aml

From: [redacted]@mattr.global>
Sent: Friday, 3 December 2021 2:03 pm
To: aml
Subject: MATTR submission to the Ministry of Justice - Review of the AML Act
Attachments: MATTR submission MoJ AML CFT Act December 2021.pdf

Hello

Please find attached MATTR's submission to the Ministry of Justice's Review of the AML Act. I hope it is helpful to the review efforts and would be very happy to talk to any of the points if that is viewed as helpful.

Please do not publish my mobile number at the bottom of this email. The document I am submitting can be published in its entirety.

Thanks [redacted]

[redacted]
CEO, MATTR

[redacted]@mattr.global

MATTR Limited
12 Madden Street
Auckland, New Zealand

mattr global
info@mattr global

Submission to the Ministry of Justice

Review of the AML/CFT Act

December 2021

Introduction and Summary

1. MATTR welcomes the opportunity to contribute to the review of the *Anti-Money Laundering and Countering Financing of Terrorism Act 2009* (the AML/CFT Act). MATTR's comments will focus only on one aspect: the utilisation of digital identities under the AML/CFT Act, primarily as set out in Section 5 of the Ministry of Justice's Consultation Document.[1]

2. MATTR anticipates that digital identities will have a key role to play as part of 'Customer Due Diligence' activities both in New Zealand and around the world, reflecting both the digital transformation of the financial services sector but also the potential benefits that more digitalised verification systems offer in terms of efficiency, security, privacy and inclusion. To that end, MATTR considers that the AML/CFT Act and its associated regulations and Codes of Practice should be modernised in order to fully integrate the use of verified digital identities; and that ensuring consistency with the Digital Identity Services Trust Framework (and any future Trust Framework Rules) must also be a priority. MATTR also considers that the modernisation of the Act to incorporate digital identities consistent with the Trust Framework will have benefits in terms of potential trans-Tasman harmonisation and the future resilience of the New Zealand system overall.

About MATTR

3. MATTR is a New Zealand organisation specialising in digital capabilities to support verifiable data and digital trust. As experts in decentralised identity, we work at W3C (World Wide Web Consortium), DIF (Decentralised Identity Foundation), OIDF (Open ID Foundation) and other technical standards bodies. MATTR is committed to interoperability and investment in building open-source reference implementations of the standards we work on. We then build and operate enterprise and government grade platforms to support wide-spread easy adoption of capabilities in a wide variety of settings.

Digital identities and the AML/CFT Act

4. The digitalisation of financial transactions is growing rapidly and indeed fast becoming ubiquitous. This means that digital tools and innovative technologies are inevitably going be part of both business models and regulatory effectiveness when it comes to the financial services sector and the activities covered by the AML/CFT Act both now and into the future.

5. MATTR anticipates that digital identities will have an increasingly key role to play as part of 'Customer Due Diligence' (CDD) activities – reflecting both the growing digitalisation of all aspects of financial transactions (meaning that traditional identity verification tools may no longer be fit-for-purpose), but also in order to achieve easier, cheaper, more secure, privacy-protecting and effective identification of individuals in the financial sector.

6. Digital identities can also enhance financial inclusion for individuals who may not have access to other forms of identification – and this may be particularly important since, as the Consultation Paper notes (page 23), the high identity standards laid out in the AML/CFT Act regime *per se* may have negatively affected financial inclusion for some people in New Zealand. The use of digital identities could also streamline and reduce potential compliance costs for other sectors such as non-profit organisations, were they to be brought under the

[1] https://www.justice.govt.nz/assets/Documents/Publications/AMLCFT-Statutory-Review-Consultation-Document.pdf

AML/CFT Act as floated in the Consultation Document, thereby enabling greater inclusion and security for those organisations.

7. The intergovernmental Financial Action Task Force (FATF), of which New Zealand is a member, has recommended the adoption of a risk-based approach to the use of verifiable and secure digital identities in relation to anti-money laundering requirements.[2] The Consultation Document likewise recognises the potential of digital identity in AML/CFT processes, noting that, "We consider that the AML/CFT regime could be a prime candidate for making use of the digital identity framework and ecosystem, and we want to ensure that the regime is set up in a way to enable digital identity to be adopted once the framework is operational", and seeking further comments from stakeholders (page 122).

(i) Consistency with the Digital Identity Services Trust Framework

8. Specifically, in Question 5.14, the Consultation Document asks what additional challenges or barriers may exist which would prevent the adoption of digital identity once the Digital Identity Trust Framework is established and operational, and how those challenges could be overcome.

9. MATTR was extensively involved in the preparatory consultations on the Digital Identity Trust Framework, and welcomed the introduction of the Digital Identity Services Trust Framework Bill which is currently before Parliament. (The consultative approach that the Government has taken is in fact fully consistent with FATF's recommendation that governments develop an integrated multi-stakeholder approach to understand the opportunities and risks relevant to digital identities, and develop regulations and guidance to mitigate those risks.) MATTR recognises that the Bill provides an important foundation for the provision of secure and trusted digital identity services to individuals and organisations.

10. However, MATTR is concerned that at the potential for inconsistency between the proposed Trust Framework and the AML/CFT Act (and its related regulations and Codes of Practice, including the existing Identity Verification Code of Practice). This risks creating confusion among both public and private-sector participants in the respective ecosystems and may potentially lead to inadvertent non-compliance – a serious concern in such high-assurance use cases. Such ambiguity across the two areas of legislation may also act as a barrier to the widespread adoption of digital identity in the financial services sector, meaning that the expected benefits noted above would not be fully realised.

11. At present, the Digital Identity Services Trust Framework Bill makes no reference to the AML/CFT Act. MATTR considers that the AML/CFT Act and associated regulations and Codes of Practice should be modernised to fully incorporate digital identities, consistent with the parameters outlined in the Trust Framework; and also, that careful consideration should be given to the Digital Identity Services Trust Framework Bill itself, and any subsequent Trust Framework Rules, to ensure that there is consistency as appropriate with the AML/CFT Act and associated regulations and Codes of Practice (as may be amended through the current review).

12. By way of an example of current potential inconsistencies between the Act and Bill, there appears to be a lack of coherence in the definitions of relevant terms. Section 13 of the AML/CFT Act refers to "verifying" identity, and specifies that this must be "done on the basis of documents, data or information issued by a reliable and independent source" (or on any other basis prescribed by regulations); but by contrast the Trust Framework Bill refers to "digital identity services" that "check the accuracy of personal information". Likewise, the Identity Verification Code of Practice under the Act refers to "electronic identity" (a "record kept in electronic form that contains authenticated core identity information about an individual"), whereas the Trust Framework Bill does not use the term "electronic identity" at all, instead referring to "digital identities" and "personal information in digital form". It may be that the Trust Framework Rules to be developed following passage of the Bill use language more consistent with the AML/CFT Act, but care should be taken to achieve consistency where possible.

[2] Financial Action Task Force, 'Digital Identity', March 2020; see https://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/Guidance-on-Digital-Identity.pdf

(ii) Consistency between the Trust Framework and the Identity Verification Code of Practice

13. The Consultation Document also asks (in Question 4.48) whether there are any forms of identity verification that businesses should be able to use. There is a strong case to modernise the Code of Practice to mandate an approach consistent with FATF standards for digital identity, as well as the Trust Framework.

14. For example, the Identity Verification Code of Practice provides that, in order to conduct electronic identity verification of a customer's name, a reporting entity must verify the name from "a single independent electronic *source* that is able to verify an individual's identity to a high level of confidence", and lists criteria for determining what kind of sources will be acceptable (for example, having regard to their accuracy, security, privacy and other concerns). It will be important to update the Code of Practice to ensure that these criteria for acceptable sources explicitly include digital identity services *providers* accredited under the Trust Framework. In parallel, care will need to be taken in designing the future Trust Framework Rules to ensure that they are fully compatible with the AML/CFT Act and Codes of Practice.

15. Similarly, the Identity Verification Code of Practice sets out guidance on the *documents* that can be relied upon to verify identity, how document certification can occur, and the steps needed to verify that information electronically. It will be important to ensure that an updated Code of Practice also includes in this list digital identity credentials that have been verified by digital identity services providers accredited under the Trust Framework. MATTR has separately proposed, in relation to the Trust Framework Bill (and for any future Rules) that provision be made to ensure that the data quality remains consistently high (for example, by enabling the updating or correction of information). This will address one of the concerns highlighted in the Consultation Document around the need for ongoing CDD.

(iii) Modernising other aspects of the Identity Verification Code of Practice

16. At the moment, there is a lack of clarity for those seeking to rely on digital identity credentials issued by different institutions. This needs to change. Modern decentralised identity capabilities that allow for verifiable credentials enable 'credential stacking' and the utilisation of signed tamper-evident data drawn from a variety of different contexts. In other words, multiple independent sources of corroboration can be used to verify identity securely and in a way that respects privacy. This can enable enhanced due diligence processes. Organisations to whom the AML/CFT Act applies must be able to leverage such tools confidently; this points to the need to clarify the use of stacked credentials in the Industry Verification Code of Practice and/or the AML/CFT Act itself.

17. The same technologies discussed in the foregoing paragraph can equally be applied in other AML/CFT activities that go beyond identity verification. For example, they can be used to issue credentials that allow the verification of source of funds and in the longer term, indeed any form of verifiable data related to AML/CFT activities. It is important that the Act recognises and creates room for these technologies to be leveraged by organisations to improve overall AML/CFT outcomes. As bad actors continue to grow more sophisticated, it is important that the AML/CFT Act and associated regulations leave open the opportunity to apply and importantly rely on credentials of this nature.

18. In this regard, it would also be useful ensure consistency between the AML/CFT regime and any future Consumer Data Right (CDR). In July 2021, the Commerce and Consumer Affairs Minister announced that he was intending to introduce a CDR in 2022. MATTR strongly supports consumer data rights, recognising the value for consumer choice and innovation in developing a mechanism for consumers securely to share data about themselves with trusted third parties. However, there will need to be very strong alignment between any CDR legislation, the proposed New Zealand Digital Identity Services Trust Framework currently before Parliament, and the AML/CFT regime, rather than seeking to establish a new parallel mechanism specifically for CDR. This is necessary to avoid confusion, implementation challenges, unwarranted compliance costs, and the inadvertent creation of barriers to innovation and adoption.

(iv) Harmonisation with Australia

19. The Consultation Document (page 108) notes that because many New Zealand and Australian businesses operate trans-Tasman, there could be a case for harmonising AML/CFT obligations across both jurisdictions as far as possible to help achieve greater efficiencies for businesses and government. Question 5.15 asks whether New Zealand should achieve greater harmonisation with Australia's regulations. Leaving aside the broader question of overall trans-Tasman harmonisation, it should be noted that there is an active workstream underway between the two governments to develop mutual recognition of digital identity services. (The Trust Framework Bill provides an important foundation to advance this work.) Mutual recognition of digital identities could at a minimum, lower compliance costs for businesses complying with the AML/CFT regime in either jurisdiction, even without higher-level harmonisation.

(v) Future resilience of the AML/CFT regime

20. As part of designing for future resilience of the AML/CFT regime, it is important to consider what enablement 'infrastructure' and other facilitation mechanisms can be provided to support confidence and trust. For example, strengthening assurance levels with greater due diligence as part of establishing legal entities (companies, trusts, charities and all kinds of organisations), can create a significant lift in overall confidence levels in chains of trust and data supply chains that are critical to effective AML/CFT practices. One way to achieve this would be by creating pathways for companies, charities, trusts and other types of legal structures to enter into enhanced due diligence to achieve a high-assurance New Zealand Business Number digitally verifiable credential. This would create the opportunity for all verifiable data signed by these trusted organisations to be grounded in a high confidence anchor point. As the AML/CFT Act places requirements on parties to fulfil due diligence requirements with customers, it is important that the Government also make reasonable efforts to support entities in fulfilling their obligations. These types of initiatives can provide very practical ways to improve confidence and establish the basis for resilience of the AML/CFT regime, while at the same time increasing opportunities for high confidence mutual recognition initiatives between jurisdictions.

21. Finally, Question 5.16 asks how to ensure that the AML/CFT system is resilient to long- and short-term challenges. In short, we are witnessing a digital transformation on an unprecedented scale. Forecasts made prior to the pandemic predicted that digital payments would reach 726 billion transactions by 2020; and that by 2022, 60 percent of world GDP would be digitalised.[3] Of course, through the pandemic we have subsequently seen significant acceleration of this process of digitalisation across all aspects of the economy, in New Zealand and worldwide. Fully integrating digital identities into the AML/CFT Act and associated regulations and Codes of Practice would make an important contribution to 'future-proofing' the AML/CFT regime and to help ensure that New Zealand businesses are better enabled to operate safely and successfully on the world stage.

[3] Quoted in the FATF guidance on digital identity; see https://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/Guidance-on-Digital-Identity.pdf