based on financial and corporate secrecy.

Australia and New Zealand are no exceptions.According to Australia's Anti-Money Laundering and Counter-Terrorism Financing Act (2006), a reporting entity must monitor its customers in order to ensure that it does not facilitate or participate in money laundering or financing of terrorism (s 36 of the Act).[2] Equally, The Anti-Money Laundering and Countering Financing of Terrorism Act (2009) of New Zealand stipulates that "a reporting entity must conduct ongoing customer due diligence and undertake account monitoring" (Section 31). The former includes regular review of customer information and taking into consideration the details collected at the onboarding stage and the risk level involved.[3]

Therefore, CDD is not a one-off event. Risks may change over time because people, goods and services move fast in today's globalised economy, sometimes making it very difficult even for crime-stoppers to keep track. As part of their risk assessment, reporting entities are required to identify the inherent risks associated with their business and adopt adequate measures to mitigate and manage them.

1 https://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/fatf%20recommendations%202012.pdf
2 https://www.legislation.gov.au/Details/C2020C00362
3 https://www.legislation.govt.nz/act/public/2009/0035/latest/DLM2140875.html

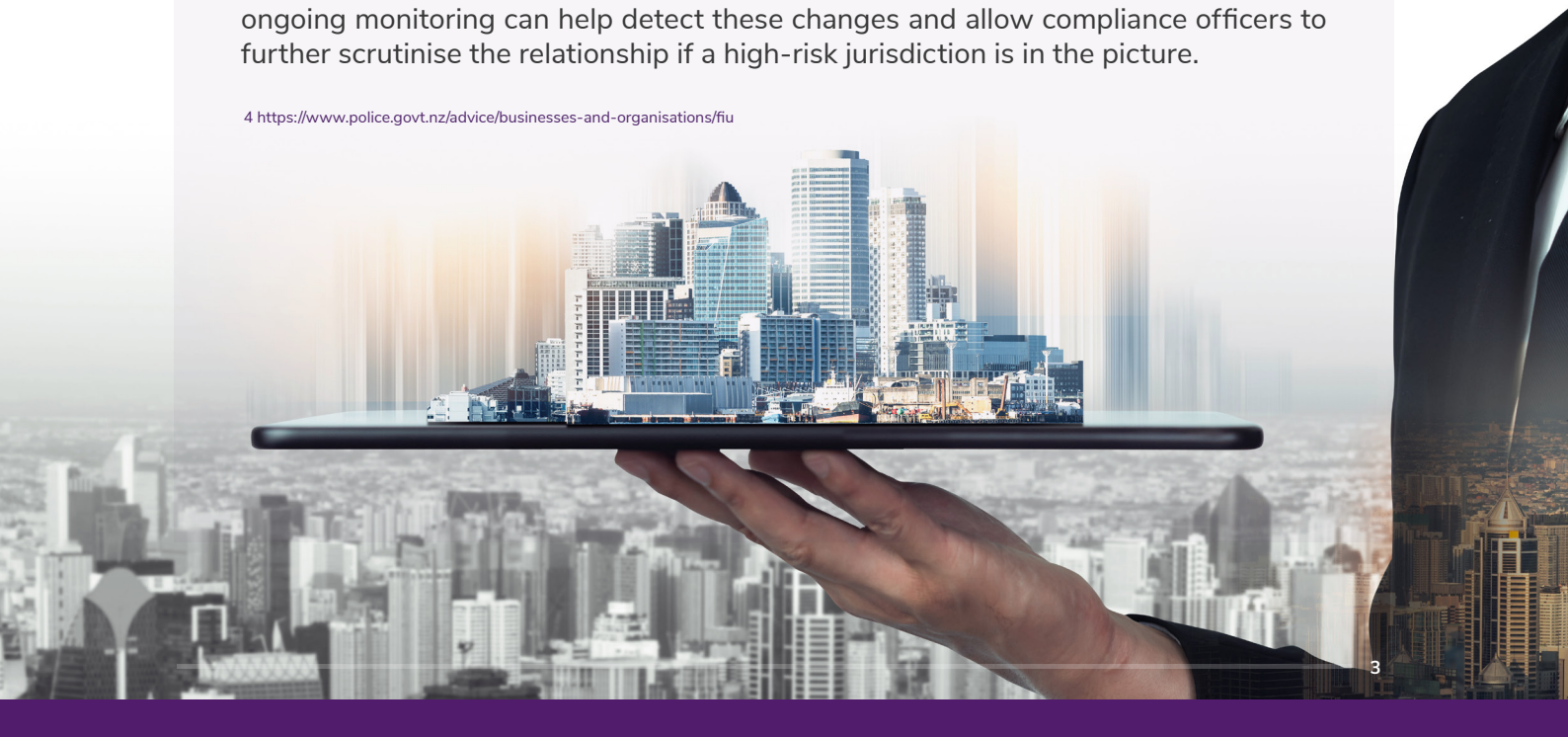
Naturally, client and geographical risks are the elements of the inherent risks that are among the most dynamic ones.

Client information can become old-dated at any time due to an array of reasons – people change their marital status, pursue different career opportunities and their occupation and income can vary. ID documents expire or may be stolen, and contact details may stop being valid too. All these details are of essential importance to reporting organisations because they let them know not only who their clients are but also what they do and ultimately – what can be expected from them. The latter will help identify any atypical behaviour that may be a red flag for wrongdoing, which has to be reported to the relevant financial intelligence unit, in the case of Australia and New Zealand – AUSTRAC and the FIU which sits within the Financial Crime Group framework and is a structure within the New Zealand Police.[4]

Another important step of the CDD process, which should take place at the establishment of the relationship, but also on an ongoing basis, is running client names against politically exposed persons (PEP), sanctions and regulatory lists and checking publicly available media stories for information about involvement in criminal activities and violations of international and local norms. Considering the many armed conflicts, the political instability and the economic confrontation between major and smaller players across the globe in the past decade, these details can change literally overnight. A person may fall asleep as a wealthy entrepreneur and wake up in the next morning as an individual investigated for bribing foreign officials and trying to launder their illicitly obtained funds through offshore corporations. A prominent politician may end up in a terrorist or sanctions list because his country is at odds with another nation.

Geographic risk is also an important component of inherent risk. The challenge is with non-transparent jurisdictions where secrecy laws provide anonymity to companies and individuals that may be involved in illegal activities. Their detection is very difficult and access to important details like shareholding structures, beneficial owners and directors are not accessible even for investigators. Therefore, reporting entities have to obtain information about the location, in which their clients reside and do business, and ensure that whenever transactions originating or passing through risky jurisdictions occur, they are duly monitored and reported when suspicions arise. Since people move addresses all the time, as do companies, albeit less frequently, ongoing monitoring can help detect these changes and allow compliance officers to further scrutinise the relationship if a high-risk jurisdiction is in the picture.

4 https://www.police.govt.nz/advice/businesses-and-organisations/fiu



This principle has also been confirmed by AUSTRAC, which states that AML programs should consist of two parts: Part A, which must include processes and procedure to help reporting entities identify, mitigate and manage the ML and TF risks they may face; and Part B, which is focused on the measures for identifying customers and beneficial owners of corporate clients, including those that are PEPs.

Ongoing customer due diligence (OCDD) systems and controls are a mandatory element of Part A and are in place "to make sure information collected about a customer or beneficial owner is reviewed and kept up to date, and to determine whether extra information should be collected and verified. OCDD includes having transaction monitoring and enhanced customer due diligence (ECDD) programs".[5]

Even though regulated companies are not required to ascertain whether a crime has been committed by the clients, nor investigate the crime itself, they are expected to apply KYC procedures and ongoing due diligence, and to monitor transactions in order to prevent being unintentional accomplices in money laundering and terrorism financing activities.

What many financial institutions in Australia and New Zealand do, however, is limited only to the checks at the onboarding stage. These organisations tend not to put efforts to keep their books up to date, especially for commercial clients, which exposes them to compliance, regulatory, legal, operational, financial and reputational risks that are be difficult to remediate. It is not surprising then, that regulators in Australia and New Zealand have taken enforcement actions against a list of companies that did not keep up with their obligations. In September 2020, Sidney-headquartered Westpac agreed to pay the record 1.3-billion-Australian-dollar penalty for having committed over 23 million contraventions of the AML/CTF Act, including for ongoing customer due diligence failures.[6] On 20 June 2018, a A$700-million pecuniary penalty was imposed on the Commonwealth Bank of Australia (CBA) for similar violations, among them non-compliance with s 36 of the Anti-Money Laundering and Counter-Terrorism Financing Act.[7] In 2017, gaming company Tabcorp, had to pay A$45 million for AML/CTF deficiencies. Paul Jevtovic, AUSTRAC's chief executive officer at the time, stated that Tabcorp's "money laundering and terrorism financing function was at times under-resourced".[8] One of the identified deficiencies was that "Tabcorp's written EDD program did not include appropriate systems and controls to determine whether to re-screen employees who were transferred or promoted to certain positions".[9]

5 https://www.austrac.gov.au/business/how-comply-guidance-and-resources/amlctf-programs/amlctf-programs-overview
6 https://www.austrac.gov.au/sites/default/files/2019-11/20191120%20Westpac%20Concise%20Statement%20FILED%2019008953.pdf
7 https://www.judgments.fedcourt.gov.au/judgments/Judgments/fca/single/2018/2018fca0930
8 https://www.abc.net.au/news/2017-03-16/tabcorp-fined-$45-million-for-breaching-money-laundering-laws/8360164
9 https://www.judgments.fedcourt.gov.au/judgments/Judgments/fca/single/2017/2017fca1296

In New Zealand, regulators like the Department of Internal Affairs, are taking enforcement actions not only against corporate entities, but also against the persons who run them, regardless of whether the company is small or large. One such example is the case from July 2020 against Auckland-based money remitter OTT Trading Group Limited (OTT) and Christchurch-based money remitter, MSI Group Limited (MSI) that were fined NZ$3.1 million and NZ$4.485 million, respectively, for AML/CTF breaches, including for failing to conduct customer due diligence and monitor their clients. MSI had never submitted an annual AML/CTF report.[10] The judgement followed restraining injunctions against three individuals associated with OTT and MSI from May 2020. One employee was banned from occupying the position of a compliance officer of any reporting entity, and the respective directors of OTT and MSI were restrained from serving as senior managers of any reporting entity or engaging in any business activity that would make them a reporting entity under the AML/CFT Act.[11]

The examples above show that the consequences for non-compliance are multifaced and setting the risk tolerance high may not be the best strategy for reporting organisations. The abuse of the financial system for illegal purposes harms communities, undermines legal businesses, and tarnishes the reputation of those countries that do not do enough to counter it. This is why, by maintaining a comprehensive AML/CTF program that follows the letter of the law, obliged entities will not only protect themselves, but will also contribute to a safer environment which is beneficial for them, their clients and the state.

How can illion help?

illion has some of the most advanced and sophisticated data systems in Australia and New Zealand to help organisations navigate through the maze of rules and regulations and protect them from unintended breaches.

illion has demonstrated experience and expertise in the financial sector, with insights and knowledge of systems, data, processes and people.

illion can help companies build risk protection into their normal operations, ensuring the delivery of a successful AML compliance risk management program.

Find out more at:

illion.com.au

illion.co.nz

10 https://forms.justice.govt.nz/search/Documents/pdf/jdo/be/alfresco/service/api/node/content/workspace/SpacesStore/8fafe951-00a0-413b-9a4a-3d2479f53ff5/8fafe951-00a0-413b-9a4a-3d2479f53ff5.pdf

11https://forms.justice.govt.nz/search/Documents/pdf/jdo/61/alfresco/service/api/node/content/workspace/SpacesStore/7105e592-f145-4aa9-9ea0-6b16ed3f2a5b/7105e592-f145-4aa9-9ea0-6b16ed3f2a5b.pdf

About illion

illion is the leading independent provider of trusted data and analytics products and services in Australasia, with the company's consumer and commercial registries representing a core element of Australia and New Zealand's financial infrastructure.

We leverage consumer and commercial credit registries, which comprise data on over 24 million individuals and over 2 million commercial entities, to provide end-to-end customer management solutions to clients in the financial services, telecommunications, utilities and government sectors.

Trusted Insights. Responsible Decisions.

illion