Improving Access to DIA held Biometric Databases to drive New Zealand innovation and growth

3 February 2025

Principal Author: Vincent McCartney

Reviewers: Tina Groark, Colin Wallis, Jason Roberts

Background

On October 2nd, a Roundtable meeting was called to assemble private sector representatives to meet with Minister Bayly, the Commerce Commission and the Financial Markets Authority (FMA) to discuss the perceived barriers to innovation in the FinTech ecosystem. The meeting focused on fostering New Zealand's FinTech ecosystem through initiatives like the FinTech sandbox and addressing regulatory challenges. The meeting concluded with plans to establish a working group to explore a Fintech sandbox and among other action items explore digital identity standards and related matters to enhance market competitiveness. There was universal Roundtable support for the notion that robust digital identity is foundational to customers engaging in a thriving FinTech ecosystem and Aotearoa's digital economy more broadly.

An informal working group was indeed established from the Roundtable attendees, with a smaller group of applicable industry representatives (see above) meeting with Commerce Commission representatives on October 15th to outline the nature of concerns in the area of digital identity verification and in particular the monopoly that the Department of Internal Affairs (DIA) services currently have regarding access to biometric data it holds, which in turn is reflected in the current AML/CFT regulatory regime thereby impacting innovation.

That initial paper (Appendix 1 in this paper) was passed to the FMA, the Commerce Commission and the private sector industry Roundtable leads on November 18, 2024. It was subsequently added to the pre-reading papers passed to the Minister in advance of the next Roundtable meeting on December 6th.

The initial paper was consequently tabled at the December 6th Roundtable meeting. Arising from topics discussed, the small group was asked to prepare a second paper specifically in relation to Biometric data held by DIA that a small number of industry service providers in the business of undertaking identity confirmation, need access to when consent from the person has been granted to do so.

Purpose of this paper

This second paper outlines industry's concerns with regard to the current state that, unintentional or otherwise, has the effect of dampening competition and innovation, and explores potential solutions to these issues. This paper will explore how positive outcomes could be achieved by reducing the current potential for a DIA monopoly in terms of accessing people's biometric data held on their behalf by DIA.

The brief was to find a solution to how NZ RegTech companies and Digital Identity credential issuers (collectively referred to as 'Intermediaries' herewith) could directly access the biometric images (i.e. Passport photos) held by the DIA rather than the current state which sees them required to use their competition's RealMe/Identity Check services, which are considered both cost & innovation prohibitive solutions. Two options are summarised below - an ideal solution considered longer term because it requires changes to legislation and a short term solution as a stop gap by adopting the pragmatic approach to biometric database access used in Australia.

The two options identified in this paper can be summarised as:

- Longer term option, which requires legislative change so will take some time to achieve. This option enables intermediaries, with the consent of the customer, to retrieve the biometric data associated with the customer's passport, visa or driver's license.

- Short term option, which can be achieved within the current regulatory constraints. With this option, once an intermediary has confirmed the identity data, it can take the extra step of submitting a photo for comparison against the photo on record for the customer's passport, visa or driver's license.

Each option incrementally adds improvements to the current state, which helps Intermediaries drive innovation, increase competition and reduce costs for consumers.

Desired Outcomes

The primary desired outcome is to increase innovation, which in turn will drive growth and improve customer outcomes through lower costs and better digital experiences.

To enable these outcomes, intermediaries require:

1. Expanded Database Access for Intermediaries to include biometric data

2. Reduced costs for accessing the data

Database Access: Current state and challenges to improvement

Background

The Identity Information Confirmation Act 2012 ('IICA') governs access by Government departments and Intermediaries to personal information held by the DIA.

The non-biometric data held (e.g. Passport Number, Name and Date of Birth) can currently be confirmed by Intermediaries via APIs if they have a 'Confirmation Agreement' in place with the DIA.

The IICA currently specifies that the responses to the verification of data requests are either "Consistent", "Not Consistent", or "Exception". In practice, an API response also includes a line by line breakdown of each element (e.g. Surname) in the same response format.

The biometric data held (i.e. photo) is not currently available for verification/matching via any means as there are no external APIs available to Intermediaries.

The current publicly available information is that this information will be matched via the Identity Check service, once the relevant APIs have been made available to Intermediaries. This biometric matching can be performed under the IICA and will result in similar responses to the non-biographical data matching.

> "Identity Check is a safe and secure online identity verification service, developed by Te Tari Taiwhenua Department of Internal Affairs. Identity Check works by confirming the identity information provided by a user online against the New Zealand Passport or Driver Licence databases." [accessed 23/01/25]

The Identity Check service also accesses NZTA Driver Licence biometric data. DIA is permitted to do this via an amendment to the Land Transport Act 1988. When the Land Transport Act was being updated, this change in who can access biometric data was not extended to Intermediaries.

Intermediaries access non-biometric data held by the NZTA via separate agreements and API connections directly with the NZTA.

Potential challenges with improving database access

Privacy

There will inevitably be privacy concerns if carte blanche access to the Passport database is given, but this is not being sought. Instead controlled access is being sought in all of the scenarios described in this paper.

The Privacy Commissioner's announcement of the Code of Practice for Biometrics in December, while well intentioned, adds a further dimension to the complexity of the problem faced by intermediaries that access biometrics images because of the uncertainty introduced by new regulation that could be subject to differing interpretations between the OPC and intermediaries. Examples are the requirement for a robust data Privacy Impact Assessment and the proportionality test to determine whether the use of biometrics is justified vis a vis non biometric alternatives. One of the key customer benefits of consented biometrics identification and verification is speed and convenience because it can be carried out 'in the onboarding flow'. Of course non biometric and offline alternatives are available but they have a deadening effect on the customer experience.

Other regulations

Additionally, if intermediaries opted in to be accredited under the Digital Identity Trust Framework (DISTF) directly, or were subject to the Customer Product and Data Act expected later this year that leans into the DISTF for the digital identity and verification components, then external audit is a requirement. The accreditation burden of these can be perhaps partly

mitigated if the intermediary has invested in achieving and holding current, a ISO27001 (or equivalent) certification.

Technology

In the absence of a public statement to the contrary, DIA may not have the development budget available to make the necessary API changes to enable greater database access. However, it is our understanding that the next phase of API developments for Identity Check (which will make it available to Intermediaries) are yet to be agreed upon, so this is the perfect time to divert resources into API changes that will enable the changes requested in this paper.

Legislation Changes

Changes may be required to the IICA to allow for images to be returned to the Intermediary to allow for the pragmatic Short-Term Solution (see below).

Costs

Background

The cost of performing confirmation checks in New Zealand are significantly above and out of line with Australia that has an equivalent service (ID Match). Ultimately these costs are passed on to customers, either directly or indirectly, resulting in a worse outcome for them.

Looking at the chart below, on the face of it, it seems hardly credible that DIA is merely recovering direct cost of offering the service. Could it be using its monopoly to charge higher fees that are used to underwrite its service costs more broadly? For the good of the digital economy to increase technology adoption and improve productivity, it should make the price as low as possible and reduce barriers to entry.

Confirmation Check Cost	Australia	New Zealand	NZ price difference
Non-Biometric Data	A$0.40 (~NZ$0.44)	NZ$1.00	+127%
Biometric Data	A$0.40 (~NZ$0.44)	NZ$5.00	+1036%

To note:

- *The New Zealand Non-Biometric Data cost was as low as $0.15 until early 2023.*
- *The equivalent Australian Biometric Data service matches the Intermediary's captured image. The New Zealand price listed is for RealMe, which captures the image on the Intermediary's behalf.*

Options Available

	Longer-Term Solution	Short-Term Solution

Improved Database Access for Intermediaries	Intermediaries have direct access to the biometric information so that they can perform their own matching. See Appendix 2 for more information on this Longer-Term Solution.	The Intermediary captures the image of the subject being identified, sends this to the DIA for matching in the same way that Non-Biometric data is matched. This would be the same as the Australian equivalent.
Reduced Costs	The pricing for Biometric and Non-Biometric data matching is the same as or similar to the Australian equivalent.	The pricing for Biometric Data matching is the same as the Non-Biometric data matching.

The Pragmatic Short-Term Solution

The 3 main pushbacks against the Longer-Term Solution are likely to be:

1. Privacy concerns
2. Potential Legislative changes
3. DIA cost/revenue loss implications

These concerns could be mitigated by the pragmatic Short-Term Solution which would allow the Intermediaries to use their own technology to capture the face of the subject, and for this to be sent to the Identity Check service for matching. This is the approach that the Australian Government has landed on with its ID Match service.

This approach, combined with pricing in line with or close to Australia's, would not solve the monopolistic question but would largely appease the sector as it would allow Intermediaries to innovate without being burdened by having to use technology that doesn't fit in with their UX at a reasonable price.

Additionally, technology is rapidly changing and opportunities for fraud are on the rise. So having multiple organisations whose entire business model relies on successfully verifying a customer's identity, including liveness checks and face capture, along with the competitive market that naturally arises as a result, would encourage faster adoption of new innovations.

Who will benefit from the requested changes?

Beneficiary	Sector	How
Intermediaries	AML	Cost reduction, innovation enablement
Intermediaries	Digital Identity Verifiable Credentials	Cost reduction, innovation enablement, increased usage
Reporting Entities	AML	Cost reduction
Consumers	AML	Cost reduction (less passed on by Reporting Entities in providing their service)
Consumers	Digital Identity	Increased usage as reduced costs would enable more acceptance of Digital Identity in day to day transactions
Department of Internal Affairs	AML & Digital Identity	Reduced reliance on maintaining a biometric tool for the public sector, and therefore reduced costs.

Summary Recommendation

The Minister, the Commerce Commission, the FMA and the DIA are asked to support and adopt the pragmatic Short-Term Solution because it:

1. Allows Intermediaries to capture Biometric images and send them to the DIA for matching.
2. Significantly reduce the current costs for carrying out these checks to a level significantly closer to the Australian equivalent.

We do not believe that these changes would require a change in Legislation, but point 1 would require technical changes at the DIA to allow for these API calls.

In addition, we recommend DIA provide access to biometrics (with appropriate security safeguards of course) as part of its next update to the Identity Information Confirmation Act 2012.

Appendix 1

The AML/CFT Act, Digital ID and the role of the Government - levelling the field for access to biometric data

28 November 2024

Principal Author: Vincent McCartney

Reviewers: Tina Groark, Colin Wallis, Jason Roberts

Introduction

On October 2nd, a Roundtable meeting was called to assemble private sector representatives to meet with Minister Bayly, the Commerce Commission and the Financial Markets Authority to discuss the perceived barriers to innovation in the FinTech ecosystem. The meeting focused on fostering New Zealand's FinTech ecosystem through initiatives like the FinTech sandbox and addressing regulatory challenges. The meeting concluded with plans to establish a working group to explore a Fintech sandbox and among other action items explore digital identity standards and related matters to enhance market competitiveness. There was universal Roundtable support for the notion that robust digital identity is foundational to customers engaging in a thriving FinTech ecosystem and Aotearoa's digital economy more broadly.

An informal working group was indeed established from the Roundtable attendees, with a smaller group of applicable industry representatives (see above) meeting with Commerce Commission representatives on October 15th to outline the nature of concerns in the area of digital identity verification and in particular the monopoly that DIA services currently have regarding access to biometric data it holds, which in turn is reflected in the current AML/CFT regulatory regime thereby impacting innovation. It has been seen by - but not reviewed by - the wider working group and (whether in this or some other summarised form) will be added to the pre-reading papers back to the Minister in advance of the next Roundtable meeting on December 6th.

This is the written version of that verbal discussion with the Commerce Commission on October 15th around the problem definition with follow-on impacts and what could be done to remove the barrier thereby creating a more equitable field for competitors to innovate and customers to benefit. It is conceivable though by no means certain, that regulatory and technical challenges raised here could form part of the suite of work for proposed FinTech sandbox.

Background

1. The Department of Internal Affairs (DIA) holds the register for and is the custodian of official Passport information (also Births, Deaths, Marriages with access to some other authoritative sources of personal information across Government e.g. Drivers Licences).
2. The non-biometric data (Name, Date of Birth etc) has been available for access by approved private companies ('Intermediaries') since at least 2013, following the passing of the Electronic Identity Verification Act 2012 (and the subsequent Electronic Interactions Reform Act 2017) and the Identity Information Confirmation Act 2012. Access to non-biometric data provides a gateway for Reporting Entities to verify their customer's supplied data.
3. Biometric data (photographs) has never been made available to Intermediaries, though is referenced in legislation noted above.
4. The DIA is one of the three current NZ AML/CFT regulators. The other two are the Financial Markets Authority and the Reserve Bank of New Zealand.
5. The three regulators currently provide guidance papers on aspects of the AML/CFT Act jointly.
6. It was announced in October 2024 that the DIA will become the sole regulator for AML/CFT in New Zealand.
7. In 2013, the DIA launched RealMe to allow individuals to access government services safely and securely.
8. In 2023, the DIA launched "Identity Check" building on its RealMe work. The Identity Check service is a Digital ID that binds the customer to their identity document by accessing the biometric data from its databases. This service has access to NZ Passports and NZ Driver Licences biometric data.
9. Intermediaries have been requesting, for 6+ years, for the same level of access to the biometric data that the DIA has granted its own services. All requests have been turned down on grounds of current legislation not permitting it, while no timeline is given as to if or when the legislation might be amended.
10. The AML/CFT regulators published the "Explanatory Note: Electronic Identity Verification Guideline For Part 3 – Amended Identity Verification Code of Practice 2013" in July 2021 ('Explanatory Note"), further clarifying what was required when verifying the identity of your customer.
11. In 2023, the Digital Identity Services Trust Framework Act 2023 ('DISTF') was passed. A Digital Identity Services Provider complying with and becoming accredited under the Act is optional, rather than mandatory.
12. In 2024, the Trust Framework Authority (the regulator) and the Trust Framework Board governance) were established under the auspices of the DIA.

Problem Overview

The DIA's RealMe and Identity Check services are currently, and for the foreseeable future seemingly continue to be, the only services that have access to the biometric data held by the DIA. These services include performing the customer's face capture and the subsequent biometric matching to the Passport record.

Whilst this limited approach continues, New Zealand consumers and companies will have no choice but to access this biometric data via the RealMe or Identity Check services which means that these services are monopolistic in nature – unintended or otherwise. This approach both increases costs that are ultimately passed through to the customer and stifles innovation.

Two problematic aspects are detailed below:

Problem 1: AML/CFT Identity Verification

The Explanatory Note allows for two ways/standards for a Reporting Entity to reach the required standards for verifying their customers electronically. These are either via a Single Independent Source or via Two Independent Sources.

To be able to meet the Single Independent Source standard, the customer needs to be verified biometrically and to a high level of confidence. Footnote 1 of the Explanatory Note states that “only a verified RealMe identity can meet this requirement in New Zealand”.

To be able to meet the Two Independent Sources standard, the customer needs to be verified against two independent sources and bound to their identity via another mechanism. The sources used are typically the data component of the NZ Passport or NZ Driver Licence databases, and a data component of another database such as a credit bureau record. The binding mechanism is typically via a biometric match of images captured by the Intermediary. These images are the face of the customer performing the verification and a copy of their identity document that the customer supplied at the point of verification.

Whilst the Two Independent Sources approach offers flexibility, the downsides are:

- It can potentially increase the cost of performing a verification as more than two sources are required to successfully get a positive outcome;
- Poor customer experience since the failure rate increases due the customer needing to be found & verified in multiple databases; and

- There is an increased fraud risk as the biometric matching is performed against information (image of an ID document) supplied by the customer. Whilst anti-tampering checks can be performed on the identity document, they are not foolproof.

Despite the advantages that the DIA’s services has in terms of being singled out by the AML regulators, and the theoretical simplicity of only being verified from one source being better for the customer, it has not necessarily always been the dominant identity verification provider in the market since its launch.

Additionally, there have been a number of local and international Regulatory Technology (‘RegTech’) companies (who are also Intermediaries) who together have mounted competition in the identity verification market via innovation, competition, usability and cost reduction. These companies have driven the overall costs down for an identity verification and have allowed New Zealand FinTech companies to scale (via secure, quick customer

onboarding), innovate, and bring more competition to New Zealand financial services markets. But how long might the status quo remain?

A Future Danger

With the DIA becoming the sole regulator for the AML/CFT Act, it is conceivable that it could update its guidance notes once again to more strongly promote the RealMe or Identity Check services. If this occurs, then the Reporting Entities will have little choice but to either switch from their current RegTech provider to the DIA's services or to ask their RegTech provider to integrate the DIA's services.

This outcome would further entrench the monopolistic position of the DIA's services (whether unintended or otherwise), increase costs, and could force RegTech companies out of the New Zealand market, therefore reducing competition and customer value further.

Problem 2: The future of Digital Identity in New Zealand

As noted above accreditation under the DISTF regulation is optional. A Digital Identity Service Provider/issuer does not technically need to issue their Digital Identity in line with the Trust Framework Rules. The Trust Framework Rules lean into best practice around verifying the biometric information against the source databases.

But in reality, for a Digital Identity to be trusted and to be widely used, then consumers and businesses will need to have a high level of confidence in the authenticity of verification that was performed. Therefore, Digital Identity issuers will need to opt-in to get accredited under the DISTF.

As the only access to the underlying biometric information is currently via the RealMe and Identity Check services, Digital Identity Service Providers/issuers will have no choice but to incorporate these services into their process and therefore adding an unnecessary layer of cost to their products and limiting their scope for innovation.

The Ask

The DIA is currently competing against the private sector with RealMe and Identity Check, which in itself is perfectly fine. However, it is doing this in a manner that is monopolistic – be it unintended or otherwise - due to its sole restricted access to the underlying biometric data held in the register and requiring that this data is accessed via their commercial services on account of existing legislation.

The ask is that the Commerce Commission require the DIA to make the necessary regulatory changes to allow private sector companies to directly access the biometric data that it holds, so that private sector issuers can perform the biometric matching themselves and achieve a high level of confidence that the customer is who they claim to be.

The Benefits

If Digital Identity Service Providers from the private sector were able to directly access the biometric data held by the Department, then increased innovation and competition would

result, leading to a better outcome for customers in terms of better user experiences and reduced costs since the costs charged to the Reporting Entities would be lowered.

Appendix 2

Intermediaries have direct access to the biometric information so that they can perform their own matching.

This isn't a proposal to allow carte-blanche opening of the biometric information to the public, instead it is to make amendments to Section 9, part 4, of the IICA to allow for information about the subject of the check to be returned.

Suggested operational structure following the change in legislation.

Question	**Answer**
Who can access the biometric images?	Only authorised intermediaries who have been approved for access. There are currently 9 Intermediaries authorised for non-biometric access.
How would the images be accessed?	Via an API
What controls would be in place to restrict access to the entire biometric database(s)?	The biometric information would only be supplied if a corresponding non-biometric match request resulted in a 100% match ('Consistent'). The Consistent result could be accompanied by a one-time use 'key' that could be used to retrieve the image.
How would the retrieved biometric image be matched?	The intermediary would use their own biometric facial recognition software to perform the match. The matching would be against the real-time image capture of the subject's face. Note: DINZ is working on creating a 'Kiwi faces dataset' of anonymous individuals that explicitly consent to undergo 2D and 3D verification, so that any vendor can test its software performance and improve its algorithms as a result.
What would happen to retrieved biometric image following the matching process?	The Intermediary would be required to automatically delete the retrieved biometric image as soon as practicable (within 24-hours).
Would the retrieved biometric image be able to be shared with any 3rd party?	No. The image would not be able to be shared, this would be consistent with the current IICA.
Are there any other Privacy or Security implications?	All Intermediaries that access the biometric images must have completed a Data Privacy Impact Assessment, and must have

	a current ISO27001 (or equivalent) certification.
Would the biometric information be available to non-NZ companies?	Only approved Australian and New Zealand Intermediaries would have access to the biometric information.

DocuSigned by:
Colin Wallis
F84DA1755B8C410...

2/2/2025