

aml

From: [REDACTED]@illion.com.au>
Sent: Friday, 3 December 2021 11:45 am
To: aml
Cc: [REDACTED]
Subject: Consultation - AML/CFT Act
Attachments: 03.12.2021_illion_Submission to AMLCFT consultation - FINAL.pdf

Dear Sir

Please find attached illion's submission on the consultation around the AML/CFT Act. Please let me know if you have any questions about our submission.

[REDACTED]
Head of Product

L20/201 Elizabeth Street
Sydney NSW 2000

[REDACTED]
www.illion.com.au



Note: This email, including any attachments, is confidential. If you are not the intended recipient of this email, you must not use, print, distribute, copy or disclose its content to anyone. If you have received this email in error, please advise the sender and delete all copies of it from your system.



3 December 2021

AML/CFT consultation team
Ministry of Justice
SX 10088
Wellington 6140
By email: aml@justice.govt.nz

Consultation — AML/CFT Act review

Dear Sir/Madam,

As a major Credit Reporting Body within the Australian and New Zealand credit landscape, illion (formerly Dun & Bradstreet Australia and New Zealand) welcomes the opportunity to provide this submission to the AML/CFT consultation team of the Ministry of Justice regarding the review the *Anti-Money Laundering and Countering Financing of Terrorism Act 2009* (the **Act**). illion acknowledges the Government's intent to consult with industry and holistically analyse the state of the regime, and the broader need to strengthen New Zealand's capability to combat money laundering and the financing of terrorism.

illion is committed to providing solutions that assist reporting entities in meeting their anti-money laundering (**AML**) obligations in a manner that protects the entities by enabling them to understand who their customers are. Furthermore, we ensure that our internal processes support cost-effective compliance activities.

As a data insights and analytics business, illion transforms data into meaningful information, and believes that quality data is the foundation of its continued success in helping businesses (including banks) manage risk and secure appropriate customer outcomes.

About illion

illion is the leading independent provider of data and analytics products and services across Australasia. The organisation's consumer and commercial credit registries make up a central component of Australia and New Zealand's financial infrastructure and are used to deliver end-to-end customer management solutions to clients.

Introduction

The shift to an online economy is driving an explosion in the volume and complexity of data. This trend is creating an increasing need for central registries and data providers that can be depended on to securely collate, house, verify, filter and manage valuable datasets, and then convert these into accurate insights to power real-time decision making and risk management.

Illion operates in this market, witnessing firsthand how each of our customers work to comply with the current AML legislation and the challenges they face. Each reporting entity is required to assess the money laundering risk of products they offer and the customer base they serve, and are required to develop an AML program that reflects this specific risk. While the Act specifies minimum standards for Know Your Customer (be they individuals or businesses), in practice each organisation may take a different approach in terms of the acceptable data sets to match against, what constitutes a match against a data set and the number of data matches required.

Illion has collated below our observations, organised by subject area as referenced in the consultation document.

Part 4. Preventive measures

What information needs to be obtained and verified

- Obligations for legal persons and legal arrangements

4.22. Should we issue regulations to require businesses to obtain and verify information about a legal person or legal arrangement's form and proof of existence, ownership and control structure, and powers that bind and regulate? Why?

4.23. Do you already obtain some or all of this information, even though it is not explicitly required? If so, what information do you already obtain and why?

4.24. What do you estimate would be the impact on your compliance costs for your business if regulations explicitly required this information to be obtained and verified?

Illion is supportive of the need to Know Your Customer and keep Knowing Your Customer. For individuals and the majority of entity types the information is available in New Zealand and Illion (and our competitors) have solutions that are able to automate the collection and verification of identity in real-time with minimum input from customers.

- Source of wealth versus source of funds

4.25. Should we issue regulations to prescribe when information about a customer's source of wealth should be obtained and verified versus source of funds? If so, what should the requirements be for businesses?

4.26. Are there any instances where businesses should not be required to obtain this information? Are there any circumstances when source of funds and source of wealth should be obtained and verified?

4.27. Would there be any additional costs resulting from prescribing further requirements for source of wealth and source of funds?

At present establishing source of wealth and source of funds is typically a manual process. We have seen in other jurisdictions (for example the UK and Australia) the emergence of solutions that utilise open banking transaction data to establish source of wealth and source of funds.

As regulations and technologies evolve it should become increasingly possible to establish source of wealth and source of funds automatically.

Reasonable steps to verify information obtained through CDD

- Identity Verification Code of Practice

4.45. Do you encounter any challenges with using IVCOP? If so, what are they, and how could they be resolved?

4.46. Is the approach in IVCOP clear and appropriate? If not, why?

4.47. Should we amend or expand the IVCOP to include other AML/CFT verification requirements, e.g. verifying name and date of birth of high-risk customers verifying legal persons or arrangements, ongoing CDD, or sharing CDD information between businesses?

4.48. Are there any identity documents or other forms of identity verification that businesses should be able to use to verify a customer's identity?

4.49. Do you have any challenges in complying with Part 3 of IVCOP in relation to electronic verification? What are those challenges and how could we address them?

illion has concerns with the updated EV Guidelines (Explanatory Note: Electronic Identity Verification Guideline – July 2021), specifically around the definition of Biometrics and the promotion of the RealMe service in exclusion to all other solutions (we refer to note 1 on page 3 that states “At the time of publication, only a verified RealMe identity can meet this requirement in New Zealand”).

We understand that section 8 of the guidelines defines an electronic source as not including either:

- *A selfie photo or video received from the person being dealt with online, including audio-visual link or video conferencing technology.*
- *An uploaded image of the person's identity document(s).*

We recognise that a ‘Biometric’ solution that uses a mobile phone app to capture the applicant's image and an image of the applicant's photo ID does not meet these requirements as they are written.

We do however note that RealMe would only meet these requirements for passports as we are not aware that RealMe has access to the NZTA database of driving license images. Consequently we request that for the sake for clarity the guidelines are updated to state that RealMe only meets the requirement for NZ Passports.

Moving forwards we would also welcome continued engagement with the wider industry around the Digital Identity Trust Framework. The opportunity exists to utilise this framework to facilitate commercial access to the DIA Passport database and NZTA driving license database to enable multiple compliant providers of Biometrics solutions to compete in the NZ market.

- Verifying the address of customers who are natural persons

4.50. What challenges have you faced with verification of address information? What have been the impacts of those challenges?

4.51. In your view, when should address information be verified, and should that verification occur?

4.52. How could we address challenges with address verification while also ensuring law enforcement outcomes are not undermined? Are there any fixes we could make in the short term?

In illion's experience verification of address information has been challenging in New Zealand due to two primary issues:

- *Some addresses contain place names which have both English and Maori names. This can cause issues where upon verification, the supplied address is in an alternative language to the one stored on the database which is being used for verification.*
- *Certain street types are not classified as street types by the NZ post which supports a number of address validation tools.*

Beyond the issues mentioned above, address information is also difficult to verify as keeping address information up-to-date on databases required a lot more effort and compliance than the Name or Date of birth.

Possible solutions could include specifying which component of the address suffices as a match when verified. For example, verifying the post code (in addition to verifying the Name and Date of Birth).

- Ongoing customer due diligence and account monitoring

4.61. Are the ongoing CDD and account monitoring obligations in section 31 clear and appropriate, or are there changes we should consider making?

Illion provides regular assistance with AML Ongoing Customer Due Diligence on both sides of the Tasman. In our experience we see that the regulator's requirements are not well understood when it comes to ongoing CDD, resulting in a wide variety of approaches being taken by Reporting Entities. While entities have put a lot of effort in implementing compliant onboarding processors, they still struggle to manage ongoing KYC. Illion's view is that additional guidance would be very welcome in this area.

- Conducting CDD on existing (pre-Act) customers

4.71. How could we ensure that existing (pre-Act) customers are subject to the appropriate level of CDD? Are any of the options appropriate and are there any other options we have not identified? What would be the cost implications of the options?

Illion has wide experience of AML Uplift programmes on both sides of the Tasman, working with Reporting Entities of all sizes. While there is a cost to an AML Uplift programme, in our experience it is possible to uplift and update the information held on the vast majority of pre-commencement customers automatically, without needing to contact the customer by using automation.

Requiring pre-commencement customers to be brought up to the same CDD standard as post commencement ensures all customers are known, removing the possibility that pre-commencement customers may be an AML risk.


Conclusion - The power of data and analytics and technology to limit cost of compliance burden

New technology, greater availability of data and RegTech have proven to have a positive impact on the compliance burden, increasing productivity, preserving customer experience and enabling deeper analysis of new data sets to better fight financial crime.

Data providers like illion have a key role to play in facilitating customers due diligence. We help by removing the large part of human involvement onboarding and due diligence exercises and allow reporting entities to focus on AML risk in a timely and cost-effective manner. For example, we provide Know Your Customer and monitoring solutions that operate at speed and scale. At customer onboarding we can screen individuals or non-individuals in real-time. For ongoing customer due diligence we can perform electronic ID Verification on over 0.5 million individuals overnight.

Open Banking further expands the information that can be accessed by Reporting Entities to streamline customer identification while better identifying AML risk, for example being able to verify source of funds or source of wealth using Open Banking transaction data. In the UK providers such as Thirdfort are integrating biometrics, Electronic ID Verification and Open Banking Data elements to allowing subscribers to collect and verify the bulk of the “critical data elements” (CDEs) required to be verified by the UK regulator.

The combination of expanding data availability and increasing technological capability provides New Zealand legislators the opportunity to expand the scope of AML legislation, to ensure that New Zealand has a world leading financial system and to deliver enhanced protection from money laundering to its Citizens, without placing an unreasonable cost on providers of financial services.

If there are any questions or concerns arising from this submission, please feel free to contact me at any time at  [@illion.com.au](mailto:illion.com.au).

Yours sincerely,



Head of Product