aml

From: [redacted]@nztech.org.nz>
Sent: Thursday, 2 December 2021 1:27 pm
To: aml
Cc: [redacted]@digitalidentity.nz; [redacted]
Subject: DINZ AML-CFT Submission (report and review)
Attachments: Digital-Identity-New-Zealand-AML_CFT-Report_20-October-2020_FINAL.pdf; DINZ Submission AML CFT review December 2 2021.pdf

To whom it may concern,

Please find attached two documents as the submission from Digital Identity NZ to the AML-CFT Review.

The contact person is [redacted] who is copied into this email.

Can you please confirm that you have received this submission.

Many thanks

Kind regards

[redacted]
[redacted] Adviser, NZTech
[redacted]

Website | LinkedIn | Facebook | Twitter

Subscribe to the NZTech newsletter

DIGITAL IDENTITY.NZ

THE RELIANCE AND REUSE OF IDENTITY VERIFICATION FOR AML/CFT PURPOSES

Legal input provided by

MinterEllisonRuddWatts

ISSUED OCTOBER 2020

CONTENTS

APPENDICES

1. EXECUTIVE SUMMARY

More and more New Zealanders are using online services as a primary means of interaction, with a 2020 Digital Identity NZ report[1] finding that two thirds are more likely to go online than face to face. This effect has undoubtedly been impacted by COVID-19, yet even 'Before Covid' worldwide trends indicate an ever-increasing reliance on digital. Digital payments are growing at an estimated 12.7 percent annually, and are forecast to reach 726 billion transactions annually by 2020[2]. By 2022, an estimated 60 percent of world GDP will be digitalised[3].

An increasing reliance of online and remote interaction, especially in the establishment of proof of identity for new customers, has placed increased pressure on organisations to validate and prove the identity of prospective customers without the physical presentation of paper based documentation.

Digital Identity NZ is a not for profit association of member organisations committed to improving our online interactions; reducing friction, improving productivity and maintaining privacy and security. Emerging technologies and practices can enable effective sharing of personal information and/or trustworthy and verified evidence that credentials are genuine (e.g. the W3C Verifiable Credential standard). This emerging digital identity ecosystem has the potential to decrease costs by putting users in control of their digital identity information, and in the context of AML/CFT, enabling them to re-use their digital identity information and attributes, whilst maintaining or even enhancing privacy and security.

This Report was commissioned to answer the question, *Can an individual re-use identity verification obtained through an AML/CFT process and still meet the regulatory requirements of all Reporting Entities involved?* taking into account these emerging technologies and practices.

The AML/CFT legislation and guidelines are complex and multifaceted. A key aspect of the regime is the due diligence associated with identifying and verifying customers' identities. In New Zealand there is extensive support for a 'risk-based' approach to customer onboarding, meaning that organisations subject to AML/CFT legislation (Reporting Entities) are encouraged to adopt a varying approach to customer onboarding based on risk factors. Whilst this approach empowers Reporting Entities to design processes and procedures that are 'fit for purpose' for their circumstances, it makes any process of sharing or reuse of identity information more challenging.

The AML/CFT Act provides for certain ways for a reporting entity to rely on a third party to carry out its Core KYC obligations, by relying on:

- Another member of its business group (i.e. DBG Reliance);
- An authorised agent (i.e. Agency Reliance); or
- Another reporting entity[4] in two ways:
  - Reporting Entity Reliance; or
  - Approved Entity Reliance (which has yet to be activated by the Government).

Reliance between reporting entities, such as the Participating Banks, is used less frequently than may be expected. This appears to be because responsibility typically remains with the institution relying on the third party, including for the third party's failure. The difficulties of supervising third parties and the need to

[1] digitalidentity.nz/2020/07/27/new-nz-research-highlights-work-needed-to-improve-care-of-personal-information/
[2] Capgemini & BNP Paribas (2018), *World Payments Report 2018*, accessed online at: https://worldpaymentsreport.com/wp-content/uploads/sites/5/2018/10/World-Payments-Report-WPR18-2018.pdf
[3] International Data Corporation (IDC), IDC FutureScape: Worldwide IT Industry 2019 Predic ions
[4] As indicated in section 5.2.3 and Appendix 6 (section 14.6.3) below, it is arguable that en ities other than reporting entities could be approved as "approved entities" under the AML/CFT Act, sections 33(3A) and 154(1)(ac), but we think that was not the original intent.

negotiate and agree to commercial, liability and information sharing terms between them mean there are many regulatory and practical barriers to the adoption of these AML/CFT reliance regimes by the banks.

The penalties for non-compliance is likely to be one key reason for the seemingly high degree of risk aversion institutions have towards their Core KYC compliance (and also general AML/CFT compliance). In addition to regulatory penalties, there are a number of impediments that present obstacles for risk averse organisations. These include concerns around privacy, perceptions of collusion or anti-competitive behaviour and the potential for third party liability.

These issues are not insurmountable. Cabinet has confirmed that a Digital Identity Trust Framework based on legislation will be developed[5]. The Trust Framework will be a regulatory regime that ensures that identity service providers operate under common rules and standards. The Department of Internal Affairs (DIA) will develop an Interim Trust Framework, which will enable the Trust Framework rules to be developed and tested with digital identity providers, while the legislation is being drafted (Digital Identity Bill). This presents an exciting opportunity for New Zealand to learn and lead the creation of future focused frameworks.

The Digital Identity Bill is scheduled to be introduced to the House in 2021. This legislation will enable providers to be legally accredited against the Trust Framework rules, which will be based on existing and developing standards.

The Trust Framework will support the development of security and privacy enhancing and interoperable approaches to digital identity services, to maximise benefits for citizens, the economy and society. The Trust Framework will also ensure that citizens and businesses can have trust and have confidence that their identity information is being handled appropriately.

The DIA have indicated that as part of the Interim Trust Framework development they will be testing a range of approaches through pilot programmes with public and private sector organisations. This presents an opportunity to explore how this Digital Identity Bill could be used to improve how AML/CFT is conducted in New Zealand, while remaining in line with the Financial Action Task Force's (FATF) principles and guidance.

Background information to the DITP's work on a New Zealand Government Trust Framework is set out in Appendix 1. Additional background information on Trust Frameworks drawn from international collaborations is set out in Appendix 2.

The Trust Framework approach is also recognised internationally, with FATF recently endorsing the use of digital identity technologies in the FATF Digital Identity Guidance. The FATF recommends that the AML/CFT Supervisors and the Ministry of Justice assess how the AML/CFT regime accommodates the use of digital identity systems for CDD. The FATF also recommends these government bodies develop clear guidelines or regulations to allow appropriate, risk based use of reliable independent digital identity systems.

The Trust Framework could potentially, and over time contribute to a material change to the status quo, in addition to one or more of the following:

(a) The activation of the Approved Entity Reliance regime;

(b) The establishment of a framework of Reporting Entity Reliance involving reporting entities who are fully compliant with identification management standards and best practice, and can provide authoritative assurance of AML/CFT compliance;[6]

(c) Changes to the AML/CFT regime;

[5] digital.govt.nz/news/development-of-digital-identity-trust-framework-confirmed/
[6] This framework would be designed and established on the presumption the Approved Entity Reliance regime has not been ac ivated.

(d) Enable the existing AML/CFT requirements to be satisfied through purely digital means.

All of the above are briefly summarised in the table below, and explored in more detail in this Report.

RECOMMENDATIONS AND NEXT STEPS
1. Industry and government agencies (including the AML/CFT Supervisors and the Ministry of Justice) collaborate to inform and make use of the Interim Trust Framework • Utilising the Interim Trust Framework, foster a commercial and regulatory environment that enables new electronic identity credentials to be used by Reporting Entities to conduct Core KYC. • Work with the Privacy Commissioner to develop a code of practice on information sharing for AML/CFT under the Interim Trust Framework.
2. The DIA to lead the legislative programme to introduce the Digital Identity Bill, in conjunction with Government agencies and Industry, including; • Clarifications on electronic identity verification in the AIVCOP. • Amending the AIVCOP to consider sufficiently-robust uses of digital identity technologies to be deemed comparable to face-to-face verification. • Updating the AIVCOP to cover the verification of address information. • Expand the liability safe harbour provisions in the EIVA for issuers of identity using new electronic identity platforms. • The Ministry of Justice to consider the New Zealand Government Trust Framework as part of its statutory review of the AML/CFT Act in 2021, in consultation with the AML/CFT Supervisors and reporting entities.
3. AML/CFT Supervisors seek to update regulation, as part of its statutory review of the AML/CFT Act in 2021 through the incorporation of the Trust Framework and the FATF's Digital Identity Guidance, in collaboration with industry. • Assess existing guidelines and regulations and/or develop clear guidelines or regulations allowing the appropriate, risk based use of reliable, independent digital identity systems regulated for AML/CFT purposes, including clarifying that non-face-to-face on boarding may even be low-risk for CDD, when digital identity systems with appropriate assurance levels for identification, verification and authentication are used. • Consider the merits of removing address information from mandatory Core KYC, and/or examine the merits of replacing it with other criteria. • Establish a framework for Reporting Entity Reliance that would be developed and tested by reporting entities and other organisations accredited under the Trust Framework.
4. Activate the Approved Entity Reliance regime • The Ministry of Justice issue official guidance on the criteria to become an approved entity in considering the MOJ 2017 Report. • Approving entities so that the regime can be used, with appropriate vetting and supervision processes involved.

Capitalised terms and expressions in this Report are defined in the Glossary on page 37.

2. INTRODUCTION

2.1 PURPOSE OF THIS REPORT

The FATF released the FATF Digital Identity Guidance in March 2020.[7] In it, the FATF endorses the use of digital identity technologies and frameworks as an innovative solution to CDD. More information on the FATF is set out in Appendix 3. More information on the background and relevance of FATF Digital Identity Guidance to this Report is in Appendix 4. The FATF's recommendations in the FATF Digital Identity Guidance are in Appendix 5.

Digital Identity NZ chose the AML/CFT regime as a use case for the New Zealand Government Trust Framework which the DITP is developing, in collaboration with some of Digital Identity NZ's members (including several of the Participating Banks, Mattr Limited and other technology service providers) and other organisations, have been collaborating on.

The New Zealand Government Trust Framework is designed to form the basis for a digital identity ecosystem in New Zealand.[8] More background information to the New Zealand Government Trust Framework is described in Appendix 1. Digital Identity NZ's view of how one hypothetical Trust Framework might operate is described in Appendix 2.

Digital Identity NZ and its collaborators share the prevailing theory that reporting entities caught by the regime have been experiencing at least some challenges in collecting and verifying Core KYC information.

Digital Identity NZ[9] commissioned this Report, with legal input from MinterEllisonRuddWatts in March 2020, for the purpose of identifying current legal and regulatory issues and constraints to reporting entities in sharing Core KYC information with each other, to partly meet their obligations to perform Core KYC under the AML/CFT Act. From this, the Report will identify the legal and regulatory implications of Core KYC being re used by reporting entities. The possibility of performing Core KYC electronically will also be discussed briefly. The Report is intended to briefly explore possible solutions to the legal and regulatory issues recognised, including digital identity solutions in use or in development.

2.2 AML/CFT REGIME

New Zealand's AML/CFT Act,[10] was put in place with the following purposes:

- To detect and deter money laundering and the financing of terrorism; and
- To maintain and enhance New Zealand's international reputation by adopting, where appropriate in the New Zealand context, recommendations issued by the FATF,[11] an intergovernmental body mandated to set standards and promote effective implementation of legal, regulatory and operational measures for combating money laundering and terrorist financing; and
- To contribute to public confidence in the financial system.

The parts of the AML/CFT regime which are relevant to this Report are summarised in Appendices 6 – 8, and in particular:

- Appendix 6 includes a summary of the obligation to conduct Core KYC as well as the various types of CDD. The Appendix describes the requirements for verifying a person's identity and the implications of

[7] Financial Action Task Force, *Guidance on Digital Identity* (Financial Ac ion Task Force, Paris, 2020).
[8] dia.govt.nz/diawebsite.nsf/Files/Proactive-releases/$file/Ministers-Cabinet-paper-Developing-Options-for-a-New-Approach-to-Digital-Identity-1.pdf
[9] Digital Identity New Zealand is part of New Zealand Technology Industry Associated Incorporated, an incorporated society registered in New Zealand.
[10] The AML/CFT Act is discussed in more detail in Appendices 1-3.
[11] Financial Action Task Force, *International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation* (Financial Action Task Force, Paris, 2012-2019).

AIVCOP. The three forms of reliance available under the AML/CFT Act – DBG Reliance, Agency Reliance and Reporting Entity Reliance (to which Approved Entity Reliance applies to) are also examined.

- Appendix 7 examines the AML/CFT codes of practice, as well as the only AML/CFT code of practice to date, the AIVCOP.
- Appendix 8 briefly explores the other types of information required for CDD.

The AML/CFT Act came into force on 30 June 2013 for an original cohort of "reporting entities" (including "financial institutions" and "casinos") and in many ways it reflects the FATF Standards, particularly in relation to CDD, FATF Recommendation 10. More information on the FATF Standards relevant to this Report is described in Appendix 3.

The Act's coverage was extended during 2018 and 2019 to a wider range of reporting entities including "designated non-financial businesses and professions" (e.g. lawyers, accountants, real estate agents, and trust and company service providers), "high value dealers" and the Racing Industry Transition Agency.[12]

One of the core obligations of "reporting entities", is to conduct CDD on their customers as well as other types of people. This includes identifying and verifying the full names, dates of birth and residential addresses of natural persons as customers, beneficial owners, persons acting on behalf of customers or persons on whose behalf a customer has acted (i.e. "Core KYC"), at the time of establishing a business relationship, and thereafter for subsequent and ongoing CDD. Core KYC is the primary concern of this Report.

The AML/CFT Act requirement to conduct CDD is a major step in facilitating the detection and prosecution of those committing crimes in New Zealand and overseas, with the direct or indirect proceeds of over $1 billion per year estimated to be laundered through New Zealand business, as well as meeting international expectations (including of other countries operating within the FATF framework).[13] This matters to New Zealand in terms of its international trade, and its general good standing in the international community.

At the same time, undertaking CDD imposes direct and indirect costs, not only on reporting entities and their customers, but also on the New Zealand economy more broadly. Accordingly, CDD needs to be undertaken as efficiently as possible, while still meeting the primary objectives of the AML/CFT Act regime.

Under the AML/CFT Act, reporting entities are, in certain circumstances, able to rely on the CDD performed by third parties, including other reporting entities, to meet their obligation to perform CDD on a person. However, reporting entities are ultimately liable for the CDD performed by third parties for various reasons. There appears to be liability, regulatory and policy barriers to the widespread adoption of the reliance frameworks under the AML/CFT Act. These issues are addressed in more detail in section 4.2.2 and Appendix 6.

New technologies designed to simplify CDD processes and reduce some of the associated costs, including digital identity platforms which would theoretically give Holders the power to control who can observe or access their verified identity data, will naturally be beneficial to the economy and society, however they also carry risks. Important legal issues or even legal barriers like privacy law, the liabilities of the technology providers, issuers of identity credentials and reporting entities, need to be resolved before these technologies can be adopted at scale.

The subset of these technologies focused on building digital identity frameworks, which allow a person and their identity to be verified to a high degree of confidence, appears in line with some of the FATF's recommendations for authorities in the FATF Digital Identity Guidance. A digital identity solution that makes

[12] Each as defined in section 5 of the AML/CFT Act.
[13] keepourmoneyclean.govt.nz/.

CDD simpler for reporting entities and the people that CDD is conducted on, could supplement or even solve the lukewarm adoption of most of the AML/CFT Act's reliance frameworks (the exception is Agency Reliance, which is being used in practice).

3. METHODOLOGY/TERMS OF REFERENCE

3.1 APPROACH OF THE REPORT

Digital Identity NZ engaged MinterEllisonRuddWatts to provide legal input to this Report. MinterEllisonRuddWatts is a leading full service New Zealand law firm, with offices in Auckland and Wellington. The scope of MinterEllisonRuddWatts' engagement is set out in Appendix 9.

MinterEllisonRuddWatts' research for this Report included a review of guidance and the only code of practice (the AIVCOP) released by the AML/CFT Supervisors to date. MinterEllisonRuddWatts also reviewed the FATF Standards and the FATF Digital Identity Guidance. A bibliography is included in page 40.

MinterEllisonRuddWatts prepared the Questionnaire for the Participating Banks', and AML/CFT Supervisors' response. The Participating Banks' involvement with the preparation of this Report (the six largest banks in New Zealand based on total deposits) was crucial to understanding real-world issues faced by the AML/CFT Act's largest reporting entities when performing Core KYC. The Questionnaire sought confidential and legally privileged opinions or observations on any issues or inefficiencies arising from reporting entities' obligations to perform Core KYC, as well as any perceived risks and benefits to adopting different processes and technologies when conducting Core KYC. Not all Participating Banks responded to the Questionnaire. More information about the Questionnaire is provided in Appendix 10.

MinterEllisonRuddWatts sought and received separate and additional input from various members of the Core Group. The AML/CFT Supervisors provided a "macro" perspective on the frictions encountered by their reporting entities. They also shared important but non-confidential insights into the many political implications of the AML/CFT regime.

The Report has been written for a person who is not familiar with the AML/CFT regime. To assist readers, sections below containing substantive legal analysis begin with a brief summary of its contents, which are in *italics*.

3.2 LIMITATIONS OF THE REPORT AND DISCLAIMERS

The scope of the analysis in this Report is limited to Core KYC. Core KYC does not apply to corporate or unincorporated entities except in relation to beneficial ownership. Core KYC also does not address CDD in its entirety (whether simplified, standard or enhanced for natural persons), or politically exposed person assessments. The Report presumes that any reporting entity required to perform Core KYC is not otherwise exempted from this obligation under any regulations made under the AML/CFT Act, such as the Anti-Money Laundering and Countering Financing of Terrorism (Exemptions) Regulations 2011.[14] Further, the Report is not concerned with reporting entities' obligation to conduct ongoing monitoring of its customers (ongoing CDD) or CDD subsequent to onboarding customers. However, for completeness, see Appendix 6, Ongoing CDD.

Any recommendations or courses of action set out in this Report are included primarily for consideration by relevant governmental agencies of their public policy implications. Without limitation, this Report is not intended to recommend any agreement, arrangement or understanding between Participating Banks, the members of Digital Identity NZ or other persons, to address any barriers or limitations to the AML/CFT regime highlighted, prior to further advice in relation to the competition law and other legal implications of doing so being obtained.

[14] Anti-Money Laundering and Countering Financing of Terrorism (Exemptions) Regulations 2011.

The Report is only intended to consider the identified legal or regulatory issues under New Zealand law, and it will not be comprehensive on such issues – for example, Commerce Act 1986 implications are explicitly excluded from the scope of this Report. The Report does not contain an exhaustive analysis of all possible forms of statutory liability or all possible statutory duties applicable to reporting entities or issuers of identity.

The Report has not considered overseas jurisdictions' attitudes or approaches to the issues considered in the Report. It does not address the issues which may arise under the laws of any other jurisdiction, and further advice should be taken in that regard before acting on this Report. Further, it does not consider other issues which may be relevant to its scope (e.g. commercial, economic, technological, etc).

This Report is intentionally general in nature. Individuals should seek professional advice before taking any further action in relation to the matters dealt with in this Report. The views expressed are Digital Identity NZ's own. This Report, and any input provided by MinterEllisonRuddWatts, does not constitute legal advice to any person other than Digital Identity NZ, in accordance with its terms of engagement.

This Report does not necessarily reflect the supervisory position of the AML/CFT Supervisors or the Ministry of Justice. It does not reflect the opinions of the members of Digital Identity NZ who were requested to provide comment on various aspects of some of the issues raised in this Report.

4. ISSUES WITH THE AML/CFT REGIME

4.1 FRICTIONS ARISING FROM CORE KYC

Conducting Core KYC can be a costly exercise, and the inefficiencies around repetition of and human error in CDD processes increases that cost. Differences in processes between reporting entities result in inconsistent and confusing customer experiences.

Since the AML/CFT regime came into force, many people in New Zealand who are (or have sought to be) a customer of a bank, a finance company, a life insurer, financial adviser, a remittance service or foreign exchange bureau, a lawyer, an accountant, a real estate agent, or other reporting entity have experienced some of the challenges of Core KYC. These can include:

- A requirement to provide evidence of identity, which is not always available to the individual, for example, for the poor or elderly or homeless (including the "hidden homeless"[15]);
- A requirement to provide the same evidence of identity multiple times, on engagement with each new and different reporting entity, but also to different parts of the same reporting entity or at different times;
- Different standards and requirements being imposed by different reporting entities, so that a potential customer may not have the correct evidence of identity readily accessible;
- A requirement to physically visit a reporting entity's premises to perform face-to-face Core KYC on a person, which can be particularly challenging for those people, with disabilities, who do not live in a metropolitan centre, without available transportation, or who prefer to use digital services; and
- Human error from within the reporting entity, resulting in the customer needing to perform additional and otherwise unintended steps before CDD is completed.

These costs could, at the extreme, also result in at least some people being totally or partially excluded from the financial system and mainstream society, if they cannot complete Core KYC for various reasons, usually due to inadequate evidence of documentation. As a result, these people are denied from consuming reporting entities' products and services.

The same costs also increase reporting entities' overall financial cost of complying with the AML/CFT Act, and their willingness to adopt new technologies to reduce some of these costs. These costs may disincentivise reporting entities from providing services to customers who they perceive to present higher onboarding costs.

More broadly, for the New Zealand economy, these costs have the potential to contribute to inertia in the speed and rate of some customers switching their service providers, and a reduction in the volume and velocity of certain types of transactions in the economy, with possible reductions in competition. They may blunt the impact of government sponsored initiatives such as "open banking"[16]. Further, these costs may slow the uptake of particular digital services, potentially impacting productivity and growth generally – at least relative to other developed economies.

New Zealand is not alone in facing these issues. The FATF recently issued its FATF Digital Identity Guidance, which explicitly clarifies that "non face-to-face customer identification and transactions that rely on reliable, independent digital ID systems, may present a standard level of risk, and may even be lower risk". The guidance also references financial inclusion goals of FATF, and the benefits of responsible financial innovation.

[15] stuff.co.nz/national/116095068/the-hidden-homeless-alarming-child-and-youth-homelessness-in-auckland.
[16] consumer.org.nz/articles/what-is-open-banking.

4.2 THE PARTICIPATING BANKS' RESPONSES TO THE QUESTIONNAIRE

4.2.1 The Participating Banks' responses to the Questionnaire

The Participating Banks have observed some issues performing Core KYC.

The Participating Banks all emphasised the administrative costs of conducting Core KYC in the Questionnaire. These administrative costs included financial costs,[17] and also time related costs. These costs were seen to be magnified by (or at times due to) different business units within a bank needing to perform Core KYC on the same customer because of different or unaligned internal processes. Human error, from both within the reporting entity (i.e. its employees and contractors) as well as the customer, was seen as another issue related to the administrative and procedural nature of Core KYC. While this risk has been mitigated through staff training and technological investments made by some of the Participating Banks, the costs caused by human error were clear, particularly the need to perform additional and otherwise unintended steps in order to complete Core KYC on a person. One common example was of people having to return to a bank's premises because the bank's employees hadn't adequately verified these people's residential addresses.

Several of the Participating Banks often require people to physically visit a branch, known as "face-to-face" Core KYC, in line with the verification standards set in AIVCOP.[18] In part, that may be because face-to-face Core KYC is assured to be a lower risk than electronic identity verification even though as the FATF Digital Identity Guidance points out, that is not necessarily the case. Face-to-face Core KYC has apparently been problematic for some customers, particularly customers who live in rural regions of New Zealand.[19]

At least one Participating Bank noted only approximately 10 percent of new customers successfully completed its Core KYC using electronic identity verification without the need to visit one of its branches. The friction of biometric solutions and the general requirement for two independent reliable data sources was suspected to be contributing factors to the low numbers of customers having their identity verified through electronic means.

Significantly, the Participating Banks reported having experienced difficulties verifying the residential address of their customers. Often bank statements are now delivered electronically, and some customers do not have readily available evidence of place of residence – especially if they are not the owner or the named tenant on a lease. The topic of verifying a person's residential address is explored further in section 4.5 below.

With banks having different AML/CFT processes, risk profiles and risk tolerances, their mutual customers have had to follow different Core KYC processes across the reporting entities (noting however, that these processes are largely consistent in many areas). Responses to the Questionnaire raise the possibility of this leading to poorer customer experiences.

The frictions experienced by the Participating Banks and part of their customer base, because of Core KYC, detracted from the customers' experience. One of the potential consequences of this was the propensity for some people to withdraw from the Core KYC process before it was completed. It is not clear what happened with those potential customers: whether they stayed with an existing reporting entity relationship or found another reporting entity whose process is easier to comply with.

But at least at the margins, this has the potential to exclude some people from consuming banks' financial products and services, a point raised by a Participating Bank.

---

[17] (i.e. AML/CFT compliance related investments, data storage costs, additional staff requirements, staff training, etc)
[18] See Appendix 7 for more information on he AIVCOP.
[19] Face-to-face Core KYC will likely become even more problematic rural customers, given the continuing trend of bank branch closures throughout rural New Zealand - nzherald.co.nz/personal-finance/news/article.cfm?c_id=12&objectid=12203497.

4.2.2 Frictions arising from compliance with the AML/CFT Act

Only some reliance provisions are used by reporting entities, as significant regulatory risk remains with the relying reporting entity and practical difficulties in designing those arrangements hinders that use.

The Participating Banks highlighted the unused status of the Approved Entity Reliance regime and that the Reporting Entity Reliance and Agency Reliance regimes are seldom used between banks.

The regulatory risks to a bank relying on a third party to perform Core KYC given that ultimate responsibility for compliance remained with the bank (as a reporting entity) was consistently emphasised. On the other hand, the legal risks to the third party performing Core KYC was another barrier. Difficulties associated with supervising third parties and the need to agree to commercial, liability and information sharing terms between the banks, meant there were many regulatory and practical barriers to the adoption of these AML/CFT reliance regimes by the banks.

There may also be competitive reasons between reporting entities where one has to exercise close supervision of the other, with the risk of access to commercially sensitive information disincentivising the formation of a reliance relationship.

4.2.3 Observed frictions in the use of electronic identity verification

Electronic identity verification is currently being used by reporting entities, but this use is often deficient.

In April 2019, the FMA released a report on its monitoring of reporting entities and their compliance with the AML/CFT regime over a two year period. It found that reporting entities often **did make use of electronic identity verification** to identify and verify their customers, but this use contained a number of deficiencies. These included the reporting entity failing to clearly describe how the relevant criteria was satisfied, using two sources of identification but in a process that was not described in its AML/CFT programme, or having an electronic verification process in its AML/CFT programme that does not align with the AIVCOP. [20]

Questionnaire responses indicated mixed adoption of electronic identity verification with concerns being expressed as to the level of reliance that was provided.

4.3 RECOURSE AND LIABILITY

4.3.1 Recourse and liability under the AML/CFT Act

Reporting entities that fail to conduct Core KYC are obliged to terminate existing business relationships and not re-establish them, refuse to carry out occasional transactions or activities, and consider whether to make a suspicious activity report. Failing to satisfy CDD obligations is a civil liability act, but knowingly or recklessly doing so can bring criminal liability.

A reporting entity is ultimately responsible for complying with its Core KYC obligations under the AML/CFT Act.[21] Therefore, a reporting entity relying on the Core KYC performed on a customer by a third party, is ultimately responsible for ensuring the Core KYC performed meets the requirements of the AML/CFT Act. This applies even if that third party (as a reporting entity), performed Core KYC on a person for its own compliance with the AML/CFT Act. More information on AML/CFT reliance is in Appendix 6 below (section 14.6).

[20] Financial Markets Authority *Anti-money laundering and countering financing of terrorism: Monitoring report 1 July 2016-30 June 2018* (April 2019) at 9.
[21] AML/CFT Act, section 33(3).

If a reporting entity is unable to meet its Core KYC obligations in relation to a customer, that reporting entity must:

- Terminate the existing business relationship that it has with that customer;[22]
- Not re-establish that business relationship;[23]
- Not carry out any occasional transaction or activity with or for them;[24] and
- Consider whether it should make a suspicious activity report (only disclosing that possibility to prescribed persons).[25]

Part 3 of the AML/CFT Act provides both a civil and a criminal enforcement regime for non-compliance. Failing to comply with requirements under the AML/CFT Act, including failing to conduct required Core KYC, will constitute a "civil liability act".[26] Furthermore, a person who knowingly or recklessly fails to conduct Core KYC could be criminally liable.[27] The courts will deem a person to be "reckless" where he or she is aware of a risk and, having regard to that risk, acts in a manner that a reasonable and prudent person doing their best to comply with the law would not take.

4.3.2 Penalties under the AML/CFT Act

The consequences of a civil liability act can be a formal warning, an enforceable undertaking, an injunction or a pecuniary penalty.

Where a civil liability act is alleged, an AML/CFT Supervisor may issue a formal warning, accept an enforceable undertaking (and seek a court order for any breach thereof), seek an injunction or apply to the court for a pecuniary penalty.[28]

The pecuniary penalty may be paid to the Crown or another person specified by the court, and may be, depending on the obligation breached, up to $200,000 for an individual or $2 million for a body corporate or partnership.[29] In determining an appropriate pecuniary penalty, the court must have regard to all relevant matters, including:[30]

- The nature and extent of the civil liability act;
- The likelihood, nature, and extent of any damage to the integrity or reputation of New Zealand's financial system because of the civil liability act;
- The circumstances in which the civil liability act occurred; and
- Whether the person has previously been found by the court in proceedings under this Act to have engaged in any similar conduct.

A reporting entity or person found criminally liable under the AML/CFT Act, could be liable for, a term of imprisonment of not more than two years and/or a fine of up to $300,000, if an individual or, a fine of up to $5 million, if a body corporate or partnership.[31]

Where civil and criminal liability overlaps, a court cannot impose a further penalty under either if a penalty has already been imposed under either in relation to the (or substantially the) same conduct.[32] Proceedings

[22] AML/CFT Act, section 37(1)(b).
[23] AML/CFT Act, section 37(1)(a).
[24] AML/CFT Act, section 37(1)(c).
[25] AML/CFT Act, section 37(1)(d) and 37(1)(e).
[26] AML/CFT Act, section 78.
[27] AML/CFT Act, section 91.
[28] AML/CFT Act, section 79.
[29] AML/CFT Act, section 90(3).
[30] AML/CFT Act, section 90(4).
[31] AML/CFT Act, section 100.
[32] AML/CFT Act, section 74(1).

for more than one civil penalty can be brought in relation to the same conduct or even substantially the same conduct, but no more than one penalty will need to be paid.[33]

Toogood J in *Department of Internal Affairs v Ping An Finance (Group) New Zealand Company Limited*[34] oversaw the first pecuniary penalty decision under the AML/CFT Act and set the judicial approach to setting pecuniary penalties. The respondent in *Ping An* was seen to have "wholesale disregard" for complying with the AML/CFT Act's requirements, including widespread failure to perform CDD on its customers. His Honour highlighted the importance of CDD under the AML/CFT regime before he imposed a fine of $1.495 million[35] on the respondent for failing to conduct CDD (pecuniary penalties totalled $5.29 million for all of Ping An Finance's breaches of the AML/CFT Act).[36]

Since *Ping An Finance (Group)*, the DIA has succeeded in two more civil proceedings against reporting entities for non-compliance with AML/CFT obligations (including the CDD obligations). In 2018, Qian Duo Limited was required to pay $356,000 in pecuniary penalties, while in 2019, Jin Yuan Finance Limited was ordered to pay a pecuniary penalty of approximately $4 million.[37]

The first criminal prosecution under the AML/CFT Act recently concluded. Jiaxin Finance Limited, Mr Qiang Fu and Ms Fuqin Che, received fines of $2.55 million, $180,000 and $202,000, respectively, for failing to conduct CDD (knowingly or recklessly, which is a criminal offence)[38] as well as other offences under the AML/CFT Act.[39] The parties had been found guilty of criminal offences relating to 311 transactions worth approximately $53 million in total.[40] Walker J highlighted the deterrent purpose of the AML/CFT while setting the fines.

The penalties in the AML/CFT regime underscore the importance of the regime. The penalties incentivise compliance[41], which is important to support New Zealand's access to international financial markets and banking networks. But they also strongly incentivise risk aversion – in this case in the form of reliance on others. The precedents set for pecuniary penalties under the AML/CFT Act (albeit for extraordinary levels of non-compliance) also highlights the enormous risks to reporting entities for their non-compliance, in addition to the damage to their reputations (among other consequences).

4.3.3 Reputational risk

Allegations of breaching the AML/CFT regime carries immeasurable harm to a reporting entity's reputation.

The reputational risks of non-compliance also create powerful incentives, even where there is only a public warning. Those have recently been highlighted by AUSTRAC's legal action against banks in Australia for alleged failures to comply with the equivalent regime in Australia's Anti-Money Laundering and Counter-Terrorism Financing Act 2006.[42] Those actions (or even the announcement of intended action) resulted in significant negative media publicity, and contributed to significant drops in share price. They have also been a contributor to the restructuring of the board and senior management, of those banks. [43]

---

[33] AML/CFT Act, section 74(2).
[34] *Department of Internal Affairs v Ping An Finance (Group) New Zealand Company Limited* [2017] NZHC 2363.
[35] *Ping An Finance* at [126].
[36] *Ping An Finance* at [107]. His Honour stated: "Customer due diligence helps reporting entities to understand customers and the associated risk. Without CDD, a reporting entity is vulnerable to being exploited and offering a safe harbour for money laundering or financing terrorism. As the AML/CFT regime is heavily reliant on reporting entities providing information relating to customer identity to the police, the entire efficacy of the system is undermined by non-compliance."
[37] The DIA has also recently brought its fourth civil proceedings and the first criminal proceedings under the Act. The criminal proceedings were brought against an unnamed company and two employees accused of failing to report several suspicious transactions wor h more than $53 million.
[38] AML/CFT Act, section 91.
[39] *R v Jiaxin Finance Limited, Qiang Fu and Fuqin Che* [2020] NZHC 366. The other criminal offences involved failing to keep adequate records to a suspicious transaction under section 95, and to report a suspicious transaction under section 92. Ms Fuqin Che was also convicted under section 101 for structuring a transaction to avoid the application of one or more AML/CFT requirements.
[40] *R v Jiaxin Finance Limited, Qiang Fu and Fuqin Che* [2019] NZHC 3058.
[41] Circumstances of lower risk may not be seen as warranting the costs and intrusion involved in determining a person's identity at a higher level of confidence for Core KYC purposes, however the risk of prosecution may leave reporting entities reluctant to take that risk.
[42] Anti-Money Laundering and Counter-Terrorism Financing Act 2006 (Cth).
[43] theaustralian.com.au/na ion/cba-blasted-over-breaches-as-700m-fine-laid-down/news-story/f31fb8c5251e8889d2d3da15a88ad723.

These events have likely contributed to additional conservativism on the part of reporting entities in New Zealand, given the risk of non-compliance goes beyond penalties imposed under the AML/CFT Act. Again, a result is a reluctance to rely on other reporting entities.

4.3.4 Implications of failing to perform Core KYC under the AML/CFT Act

Failure to conduct Core KYC is a civil liability act. A reporting entity's culpability will depend on several factors in the context, including its oversight of a third party it is relying on.

Under Reporting Entity Reliance and Agency Reliance, a reporting entity who has failed to perform Core KYC to the required standards of the AML/CFT Act, because of any failures by the third party relied upon, will commit a civil liability act. Theoretically, Approved Entity Reliance, which has yet to be activated by regulations on the recommendation of the Minister of Justice, would otherwise be available to reporting entities who engage in Reporting Entity Reliance. The courts have not dealt with a reporting entity who has failed to perform Core KYC (and therefore its obligation to perform CDD) due to a third party relied upon.

A reporting entity's culpability will depend on a number of factors, including the adequacy and effectiveness of its procedures, policies and controls for how the third party may perform Core KYC on the reporting entity's behalf, as well as the quality of its oversight of the third party to ensure the standards of the AML/CFT Act are met. The courts could find a reporting entity who has knowingly done neither, to have a level of culpability that slightly resembles, but is likely less than, the culpability of the respondent in the *Ping An Finance (Group)* proceeding. In this scenario, the reporting entity's vulnerability to money laundering or financing terrorism exploitation, could be seen to be somewhat comparable to Ping An Finance (Group) New Zealand Company Limited.

4.3.5 Recourse and liability in the common law and under the Fair Trading Act 1986

An arrangement for a reporting entity to rely on a third party for CDD purposes creates potential liability for the third party. Similarly, an issuer of identity records may also be liable to a reporting entity that has relied on those records for Core KYC.

New Zealand's legal framework raises issues with potential liability and recourse between entities in the common law, specifically:

- By a reporting entity ("Entity A") against another reporting entity ("Entity B"), where Entity A has relied on the Core KYC carried out by Entity B; and
- By Entity A against an issuer of identity records (such as DIA) where Entity A has relied on incorrect identity records provided to conduct Core KYC.

Entity A vs Entity B

Negligence

Negligence could be the strongest cause of action available to reporting entities relying on a third party.

One key potential source of recourse is the tort of negligence.[44] A claim in negligence needs the following elements[45]:

- Entity B owing Entity A a duty of care;
- Entity B breaching that duty of care (i.e. was careless);
- Entity A suffering damage that was caused by Entity B's breach of duty; and

[44] Another possibility is the related claim of negligent misstatement, discussed at [0].
[45] *Tort – A to Z of New Zealand Law,* (online edition, Thomson Reuters), [59.5.1].

- The damage caused not being too remote (i.e. a proximate consequence).

A claim of negligence against Entity B is feasible and it may eventuate in some cases, subject to at least two caveats:

- Given that Entity A's consent is required, Entity B would likely impose conditions on Entity A's reliance, in order to attempt to exclude or mitigate any liability in negligence (or otherwise), when providing any Core KYC information. We would expect a strict limitation on any liability.
- If a successful negligence claim was made out, there could be a counter claim for contributory negligence if Entity A didn't have policies and procedures in place to actively communicate standards, and it didn't monitor compliance with Entity B, as required by the AML/CFT Act.[46]

More analysis on the possibility of a cause of action in negligence is set out in Appendix 11.

Fair Trading Act 1986

The Fair Trading Act 1986 could be used by a reporting entity relying on a third party.

It may be possible for Entity A to bring a claim against Entity B under the FTA for misleading or deceptive conduct in trade.[47] A misrepresentation of a fact will constitute misleading conduct, and Entity B need not have intended to mislead (or to have been negligent).[48] The question is whether the conduct, examined objectively, is deceptive or misleading in the circumstances. Civil damages can be awarded if it can be shown that Entity A suffered loss or damages as a result of Entity B's breach.[49]

If Entity B is simply acting as a "conduit" to pass on information from someone else without endorsing it (and makes that clear), Entity B will not be liable.[50] That seems unlikely in the present case however, where Entity B has to consent to their Core KYC being relied upon, and is essentially endorsing the underlying information. However, as for negligence, Entity B may seek to contractually exclude or limit liability under the FTA, which is possible in some circumstances where both parties (as here) are in trade.[51]

Fiduciary duties

The existence of fiduciary duties by a third party to a relying reporting entity should be considered.

Where Entity B has consented to Entity A relying on its Core KYC, Entity B could be deemed to be Entity A's agent for Core KYC purposes (especially in the case of Agency Reliance), with some resulting fiduciary obligations.[52] In practice however, tortious duties (and even contractual duties, if a contractual relationship is formed) are likely to be more relevant. This is because it is more likely that Entity B would breach a duty of care in tort (see the previous discussion on negligence), than breach core fiduciary duties (which are to avoid unauthorised personal benefit from the relationship; to avoid conflict between personal interest and duty to the beneficiary; to avoid divided loyalties, etc). Failing to take reasonable care, without anything more, is not a breach of a fiduciary duty. If all that can be shown is that a plaintiff has suffered loss because of the defendant's negligence, there will be no fiduciary breach.[53]

---

[46] In such a case, Entity A would likely also not have the 'reasonable cause to believe' Entity B had conducted CDD to at least the standard required by AML/CFT Act, section 33(3A)(b).
[47] Fair Trading Act 1986, section 9.
[48] *Burrows, Finn and Todd on the Law of Contract in New Zealand*, (LexisNexis NZ Limited, 6th edition, 2018) at 11.3.2(b) and (c)
[49] Fair Trading Act 1986, section 43 and *Burrows, Finn and Todd on the Law of Contract in New Zealand*, (LexisNexis NZ Limited, 6th edition, 2018) at 11.3 3.
[50] *Burrows, Finn and Todd on the Law of Contract in New Zealand*, (LexisNexis NZ Limited, 6th edition, 2018) at 11.3.3
[51] Section 5D Fair Trading Act 1986
[52] See *Equity – A to Z of New Zealand Law* (online ed, Thomson Reuters), paragraph 26.17.2.3
[53] See *Equity – A to Z of New Zealand Law* (online ed, Thomson Reuters), paragraph 26.17.2.2

Entity A vs Issuer of incorrect identity record

Negligence, negligent misstatement and breach of a statutory duty should be considered by issuers of identity credentials.

Entity A has several potential causes of action it might be able to use to seek recourse against an issuer of identity records (like the DIA), including:

- Negligence (see above and Appendix 11);
- Negligent misstatement; or
- Breach of a statutory duty.

However, these causes of action could only be available if the issuer doesn't have any statutory immunity against civil claims for damages arising during the course of carrying out its statutory functions.[54] It is also unlikely that any claim under the FTA for misleading or deceptive conduct would be possible in relation to a government department or authority issuing identity records. Where carrying out statutory (or regulatory) functions, such entities are unlikely to be acting "in trade".[55]

Negligent misstatement

A cause of action for negligent misstatement against an issuer of identity credentials will likely depend on the reasonableness of reliance and policy factors.

A claim for negligent misstatement may be available against an issuer of identity records (and, potentially, Entity B). The following elements would need to be established:

- Entity A relied upon the statement complained of; and
- A duty of care exists given the circumstances in which the statement was given.

In terms of reliance, it must also be reasonable for Entity A to rely upon the issuer's "statement" (such as the contents of the identity document). The first limb seems likely to apply to identity documents issued by government agencies. However, it's less clear if the government agency owes a duty to Entity A. The law, generally, deems a defendant to have assumed responsibility and find damages to be not too remote, if when the statement was made, the defendant foresaw or should have foreseen that the plaintiff would reasonably place reliance on the statement. This depends on the statement's purpose, i.e. the purpose for which the statement was made and the purpose for which the plaintiff relied on it (and, in particular, whether they were the same purpose).[56]

Policy factors will also be relevant as there are legitimate public interests in government entities being able to perform their role without the "chilling effect" of undue vulnerability to negligence actions.[57] However, where a key role of the public entity is to issue identity documents for the purpose of proving identity, that may somewhat fall away. Nevertheless, the damage suffered must still not be too remote.

Breach of statutory duty

The existence and scope of statutory safe harbours are relevant to potential breaches of statutory duties by an issuer of identity credentials.

---

[54] For example, sec ion 65 of the Electronic Identity Verification Act 2012; section 91B of the Births, Deaths, Marriages and Relationships Registration Act 1995; and section 20 of the Identity Informa ion Confirmation Act 2012. Any statutory immunity could be carved out for the issuer's bad faith or gross negligence.

[55] For example, *Marina Holdings Ltd (in rec) v Thames-Coromandel District Council* (2010) 12 NZCPR 277 at [54]-[55] (a council issuing a code compliance certificate was not ac ing in trade for the purposes of the Fair Trading Act); *Dental Council of New Zealand v Gibson*, HC Auckland, CIV-2010-404-000230, 3 June 2010 at [46] (disciplinary bodies deciding complaints were carrying out statutory functions and not acting in trade).

[56] *Attorney-General v Carter* [2003] 2 NZLR 171 at [22] – [27], and *Marina Holdings Ltd (in rec) v Thames-Coromandel District Council* (2010) 12 NZCPR 277 at [31]-[32]

[57] *Attorney-General v Carter* [2003] 2 NZLR 171 at [35]

There is no such thing as "negligent" breach of a statutory duty. If (and only if) the statute creates a duty to take care, breaching that duty in itself is a breach of the statutory duty.[58] It also appears to be difficult to establish a breach of statutory duty.[59] The ability to do so depends on the construction of the statute in question, and the courts will ask whether Parliament intended to confer a private right of action on a person who suffered harm as a result of a breach of the duty. The courts are only prepared to do so in limited circumstances.[60]

One example of a right to claim damages for breach of a statutory duty can be found in *Cashmere Pacific v NZ Dairy Board*. The Registrar of Companies in this case, was found to have failed to maintain a proper record of registration of a debenture, with the court considering that there was "clearly of necessity a reliance" on the Register as the official record, maintained pursuant to the statute.[61]

4.4 DIFFERENCES IN TIME

Different entities may collect Core KYC at different points in time. This creates a risk of information being outdated where one entity later relies on information collected earlier by another entity.

A reporting entity must perform Core KYC[62] when:

- It establishes a business relationship with a new customer;
- Its customer seeks to conduct an occasional transaction or activity through it; or
- For existing customers, according to the level of risk involved, if there has been a material change in the nature or purpose of its business relationship with that customer and it considers that it has insufficient information about that customer.

Reporting entities who share a common customer will likely need to perform Core KYC on that customer at different times. This could be due to the different commercial natures of their relationship with the customer, as well as the different times they form their business relationship with the customer.

For the purposes of Reporting Entity Reliance, a reporting entity could receive Core KYC performed by a third party that is outdated,[63] in situations where the third party has not needed to perform subsequent Core KYC on the customer and ongoing Core KYC has not been performed. The reporting entity relying on the third party would need to perform its own Core KYC to comply with its obligations under the AML/CFT Act. This will place additional administrative burdens on the reporting entity as it will need to have its own procedures, processes and controls in place to perform Core KYC on a person itself. These procedures, processes and controls must also be reflected in the reporting entity's AML/CFT programme. The risk to the reporting entity of receiving outdated information could be mitigated if the reporting entity is able to rely on more than one third party to perform Core KYC on a common person (i.e. a customer or beneficial owner, etc). Naturally, the more reporting entities perform Core KYC on the same person, the more likely that at least one reporting entity holds Core KYC information on that customer that is not outdated.

---

[58] *Attorney-General v Carter* [2003] 2 NZLR 171 at [41]-[44].

[59] *Tort – A to Z of New Zealand Law,* (online edition, Thomson Reuters), [59.8.2.02]: "*It would be fair to say that these days the tendency is to find against liability".*

[60] *Tort – A to Z of New Zealand Law,* (online edition, Thomson Reuters), [59.6.6] and [59.8].

[61] *Cashmere Pacific v NZ Dairy Board* (1995) 8 PRNZ 661 at 669-671. The statute expressly required the Registrar to keep such a register. Note also *Altimarloch Joint Venture Limited v Moorhouse* HC Blenheim CIV-2005-406-91, 3 July 2008 at [144] – 153], finding breach of a statutory duty of care to a purchaser in issuing an inaccurate LIM. On the other hand, see *Attorney-General v Carter* [2003] 2 NZLR 171 at [46] where the Ministry of Transport was required by statute to issue ship survey certificates, but there was no statutory obligation requiring them to take care in doing so. Accordingly, there was no claim possible that the Ministry issued the certificate negligently, but, if at all, only for issuing it erroneously. The Court of Appeal declined to find any such duty or breach.

[62] There are additional circumstances in which Core KYC information may need to be obtained / verified / reverified / updated, or whether s11(4) prevails.

[63] Core KYC could become outdated if, for example, the customer has changed their, name or residential address.

As described above, a reporting entity may reuse documents, data or information that it has previously obtained and verified through conducting CDD, except where it has reasonable grounds to doubt the adequacy or veracity thereof.[64]

Importantly, the FATF Standards also support this ability for an entity to rely on previous identification and verification steps that it has taken unless there are doubts as to their veracity.[65] That said these expressly relate to an entity **relying on its own past CDD activities**, rather than the past CDD activities of another entity, and are placed separately from the third-party reliance provisions.

However, they do add further support to the notion that previously obtained and verified CDD information can be legitimately useable where there is no reason to doubt its continued accuracy. The length of time between this verification and reliance may, of course, be an element in such doubt, but it would be the total assessment of that doubt (rather than mere time in isolation) that would determine the usability of particular information.

For the purposes of Agency Reliance, it is not likely that these timing issues will apply to a reporting entity relying on the Core KYC performed by a third party. The reporting entity would be expected to engage the third party to perform subsequent Core KYC and/or ongoing Core KYC on the customer to comply with its obligations under the AML/CFT Act.

4.5 VERIFYING A PERSON'S RESIDENTIAL ADDRESS

In practice, many documents which are being used to verify a person's residential address, like utility bills, appear to be not fit for purpose. This underscores some of the inherent challenges of verifying a person's address.

Core KYC under the AML/CFT Act requires reporting entities to verify the residential address of its customer, the beneficial owners of its customer and any person acting on behalf of its customer.[66] AIVCOP states that a reporting entity can verify a person's address using documents, data or information issued by a reliable and independent source. AIVCOP however explicitly states it does not prescribe the way in which reporting entities can fulfil this obligation.[67] The use of documents issued by organisations which are not normally used for the purposes of evidencing a person's identity, provides some relief for reporting entities but it has limitations in practice.

There is no universally applicable legal requirement for official registration of residential address, (although those entitled to vote do have obligations under the Electoral Act 1993, this is not well enforced).

Further, not all persons have a residential address (for example the homeless, or others with transitory life styles, including for certain types of work). Even if they do at a point in time have a residential address, it may change frequently and any number of times.

Moreover, even when a person has an address, evidencing that address can be difficult. Common examples may be persons residing with family members, e.g. adult children residing with parents, or the elderly residing with their adult child. Another example is a group flatting situation where not all residents will be formally tenants in the tenancy agreement.

The most common approach in practice is the use of a utility company's invoice as evidence of a person's residential address (i.e. utility bill). Utility companies, such as telecommunications companies, power companies, water companies and gas companies, generally provide their goods and services to a fixed

[64] AML/CFT Act, section 11(4).
[65] Financial Action Task Force, *International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation* (Financial Action Task Force, Paris, 2012-2019) at 61 (Interpretive Note to Recommendation 10).
[66] AML/CFT Act, sections 11, 15(d) and 16.
[67] Amended Identity Verifica ion Code of Practice 2013, at 2.

place of residence, and in some cases, install proprietary devices in the place of residence to be able to deliver their goods and services and monitor their consumption. On this basis, utility companies are considered to have an incentive to determine the residences to which they're delivering their goods and services to with certainty. Though, in recent times some utilities (e.g. telephone) are now mobile – i.e. they do not attach to an address.

However, even when the utility is tied to a fixed address, not all or even any of the individuals residing there may be the bill payers (e.g. in the scenarios mentioned above).[68] In this scenario, a utility bill could be used as evidence that a place of residence exists, but it could not be used as evidence that it is the residential address of any person other than the bill payer(s), if indeed that person resides there. Some New Zealanders are not the payer for any utilities tied to a particular address, at all.

The EOI Standard is a good practice guide for government agencies that regularly establish and confirm the identities of individuals accessing their services. The EOI Standard is not formally part of the AML/CFT regime, and following the standard does not necessarily mean a reporting entity has performed Core KYC to the standard required under the AML/CFT Act. More information about the EOI Standard is set out in Appendix 12.

However, the EOI Standard does provide a reference point. It recognises utility bills as a "supporting" document for proving a person uses a particular identity in the community, and this has become common practice under the AML/CFT regime.[69]

The limitations of using a utility bill to verify a person's residential address, reflects the broader issues of including a person's residential address as one criteria for establishing a person's identity under the AML/CFT Act.

4.6 RELIANCE ON THIRD-PARTY VERIFICATION OF A PERSON'S IDENTITY

Although reliance on third parties for CDD purposes is permitted by the AML/CFT Act, those provisions are less used (than would be optimal). While the FATF Standards also allow for third party reliance, they do not go as far in the New Zealand regime.

It would be reasonable for reporting entities engaging in Reporting Entity Reliance or Agency Reliance to expect to use these forms of reliance and reduce the administrative time and costs of performing Core KYC on a person, on the presumption that such Core KYC has already been performed by a third-party.

However, as discussed in Appendix 6 (section 14.6.1), for Agency Reliance purposes, a reporting entity must have adequate and effective procedures, policies and controls for how the third party may perform Core KYC on the reporting entity's behalf, and it must monitor the third party to ensure the standards of the AML/CFT Act are met.

Similarly, for Reporting Entity Reliance purposes (and Approved Entity Reliance purposes), a reporting entity must have reasonable cause to believe that the third-party has conducted Core KYC to the AML/CFT Act's standards (at least). The administrative burden of these requirements could negate or even exceed the administrative benefits of Agency Reliance to the reporting entity, and to a lesser degree, Approved Entity Reliance.[70] Approved entities are required to be prescribed by regulation, and none have been yet.

---

[68] For example, this includes a place of residence that accommodates a family but is owned by a family trust. Another example is a place of residence that accommodates individuals that are unrelated to each other (i.e. a flatting situation), of which, only one individual is the tenant under the tenancy agreement.

[69] dia.govt.nz/diawebsite.nsf/wpg_URL/Resource-material-Evidence-of-Identity-Standard-Index?OpenDocument at page 75.

[70] For the purposes of Approved Entity Reliance, a reporting entity must have reasonable cause to believe that the third party has conducted relevant CDD procedures to at least the standard required by the AML/CFT Act. There is no specific guidance on this point from the AML/CFT Supervisors. Mere prescription as an approved entity under the AML/CFT Act could be enough for a reporting entity to have reasonable cause of its belief. However, the more prudent and appropriate interpretation of this requirement, is that a repor ing en ity is required to inspect and to form a reasonable belief that the approved entity's procedures for performing CDD meets the standard required by the AML/CFT Act, before it can have reasonable cause of its belief.

A reporting entity must have "reasonable cause to believe the approved entity has conducted relevant Core KYC at least to the standard required by the AML/CFT Act." Oversight over an "approved entity", should likely be less onerous for a reporting entity for Approved Entity Reliance purposes, than if it were required to oversee a non-reporting entity for Agency Reliance purposes, because the approved entity / reporting entity itself is subject to supervision by the AML/CFT Supervisors.

However, despite this prospect of reduced effort and compliance costs, there are inherent drivers which would dissuade its use at any material scale – including the reality that a reporting entity relying on a third party remains ultimately responsible for its own compliance. In any event, the former may not have sufficient confidence in the latter to risk relying on them. The former may also deem it more efficient across various measures to continue to perform the activity itself.

Importantly, the Ministry of Justice has not put Approved Entity Reliance into effect, as no entities have been approved. This may or may not be a deliberate choice, as the Ministry of Justice has expressed a number of concerns about how it would operate in practice.[71]

Recommendation 17 from the FATF Standards permits reporting entities[72] to rely on third parties for CDD purposes, subject to certain criteria (see Appendix 3 for more information on FATF Recommendation 17). However, this recommendation also states that "the ultimate responsibility for CDD measures remains with the [reporting entity] relying on the third party" in those situations. On this basis, putting Approved Entity Reliance into effect would be inconsistent with the FATF Standards.[73] Furthermore, this form of reliance is arguably not reconcilable with one of the AML/CFT Act's purposes (which is to adopt the FATF Standards).[74] Although that purpose is expressly subject to it being "appropriate in the New Zealand context",[75] a cogent argument would need to be made as to why the New Zealand context makes it appropriate for reporting entities to be able to escape liability.

The ability to rely on an approved entity to fulfil obligations, free from liability for those obligations, presupposes that the situation in which the approved entity conducted CDD is the same as the situation in which the relying reporting entity requires CDD. As well as the concerns about differences in time in section 4.4 above where circumstances may have changed in the meantime and previously accurate CDD information may have become outdated, there is also the fact that the level of risk, and accordingly the level of CDD required, may differ between those situations.[76] The focus may, for present purposes, be confined to Core KYC, which is less affected by different levels of risk than the full array of CDD information. However, as the Approved Entity Reliance regime could be applied to all CDD procedures under the AML/CFT Act,[77] it would have to be considered more widely appropriate before it could be put into effect.

4.7 PRIVACY LAW

The Privacy Act 1993 is relevant to the success of any form of widespread reliance amongst reporting entities. Obtaining people's consent before sharing Core KYC information will be imperative.

A reporting entity collects Core KYC to comply with its obligations under the AML/CFT Act. Core KYC is 'personal information' under the Privacy Act. The Privacy Act does not give reporting entities an overriding power or authority to share Core KYC information with other reporting entities as of right. Therefore,

[71] Ministry of Jus ice *Anti-Money Laundering and Countering Financing of Terrorism: Departmental Report for the Law and Order Committee* (May 2017) at [299]-[302].
[72] "Financial institutions" in the terms of the FATF Standards, but for present purposes this means reporting entities.
[73] Ministry of Jus ice *Anti-Money Laundering and Countering Financing of Terrorism: Departmental Report for the Law and Order Committee* (May 2017) at [290].
[74] AML/CFT Act, section 3(1)(b).
[75] AML/CFT Act, section 3(1)(b).
[76] Ministry of Jus ice *Anti-Money Laundering and Countering Financing of Terrorism: Departmental Report for the Law and Order Committee* (May 2017) at [302].
[77] AML/CFT Act, section 33(1).

reporting entities are subject to, and must comply with, the IPPs of the Privacy Act in relation to the collection and disclosure of Core KYC to third-parties.

Therefore, for Entity B to share Core KYC with Entity A in a manner that is compliant with the Privacy Act:

- Entity B will need to advise individuals that Core KYC may be disclosed to Entity A;[78]
- Entity B will need to obtain informed consent to the proposed information sharing from the Data Subject, which must be obtained prior to the disclosure to information sharing;[79] and
- Entity A needs to confirm to Entity B that it will receive and use the Core KYC for the sole purpose of conducting Core KYC.[80]

It is possible for digital identity platforms to be developed (or which may have already been developed), that would enable Entity A to receive confirmation that a person's verified Core KYC exists, without ever receiving the person's personal information.

4.7.1 Privacy Act obligations

Reporting entities looking to disclose Core KYC should obtain consent from the subjects of the Core KYC to both collect and disclose it.

Consent to the collection and use of Core KYC should be sought by a reporting entity from a Data Subject at the time Core KYC is collected. There would be risk in assuming that the Data Subject's initial consent to provide Core KYC stretches to the disclosure of Core KYC to another reporting entity (to enable that reporting entity to comply with its AML/CFT obligations). This is because it's unlikely the Data Subject reasonably contemplated this disclosure at the time Core KYC was provided to the first reporting entity.

Accordingly, should reporting entities wish to share Core KYC, reporting entities will need to:

- Advise the Data Subject that Core KYC may be shared with third parties at the time Core KYC is collected;[81] and
- Obtain the Data Subject's 'authorisation' to the disclosure of their personal information.[82]

To obtain consent, Entity B could either:

- At the time of collecting Core KYC, expressly seek the consent of the Data Subject to further sharing of the Core KYC for the purposes of conducting additional Core KYC by Entity A (i.e. by an 'opt in' mechanism); or
- If an 'opt in' is not obtained or not practicable, obtain consent from the Data Subject prior to each further disclosure to Entity A.

A Data Subject can complain to the Privacy Commissioner if Entity B didn't comply with its Privacy Act obligations. Damages could be awarded if a Data Subject can establish that there has been an interference with their privacy and that they have suffered harm. Entity B could also be subject to a fine of up to $2,000 (under the existing Privacy Act, which may be increased under the proposed law). While compensation and fines are low, reputational damage resulting from a complaint will likely be considerable.

[78] For the purposes of IPP3.
[79] For the purposes of IPP11.
[80] For the purposes of IPP10.
[81] For the purposes of IPP3.
[82] For the purposes of IPP11(d).

4.7.2 Sharing of information between reporting entities and AML/CFT Supervisors

Disclosure of information to government agencies, such as the AML/CFT Supervisors, may involve different treatment.

The privacy policy (or in some instances, the product and/or service terms and conditions) of a reporting entity would need to specify that the reporting entity may disclose Core KYC to governmental agencies before doing so.[83] Assuming the privacy policy or terms of services of a reporting entity specifies this, any disclosure of Core KYC by a reporting entity to its AML/CFT Supervisor would be permitted as it would be directly related to the purposes in connection with which the information was obtained.[84]

Even if this disclosure was not expressly provided for in a reporting entity's privacy policy or terms of service, a reporting entity's disclosure of Core KYC to its AML/CFT Supervisor would likely still be permissible.[85] Under these exceptions, Core KYC could be disclosed where the reporting entity is:

- Satisfied on reasonable grounds that the disclosure is necessary for a law enforcement agency to prevent, detect, investigate, prosecute or punish criminal offences or breaches of laws;[86] or
- Where the disclosure of the information is necessary to enable an intelligence and security agency to perform any of its functions".[87]

In any event, the AML/CFT Supervisors have broad inspection powers under the AML/CFT Act.[88] An AML/CFT Supervisor could require, the production of or, access to, Core KYC information from a reporting entity that is under its supervision (among other things).

4.7.3 Storage and security of Core KYC

Reporting entities are required by an IPP to protect Core KYC that they hold.

One of the IPPs requires agencies that hold personal information to ensure that the information is protected, by such security safeguards as it is reasonable in the circumstances to take, against loss and access, use, modification, or disclosure.[89] Where reporting entities have obtained Data Subjects' consent, and are sharing Core KYC, appropriate safeguards should be put in place to guard against loss and unauthorised disclosure. Such information should be held in encrypted form where feasible.

4.7.4 Approved Code of Practice

An Approved Code of Practice from the Privacy Commissioner could amend the standards of IPPs to enable the sharing of Core KYC.

A person or persons can apply to the Privacy Commissioner with a request to issue an approved code of practice in relation to information sharing for Core KYC purposes. Approved codes of practice amend or vary the operation of IPPs to a more or less stringent standard.[90]

This mechanism could theoretically be used by a group of reporting entities, like the Participating Banks, and other ecosystem participants of the New Zealand Government Trust Framework, to make a joint

[83] The AML/CFT Supervisors are government agencies.
[84] And consistent with IPP11(a).
[85] Permissible under IPP11(e)(i) and (fa).
[86] For the purposes of IPP11 (e)(i).
[87] For the purposes of IPP11 (fa).
[88] AML/CFT Act, section 132(2)(a) and (b).
[89] For the purposes of IPP 5.
[90] Privacy Act, sec ion 46.

application under the Privacy Act,[91] in order to procure the issuance of a code of practice to enable them to share Core KYC between themselves.

Following receipt of a request, the Privacy Commissioner will consider the merits of such a code and determine whether it is appropriate for a code to be issued.[92]

[92] MinterEllisonRuddWatts recommends the exploration of this process.

5. POSSIBLE SOLUTIONS

5.1 TECHNOLOGICAL SOLUTIONS

5.1.1 New electronic identity technologies

New and reliable electronic identity technologies will likely be of tremendous assistance to reporting entities conducting Core KYC. Widespread use by reporting entities would need some combination of strong industry leadership driving adoption, robust technological innovation, changes to the EIVA and/or AML/CFT Supervisors' support (through new official guidance or a new code of practice safe harbour). The New Zealand Government Trust Framework may either be the focal point to greater adoption of electronic identity technologies or merely one supporting factor. However, without legal change as described above these benefits may not be realised.

The DITP's work on the New Zealand Government Trust Framework, alongside the private sector and other government agencies, embodies the government's recognition of the importance of having a trusted and reliable system for New Zealand digital identity in an ever growing local and global digital economy. Core KYC is one of a number of use cases for the application of digital identity technology solutions. The level of collaboration already shown must continue before any New Zealand Government Trust Framework containing an ecosystem of participants with divergent and competing interests can be successfully established.

In terms of the Core KYC use case for digital identity, the AIVCOP provides that a reporting entity can satisfy electronic identity verification requirements from a single source that is able to verify an individuals' identity to a high level of confidence. Only an electronic source that incorporates biometric information or information which provides a level of confidence equal to biometric information enable an individual's identity to be verified to a high level of confidence. Biometric information includes measurements of an individual's physical characteristics that can be recorded and used for comparison and automated recognition of that individual (e.g. photographs, iris structure or fingerprint information).[93]

There are various electronic identity solutions in development in New Zealand and overseas, which provide "centralised" or "decentralised" digital identity platforms for businesses and individuals to connect and for reporting entities to verify individuals' identity electronically. Centralised digital identity platforms tend to have a middle person acting in between the business and the individual, whereby the middle person is facilitating the interactions between the business and the individual. Decentralised digital identity platforms however, are built on the principles of an open, standards based ecosystem, that is technically designed to put the individual at the centre of their digital identity related transactions. The majority of electronic identity solutions which have been developed or are in development, require biometric verification of individuals at the time these individuals are onboarded onto the digital identity platform. These technologies are intended to allow immediate or "real-time" verification of an individual's identity.

As explored in section 4.3 above, issuers of identity records and reporting entities face various forms of liability risks. Accordingly, safe harbours from liability similar to the safe harbours under the EIVA will likely need to apply to the use of any digital identity platform, specifically issuers of identity and the digital identity platform providers themselves – otherwise the risk of liability may discourage the level of participation needed for the platform to succeed. There would inevitably be many practical challenges to adopting such safe harbours between the various participants of a digital identity platform in the form of contracts. Therefore, these safe harbours would foreseeably need to exist in statute, similar to the safe harbours under the EIVA. Amending the EIVA would likely be more efficient than enacting separate legislation, therefore amending the EIVA is recommended.

[93] Amended Identity Verifica ion Code of Practice 2013, at 2, 3.

Based on the current state of the AML/CFT regime, it is not likely that Reporting Entity Reliance or Approved Entity Reliance will be applicable to digital identity platform providers that facilitate the performance of Core KYC. It is likely that reporting entities could rely on such technology providers to perform Core KYC on their behalf using Agency Reliance. The aforementioned limitations of Agency Reliance would apply to any reporting entities relying on digital identity platform providers as their agents, however. Nevertheless, this point is only academic in nature at this stage.

Reporting entities' adoption of digital identity platforms for the purpose of performing Core KYC will require industry collaboration with the AML/CFT Supervisors and the Ministry of Justice. Digital identity platform providers will likely need to produce high levels of identity assurance to give AML/CFT Supervisors and the Ministry of Justice the comfort they need to issue the abovementioned guidance and/or updates to the AIVCOP. That said, some reporting entities will have higher risk appetites than others, therefore these reporting entities might adopt digital identity solutions for their Core KYC procedures without any changes to the AML/CFT regime. It remains difficult to forecast if **widespread adoption** of digital identity platforms is feasible without the previously mentioned reforms to the AML/CFT regime.

Ultimately the widespread adoption of new digital identity platforms will depend on a combination of strong industry leadership driving adoption, robust technological innovation, changes to EIVA and collaboration with and support from the AML/CFT Supervisors (through the publication of previously mentioned official guidance or updates to AIVCOP) and the Ministry of Justice (through amendments to the AML/CFT Act).

5.2 LEGAL SOLUTIONS

5.2.1 Alignment of AIVCOP, AML/CFT Regime and the NZ Government Trust Framework

Industry, the AML/CFT Supervisors and the Ministry of Justice align the AIVCOP with relevant parts of digital identity technologies and/or the New Zealand Government Trust Framework to ensure the New Zealand Government Trust Framework is aligned with the AIVCOP and the AML/CFT regime.

Electronic identity verification under the AIVCOP, particularly clause 17, can be tested against new and developing digital identity technologies and/or the New Zealand Government Trust Framework.

The New Zealand Government Trust Framework may be a solution to some of the previously mentioned Core KYC frictions.

There is an opportunity for reporting entities (which should be a combination of large entities like some of the Participating Banks, medium sized entities and start ups), technology providers, other possible ecosystem participants of the New Zealand Government Trust Framework, the AML/CFT Supervisors and the Ministry of Justice[94], to immediately collaborate on how the New Zealand Government Trust Framework and digital identity technologies could be aligned with the AIVCOP. The intention here would be to determine how these new developments could be the near future tool for reporting entities to meet the requirements of the AIVCOP in a more efficient manner.

While there are possibly other aspects to electronic identity verification requirements in the AIVCOP which could be explored, issues with electronic identity sources (clause 17) is one aspect that should be immediately explored. Key questions the industry could collaborate with the AML/CFT Supervisors and the Ministry of the Justice to answer are:

- "Which electronic identity sources do the AML/CFT Supervisors consider are consistently able to verify identity to a high level of confidence?";
- "What error rates by the above electronic identity sources would the AML/CFT Supervisors be comfortable with?"; and

[94] The Ministry of Jus ice is the government entity which administers the AML/CFT Act.

- "What mechanisms should electronic identity sources incorporate to link a person to a claimed identity (biometrically or otherwise)?"

Identity issuers will be crucial to the success of digital identity technologies. Similarly, TF Issuers will be the backbone of the New Zealand Government Trust Framework. Therefore, aligning these new developments with the electronic identity verification requirements in the AIVCOP and ultimately the AML/CFT regime is crucial.

Ideally this work would enable the Ministry of Justice to consider, in consultation with the AML/CFT Supervisors and reporting entities, how the New Zealand Government Trust Framework can be used within the AML/CFT regime, during its statutory review of the AML/CFT Act in 2021.

5.2.2 Reflect the FATF Digital Identity Guidance into New Zealand law

The FATF Digital Identity Guidance emphasises the value of innovation, and the fact that digital identity systems are not inherently more vulnerable to abuse, and may even bring advantages, although there are certain risks more applicable to them. This Report endorses the FATF's broad views on this issue, and encourages the AML/CFT Supervisors and the Ministry of Justice to endorse and follow its recommendations.

The FATF's recommendations for authorities in the FATF Digital Identity Guidance are laid out in Appendix 5. The FATF's two opening recommendations are:

12. *Develop clear guidelines or regulations allowing the appropriate, risk-based use of reliable, independent digital ID systems by entities regulated for AML/CFT purposes. As a starting point, understand the digital ID systems available in the jurisdiction and how they fit into existing requirements or guidance on customer identification and verification and ongoing due diligence (and associated record keeping and third-party reliance requirements).*
13. *Assess whether existing regulations and guidance on CDD across all relevant authorities accommodate digital ID systems, and revise, as appropriate, in light of the jurisdictional context and the identity ecosystem. For example, authorities should consider clarifying that non-face-to-face on-boarding may be standard risk, or even low-risk for CDD purposes, when digital ID systems with appropriate assurance levels are used for remote customer identification/verification and authentication.*

The FATF Digital Identity Guidance makes clear FATF's unequivocal support for the use of digital identity technology. Unfortunately, the timing of its release in March 2020 means it is unlikely it will be considered as part of the FATF Methodology which was the basis for this year's Mutual Evaluation of New Zealand[95].

Despite that, the industry should encourage the Ministry of Justice and the AML/CFT Supervisors to actively consider and look to implement the FATF Digital Identity Guidance because that would facilitate more efficient and effective compliance in New Zealand, allow innovation, and better align New Zealand with the future direction of other jurisdictions.

The AML/CFT Supervisors and the Ministry of Justice should be encouraged to address the FATF's two opening recommendations, by analysing the AML/CFT regime (including the AML/CFT Act, the AIVCOP and published guidance) to determine how it accommodates digital identity systems. If the parties conclude the regime doesn't accommodate the use of digital identity technology, there are strong arguments for updating the AML/CFT regime to accommodate these technologies in accordance with the FATF's opening recommendation. One way the parties could update the AML/CFT regime is to update the AIVCOP to clarify *that non-face-to-face on-boarding may be standard risk, or even low-risk for CDD purposes, when digital ID systems with appropriate assurance levels are used for remote customer identification/verification and*

[95] Now expected to issue its Report at the plenary meeting in February 2021.

authentication. The industry should engage with the AML/CFT Supervisors and the Ministry of Justice to review and update the AIVCOP in order to accommodate the greater use of digital identity technology.

5.2.3 Activate the Approved Entity Reliance regime

The approved entity regime is currently unable to be used because no reporting entities have been authorised to be an "approved entity". Approving entities would allow reporting entities to make use of these provisions, but this will require the AML/CFT Supervisors to develop an appropriate approach.

Approved Entity Reliance is not currently being used by reporting entities because approved entities have yet to be prescribed by regulations, which can be made by the Governor-General on the recommendation of the Minister of Justice.[96] Naturally, then, the foremost change necessary to bring this into use would be to prescribe at least one approved entity. However, the apparent simplicity of this approach belies its inherent issues.

The Approved Entity Reliance regime, as it stands, also does not set out a new placement of responsibility. If an entity fails to satisfy the CDD obligations of a reporting entity that is relying on it, that reporting entity is expressly not held responsible for the failure, but nothing in the AML/CFT Act would hold the entity being relied on responsible either. Under the legislation, it would appear that nobody would be held responsible for such a failure in carrying out CDD. The terms of the relationship between those entities may set out a scheme of liabilities, but there would be little incentive for them to negotiate and voluntarily create an allocation of risk of liability where there does not appear to be any such risk imposed.

Under Reporting Entity Reliance generally, the ultimate responsibility retained by the reporting entity would mean that it would have a vested interest in ensuring that the entity being relied on has robust systems to ensure CDD information is not altered internally between the time of collection for CDD and the provision of the CDD information for reliance purposes. The absence of this responsibility under Approved Entity Reliance makes this much more pronounced, as no entity has that incentive to institute or supervise those systems.

As any approved entities would need to be given their namesake approval by regulations, and thus could be formally vetted, it may be that an absence of responsibility is acceptable or could be acceptably mitigated by some form of licensing conditions.

In a similar vein, the AML/CFT Supervisors would need to develop an appropriate approach to dealing with approved entities. For example, a further level of supervision, or other compliance generally, may be necessary to reduce the risk of flawed information being relied on. The AML/CFT audit process for approved entities would also likely need to be appropriately tailored, with the added complexity and costs that such would bring.[97]

Allow selected non-reporting entities to become approved entities

As discussed in Appendix 6 (section 14.6.3), there is some ambiguity around whether non-reporting entities can be the subject of Approved Entity Reliance, although the stronger position appears to be that they cannot. On that basis, if there was an appetite for extending Approved Entity Reliance to non-reporting entities (given the need for specific approval in any case) then the AML/CFT Act would need to be amended to allow for such.

In addition, however, the aforementioned need to develop an appropriate approach to dealing with approved entities would be even more pronounced with non-reporting entities, as they wouldn't have their

[96] AML/CFT Act, section 154(1)(ac).
[97] Ministry of Jus ice *Anti-Money Laundering and Countering Financing of Terrorism: Departmental Report for the Law and Order Committee* (May 2017) at [302].

own AML/CFT obligations and would need a new framework of supervision and responsibilities to ensure that reliance on them was sufficiently robust.

Should the AML/CFT Supervisors attempt to set guidelines for authorising "approved entities", it's likely they would consider some of the following factors raised by the Ministry of Justice on this topic in the MOJ 2017 Report, including:

- An approved entity would need to demonstrate a high standard of historical compliance with the AML/CFT Act and CDD, which will need to be tested, audited and maintained by that approved entity;
- An approved entity would need to submit to higher standards of supervision by the relevant AML/CFT Supervisor;
- An approved entity would need to submit to higher standards of auditing by an AML/CFT auditor, and the AML/CFT Supervisors would need to set the standards the auditor must satisfy; and
- An approved entity would need to consent to every reporting entity that wishes to rely on it for Approved Entity Reliance purposes.

Any reporting entity that is considering testing the criteria for becoming an approved entity with its AML/CFT Supervisor, must be confident the benefits of becoming an approved entity outweigh the risks of becoming one.

5.2.4 New Zealand Government Trust Framework participants apply to the Privacy Commissioner for a code of practice on information sharing

Participants of the New Zealand Government Trust Framework could make a joint application under the Privacy Act (section 47) to procure the issuance of a code of practice to enable reporting entities, which form part of the New Zealand Government Trust Framework, to share personal information between themselves (such as Core KYC).

5.2.5 The AML/CFT Supervisors issue guidance on how certain digital identity technologies and/or the New Zealand Government Trust Framework satisfy electronic identity verification under the AIVCOP

The alignment of parts of certain digital identity technologies or the New Zealand Government Trust Framework (or both) with electronic identity verification in the AIVCOP (discussed above) should put the AML/CFT Supervisors in a position to issue formal guidance on how these new developments satisfy the AIVCOP.

Continuous collaboration between the industry, the AML/CFT Supervisors and the Ministry of Justice will inevitably be necessary in order for any form of guidance to be published. The AML/CFT Supervisors and the Ministry of Justice would certainly need to be comfortable with these developments before any type of guidance is published. The Ministry of Justice, in collaboration with the AML/CFT Supervisors, could consider any potential intermediate operational improvements to the regime (e.g. guidance, codes of practice) that could enable more use of digital identity technologies to manage ML/TF risk while reducing the compliance costs of all AML/CFT regime stakeholders.

It's not clear if AML/CFT Supervisors guidance would predicate widespread reporting entity participation in the New Zealand Government Trust Framework or use of digital identity technologies to perform Core KYC – different reporting entities have different risk appetites and it's possible some reporting entities (possibly smaller reporting entities) would value Core KYC performed efficiently over the risk of breaching their Core KYC obligations. However, it's probable that large reporting entities, like the Participating Banks, would need to be comfortable with any guidance issued by the AML/CFT Supervisors, before performing all of their Core KYC using digital identity technologies and/or within the New Zealand Government Trust Framework.

5.2.6 The AML/CFT Supervisors update the AIVCOP to reflect or incorporate aspects of certain digital identity technologies and/or the New Zealand Government Trust Framework

The AML/CFT Supervisors' publication of the guidance described above, will encourage at least some reporting entities to use digital identity technologies and/or participate in the New Zealand Government Trust Framework to perform Core KYC. It's not unforeseeable that, in time, and after careful oversight of reporting entities' use of new technologies or their participation in the New Zealand Government Trust Framework, the AML/CFT Supervisors could amend the AIVCOP by incorporating aspects of these new developments.

One of the most effective ways the AML/CFT Supervisors can endorse and enable the use of digital identity technology and/or the New Zealand Government Trust Framework for Core KYC, is by updating the electronic identity verification code in the AIVCOP. These updates should (at least) clarify that reporting entities which perform biometric identity verification on an individual to a very high standard, including through the use of two or more electronic sources which are reliable, independent and match each other, to a high level of confidence, can be considered to have verified that individual's identity to a standard that is equal or at least comparable to face-to-face verification (which is somewhat in line with a FATF recommendation to authorities in the FATF Digital Identity Guidance). One possible outcome of this update is it would give digital identity platforms a stronger onus to build biometric identity verification solutions that are accepted to be at a very high standard. Updating the AIVCOP in this manner could also enable reporting entities and digital identity platforms to avoid the need to engage Agency Reliance, and accordingly, avoid the issues associated with that form of reliance.

Should this occur, widespread use of these new developments by reporting entities would be inevitable, given the likely efficiencies they bring to the Core KYC process.

5.2.7 Amend the Electronic Identity Verification Act 2012

The EIVA could be an important tool for widespread adoption of digital identity platforms including the New Zealand Government Trust Framework.

The EIVA was enacted in the context of the New Zealand government's current online identity verification service, "RealMe" in 2013.[98] The EIVA and RealMe were the government's responses to the growing number of transactions and interactions individuals were making with public sector and private sector agencies over the internet. The Minister of Internal Affairs foresaw RealMe as an "effective tool" for AML/CFT reporting entities to help them meet their obligations under the AML/CFT Act.[99] At the time, the Minister recognised the need to align the standards of identification under the Identity Verification Code of Practice 2013 (before it was amended and became the AIVCOP) with RealMe's identification standards.[100]

The EIVA provides a safe harbour to the Crown, its Ministers, or any other person, from a cause of action for any direct or indirect loss due to the use of an electronic identity credential.[101] This safe harbour does not apply to acts or omissions that constitute bad faith or gross negligence, or otherwise are outside the functions, duties or powers under the EIVA. The DIA, which administers the EIVA and RealMe, enjoys a safe harbour from civil liability for acts or omissions contemplated by the EIVA.

RealMe is currently marketed as an online solution to help AML/CFT reporting entities' online onboarding processes.[102] As this Report's primary focus is on the AML/CFT regime, it does not attempt to comment on

---

[98] Upon the launch of the RealMe identity verification service in 2013, the DIA's "igovt logon service" became part of the RealMe service: realme.govt.nz/changelog/.

[99] dia.govt.nz/diawebsite.nsf/Files/CabPaperandMin-ElectronicIdentityVerificationBill/$file/CabPaper-Regulations-and-other-issues-to-support-the-Electronic-Identity-Verification-Bill_EGI(12)238.pdf at [35] and [36].

[100] Ibid at [35].

[101] EIVA, section 65. RealMe is the only identity verification service that this applies to.

[102] realme.govt.nz/realme-business/.

the scale of RealMe's adoption There do appear to be first-hand accounts of its difficulty to use, particularly by people who do not have enough experience using computers or mobile devices.[103]

With new digital identity technologies being developed and released by the private sector or government agencies, Digital Identity New Zealand considers these new technologies should be given the opportunity to incubate and grow on a level playing field with RealMe. The government is not and should not be in the business of picking winners, therefore it should tread carefully and cautiously permit digital identity technologies to be used and adopted regardless of the service provider. Determining how technology providers can participate in the New Zealand Government Trust Framework is another issue to consider as well.

The adoption of the New Zealand Government Trust Framework by individuals (i.e. TF Holders), reporting entities, other business and issuers of identity (i.e. TF Issuers), may require legislation to calibrate its framework and liability models appropriately, and maximise use. On this basis, it may be appropriate to amend the EIVA, so that the safe harbours available under this statute could also apply to certain participants of the New Zealand Government Trust Framework, including TF Issuers and TF Infrastructure Providers. Very similar arguments could also be made for digital identity technology providers. Any type of legislative reform to the EIVA will need careful attention by, and collaboration between, the DIA and the other parties involved.

5.2.8 Establish a framework for Reporting Entity Reliance

A contractual framework for Reporting Entity Reliance could be established by large reporting entities with strong histories of AML/CFT compliance.

Large reporting entities with strong histories of AML/CFT compliance could agree to a contractual arrangement for mutual Reporting Entity Reliance. This could take the form of an industry "code" or standards, similar to the DITP's conceptual design of the New Zealand Government Trust Framework, with agreed industry-wide performance standards, a process for confirmation of compliance with the standards, reciprocal indemnification and liability limitation provisions and a governing body comprising of members of the framework. The governing body could set and update the industry code or standards and it would be democratically elected regularly.

It is assumed that Approved Entity Reliance has not been activated in this environment, therefore any reporting entity relied on under Reporting Entity Reliance, is not an approved entity for Approved Entity Reliance purposes. Accordingly, reporting entities relying on any reporting entity within this framework, will not be able to rely on the safe harbour available under the AML/CFT Act.

This framework would require reporting entities to reach a consensus on its design, some of whom are in competition with each other. The framework would also need robust coordination and an alignment of interests and risk appetites.

A working group appointed by these large reporting entities could drive the framework's development. This framework might raise competition law issues, and this would need to be investigated further.

5.2.9 Replace the current personal address requirements

Address and its verification are problematic requirements for CDD and could be removed. Further mechanisms for verifying a person's address could be provided in an update to the AIVCOP.

A person's residential address is one of the pieces of identification information that must be collected in carrying out CDD, and is a component of Core KYC for the purposes of this Report.[104] However, as

[103] stuff.co.nz/technology/118562717/new-zealands-growing-underclass-what-happens-when-youre-stranded-on- he-wrong-side-of-the-digital-divide.
[104] AML/CFT Act, section 15(d).

described previously in section 4.5, address requirements sit in a different position to the other elements of Core KYC and verifying it in practice can be challenging.

A person's address is the only element effectively excluded from the AIVCOP (in that it is touched on, but not brought under the code of practice safe harbour), which may be indicative of difficulty in coming to a consensus as to how best to verify it. Address is even excluded by regulations from the information that must be collected in conducting Core KYC for occasional transactions,[105] which could support the notion that an address is not as central to Core KYC as its technical inclusion may imply.

Ultimately, there is an argument that the inclusion of address in mandatory CDD information is not only of limited benefit in combating ML/TF but also introduces unhelpful complexity and uncertainty into the regime.

It is likely the main reason for using multiple pieces of identity information for Core KYC is to reduce the possibility of a particular combination of information capturing more than one person, as an increased number of data points reduces the chance that they all coincide. If something was needed to replace address as one of these pieces of identity information, one alternative could be place of birth, which the FATF has recognised as constituting evidence of core attributes for establishing and verifying official identity (along with name and date of birth).[106]

Every person will have a place of birth and, being fixed at a specific point in time, it does not change. That said, it is likely that many more persons would share a place of birth (depending on how precisely it is measured) than any particular address. However, the New Zealand passport includes the person's place of birth (as well as the passports of some other OECD members like the USA, the United Kingdom and Australia), making this piece of identity information a potential alternative to a person's current residential address (if any).[107]

There are counter-arguments:

- That it is convenient for authorities to have a "last known address for individuals"; and
- That it may be more likely for two persons with the same name and date of birth to be born in the same place than to have the same current address – that is why passports tend to include a person's place of birth.

On the balance, neither argument justifies the current requirements, particularly when there appears to be a strong alternative in a person's place of birth. Conversely, a current residential address is much easier to falsify.

The AML/CFT Act could be amended so that a person's address is no longer a mandatory piece of identity information, but instead one of many pieces of information, including a person's place of birth, that a reporting entity may make use of in satisfying itself that it has identified a customer. This would require a move, at least to an extent, away from the prescriptive nature of the current Core KYC regime, towards granting reporting entities greater discretion as to how they go about determining the identity of customers (as far as it relates to the address component of identity verification). Such a flexible approach may be more in keeping with the underlying risk-based approach advocated by the FATF.

Short of outright legislative change, other actions should be taken. Specific guidance from the AML/CFT Supervisors will likely be helpful – however it will not protect entities that follow such guidance yet as it still falls short of the AML/CFT Act's requirements. Therefore, guidance to clarify the process for verifying address information in an update to the AIVCOP, with its safe harbour, would be a better alternative.

---

[105] Anti-Money Laundering and Countering Financing of Terrorism (Exemp ions) Regulations 2011, clause 6.
[106] Financial Action Task Force, *Guidance on Digital Identity* (Financial Action Task Force, Paris, 2020) at [50].
[107] "OECD" is the common acronym for he Organisation for Economic Co-operation and Development.

The absence of any sanctioned process for verifying address in the AIVCOP highlights the inherent practical difficulties of verifying a person's address

5.2.10 Agency reliance changes

Use of Agency Reliance could be encouraged by changing the placement of liability or instituting a safe harbour.

Under Agency Reliance, there is no express statement of on whom responsibility lies. However, ordinary principles of agency law apply,[108] and the reporting entity principal would accordingly still be ultimately responsible for the CDD obligations it is relying on the agent to fulfil. As a result, reporting entities are often reluctant to make use of this (amongst other forms of) reliance, as the supervision necessary to mitigate the risk of relying on the agent erodes the benefit of having someone else carry out Core KYC verification.

Encouraging more reporting entities to make use of Agency Reliance would likely require some express reduction, if not outright removal, of this ultimate responsibility. This, of course, would raise the same concern as discussed in section 4.6 above around the removal of liability being at odds with the FATF Standards.

If a change in responsibility was made by legislative change, it could avoid the issue with Approved Entity Reliance having no clear placement of ultimate responsibility, or the possibility that there is simply no responsibility remaining, by having the new provision identify where it will be placed. This would inevitably have to be on the agent, as the entire purpose of this change would be to free the reporting entity relying on the agent from responsibility, but this may simply serve to shift the current disincentive from reporting entities considering reliance on an agent to agents considering allowing a reporting entity to rely on them.

If responsibility was not imposed in this way, and as a result was not placed anywhere, it would be even more problematic than with Approved Entity Reliance. Approved entities, as described above, could be vetted or subjected to licensing or other requirements as part of the approval process, which could leave the absence of, or reduction in, total responsibility more palatable. Agents, on the other hand, would arise purely within private relationships, without that same prospect of direct regulatory oversight (unless such a system was imposed, which would likely discourage many prospective agents). This would likely be the primary concern with and obstacle to providing reporting entities making use of Agency Reliance with relief from responsibility.

Rather than amending the Agency Reliance provision itself, a code of practice (as described in Appendix 6) could be used to change the placement of responsibility by instituting a safe harbour for reporting entities relying on agents. Although some of this may involve setting conditions on how a reporting entity that is relying on an agent must operate, to be sufficiently robust it would likely also involve conditions around what types of agents can be relied on. In this way, such a conditional safe harbour would begin to resemble Approved Entity Reliance by another name (in particular, in terms of approved classes rather than particular entities), and raise very similar issues around supervision and vetting. While the well-established law of agency in the common law could be disrupted by a safe harbour for reporting entities engaging in Agency Reliance (particularly on a principal's vicarious liability for the conduct of its agent which is aligned with Agency Reliance's conception), ultimately the principle of Parliamentary sovereignty would override these jurisprudential concerns. There is at least one argument that supports the safe harbour – it could be a means to encourage greater use of Agency Reliance by removing the burden of impractically excessive levels of oversight by reporting entities over an agent. Ultimately, this Report does not endorse this solution, given that the arguments which favour the creation of a safe harbour do not outweigh the previously mentioned political and practical reasons for having a robust AML/CFT regime.

[108] Department of Internal Affairs, Accountants Guideline, issued in March 2018, at 36; and Department of Internal Affairs, Lawyers and Conveyancers Guideline, issued in December 2017, at 38.

6. CONCLUSION

6.1 CONCLUSION

Obtaining Core KYC information encounters many frictions in practice, potentially resulting in additional costs of compliance. Exploring possible solutions to these frictions is warranted.

The AML/CFT Act does not preclude the reuse of identity credentials by reporting entities to perform their Core KYC, making Reporting Entity Reliance (and Approved Entity Reliance should it be activated) available as a solution to the aforementioned issues. This is already being done by agents for the purposes of Agency Reliance.

That said, the use of Reporting Entity Reliance at any material scale is not likely, without initial action from the AML/CFT Supervisors and/or the Ministry of Justice,[109] or the creation of a reliance framework involving large reporting entities with strong histories of AML/CFT compliance to drive the use of Reporting Entity Reliance (as set out in section 5 above).

The FATF appears to be in favour of innovation in AML/CFT compliance, particularly through the use of digital identity technologies, with its recent publication of the FATF Digital Identity Guidance, which this Report endorses. Continued development and testing, and prudence in adoption, has the potential to cure at least some of the perceived frictions with Core KYC compliance.

The FATF's recommendations to authorities in the FATF Digital Identity Guidance, is a statement of intent that the AML/CFT Supervisors and the Ministry of Justice should consider and respond to soon.

6.2 NEXT STEPS/RECOMMENDATIONS

Changes can be made to the existing regime in four ways:

- AML/CFT Supervisor guidance can be issued or amended;
- AML/CFT Supervisors can issue a code of practice or amend an existing one;[110]
- Regulations can be amended;[111] and
- The AML/CFT Act itself can be amended.

With the AML/CFT Act due for a statutory review in 2021[112] it may be unlikely for any substantial changes to the AML/CFT regime to be put through ahead of that review (nevertheless, arguments for legislative change will be relevant then).

Certain AML/CFT regulations[113] are due to expire over the next two years and have been the subject of a targeted consultation.[114] With such important AML/CFT regulations under review, there may be some reluctance to push through other substantive changes to regulations in the meantime.

---

[109] Presumably, the Ministry of Justice and the AML/CFT Supervisors will work together to set he criteria for approving reporting entities for the purpose of Approved Entity Reliance. They would foreseeably also collaborate on the supervisory framework of any approved entities.
[110] AML/CFT Act, sections 63-65.
[111] AML/CFT Act, sections 153-155.
[112] AML/CFT Act, section 156A.
[113] Anti-Money Laundering and Countering Financing of Terrorism (Definitions) Regulations 2011 and the Anti-Money Laundering and Countering Financing of Terrorism (Exemptions) Regulations 2011.
[114] Ministry of Justice *Expiring AML/CFT Regulations: Targeted Consultation* (October 2019) at 8.

In light of these possible barriers to AML/CFT reform, there appears to be even stronger reasons to immediately explore how digital identity technologies can remedy some of the perceived frictions with Core KYC.

Industry collaboration with the AML/CFT Supervisors and the Ministry of Justice to align existing digital identity technologies and/or the New Zealand Government Trust Framework with the AIVCOP, might be the easiest and most appropriate next step to pursue. Should these collaborations increase the level of comfort that the AML/CFT Supervisors and the Ministry of Justice have towards digital identity technologies and the New Zealand Government Trust Framework, the AML/CFT Supervisors may then be in a better position to issue formal guidance or even update the AIVCOP to reflect these developments. Timing is critical, and aligning these avenues with the statutory review of the AML/CFT regime in 2021 is imperative.

If and when there is appetite to review the AML/CFT regime, activating the Approved Entity Reliance regime would likely be the best way of encouraging Reporting Entity Reliance. The regulations required to approve reporting entities for this purpose will likely need to impose vetting or supervision requirements over the approved entity. It's possible the greater obstacle to activating Approved Entity Reliance might be a lack of consensus around how to develop an appropriate regime, rather than a willingness to approve entities. Therefore engagement from large reporting entities, particularly the Participating Banks, of the AML/CFT Supervisors and the Ministry of Justice, might create the impetus needed to set an Approved Entity Reliance regime in motion.

Successfully implementing the New Zealand Government Trust Framework at any real scale will probably require amendments to the EIVA as well, so that safe harbours available under this statute can also apply to certain participants of the New Zealand Government Trust Framework. An identical argument could be made for digital identity technology providers. Such legislative reform should form part of the Digital Identity Bill. Any type of legislative reform to the EIVA will need careful attention by the various parties involved.

As noted earlier, this Report is subject to a number of limitations, and by necessity, it cannot be a full and thorough examination of the entire AML/CFT regime and its interaction with third-party reliance and digital identity technology. For example, further examination would be valuable in relation to CDD information (such as a person's residential address and place of birth) beyond Core KYC. Competition law, while excluded from this Report, would inevitably be a crucial consideration for an expanded reliance regime in practice. Also, as laws around the world dealing with privacy rights and information control continue to develop and expand, the increasingly large numbers of overseas entities interacting with New Zealand's AML/CFT regime will likely make these a necessary consideration for reporting entities seeking to carry out their Core KYC obligations in relation to them.

7. GLOSSARY

Agency Reliance	means reliance on an authorised agent.
AIVCOP	means the Amended Identity Verification Code of Practice 2013.
AML/CFT	means anti-money laundering and countering financing of terrorism.
AML/CFT Act	means the Anti-Money Laundering and Countering Financing of Terrorism Act 2009.
AML/CFT Supervisors	means the Reserve Bank, the DIA and the FMA.
Approved Entity Reliance	means reliance on a so-called "approved entity".
Assurance Standard	means the DIA's draft Information Assurance Standard: 2019.
CDD	means customer due diligence.
Core Group	means the Participating Banks, the AML/CFT Supervisors, the Ministry of Justice and Mattr Limited.
Core KYC	means identifying and verifying the full names, dates of birth and residential addresses of natural persons as customers, beneficial owners, persons acting on behalf of customers or persons on whose behalf a customer has acted.
Data Subject	means an individual to whom Core KYC relates.
DBG	means a designated business group.
DBG Reliance	means reliance on another member of a designated business group.
DIA	means the Department of Internal Affairs.
Digital Identity Bill	Means the bill being developed to give legal effect to the New Zealand Government Trust Framework.
Digital Identity NZ	means Digital Identity New Zealand.
DITP	means the team within the DIA which is developing the New Zealand Government Trust Framework.
EIVA	means the Electronic Identity Verification Act 2012.
Entity A	means a reporting entity that relies on the Core KYC conducted by another reporting entity ("Entity B") for the purpose of its compliance with the AML/CFT Act.
Entity B	means a reporting entity that has conducted Core KYC, which is being relied on by another reporting entity ("Entity A") for the purpose of Entity A's compliance with the AML/CFT Act.
EOI Evidential Requirements	means the evidential requirements for a person's identity in the EOI Standard.
EOI Standard	means the DIA's Evidence of Identity Standard.
FATF	means the Financial Action Task Force.
FATF Digital Identity Guidance	means the FATF's guidance on digital identity, dated March 2020.
FATF Standards	means the FATF's *International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation,* commonly known as The FATF Recommendations and their Interpretive Notes.

FMA	means the Financial Markets Authority.
FTA	means the Fair Trading Act 1986.
Holder	means an individual holding identity credentials for the purposes of the AML/CFT Act.
Identification Management Standards	means the set of requirements outlining the ongoing maintenance of relationships between entities, their identity information and any authenticators that represent the identity of an entity in different contexts. Note, this will soon replace the EOI Standards.
IPPs	means the Information Privacy Principles.
MOJ 2017 Report	means the Ministry of Justice "Anti-Money Laundering and Countering Financing of Terrorism: Departmental Report for the Law and Order Committee" (May 2017).
ML/TF	means money laundering and financing of terrorism.
New Zealand Government Trust Framework	means the New Zealand Government digital identity Trust Framework being developed by the DITP (which is an independent transition team within the DIA), in conjunction with citizens, public agencies and the private sector. This Report's understanding of the proposed New Zealand Government Trust Framework is based on information found here: digital.govt.nz/standards-and-guidance/identity/digital-identity/digital-identity-transition-programme/ and briefings received by the authors from the DITP.
Participating Banks	means ANZ Bank New Zealand Limited, ASB Bank Limited, Bank of New Zealand, Kiwibank Limited, Westpac New Zealand Limited and TSB Bank Limited.
Privacy Act	means the Privacy Act 1993.
Questionnaire	means the questionnaire prepared by MinterEllisonRuddWatts for the Participating Banks' and AML/CFT Supervisors' response.
Relier	means a reporting entity relying on another to conduct Core KYC.
Report	means this report.
Reporting Entity Reliance	means reliance on another reporting entity.
Reserve Bank	means the Reserve Bank of New Zealand.
Self-Sovereign Identity	means a model of identity management that puts the individual at the centre of their identity-related transactions, allowing them to manage their personal information cross contextually in a portable manner. Note, this definition was provided by Mattr Limited.
TF Holder	means an individual or entity in possession of one or more Verifiable Credentials, within the Trust Framework.
TF Infrastructure Provider	means an entity that provides software and/or hardware for ecosystem participants to exchange or utilise Verifiable Credentials, within the Trust Framework.

TF Issuer	means an entity that issues Verifiable Credentials to individuals or entities, within the Trust Framework.
TF Relying Party	means an entity who makes a decision or takes an action on the basis of a Verifiable Credential, within the Trust Framework.
TF Subject	means an individual or entity that a Verifiable Credential is concerned with, within the Trust Framework.
Trust Framework	means a digital identity trust framework.
Verifiable Credential	means a tamper-evident credential that has authorship that can be cryptographically verified.

8. BIBLIOGRAPHY

8.1 CASES

Altimarloch Joint Venture Limited v Moorhouse HC Blenheim CIV-2005-406-91

Attorney-General v Carter [2003] 2 NZLR 171

Cashmere Pacific v NZ Dairy Board (1995) 8 PRNZ 661

Dental Council of New Zealand v Gibson, HC Auckland, CIV-2010-404-000230, 3 June 2010

Department of Internal Affairs v Ping An Finance (Group) New Zealand Company Limited [2017] NZHC 2363

Marina Holdings Ltd (in rec) v Thames-Coromandel District Council (2010) 12 NZCPR 277

8.2 LEGISLATION AND REGULATIONS

Anti-Money Laundering and Counter-Terrorism Financing Act 2006 (Cth)

Anti-Money Laundering and Countering Financing of Terrorism (Definitions) Regulations 2011

Anti-Money Laundering and Countering Financing of Terrorism (Exemptions) Regulations 2011

Anti-Money Laundering and Countering Financing of Terrorism Act 2009

Births, Deaths, Marriages and Relationships Registration Act 1995

Companies Act 1993

Electronic Identity Verification Act 2012

Fair Trading Act 1986

Financial Markets Conduct Act 2013

Identity Information Confirmation Act 2012

8.3 BOOKS AND CHAPTERS IN BOOKS

Tort – A to Z of New Zealand Law, (online edition, Thomson Reuters)

Equity – A to Z of New Zealand Law (online ed, Thomson Reuters)

Burrows, Finn and Todd on the Law of Contract in New Zealand, (LexisNexis NZ Limited, 6th edition, 2018)

8.4 JOURNAL ARTICLES

Joy Geary "Money laundering" [2010] NZLJ 228

8.5 PARLIAMENTARY AND GOVERNMENT MATERIALS

"Acting on behalf of a customer" fact sheet, issued jointly by the AML/CFT Supervisors in August 2013

"Clarification of the position the AML/CFT supervisors are taking with respect of the Anti-Money Laundering and Countering Financing of Terrorism Act 2009 ("the Act") interpretation of a trust as a customer", issued jointly by the AML/CFT supervisors in July 2019

Amended Identity Verification Code of Practice 2013

AML/CFT Programme Guideline, issued jointly by the AML/CFT supervisors in May 2018

Beneficial Ownership Guideline, issued jointly by the AML/CFT Supervisors in December 2012

Department of Internal Affairs *Evidence of Identity Standard* (version 2.0, Department of Internal Affairs, 2009)

Department of Internal Affairs, Accountants Guideline, issued in March 2018

Department of Internal Affairs, Lawyers and Conveyancers Guideline, issued in December 2017

Enhanced Customer Due Diligence Guideline, issued jointly by the AML/CFT supervisors in December 2017

Identity Verification Code of Practice – Explanatory note, issued by the AML/CFT Supervisors in December 2017

Ministry of Justice *Anti-Money Laundering and Countering Financing of Terrorism: Departmental Report for the Law and Order Committee* (May 2017)

Ministry of Justice *Expiring AML/CFT Regulations: Targeted Consultation* (October 2019)

8.6 REPORTS

Basel Committee on Banking Supervision *Customer due diligence for banks* (Bank for International Settlements, 2001)

Financial Action Task Force, *Guidance on Digital Identity* (Financial Action Task Force, Paris, 2020)

Financial Action Task Force, *International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation* (Financial Action Task Force, Paris, 2012-2019)

Financial Markets Authority *Anti-money laundering and countering financing of terrorism: Monitoring report 1 July 2016-30 June 2018* (April 2019)

8.7 INTERNET RESOURCES

fatf-gafi.org/about/

consumer.org.nz/articles/what-is-open-banking

dia.govt.nz/diawebsite.nsf/Files/Proactive-releases/$file/Ministers-Cabinet-paper-Developing-Options-for-a-New-Approach-to-Digital-Identity-1.pdf

dia.govt.nz/diawebsite.nsf/wpg_URL/Resource-material-Evidence-of-Identity-Standard-Index?OpenDocument

dia.govt.nz/Resource-material-Information-We-Provide-Identity?OpenDocument

digital.govt.nz/standards-and-guidance/identity/identification-management/information-assurance-standard-2019/

fma.govt.nz/assets/Reports/AMLCFT-2018-Annual-Monitoring-Report.pdf

justice.govt.nz/justice-sector-policy/key-initiatives/aml-cft/info-for-businesses/working-with-others/#cdd

keepourmoneyclean.govt.nz/

nzherald.co.nz/personal-finance/news/article.cfm?c_id=12&objectid=12203497

police.govt.nz/sites/default/files/publications/fiu-nra-2019.pdf

realme.govt.nz/changelog/

realme.govt.nz/how-apply/

realme.govt.nz/realme-business/

realme.govt.nz/where-to-use-realme/#passports-immigration-and-visas

stuff.co.nz/national/116095068/the-hidden-homeless-alarming-child-and-youth-homelessness-in-auckland

dia.govt.nz/diawebsite.nsf/Files/CabPaperandMin-ElectronicIdentityVerificationBill/$file/CabPaper-Regulations-and-other-issues-to-support-the-Electronic-Identity-Verification-Bill_EGI(12)238.pdf

rbnz.govt.nz/notes-and-coins/future-of-cash/issues-paper-the-future-of-cash#6

github.com/canada-ca/PCTF-CCP/blob/master/Version1_1/FOR-PUBLIC-REVIEW-PSP-PCTF-Version%201.1.pdf

w3.org/TR/vc-data-model/

ec.europa.eu/digital-single-market/en/eu-trust-mark.

stuff.co.nz/technology/118562717/new-zealands-growing-underclass-what-happens-when-youre-stranded-on-the-wrong-side-of-the-digital-divide

ft.com/content/ef7ac354-4b8c-11ea-95a0-43d18ec715f5

9news.com.au/national/cba-action-spurs-banks-to-blow-whistle/f4c5900c-a725-4c70-9cc0-d58a73813443

theaustralian.com.au/nation/cba-blasted-over-breaches-as-700m-fine-laid-down/news-story/f31fb8c5251e8889d2d3da15a88ad723

sbs.com.au/news/cba-must-restore-trust-following-700m-fine-over-breaches

openidentityexchange.org

identity.foundation

kantarainitiative.org

sovrin.org

digital.govt.nz/standards-and-guidance/identity/digital-identity/digital-identity-transition-programme/

digital.govt.nz/standards-and-guidance/identity/digital-identity/digital-identity-transition-programme/digital-identity-trust-framework/

APPENDICES

9. APPENDIX 1

BACKGROUND TO THE NEW ZEALAND GOVERNMENT TRUST FRAMEWORK

In November 2018, the New Zealand Cabinet commissioned the Department of Internal Affairs (DIA) to develop options for a new approach to digital identity and identify any regulatory gaps over a two year period, with oversight by the Minister of Finance, the Minister for Government Digital Services, the Minister of Internal Affairs and the Minister of Commerce and Consumer Affairs. As part of its mandate, the DIA, through the Digital Identity Transition Programme (DITP), has been working with citizens, public agencies and the private sector, to explore options for a New Zealand Digital Identity Trust Framework (the New Zealand Government Trust Framework). The New Zealand Government Trust Framework is intended to set rules for ensuring digital information can be shared in a secure and trusted way.[115]

The DITP, has progressed this work through engaging with public agencies, Crown entities, digital service providers, financial institutions, academic institutions and representatives from overseas jurisdictions. This has involved researching comparable jurisdictions' digital identity framework projects, developing use cases, and completing a high-level legislative and regulatory review among other avenues. The DITP is due to report back to Cabinet on its research, engagement and analysis by October 2020.

10. APPENDIX 2

DIGITAL IDENTITY NZ'S VIEW OF HOW A TRUST FRAMEWORK FOR NEW ZEALAND COULD HYPOTHETICALLY OPERATE

This section provides an overview of the possible components of a hypothetical Trust Framework from the perspective of Digital Identity New Zealand, which aligns with work being undertaken by the DITP.

10.1 SUMMARY OF POSSIBLE TRUST FRAMEWORK COMPONENTS

It is proposed that the Trust Framework will consist of five components which together help support a trusted, coherent and sustainable future digital identity ecosystem for New Zealand.

Component One:
Participants – defining the roles of participants involved in providing digital identity services.

Component Two:
Rules – based on existing laws and standards. The rules would broadly fall into two categories, those that promote trust and those that enable interoperability.

Component Three:
Accreditation – providers wishing to join the Trust Framework will be required to be *accredited*. Independent verification of the participants adherence to the rules is necessary to ensure a functional, trustworthy and sustainable future ecosystem.

Component Four:
Legal effect – All accredited participants will be legally required to follow the Trust Framework rules. Legal enforceability supports greater trust by both legally requiring participants to follow the rules and providing a means of redressing damages and settling disputes. The rules of the Trust Framework could be made legally enforceable via legislation, contracts or a combination of both.

Component Five:
Governance – a governance body will be responsible for reviewing and updating the Trust Framework as required.

[115] digital.govt.nz/standards-and-guidance/identity/digital-iden ity/digital-identity-transition-programme/digital-identity-trust-framework/.

10.2 INITIAL DESCRIPTION OF TRUST FRAMEWORK ROLES, PROCESSES AND STANDARDS

The Standards are a means by which to assess the Processes being carried out by a Participant. This enables "Certification" of a given process. Certification will help ensure the ecosystem operates in a manner that is advantageous and consistent for all Participants. It would also be a means by which to enforce liability.

The ecosystem's Roles would be important, as they provide a framework for who is responsible for what. In a digital ID context, these could include an Issuer, Holder, Subject, Relying Party, Service Provider and Infrastructure Provider. A Role can be thought of as a logical grouping of Processes. The Standards set out how these Processes should be conducted, to ensure consistency and interoperability across different domains.[116] If the Processes adhere to the relevant Standards, that Process (or Participant providing or conducting the Process) could be Certified. Participants should be subject to regular audits by an Accrediting body (or bodies) and contractually agree to adhere to the Standards when becoming Certified.

The Processes should be defined so that they could be implemented as modular services, and be separately assessed for Certification.[117] The Framework should allow for additional processes to be added as required, and for Standards to be subject to review and improvement to meet the needs of the ecosystem as appropriate. All Processes should be able to be mapped to relevant Standards.

If a Process is 'Certified', it could be relied upon, or 'trusted'. The Trust Framework should ideally set up an Accrediting Body (or bodies) that are authorised to accredit certain entities to certify Participants.

Certification could be conveyed through a visual symbol or cue, often referred to as a "Trust Mark".[118] This would provide a clear signal as to what Processes can be reliably integrated into other Participants' products, services or platforms with certainty, without the need for bilateral or opaque agreements. This improves efficiencies, and better enables Participants to interoperate seamlessly across the ecosystem.

Certification also acts as guidance for Participants on how to fulfil the legal duties that attach to Certification (adhere to the Standards).

The Trust Framework will be more robust if it is implemented under legislation.

10.3 THE ROLE OF STANDARDS

Standards are fundamental in any cohesive ecosystem and will be the foundation for the rules. The Trust Framework should include Standards in a number of domains, including:

(a) "Identification Management Standards" (including information assurance, entity binding assurance, authentication assurance and federation assurance);[119]

(b) "Information Management standards";

(c) "Data Management standards";

(d) "Data Federation standards"; and

(e) "Technical standards" (there are a number of lower level technical standards that serve a role in providing a strong foundation for interoperability).[120]

---

[116] For example, across organisa ions, sectors and countries. These can be developed specifically for the Trust Framework, or externally referenced – for example ISO and W3C standards.

[117] See the similar approach taken in the Pan-Canadian Trust Framework and other trust frameworks outside of the Digital ID context. The modularity of the Processes facilitates inclusivity – as one Participant does not need to carry out all Processes to participate.

[118] The visual mark is typically the trademark of the certifying organisation, for example see the eIDAS EU Trust Mark for Qualified Trust Services.

[119] See Appendix 12 for more information on the Identifica ion Management Standards. As at the date of completion of substantive content of this report, these standards are still under development and the EOI standard remains in place.

[120] For example, the W3C Verifiable Credentials Data Model was ratified in 2019 as a standard way to express verifiable data on the internet. w3.org/TR/vc-data-model/.

Where the Trust Framework's standards contain an assurance level, [121] (for instance, in the domain of Identification Management), we consider that it would be appropriate for each level of assurance to have a corresponding limit on liability. For example, the highest level of assurance provided has the highest financial limit on liability, and vice versa for the lowest level of assurance. We expect that this will be helpful as it will:

(a) Ensure that liability remains within determinate bounds, and therefore give confidence to potential TF Issuers and allow them to assess their potential exposure and (where appropriate) to take out insurance accordingly; and

(b) Encourage a wider ambit of potential TF Issuers, including for 'weaker' assurances such as a charity issuing a donation invoice, and thereby facilitate a broader-reaching ecosystem, knowing that (under this proposal) liability will not be high for such TF Issuers.

10.4 LIABILITY MODEL

Clear articulation of the Roles, Processes, Standards, Certification, and Accreditation creates a robust liability model, and a more coherent ecosystem. This will help ensure that all ecosystem participants are aware of their own, and others' responsibilities.

The liability provisions could specify:

(a) The circumstances in which liability (or other penalty, for example suspension of Certification, fine, etc) could arise;

(a) Corresponding "safe harbours" for Participants, whereby they will not be liable for losses if they have met their Certification requirements;

(b) The type of losses for which claims could be made, and who could make them; and/or

(c) Limitations on liability for breach, and exemption from liability in the case of fraud by a TF Holder.

Addressing such matters in the Trust Framework would likely encourage entities to seek Certification, to enable them to benefit from the safe harbours and limitations available under them.

Greater clarity on potential liability – and the limitations on it – would improve the confidence of those participating in the contemplated ecosystem, and allow them to make educated risk-assessments, and seek the necessary insurance where appropriate. It would also provide a more level playing field between private sector TF Issuers (who have no statutory protections from the potential liability outlined in this Report) and government entities, and the RealMe service, given the immunities provided under the EIVA. There may be greater uptake of a Self-Sovereign Identity based[122] Verifiable Credential ecosystem by the private sector if there were greater clarity and appropriate limitations on liability.

The Trust Framework could operate in the following way:

(a) The Trust Framework be applied to certain test cases immediately once finalised.

(b) Implement the Trust Framework in legislation (with standards possibly existing in regulations). This will help ensure that all ecosystem Participants are aware of their responsibilities, and they're at least familiar with others' responsibilities. Properly considered legislation will likely be implemented more easily and also capture the intended purpose better, than a web of contracts between the various Participants setting out obligations and performance standards. Some drawbacks to establishing contractual relationships (as an alternative to legislation) include:

    (i) Lack of transparency to ecosystem participants that are not parties to the contract, as well as the public;

[121] The Assurance Standards are being contemplated in the Standards being developed by the DIA.
[122] w3.org/TR/vc-data-model/ .

(ii) It can result in additional effort and costs to Participants, as they seek to negotiate multiple contracts for themselves;

(iii) It could result in creating differing obligations (and quantum of liability) between different participants in the same ecosystem undertaking the same roles;

(iv) It can create complicated webs of relationships; and

(v) It will likely create greater uncertainty with Participants' liability.

(c) Each entity could, as part of becoming Certified, sign an acknowledgement of their obligation to comply with the Trust Framework's applicable standards.

(d) An Accreditation Authority (or authorities) to monitor and require compliance with those standards.

(e) A Governance Body to maintain those Standards.

(f) Clear legal liability provisions within the Trust Framework's rules, addressing and specifying the consequences for breach of the Trust Framework's rules and standards.[123]

(g) Limitations on liability, commensurate with the assurance levels and confidence that the Process provides.

11. APPENDIX 3

THE FATF AND THE FATF STANDARDS

The FATF

The FATF is an inter-governmental body established in 1989 by its member jurisdictions, which includes New Zealand. The FATF's mandate is to set standards and to promote effective implementation of legal, regulatory and operational measures for combating money laundering, terrorist financing and the financing or proliferation, and other related threats to the integrity of the international financial system. The FATF is among other things, a policy making body, which works to generate the necessary political will to bring about national legislative and regulatory reforms in these areas.[124] The FATF's standards are set in a way so that countries are able to give effect to them in the most appropriate way within their particular legal contexts.[125] The foremost manifestation of these are the FATF Standards.[126]

The FATF Standards

The FATF Standards, sets out an international standard, which countries are recommended to implement to combat the abovementioned nefarious activities.

Recommendation 10 from the FATF Standards, among other things, prohibits entities from keeping anonymous accounts or accounts in obviously fictitious names. The recommendation calls for CDD to be carried out, customer identities to be obtained and verified, and ongoing CDD and transaction scrutiny to be undertaken.[127] Higher-risk customers similarly should require more stringent measures.[128] Once identification and verification steps have been undertaken, they can be relied on for further transactions

[123] Successful adherence could be signalled with a visual signal, such as a trust mark, e.g. the EU trust mark logo – see ec.europa.eu/digital-single-market/en/eu-trust-mark.

[124] fatf-gafi.org/about/.

[125] Financial Action Task Force, *International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation* (Financial Action Task Force, Paris, 2012-2019) at 6.

[126] Financial Action Task Force, *International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation* (Financial Action Task Force, Paris, 2012-2019).

[127] Financial Action Task Force, *International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation* (Financial Action Task Force, Paris, 2012-2019) at 12 (Recommendation 10).

[128] Financial Action Task Force, *International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation* (Financial Action Task Force, Paris, 2012-2019) at 9 (Recommendation 1), 29 (Interpretive Note to Recommendation 1) and 62-65 (Interpretive Note to Recommendation 10).

unless there are doubts as to their veracity.[129] The FATF states that the obligation to conduct CDD should be set out in law, however, every country may determine how it imposes specific CDD obligations, either through law or enforceable means.

Recommendation 17 from the FATF Standards puts forward a framework for reporting entities to rely on third parties for CDD purposes. Under that framework, the relying entity also retains ultimate responsibility, and further reliance is permitted within the equivalents of DBGs. However, it also envisages that the third party is one regulated for AML/CFT purposes, and therefore is more in line with our DBG Reliance and Reporting Entity Reliance than our Agency Reliance.[130] Instead, outsourcing and agency relationships are considered distinct, on the basis that they involve an entity applying a delegating entity's CDD measures on behalf of that delegating entity. Third-party reliance, as framed by FATF, involves an entity that is regulated in its own right and carrying out its own independent CDD measures being relied on to provide that CDD information.[131]

12. APPENDIX 4

THE FATF DIGITAL IDENTITY GUIDANCE – BACKGROUND AND ITS RELEVANCE TO THIS REPORT

Context to the FATF Digital Identity Guidance

In 2019 the FATF released for public consultation (now closed) the FATF Digital Identity Guidance.[132] The FATF Digital Identity Guidance focuses on the application of Recommendation 10 from the FATF Standards, customer due diligence, to the use of digital identity systems for identification or verification at customer onboarding. The guidance recognises that in many countries, proof of official identity is provided through general-purpose identity systems, such as national identity and civil registration systems. Such systems typically provide documentary and/or digital credentials that are widely recognised and accepted by government agencies and private sector service providers as proof of official identity. Other jurisdictions have a variety of limited-purpose identity systems that are developed to provide identification, authentication and authorisation for specific services or sectors, such as taxpayer administration numbers, driver's licenses, passports, voter registration cards, social security numbers and refuge identity documents. In the absence of general-purpose identity systems in these jurisdictions, such limited-purpose systems and credentials may also be used to provide proof of official identity. The guidance also recognises new models emerging, with digital credentials provided, by or in partnership with, the private sector, which is recognised by the government as official proof of identity in an online environment (such as NemID in Denmark).[133]

The FATF Digital Identity Guidance

The FATF's views and recommendations in the FATF Digital Identity Guidance are important to this Report, since it focuses on digital identity in the context of CDD performed on individuals.[134] The document provides insights into the types of solutions the FATF may or may not be comfortable with. Any widespread adoption by reporting entities of technologies which are not in line with what the FATF has in mind, will unlikely be

---

[129] Financial Action Task Force, *International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation* (Financial Action Task Force, Paris, 2012-2019) at 61 (Interpretive Note to Recommendation 10).
[130] Financial Action Task Force, *International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation* (Financial Action Task Force, Paris, 2012-2019) at 16 (Recommendation 17).
[131] Financial Action Task Force, *International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation* (Financial Action Task Force, Paris, 2012-2019) at 78 (Interpretive Note to Recommendation 17).
[132] Financial Action Task Force, *Guidance on Digital Identity* (Financial Action Task Force, Paris, 2020).
[133] Financial Action Task Force, *Guidance on Digital Identity* (Financial Action Task Force, Paris, 2020) at 19.
[134] The FATF Digital Identity Guidance specifically looks at digital identity in the context of conducting CDD on individuals, ra her than extending further into CDD obligations, although it does recognise the value of digital identity systems to those other obligations. See Financial Action Task Force, *Guidance on Digital Identity* (Financial Action Task Force, Paris, 2020) at [42], [44].

reconcilable with New Zealand's responsibilities as a FATF member, as well as the purposes of the AML/CFT Act.

The FATF recognises the value of innovation when done responsibly and intends for its standards to encourage that in the abovementioned guidance.[135] The document is expressly non-binding, and it clarifies the existing FATF Standards (which are technology neutral) rather than seeking to amend them.[136]

The FATF recognises that given the nature of digital identity systems, they are vulnerable to certain risks. For example, systems of authentication could be fraudulently utilised, rendered inoperable by connectivity issues, or effectively placed beyond the reach of some persons if they are overly prescriptive in what non-digital documents are required. They can also raise unique concerns around data protection and privacy, and may obstruct ongoing CDD and account monitoring if information is collected by a party other than the relying entity[137]

Importantly, the FATF believes that digital identity systems are not inherently more vulnerable to abuse than other methods of ascertaining identity, and where appropriate levels of confidence can be obtained, entities should not be discouraged from using them.[138] In fact, these systems can even bring advantages to the identification process. For example, they could strengthen the CDD that is carried out by reducing the risk of human error, increasing ease of use and reducing costs, and even increase the scope of information obtained, or enhance financial inclusion by providing access to a robust form of identification.[139]

The FATF also makes clear that those that have developed digital identity systems could choose to operate as digital identity service providers, allowing other entities to outsource CDD processes to them. The FATF Standards on reporting entities relying on third parties (FATF Recommendation 17) permit reliance on entities regulated by an AML/CFT regime, and not entities which are not themselves regulated by an AML/CFT regime.[140]

Where such reliance is permitted, the FATF Standard states that the ultimate responsibility for CDD measures remains with the financial institution relying on the third party. It states that the criteria that should be met where reliance is permitted, are as follows:

(a) A financial institution relying upon a third party should immediately obtain the necessary information concerning elements (a)-(c) of the CDD measures set out in FATF Recommendation 10.

(b) Financial institutions should take adequate steps to satisfy themselves that copies of identification data and other relevant documentation relating to the CDD requirements will be made available from the third party upon request without delay.

(c) The financial institution should satisfy itself that the third party is regulated, supervised or monitored for, and has measures in place for compliance with, CDD and record keeping requirements in line with FATF Recommendations 10 and 11.

(d) When determining in which countries the third party that meets the conditions can be based, countries should have regard to information available on the level of country risk.

Digital Identity NZ's view is that this should be interpreted as meaning that a reporting entity relying on another reporting entity need not have strict legal liability for errors by that other reporting entity on which it is relying, if it has taken adequate care to establish the matters listed in paragraphs (a) to (d) above and is otherwise without fault. That is consistent with the provisions introduced into the AML/CFT Act in 2017 to

[135] Financial Action Task Force, *Guidance on Digital Identity* (Financial Action Task Force, Paris, 2020) at [31].
[136] Financial Action Task Force, *Guidance on Digital Identity* (Financial Action Task Force, Paris, 2020) at [9].
[137] Financial Action Task Force, *Guidance on Digital Identity* (Financial Action Task Force, Paris, 2020) at [117] – [138].
[138] Financial Action Task Force, *Guidance on Digital Identity* (Financial Action Task Force, Paris, 2020) at [101].
[139] Financial Action Task Force, *Guidance on Digital Identity* (Financial Action Task Force, Paris, 2020) at [106] – [111].
[140] Financial Action Task Force, *Guidance on Digital Identity* (Financial Action Task Force, Paris, 2020) at [97] – [99].

allow Approved Entity Reliance. However, to date, no "approved entities" have been designated and accordingly, that regime is not currently able to be used.

13. APPENDIX 5

THE FATF DIGITAL IDENTITY GUIDANCE – THE FATF'S RECOMMENDATIONS FOR AUTHORITIES

Note: This quoted section of the FATF Digital Identity Guidance starts at paragraph 12 of the guidance.

Recommendations for government authorities

12. Develop clear guidelines or regulations allowing the appropriate, risk-based use of reliable, independent digital ID systems by entities regulated for AML/CFT purposes. As a starting point, understand the digital ID systems available in the jurisdiction and how they fit into existing requirements or guidance on customer identification and verification and ongoing due diligence (and associated record keeping and third-party reliance requirements).

13. Assess whether existing regulations and guidance on CDD across all relevant authorities accommodate digital ID systems, and revise, as appropriate, in light of the jurisdictional context and the identity ecosystem. For example, authorities should consider clarifying that non-face-to-face on-boarding may be standard risk, or even low-risk for CDD purposes, when digital ID systems with appropriate assurance levels are used for remote customer identification/verification and authentication.

14. Adopt principles, performance, and/or outcomes-based criteria when establishing the required attributes, evidence and processes for proving official identity for the purposes of CDD. Given the rapid evolution of digital ID technology, this will help promote responsible innovation and future-proof the regulatory requirements.

15. Adopt policies, regulations, and supervision and examination procedures that enable regulated entities to develop an effective, integrated "risk-based" approach that leverages data flows, technology architecture and processes across all relevant digital ID, AML-CFT, anti-fraud and general risk management activities to strengthen all risk-related functions.

16. Develop an integrated multi-stakeholder approach to understanding opportunities and risks relevant to digital ID and developing relevant regulations and guidance to mitigate the risks. Assess and leverage, where appropriate, existing digital ID assurance frameworks and technical standards adopted by the authorities responsible for identity, cybersecurity/data protection, and privacy (including technology, security, governance and resource considerations) for assessing the assurance levels of digital ID systems for use in CDD. In line with FATF Recommendation 2, co-operate and co-ordinate with relevant authorities to facilitate a comprehensive, coordinated approach to understanding and addressing risks in, the digital ID ecosystem and to ensure the compatibility of AML/CFT requirements on digital ID systems with Data Protection and Privacy rules.

17. AML/CFT authorities could consider adopting mechanisms to enhance dialogue and cooperation with relevant private sector stakeholders, including regulated entities and digital ID service providers, to help identify key identity-related opportunities, risks and mitigation measures. Mechanisms could include a regulatory 'sandbox' approach to provide a supervised environment to test how digital ID systems interact with national AML/CFT laws and regulations. Authorities could also consider developing mechanisms to promote cross-industry collaboration in identifying and addressing vulnerabilities in existing digital ID systems.

18. Consider supporting the development and implementation of reliable, independent digital ID systems by auditing and certifying them against transparent digital ID assurance frameworks and technical standards, or by approving expert bodies to perform these functions. Where authorities do not audit or provide certification for IDSPs themselves, they are encouraged to support assurance testing and

certification by appropriate expert bodies so that trustworthy certification is available in the jurisdiction. Authorities are encouraged to support efforts to harmonise digital ID assurance frameworks and standards to develop a common understanding of what constitutes a "reliable, independent" digital ID system.

19. Apply appropriate digital ID assurance frameworks and technical standards when developing and implementing government-provided digital ID. Authorities should be transparent about how the jurisdiction's digital ID system works and its assurance levels.

20. Encourage a flexible, risk-based approach to using digital ID systems for CDD that supports financial inclusion. Consider providing guidance on how to use digital ID systems with different assurance levels for identity proofing/enrolment and authentication for tiered CDD.

21. Monitor developments in the digital ID space with a view to share knowledge, best practices, and to establish legal frameworks at both the domestic and international level that promote responsible innovation and allow for greater flexibility, efficiency and functionality of digital ID systems, both within and across borders.

Recommendations for regulated entities

22. Understand the basic components of digital ID systems, particularly identity proofing and authentication, and how they apply to required CDD elements (see Section II and Appendix A of the FATF guidelines).

23. Take an informed risk-based approach to relying on digital ID systems for CDD that includes:

    a. Understanding the digital ID system's assurance level/s, particularly for identity proofing and authentication, and

    b. Ensuring that the assurance level/s are appropriate for the ML/TF risks associated with the customer, product, jurisdiction, geographic reach, etc.

24. Consider whether digital ID systems with lower assurance levels may be sufficient for simplified due diligence in cases of low ML/TF risk. For example, where permitted, adopting a tiered CDD approach that leverages digital ID systems with various assurance levels to support financial inclusion.

25. If, as a matter of internal policy or practice, non-face-to-face business relationships or transactions are always classified as high-risk, consider reviewing and revising those policies to take into account that customer identification/verification measures that rely on reliable, independent digital ID systems, with appropriate risk-mitigation measures in place, may be standard risk, and may even be lower-risk.

26. Where relevant, utilise anti-fraud and cyber-security processes to support digital identity proofing and/or authentication for AML/CFT efforts (customer identification/verification at on-boarding and ongoing due diligence and transaction monitoring). For example, regulated entities could utilise safeguards built into digital ID systems to prevent fraud (i.e., monitoring authentication events to detect systematic misuse of digital IDs to access accounts, including through lost, compromised, stolen, or sold digital ID credentials/authenticators) to feed into systems to conduct ongoing due diligence[141] on the business relationship and to monitor, detect and report suspicious transactions to authorities.

27. Regulated entities should ensure that they have access to, or have a process for enabling authorities to obtain, the underlying identity information and evidence or digital information needed for identification and verification of individuals. Regulated entities are encouraged to engage with regulators and policy makers, as well as digital ID service providers, to explore how this can be efficiently and effectively accomplished in a digital ID environment.

[141] Note for the purposes of this report, *ongoing due diligence* means ongoing CDD.

Recommendations for digital ID service providers

28. Understand the AML/CFT requirements for CDD (particularly customer identification/verification and ongoing due diligence) and other related regulations, including requirements for regulated entities to keep CDD records.

29. Seek assurance testing and certification by the government or an approved expert body, or where these are not available, another internationally reputable expert body. Where available, participate in public sector regulatory 'sandboxes' (or other relevant mechanisms) to assess the digital ID system's assurance levels.

30. Provide transparent information to AML/CFT regulated entities about the digital ID system's assurance levels for identity proofing, authentication, and, where applicable, federation /interoperability.

14. APPENDIX 6

THE EXISTING AML/CFT REGIME

14.1 CORE KYC OBLIGATIONS OF REPORTING ENTITIES

Reporting entities are required to, among other things, collect identity information about each customer, which includes their full name, date of birth and residential address (being Core KYC).

The AML/CFT Act applies to, and imposes its obligations on, "reporting entities".[142] However, this is only to the extent that, broadly speaking, the entity's activities fall within the limits defined by the AML/CFT Act.[143]

The primary operation of New Zealand's AML/CFT regime is through the obligations imposed by the AML/CFT Act on reporting entities.[144] These obligations are set out in the table below.

REPORTING ENTITY OBLIGATIONS	
Compliance Officer	Appoint a suitably qualified compliance officer to administer and maintain the AML/CFT programme.[145]
Risk Assessment	Prepare a written risk assessment of the ML/TF risks that the reporting entity could expect in the course of running its business, including an assessment of its customers and the nature of its business.[146]
AML/CFT Programme	Establish, implement and maintain an AML/CFT programme, reflecting the risk assessment, that includes procedures to detect, deter, manage and mitigate ML/TF.[147]
Customer Due Diligence	Conduct CDD processes based on the risk assessment.[148]
Suspicious Activity Reports	Report suspicious activities and transactions to the Commissioner of Police.[149]

[142] AML/CFT Act, section 6(1).
[143] AML/CFT Act, section 6(4).
[144] A "reporting entity" is defined in the AML/CFT Act as a casino, a designated non-financial business or profession, a financial institution, a high-value dealer, the Racing Industry Transition Agency, a person or class of persons declared by regulations to be a reporting entity or another person required by an enactment to comply with the AML/CFT Act as if it were a reporting entity. Specifically excluded is any person or class of person declared by regulations not to be a reporting entity.[144] The Anti-Money Laundering and Countering Financing of Terrorism (Definitions) Regulations 2011 declare certain classes of people to be included and excluded from the definition of a reporting entity.[144] These classes of people are not specifically relevant to this Report, and therefore they are not explained in any further detail.
[145] AML/CFT Act, sections 56(2)-(5).
[146] AML/CFT Act, section 58.
[147] AML/CFT Act, sections 56(1) and 57; and AML/CFT Programme Guideline, issued jointly by the AML/CFT Supervisors in May 2018, at [29].
[148] AML/CFT Act, sections 11, 12 and 31.
[149] AML/CFT Act, sections 39A and 40.

Annual Report	Undertake a report on its risk assessment and AML/CFT programme annually.[150]
Biennial Audit	Undertake an independent audit of its AML/CFT compliance every two years (or a different time period prescribed by regulations, although no such prescriptions have yet been made) or on the request of the reporting entity's AML/CFT Supervisor.151

As this Report is focused on Core KYC, the only relevant obligation for these purposes is that of understanding CDD.

Under the AML/CFT Act, failure to perform CDD can lead to a fine of up to $200,000 for an individual or $2 million otherwise, if a civil liability act, or, a fine of up to $300,000 for an individual or $5 million otherwise, if criminally liable. The three AML/CFT Supervisors (the Reserve Bank, the FMA and the DIA) have become much more active in enforcing the AML/CFT Act.

Strict compliance with the CDD requirements is a matter that reporting entities should take very seriously.[152] It is natural for reporting entities to adopt a conservative approach towards CDD compliance. This means where there is ambiguity in the regime, such as to the approach to take in relation to identity and verification of Core KYC, many reporting entities choose to adopt the more restrictive interpretation, and unless there are clear safe harbours available to them, prefer not to rely on external entities such as agents or other reporting entities.

14.2 SUBJECTS OF CDD

CDD requirements cover customers as well as the beneficial owners of customers and persons acting on behalf of customers.

There are three categories of persons that reporting entities are required to conduct initial (and, where necessary, subsequent) CDD on. These are the reporting entity's customers, those customers' beneficial owners, and persons acting on behalf of those customers.[153] Although CDD obligations are typically triggered in relation to a customer, once triggered they will extend beyond them to their beneficial owners and persons acting on their behalf. Ongoing CDD and account monitoring will also need to be carried out by a reporting entity.[154] Ongoing CDD and account monitoring are discussed further in section 14.4.

A "customer" is defined as a new or existing customer and includes, for instance, a facility holder or a person conducting, or seeking to conduct, an occasional transaction or activity through a reporting entity. A "facility holder" is generally defined as the person in whose name a facility is established, with a "facility" defined as an account or arrangement provided by a reporting entity through which a facility holder may conduct two or more transactions (themselves broadly defined).[155]

The definition of "beneficial owner" in the AML/CFT Act is complemented by interpretative guidance, issued jointly by the AML/CFT Supervisors, as meaning any individual who owns more than 25 percent of a customer, has effective control of a customer, or is a person on whose behalf a transaction is conducted.[156] A beneficial owner is a person that meets any one of the three elements of the definition.[157] As these must be natural persons, they can be traced through multiple layers of entities, and a complex arrangement of

[150] AML/CFT Act, section 60.
[151] AML/CFT Act, sections 59(2) and 59B.
[152] Especially given the recent focus on enforcement, for example, *Department of Internal Affairs v Ping An Finance (Group) New Zealand Company Limited* [2017] NZHC 2363, *Department of Internal Affairs v Qian DuoDuo Limited* [2018] NZHC 1887 and *Department of Internal Affairs v Jin Yuan Finance Limited* [2019] NZHC 2510.
[153] AML/CFT Act, section 11(1).
[154] AML/CFT Act, section 31(1).
[155] AML/CFT Act, section 5(1) definition of "customer".
[156] The AML/CFT Act defines it as an individual that has effective control, or owns a prescribed threshold, of a customer or person on whose behalf a transaction is conducted (sec ion 5(1) of the AML/CFT Act). As joint supervisor guidance indicates the AML/CFT Supervisors' collective interpretation of the AML/CFT Act, we have proceeded on the basis of the elements as set out in that, but there does remain an argument that the two do not align.
[157] Beneficial Ownership Guideline, issued jointly by the AML/CFT Supervisors in December 2012, at [14].

layers without any reasonable explanation may be an indication that an attempt is being made to hide those individuals.[158]

Reporting entities are entitled to treat a customer that is an individual, and who is believed on reasonable grounds to not be acting on behalf of another person, to also be the beneficial owner unless there are reasonable grounds to suspect that there is another beneficial owner.[159]

A "person acting on behalf of a customer" is defined in official joint guidance as a person operating or transacting on an account or facility held by a customer.[160] This specifically means those persons with authority to act on behalf of customers, as opposed to the effective control that could make an individual a beneficial owner.[161]

14.3 TYPES OF CDD

CDD can be of different levels, with the most common (and most relevant here) being standard CDD. A reporting entity must conduct this before establishing a business relationship with, or conducting an occasional transaction for, a customer, where there is a material change in its business relationship with an existing customer so that it considers it has insufficient information about them, or it becomes aware an existing account of theirs is anonymous.

The nature of the reporting entity's customer and the transaction in question, as well as the general circumstances surrounding them, will determine which type of CDD must be conducted. This will then (as discussed in this Appendix 6 (sections 14.3.2, 14.3.4.2 and 14.3.6) determine what information the reporting entity must collect to satisfy its obligations and what verification obligations it has in relation to that information.

The three possible types of CDD are, in increasing order of detail, simplified CDD, standard CDD and enhanced CDD.[162] Where simplified or standard CDD are required, however, a reporting entity may elect to conduct CDD at a higher level.[163]

14.3.1 STANDARD CDD

As the name entails, standard CDD is the most common type. CDD to the standard level must be conducted where:[164]

- A reporting entity establishes a business relationship with a new customer;
- A customer seeks to conduct an occasional transaction or activity through the reporting entity;
- In relation to an existing customer and according to the level of risk involved, there has been a material change in the nature or purpose of the reporting entity's business relationship with that customer and the reporting entity considers that it has insufficient information about that customer;
- The reporting entity becomes aware that an existing account is anonymous; or
- Any other circumstances specified in regulations occur (although no such specifications have yet been made).

Therefore, not only must reporting entities carry out initial CDD with new customers or in respect of new occasional transactions or activities, but existing customers and accounts can also trigger a requirement to carry out subsequent CDD. Subsequent CDD is distinct from ongoing CDD and account monitoring as the

[158] Beneficial Ownership Guideline, issued jointly by the AML/CFT Supervisors in December 2012, at [17].
[159] AML/CFT Act, section 11(2).
[160] "Acting on behalf of a customer" fact sheet, issued jointly by the AML/CFT Supervisors in August 2013, at 1.
[161] Beneficial Ownership Guideline, issued jointly by the AML/CFT Supervisors in December 2012, at [29].
[162] AML/CFT Act, section 11(3).
[163] AML/CFT Act, sections 11(3)(a) and (b).
[164] AML/CFT Act, sections 14(1) and (2).

latter is a specific and distinct obligation described in section 14.4 while the former is another instance of initial CDD obligations.

The "material change" to trigger subsequent CDD in respect of an existing customer is not defined in the AML/CFT Act, but joint guidance has described it as an event, activity or situation that a reporting entity identifies that could change the level of ML/TF risk that they may encounter.[165]

What constitutes "anonymous" for an existing account is not defined in either the AML/CFT Act or guidance. However, for practical reasons it must go further than merely not having completed CDD to the required standard under the AML/CFT Act, as otherwise reporting entities would have had an immediate obligation to carry out CDD on all of their existing customers when they came under the AML/CFT regime. Rather, it likely contemplates a more comprehensive lack of information about the customer, being without any identification whatsoever rather than simply identification short of the required standard.

Where a reporting entity has already obtained and verified any documents, data or information for CDD purposes under the AML/CFT Act, and is subsequently required to conduct CDD, it is not required to obtain or verify those documents, data or information again unless it has reasonable grounds to doubt their adequacy or veracity.[166]

14.3.2 INFORMATION REQUIREMENTS

Standard CDD requires obtaining from customers, their beneficial owners and persons acting on their behalf full names, dates of birth, addresses or registered offices, company identifiers or registration numbers, and (for non-customers) relationships with the relevant customers. These multiple pieces of information are used together to reduce the risk of coincidental similarities in identity information.

Information lies at the heart of CDD.[167] In particular, the robust operation of AML/CFT laws around the world hinges on law enforcement agencies being able to identify persons that have acted in a particular context, so that they can carry out investigations and, if necessary, prosecutions.[168]

Though not specific to AML/CFT requirements, the DIA has described in published statements a description of the concept of identification as "the process of associating identity-related attributes with a particular person".[169] This involves establishing that the claimed identity is a valid one, that the person claiming the identity is connected to that identity, and that that person uses that identity within the community. These elements each provide different evidence around identification, and operate together to determine it with confidence.[170]

For standard CDD, a reporting entity must obtain from the relevant persons (being the customers as well as their beneficial owners and persons acting on their behalf) the following identity information:[171]

- Their full name;
- Their date of birth;
- Their address or registered office;
- Their company identifier or registration number;
- For beneficial owners, or persons acting on behalf, of a customer, their relationship to that customer; and
- Any further information prescribed by regulations (although no such prescriptions have yet been made).

---

[165] AML/CFT Programme Guideline, issued jointly by he AML/CFT Supervisors in May 2018, at [9]; and Enhanced Customer Due Diligence Guideline, issued jointly by the AML/CFT Supervisors in December 2017, at [12].
[166] AML/CFT Act, section 11(4).
[167] Basel Committee on Banking Supervision *Customer due diligence for banks* (Bank for Interna ional Settlements, 2001) at [21].
[168] Joy Geary "Money laundering" [2010] NZLJ 228 at 230.
[169] Department of Internal Affairs *Evidence of Identity Standard* (version 2.0, Department of Internal Affairs, 2009) at [5.2]. The Evidence of Identity Standard is referred to in the Identity Verification Code of Practice – Explanatory note at page 5.
[170] Department of Internal Affairs *Evidence of Identity Standard* (version 2.0, Department of Internal Affairs, 2009) at [5.2].
[171] AML/CFT Act, section 15.

Therefore, the only pieces of required identity information that fall within Core KYC for the purposes of this Report are the full name, date of birth and residential address, and even then, it will only be those of natural persons.

The use of multiple pieces of information in identifying a customer stems from the fact that any one piece of information may, by coincidence or otherwise, link to multiple persons. Many persons will be born on any particular date, groups of persons may reside at any particular address, and even a full name may be shared. By combining different pieces of information, the chance of any particular combination of information capturing multiple persons is reduced, and it is more likely that it can be confidently and robustly connected with a single unique individual.

Address is notably different from the other pieces of Core KYC information. For example, legal name and date of birth are things that everyone has, do not change (other than, for legal name, where changed through a legal process), and most are registered with the DIA. A person's residential address on the other hand, is not fixed or determined by a legal registration. A person may simply not have one, or have one that changes every day, and even if they do have a fixed one, there may not be any evidence to verify it (for example, a lodger, such as one living with parents, may not be named in any tenancy agreement or utility service, and now that the postal service is not operated daily, they may not make use of it).

Other information required to be collected for CDD purposes are briefly explored in Appendix 8.

14.3.3 VERIFICATION REQUIREMENTS

Reporting entities must take reasonable steps to verify CDD information on the basis of documents, or data and information issued by a reliable and independent source. This must generally be done before establishing a business relationship or conducting an occasional transaction or activity, but can in some cases be done afterwards.

For standard CDD (including Core KYC), a reporting entity must:[172]

- Take reasonable steps to satisfy itself that the identity information obtained is correct;
- According to the level of risk involved, take reasonable steps to verify:
  - The identity of any beneficial owner of a customer to satisfy itself that it knows who the beneficial owners are; and
  - The identity and authority of any person acting on behalf of a customer to satisfy itself that it knows who those persons are and that they have authority to act on behalf of that customer; and
- Verify any other information prescribed by regulations (although no such prescriptions have yet been made).

Identity information obtained for CDD purposes must also be appropriately verified before a business relationship is established or an occasional transaction or activity is conducted.[173] For standard CDD (and for this Report's purposes, Core KYC), however, this verification can be completed after the establishment of a business relationship if it is essential normal business practice is not interrupted, ML/TF risks are effectively managed through appropriate risk management procedures and the verification is completed as soon as practicable after that establishment.[174] Ambiguity around exactly what would constitute "essential" for normal business practice to not be interrupted, or what precisely the consequences of failing to verify information "as soon as practicable" are, may leave reporting entities reluctant to rely on this.

[172] AML/CFT Act, section 16(1).
[173] AML/CFT Act, section 16(2).
[174] AML/CFT Act, sections 16(3).

This verification must be done on the basis of documents, data or information issued by a reliable and independent source, or on any other basis prescribed for particular circumstances by regulations (although no such prescriptions have yet been made).[175]

14.3.4 SIMPLIFIED CDD

Circumstances

CDD to at least the simplified level must be conducted where:[176]

- A reporting entity establishes a business relationship with a customer of one of the specified types;
- A customer of one of the specified types conducts an occasional transaction or activity through the reporting entity; or
- Any customer conducts a transaction or obtains a product or service specified in regulations through the reporting entity (although no such specifications have yet been made).

Types of customers specified for these purposes include listed issuers, certain government departments (and foreign equivalents located in countries with sufficient AML/CFT systems), certain local authorities, the New Zealand Police, State enterprises (and foreign equivalents located in countries with sufficient AML/CFT systems), Crown entities, registered banks and licensed insurers.[177]

A reporting entity may also conduct simplified CDD on a person acting on behalf of one of its customers where the reporting entity has a business relationship with that customer at the time the person acts on its behalf and has conducted CDD on that customer.[178]

Information requirements

A reporting entity only needs to obtain about a person acting on behalf of a customer, their full name, date of birth, relationship to that customer, and any further information prescribed by regulations (although no such prescription has yet been made).[179] Therefore, the only pieces of required identity information that fall within Core KYC for simplified CDD are the full name and date of birth (and not address, which is required for standard CDD) of natural persons.

Verification requirements

Verification of information for simplified CDD must be carried out before a business relationship is established, an occasional transaction or activity is conducted, or a person acts on behalf of a customer.[180]

A reporting entity must only, according to the level of risk involved, verify the identity and authority of any person acting on behalf of a customer to satisfy itself that it knows who the person is and that they have authority to act on behalf of that customer.[181] In verifying this authority, a reporting entity is entitled to rely on an authority provided in an application form or other document provided to it that shows a person's authority to act or transact on an account.[182]

[175] AML/CFT Act, section 13.
[176] AML/CFT Act, section 18(1).
[177] AML/CFT Act, section 18(2).
[178] AML/CFT Act, section 18(3).
[179] AML/CFT Act, section 19.
[180] AML/CFT Act, section 20(2).
[181] AML/CFT Act, section 20(1).
[182] AML/CFT Act, section 20(3).

14.3.5 ENHANCED CDD

Circumstances

CDD to the enhanced level must be conducted where:[183]

- A reporting entity establishes a business relationship with a customer of one of the specified types;
- A customer of one of the specified types seeks to conduct an occasional transaction or activity through the reporting entity;
- A customer seeks to conduct a complex and unusually large transaction, or unusual pattern of transactions, without an apparent or visible economic or lawful purpose;
- The reporting entity considers that the level of risk involved is such that enhanced CDD should apply to the situation;
- The reporting entity is required to make a suspicious activity report to the Commissioner of Police; or
- Any other circumstances specified in regulations occur (although no such specifications have yet been made).

Types of customer specified for these purposes are trusts or other vehicles for holding personal assets, non-resident customers from countries with insufficient AML/CFT systems or measures in place, and companies with nominee shareholders or shares in bearer form.[184]

The AML/CFT Act also imposes modified enhanced CDD obligations in other specified situations, such as in relation to politically exposed persons, wire transfers, correspondent banking relationships, or new or developing technologies or products that might favour anonymity.[185]

Subsequent enhanced CDD can be triggered in relation to existing customers. Joint guidance describes one of the applicable triggers as there being a material change in the nature and purpose of the customer's business relationship with the reporting entity, which may require standard CDD but also enhanced CDD.[186] Another trigger is if there is insufficient information held by the reporting entity about an existing customer. Enhanced CDD could equally be triggered under certain provisions of the AML/CFT Act for high risk situations.[187]

It could be argued on the wording of the AML/CFT Act that a reporting entity, at any time considering the level of risk to be such that enhanced CDD should apply to a particular situation, could require enhanced CDD to be conducted.[188] However, joint guidance has listed that as a trigger for enhanced CDD in relation to new customers and not existing customers.[189] Therefore, it appears that merely considering a situation to involve a high level of risk will not itself trigger a requirement to conduct enhanced CDD, but if there were a material change in a relationship that triggered CDD requirements, then that level of risk would raise it to enhanced CDD.

14.3.6 INFORMATION REQUIREMENTS

Noting that, as set out in this Appendix 6, different situations can impose different requirements for enhanced CDD, a reporting entity must in general obtain, in addition to the standard CDD identity information, further identity information.[190] However, of that, information on the source of the funds or the wealth of customers and descriptions of classes or types of beneficiary, or the objects, of particular types

[183] AML/CFT Act, sections 22(1) and 22A.
[184] AML/CFT Act, section 22(1).
[185] AML/CFT Act, sections 22(2)-(5).
[186] Enhanced Customer Due Diligence Guideline, issued jointly by the AML/CFT supervisors in December 2017, at [31].
[187] AML/CFT Act, sections 22(1)(c) - (d), 22(3) or 22A. Section 22(1)(c) or (d) could apply to an exis ing customer, any other customer at any point in a business relationship, or a new customer, including a new customer conducting an occasional transaction.
[188] AML/CFT Act, section 22(1)(d).
[189] Enhanced Customer Due Diligence Guideline, issued jointly by the AML/CFT supervisors in December 2017, at [24] and [31].
[190] AML/CFT Act, section 23.

of trusts (noting that the AML/CFT Act treats trusts as being able to be considered customers)[191] would fall outside Core KYC, as would further information prescribed by regulations (although no such prescriptions have yet been made).

The names and dates of birth of beneficiaries of other types of trusts are of the type of information associated with Core KYC, but they wouldn't technically be captured by it unless the beneficiaries would otherwise be captured as beneficial owners of their trusts (either through having a sufficient level of ownership or, under the joint guidance interpretation, being persons on whose behalf the trusts conduct transactions). Therefore, in effect, the additional information requirements brought by enhanced CDD are not relevant for purposes of Core KYC.

14.3.7 VERIFICATION REQUIREMENTS

Verification of information for enhanced CDD must be carried out before a business relationship is established or an occasional transaction or activity is conducted, and this can apply to existing customers.[192] However, in line with standard CDD, this verification can be completed after the establishment of a business relationship if it is essential normal business practice is not interrupted, ML/TF risks are effectively managed through appropriate risk management procedures and the verification is completed as soon as practicable after that establishment.[193]

A reporting entity must still carry out the verification requirements of standard CDD set out in this Appendix 6 (section 14.3.3),[194] although joint guidance has suggested that increased or more sophisticated measures may be needed to constitute reasonable steps for enhanced CDD than for standard CDD.[195] The further verification requirements in relation to source of funds or wealth information, or other information prescribed by regulations (although no such prescriptions have yet been made), would fall outside the considerations for Core KYC.

14.4 ONGOING CDD

As well as any initial and subsequent CDD obligations, a reporting entity must also carry out ongoing CDD and account monitoring in relation to its customers, to ensure that the business relationship and transactions related to each customer are consistent with the reporting entity's knowledge of that customer and their business and risk profile, and to identify any grounds for reporting a suspicious activity.[196] This monitoring should be more frequent and thorough in relation to higher-risk customers than lower-risk customers.[197] Ongoing CDD and account monitoring are beyond the concept of Core KYC in this Report, as they involve tracking other information to determine consistency in an entity's activities.

14.5 COMMON STANDARDS

14.5.1 Risk-based approach

The FATF advocates a risk-based approach to AML/CFT regulation, keeping requirements proportional to risks. This is reflected in the New Zealand AML/CFT regime although the mandatory language used in the drafting of some of the AML/CFT Act's provisions may have the effect of disincentivising the adoption of a risk-based approach by some reporting entities at times.

The EOI Standard is referenced in the AIVCOP, but is drafted with a broader scope than AML/CFT and does not necessarily with reference to the FATF Standards. However, the EOI Standard can provide

[191] "Clarification of the position the AML/CFT supervisors are taking with respect of the Anti-Money Laundering and Countering Financing of Terrorism Act 2009 ("the Act") interpretation of a trust as a customer", issued jointly by the AML/CFT supervisors in July 2019, at 1.
[192] AML/CFT Act, section 24(2). For existing customers, see AML/CFT Act, sections 22(1)(c) – (d) and s22(3).
[193] AML/CFT Act, section 24(3).
[194] AML/CFT Act, section 24(1).
[195] Enhanced Customer Due Diligence Guideline, issued jointly by the AML/CFT supervisors in December 2017, at [57].
[196] AML/CFT Act, sections 31(1) and (2).
[197] Enhanced Customer Due Diligence Guideline, issued jointly by the AML/CFT Supervisors in December 2017, at [26] and [29].

insights into the DIA's expectations for ascertaining the identity of persons. The DIA recognises that it is not feasible to prove the identity of individuals with certainty, as this would require a process so cumbersome and intrusive that its costs would greatly outweigh any benefits. Accordingly, a risk-based approach is suggested, connecting the level of confidence required to the risks of the circumstances in question.[198]

Circumstances of lower risk may not be seen as warranting the costs and intrusion involved in determining identity at a higher level of confidence,[199] but the risk of being prosecuted may leave reporting entities reluctant to take that risk.

A risk-based approach is also recommended by the FATF which suggests that systems should be designed with the goal of keeping ML/TF prevention or mitigation measures "commensurate with the risks identified", to allow the efficient allocation of resources across the wider regime.[200] Such an approach is also reflected in the New Zealand AML/CFT regime.[201] However, the mandatory language in the drafting of some of the AML/CFT Act's provisions could have the effect of disincentivising the adoption of a risk-based approach by some reporting entities at times. For example, reporting entities are obliged to obtain a prescribed set of information from customers, including (amongst other things) Core KYC.[202] A person's residential address is a component of Core KYC that can be more problematic to deal with in practice than the person's full name and date of birth, but regardless of how a reporting entity assesses its impact on the risk around a particular customer it must still be obtained.[203]

In a similar vein, although only reasonable steps are required in verifying some CDD information (as discussed in this Appendix 6 (section 14.3.3)[204] the fact that some of the surrounding provisions make express reference to taking reasonable steps "according to the level of risk involved",[205] and that one does not, at least raises the question of how much the "reasonable steps" required to verify Core KYC can legitimately be based on the level of risk.

14.5.2 Code of practice

An AML/CFT Supervisor can create codes of practice to assist reporting entities in complying with their AML/CFT obligations by establishing safe harbours. So far, only the AIVCOP has been created in this way, which covers the verification of names and dates of birth.

Under the AML/CFT Act, each AML/CFT Supervisor is able to (at the direction of their responsible Minister) prepare codes of practice (or amendments to, or revocations of, existing codes) for the activities of their reporting entities, to assist them in complying with some or all of their obligations under the AML/CFT Act.[206]

To date, the AIVCOP is only the code of practice that has been created in this way. This applies to all reporting entities in all AML/CFT sectors, and is recognised by all three AML/CFT Supervisors.[207] Specifically, it covers the verification of the names and dates of birth of customers (using that term broadly to cover customers properly, their beneficial owners and persons acting on their behalf)[208] that are both natural persons and assessed by the relevant reporting entity as being low to medium risk.[209] AIVCOP prescribes two methods for verifying a person's identity: through documentary means and through electronic means.

---

[198] Department of Internal Affairs *Evidence of Identity Standard* (version 2.0, Department of Internal Affairs, 2009) at [5.2].
[199] Department of Internal Affairs *Evidence of Identity Standard* (version 2.0, Department of Internal Affairs, 2009) at [7.2].
[200] Financial Action Task Force, *International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation* (Financial Action Task Force, Paris, 2012-2019) at 9 (Recommendation 1) and 29 (Interpretive Note to Recommendation 1).
[201] See, for example, references to "the level of risk involved" in the AML/CFT Act, sec ions 12, 14(1)(c), 16(1) and 58(3)(c).
[202] AML/CFT Act, section 15.
[203] AML/CFT Act, section 15(d).
[204] AML/CFT Act, section 16(1)(a).
[205] AML/CFT Act, sections 16(1)(b) and (c).
[206] AML/CFT Act, sections 63(1)-(3) and 65.
[207] Amended Identity Verification Code of Practice 2013, at 3.
[208] Amended Identity Verification Code of Practice 2013, at 2; and AML/CFT Act, sec ion 11(1).
[209] Amended Identity Verification Code of Practice 2013, at 3.

The AML/CFT codes of practice and the AIVCOP are analysed further in Appendix 7.

14.6 RELIANCE ON THIRD-PARTY VERIFICATION OF A PERSON'S IDENTITY

14.6.1 Types of reliance

Reporting entities can, under the AML/CFT Act, rely on certain third parties to carry out their CDD procedures, which their AML/CFT programmes must account for. These third parties can be members of the same designated business group as the reporting entity, authorised agents of the reporting entity, or other reporting entities.

The AML/CFT Act provides for certain situations where a reporting entity may rely on a third party to carry out the CDD procedures required of the reporting entity. These are reliance on:

- DBG Reliance;
- An authorised agent (i.e. "Agency Reliance"); or
- Another reporting entity (i.e. "Reporting Entity Reliance"), including reliance on a so-called "approved entity" (i.e. "Approved Entity Reliance").

Where a reporting entity does rely so on a third party, its AML/CFT programme must include adequate and effective procedures, policies and controls for providing when, and setting out the procedures for how, the third party may conduct the relevant CDD on behalf of the reporting entity.[210] Reporting entities relying on third parties should clearly communicate these procedures, policies and controls, as well as their CDD requirements, to those third parties, and actively monitor them to ensure that they are carrying out that CDD to the required New Zealand standards.[211]

DBG Reliance

A reporting entity that is a member of a DBG may rely on another member of that DBG to, among other things, conduct the CDD procedures required under the AML/CFT Act as long as the relevant information is given to them within the required timeframes. This means that the identity information obtained must be given to the reporting entity before the business relationship is established or the occasional transaction or activity is conducted, and that the verification information obtained must be given to it as soon as practicable on (and within five working days of) its request after that business relationship is established or that occasional transaction or activity is conducted.[212] There are currently hundreds of DBGs established for reporting entities.

The criteria required to qualify for membership in a DBG (in summary):

- Being related[213];
- Providing a service under a joint venture agreement with, each other member; or
- Being one of a specified list of government departments, as well as the fact that an entity can only be the member of a single New Zealand DBG,

  means that this is unlikely to be a practical form of reliance for many reporting entities in New Zealand.[214] Generally this form of reliance works reasonably well. However, given the corporate structure of some business groups, the technicalities of the required relationship for this form of reliance are not met (i.e.

[210] AML/CFT Act, section 57(1)(k).
[211] AML/CFT Programme Guideline, issued jointly by he AML/CFT supervisors in May 2018, at [65].
[212] AML/CFT Act, section 32(1).
[213] The AML/CFT Act, in the section 5(1) DBG defini ion, refers to, among other things and without limitation, sections 2(3) of the Companies Act 1993 and 12(2) of he Financial Markets Conduct Act 2013 and their definitions of "related" for companies and bodies corporate respec ively. These cover situations where the entities are a holding company and subsidiary, one entity (or an entity related to that entity, or members of that entity) directly or indirectly holds more than half of the issued shares or voting products of the other entity, the businesses of the entities have been so carried on that the separate business (or a substantial part thereof) of each entity is not readily identifiable, or there is another entity that both of the entities are related to. The DBG definition also refers to related, law firms, conveyancers, accounting prac ices, trust and company service providers, real estate agents, high-value dealers, money transfer agents or sub-agents.
[214] AML/CFT Act, section 5(1) definition of "designated business group".

the relationship between a fund manager and the funds it manages). This form of reliance likely won't be available to reporting entities which are wholly independent of one another, such as any reporting entities which are part of a Trust Framework that are independent of one another.

Agency Reliance

A reporting entity may authorise another person as its agent and then rely on them to conduct its CDD procedures, and to obtain the information it requires for CDD purposes, under the AML/CFT Act.[215] An "agent" is not defined in the AML/CFT Act, and ordinary principles of agency law apply.[216] This form of reliance implies a relationship of principal and agent (i.e. a superior and a subordinate). Where this relationship dynamic exists for other commercial reasons, this works well, and it is well used. However, where this relationship dynamic does not exist, it can be problematic, since it generally requires the principal to have active supervision of and have access to the agent's business information.

Reporting Entity Reliance

A reporting entity may rely on another reporting entity (or the equivalent in another country with sufficient AML/CFT systems) to conduct the CDD procedures required of the former under the AML/CFT Act where the latter:[217]

- Has a business relationship with each of the relevant customers;
- Has conducted relevant CDD procedures on the relevant customers to at least the standard required by the AML/CFT Act and has provided to the relying reporting entity the relevant:
  - Identity information before the relying reporting entity establishes a business relationship with or conducts an occasional transaction or activity for a relevant customer; and
  - Verification information as soon as practicable on (and within five working days of the) request by the relying reporting entity; and
- Consents to conducting the CDD procedures for, and to providing all relevant information to, the relying reporting entity.

Any other conditions prescribed by regulations must also be complied with (although no such prescriptions have yet been made).[218] In practice, reporting entities seldom use this form of reliance given the competitive drivers between them as well as difficulties agreeing to allocations of liabilities between themselves.

Reporting Entity Reliance is seldom used in practice. As discussed in more detail in section 5.2.3 above, not only would the reporting entity relying on another retain ultimate responsibility and thus have to incur oversight costs that erode any benefit from the reliance, but the reporting entity being relied on may also be exposed to potential liability because of it.

14.6.2 Restrictions on use

Information collected by a third party being relied on for CDD purposes can only be used for the purpose of complying with the AML/CFT Act.

Where a reporting entity is relying on a third party to conduct CDD (under DBG Reliance, Reporting Entity Reliance or Agency Reliance), and information is obtained by the third party, that third party can only use that information for the purpose of complying with the AML/CFT Act.[219] This, of course, ties in with the restrictions on the use of information under the privacy law regime, as discussed in section 4.7 above.

---

[215] AML/CFT Act, section 34.
[216] Department of Internal Affairs, Accountants Guideline, issued in March 2018, at 36; and Department of Internal Affairs, Lawyers and Conveyancers Guideline, issued in December 2017, at 38.
[217] AML/CFT Act, section 33(2).
[218] AML/CFT Act, section 33(2)(e).
[219] AML/CFT Act, section 35.

14.6.3 Responsibility

Although reporting entities can rely on third parties for CDD purposes, ultimate responsibility for their CDD obligations remains with them. The exception to this is Approved Entity Reliance.

Under each of DBG Reliance and Reporting Entity Reliance, the relying reporting entity expressly retains ultimate responsibility for its own compliance with its AML/CFT obligations.[220] Although no explicit statement to that effect is made in the provision for Agency Reliance, as ordinary principles of agency law apply, the ultimate responsibility for compliance will also remain with the relying reporting entity.[221]

The AML/CFT Act does, however, in Approved Entity Reliance provide a specific exception to this general rule that the relying reporting entity is responsible for its own compliance when relying on a third party for CDD purposes. This is where:[222]

- The relying reporting entity is acting in good faith in relying on the third party;
- The relying reporting entity has reasonable cause to believe that the third party has conducted relevant CDD procedures to at least the standard required by the AML/CFT Act;
- The third party being relied on is an approved entity or within an approved class of entities; and
- Any conditions prescribed by regulations are complied with (although no such prescriptions have yet been made).

An "approved entity" is an entity which is prescribed by regulations as an approved entity or falls within a class of entities prescribed by regulations as a class of approved entities.[223] To date, no entity or class of entity has been so prescribed, and as a result Approved Entity Reliance and its exception from responsibility cannot be used yet.

There appears to be some ambiguity around how the scope of Approved Entity Reliance is interpreted. Under the terms of the AML/CFT Act, being an approved entity is not expressly limited to reporting entities.[224] However, the provision providing for Approved Entity Reliance both describes the entity being relied on as a "reporting entity" being relied on and is a subsection within the Reporting Entity Reliance section.[225] On the other hand, guidance from the DIA lists Approved Entity Reliance as its own fourth branch of permitted reliance (separate from DBG Reliance, Reporting Entity Reliance and Agency Reliance).[226] We recommend that this issue be clarified by the Ministry of Justice and in any event addressed during the AML/CFT Act's statutory review in 2021.

Therefore, while it appears arguable that a non-reporting entity could be prescribed as an approved entity, nothing in the AML/CFT Act actually allows for reliance on an approved entity by virtue of their status as such alone. Furthermore, the exception from responsibility for CDD obligations is expressly tied to Reporting Entity Reliance, so even if a non-reporting entity could be prescribed as an approved entity, that wouldn't have any effect. This is an area that requires clarification in order to maximise the potential for efficiency creation when completing Core KYC.

[220] AML/CFT Act, sections 32(2) and 33(3).
[221] Department of Internal Affairs, Accountants Guideline, issued in March 2018, at 36; and Department of Internal Affairs, Lawyers and Conveyancers Guideline, issued in December 2017, at 38.
[222] AML/CFT Act, section 33(3A).
[223] AML/CFT Act, section 5(1) definition of "approved entity".
[224] AML/CFT Act, section 5(1) definition of "approved entity".
[225] AML/CFT Act, sections 33(3A)(b) and (c).
[226] Department of Internal Affairs, Accountants Guideline, issued in March 2018, at 36; and Department of Internal Affairs, Lawyers and Conveyancers Guideline, issued in December 2017, at 38.

15. APPENDIX 7

AML/CFT CODES OF PRACTICE AND THE AIVCOP

AML/CFT codes of practice

Once a code of practice has been approved by the relevant responsible Minister,[227] it offers a safe harbour to reporting entities. Where the code provides for a means of satisfying a particular obligation under the AML/CFT Act, a reporting entity that complies with those provisions will be deemed to also be complying with that obligation.[228] Such a code does not mandate any specific form of compliance, and a reporting entity may still comply with AML/CFT obligations through other equally effective means.[229] However, a reporting entity may not rely on complying with AML/CFT obligations through other equally effective means as a defence to an act or omission on its part, unless it has given notice in writing to the AML/CFT Supervisor that it has opted out of compliance with the code of practice and it intends to satisfy its obligations by some other equally effective means before the act or omission occurred.[230]

Courts are also obliged to consider a relevant code of practice when determining whether a person charged with an offence around failing to comply with a provision of the AML/CFT Act has failed to so comply, whether to impose an injunction under the AML/CFT Act or whether to impose a pecuniary penalty under the AML/CFT Act.[231]

The AIVCOP

Customers assessed as being high risk are not covered by the AIVCOP, and increased or more sophisticated measures would be needed there.[232] However, the AIVCOP does recognise that the type of CDD required does not alone determine the level of risk involved, and that it would even be possible for a customer to require enhanced CDD while still being low to medium risk.[233]

The AIVCOP first describes the requirements for documentary verification of identity, being either a form of primary photographic identification, a form of primary non-photographic identification in combination with a secondary or supporting form of photographic identification, or a New Zealand driver licence in combination with one of a further set of specified documents.[234] Such verification needs to be carried out face-to-face with the customer or on the basis of copies certified by a trusted referee,[235] being an independent person of at least 16 years of age that is one of a range of specified professions.[236]

The final part of the AIVCOP covers electronic identity verification, defined as the use of a record kept in electronic form and containing authenticated core identity information about an individual to verify that individual's identity, remotely or otherwise without face-to-face contact,[237] when a reporting entity is conducting CDD.[238] This requires both confirming identity information through an electronic source (or sources) and matching the person whose identity is being verified to the identity that they are claiming.[239] Electronic sources will generally be information maintained by government bodies, or otherwise under legislation.[240]

---

[227] AML/CFT Act, section 64.
[228] AML/CFT Act, section 67(1)(a).
[229] AML/CFT Act, sections 67(1)(b).
[230] AML/CFT Act, sections 67(2).
[231] AML/CFT Act, sections 67(3)-(5).
[232] Amended Identity Verification Code of Practice 2013, at 2.
[233] Amended Identity Verification Code of Practice 2013, at 3, n 2. Ultimately this would have to come down to a reporting entity's assessment in the particular circumstances, and be influenced by whe her, for example, the enhanced CDD was triggered by considerations of risk or mandated by the type of customer.
[234] Amended Identity Verification Code of Practice 2013, at 4-5.
[235] Amended Identity Verification Code of Practice 2013, at 5.
[236] Amended Identity Verification Code of Practice 2013, at 6.
[237] Identity Verification Code of Practice – Explanatory note, issued by the AML/CFT Supervisors in December 2017, at [4].
[238] Amended Identity Verification Code of Practice 2013, at 6-7.
[239] Identity Verification Code of Practice – Explanatory note, issued by the AML/CFT Supervisors in December 2017, at [5].
[240] Identity Verification Code of Practice – Explanatory note, issued by the AML/CFT Supervisors in December 2017, at [6].

Notably, the AIVCOP does not provide for the verification of address information, instead referring back to the AML/CFT Act and stating that it must be done "using documents, data or information issued by a reliable and independent source".[241] It is not clear exactly why the AIVCOP excludes this element. As mentioned above, a person's residential address is the most difficult element of Core KYC to verify, therefore an update to the AIVCOP providing examples of ways in which addresses can be verified would be particularly useful. To the extent that the AML/CFT Supervisors prefer not to prescribe verification methods, formal guidance as to steps that might be considered reasonable would assist.

To capture the benefit of the AIVCOP, electronic identity verification requires that:[242]

- Names be verified from either a single independent electronic source able to verify an individual's identity to a high level of confidence (necessarily through biometric information or other information providing an equal level of confidence)[243] or at least two independent, reliable and matching electronic sources (even if both sources are obtained from one provider);
- Dates of birth be verified from at least one reliable and independent electronic source;
- The person's details be checked against the reporting entity's customer records, to ensure that the same identity information or documents have not been used by another person;
- In determining reliability and independence of sources, the reporting entity consider their accuracy, security, privacy and method of information collection, as well as whether they have an incorporated mechanism to determine whether the person can be linked to the claimed identity, whether the information is maintained by a government body or pursuant to legislation, and whether the information has been additionally verified from another reliable or independent source; and
- The reporting entity's compliance programme describes the forms of electronic identity verification methods that are considered reliable and independent and the circumstances in which they will be used for identity verification, how the methods have regard to the reliability and independence considerations described above, and any additional methods that will be used to supplement, or mitigate any deficiencies in, this verification process.

Where an electronic source has not incorporated a suitably robust mechanism to determine whether the person can be linked to the claimed identity (being one of the reliability and independence factors described above), a reporting entity may adopt additional measures to supplement, or mitigate any deficiencies in it.[244]

Examples of such measures include requiring the first credit into an account being established for a customer to be from another of the customer's accounts at another reporting entity, contacting the customer by letter or phone at or on a verified address or number respectively before their account is made operational, or robust steps to confirm that any identification documents electronically provided by the customer are authentic and belong to that customer.[245] In practice, verification of a person's address using their landline is difficult, since more and more people have mobile phone numbers exclusively and at the expense of landlines. Mobile phone numbers are unlikely to be helpful in verifying a person's address. These types of people tend to find it difficult to complete a reporting entity's Core KYC process.

[241] Amended Identity Verification Code of Practice 2013, at 2.
[242] Amended Identity Verification Code of Practice 2013, at 7.
[243] Identity Verification Code of Practice – Explanatory note, issued by the AML/CFT Supervisors in December 2017, at [8].
[244] Identity Verification Code of Practice – Explanatory note, issued by the AML/CFT Supervisors in December 2017, at [14].
[245] Identity Verification Code of Practice – Explanatory note, issued by the AML/CFT Supervisors in December 2017, at [15].

16. APPENDIX 8

OTHER INFORMATION REQUIRED FOR CDD

As well as the identity information described above, when conducting CDD, a reporting entity must also obtain information on the nature and purpose of the proposed business relationship between it and the customer in question.[246] Where a reporting entity is conducting standard CDD, it must also obtain sufficient information to determine whether enhanced CDD should be conducted.[247]

In carrying out ongoing CDD and account monitoring, a reporting entity must have regard to the type of CDD conducted when the business relationship was established as well as the level of risk involved, and must involve (at least) regularly reviewing the customer's account activity and transaction behaviour, any other information the reporting entity holds about the customer, and anything further prescribed by regulations (although no such prescriptions have yet been made).[248]

These further pieces of information lie outside Core KYC, and are beyond the scope of this Report. However, obtaining discrete pieces of information (in the form of Core KYC) from another entity does remove the contact with the customer that a full CDD process would generally entail. Without that direct context, it would be more difficult for a reporting entity to obtain sufficient information to determine whether enhanced CDD should be conducted.

17. APPENDIX 9

SCOPE OF MINTERELLISONRUDDWATTS' ENGAGEMENT

As set out in paragraphs 5 and 7 of MinterEllisonRuddWatts's letter of engagement with Digital Identity NZ, MinterEllisonRuddWatts was engaged to provide legal input to this Report by exploring the matters below.

- Identifying issues and constraints arising from the applicable New Zealand legal and regulatory context, in relation to issues that impede Reporting Entities (as defined in the AML/CFT Act) in relation to the sharing of digital identity, or provide opportunities for sharing of identity to occur under the AML/CFT Act. The report will address the question '*can an individual re-use identity verification obtained through an AML/CFT process and still meet the regulatory requirements of all Reporting Entities involved?*' The report will be shared openly with the wider Digital Identity community in New Zealand with the objective of providing greater certainty on the roles Reporting Entities, service providers and issuers of identity attributes, for AML/CFT Act purposes, may play in the emerging digital identity ecosystem.
- For the purposes of the Report, the concept of "identity" under the Reliance Framework will be limited to obtaining and verifying the full name, date of birth and residential address of natural persons as customers, beneficial owners or persons acting on behalf of customers to conduct initial simplified or standard conduct CDD; it will not extend to identifying or verifying corporate entities, or additional information required for enhanced CDD, or for politically exposed persons ("Core KYC"). For certainty, conducting ongoing monitoring or CDD subsequent to onboarding the customer is excluded from the scope of the Report. This analysis will be used to inform and engage with the DIA Digital Identity Programme on the developing Trust Framework, and with the FATF who will be assessing New Zealand's AML/CFT performance in February and March 2020.
- MinterEllisonRuddWatt's initial work identified some of the following legal and regulatory issues in relation to the Reliance Framework which have been covered under the Report:
  - The obligations of a Reporting Entity to conduct Core KYC under the AML/CFT Act;

[246] AML/CFT Act, sections 21, 17(a) and 25.
[247] AML/CFT Act, section 17(b).
[248] AML/CFT Act, sections 31(3) and (4).

- AML/CFT Supervisor expectations and guidance as to how those obligations are complied with;
- The current form and status of the approved entity regime under the AML/CFT Act;
- Implications for Reporting Entities, service providers and issuers of identity credentials, including where a customer for the purposes of the AML/CFT Act (Holder) uses identity attributes that may not have been explicitly supplied for the purpose of reliance for AML/CFT Act purposes (e.g. a utility company providing evidence of address);
- Legal recourse and liability between reporting entities relying on another to conduct Core KYC **(Reliers)** and service providers both under the AML/CFT Act, and also under other statutory regimes and common law;
- Implications on the enablement of real-time onboarding of customers (i.e. the digital identity solutions sought need to contemplate a real-time decision);
- The existence or not of common standards for information and verification and differences in time between when information is gathered, verified and used;
- The implications, for a Relier conducting ongoing monitoring/subsequent Core KYC, of using initial identity information received from a service provider or from a Holder;
- The use and potential reuse of existing customer identity proofs and Core KYC assets, including implications for ongoing monitoring and CDD;
- Other rules of law controlling the use of personal information, including privacy legislation (such as the Privacy Act);
- Actions achievable within the current legal framework, and actions that are not achievable within the current legal framework; and
- The implications of a Holder terminating their relationship with a Reporting Entity, and associated record keeping obligations under the AML/CFT Act.

18. APPENDIX 10

MORE ON THE QUESTIONNAIRE

Responses to MinterEllisonRuddWatts' Questionnaire for the Participating Banks and the AML/CFT Supervisors provided many real world insights into some of the issues with Core KYC (and some aspects relevant to the AML/CFT Act). The Participating Banks' responses to the Questionnaire provided first-hand insights into their experiences conducting Core KYC and as well as their compliance with parts of the AML/CFT Act. The AML/CFT Supervisors on the other hand, shared their observations of reporting entities' experiences complying with the obligation to conduct Core KYC, taken from their various interactions with the reporting entities they oversee.

19. APPENDIX 11

NEGLIGENCE

The question of whether Entity B owes Entity A duty of care is crucial to any cause of action in negligence. There doesn't appear to be any New Zealand case law that has considered this question. Accordingly, the courts would likely find any duty of care to be novel in nature. In these circumstances, the courts:

- Would need to determine whether Entity B should have reasonably foreseen injury to Entity A, as a person closely and proximately affected by Entity B's conduct; and

- Would need to weigh up the broader social/policy implications for recognising or denying the existence of a duty in the circumstances.[249]

The AML/CFT Act is relevant. The type of reliance between Entity A and Entity B would need to be common place in the industry. Entity A would need to have controls in place over Entity B (including some form of active monitoring).[250] In any event, the duty must also act coherently in the legal system as a whole.[251]

Given that under the AML/CFT Act, Entity B must consent to its Core KYC being relied upon by Entity A,[252] it seems likely that a duty of care could be established. This would arguably be a reasonable outcome from a policy perspective. The parties would be in contact with each other, and Entity B would know that Entity A would be using the information provided to not have to conduct its own Core KYC.

The damage caused (and its remoteness) in the event the duty is breached, would need to be assessed to ensure there is no break in the causal chain or some intervening factor. In some cases, it could be argued the damage caused by Entity B to Entity A is not too remote.

One hypothetical example of negligence could be where Entity A relied on Entity B's Core KYC, before Entity A started a business relationship with a customer. Entity A would then enter into a loan agreement with that customer, despite that customer having provided a false identity in its Core KYC with Entity B. Because of the identity fraud, Entity A's customer is able to abscond with the loan money, to Entity A's detriment.

20. APPENDIX 12

THE EOI STANDARD

Note: as at the date of this Report, the EOI Standard is in force and it has not been superseded by the Identification Management Standards.

The EOI Standard is a good practice guide issued by the DIA for government agencies that regularly establish and confirm the identity of individuals accessing their services.[253] Private organisations can also choose to use the standard for services that contain identity-related risk. The EOI Standard is part of a number of New Zealand authentication standards for online and offline service delivery designed to assist agencies to meet the goal of transforming government through the use of the internet. The standard's focus is on an organisation's contact with an individual accessing a service(s).

Broadly, the three components for establishing identity under the standard are:

- Evidence that the claimed identity is valid;
- Evidence that the presenter links to the claimed identity; and
- Evidence that the presenter uses the claimed identity.

The evidential requirements for a person's identity in EOI Evidential Requirements sets out various processes an agency must undertake to determine the identity of a person based on low, moderate and high levels of confidence.[254]

In summary, higher levels of confidence are justified if an agency collects multiple identity documents or records from a person which may or may not be verified by the agency in person or otherwise verified by a trusted referee. Higher levels of confidence tend to include comparisons of the identity documents or record

[249] *Tort – A to Z of New Zealand Law,* (online edition, Thomson Reuters), [59.5.2.04].
[250] Section 33 AML/CFT Act and AML/CFT Programme Guideline, May 2018, [61] – [65].
[251] *Tort – A to Z of New Zealand Law,* (online edition, Thomson Reuters), [59.5.4].
[252] AML/CFT Act, section 33(2)(d).
[253] dia.govt.nz/diawebsite.nsf/wpg_URL/Resource-material-Evidence-of-Identity-Standard-Index?OpenDocument.
[254] dia.govt.nz/diawebsite.nsf/wpg_URL/Resource-material-Evidence-of-Identity-Standard-Index?OpenDocument at 7.7.1, table 8.

against the source records of an identity issuing agency (i.e. the DIA's identity services). Parts of the EOI Evidential Requirements will soon be replaced by the Identification Management Standards which is currently in draft form.[255]

Digital Identity NZ is leading a united approach to digital identity for the benefit of all New Zealanders.

We are a purpose driven, inclusive, membership funded organisation, whose members have a shared passion for the opportunities that digital identity can offer.

Digital Identity NZ's mission is to create a digital identity ecosystem that enhances Kawanatanga (honourable governance), Rangatiratanga (self-determination and agency) and Oritetanga (equity and partnership), for all people in New Zealand.

Digital Identity NZ
L1 Building C, 14-22 Triton Drive, Auckland 0632, New Zealand
Ph +64 9 475 0204
www.digitalidentiynz.nz

[255] digital.govt.nz/standards-and-guidance/identity/identification-management/about-the-identification-standards/