Digital Identity Services Trust Framework Bill

Government Bill

As reported from the Economic Development, Science and Innovation Committee

Commentary

Recommendation

The Economic Development, Science and Innovation Committee has examined the Digital Identity Services Trust Framework Bill and recommends that it be passed. We recommend all amendments unanimously.

Introduction

About the bill

Digital identity services are tools, products, and services that allow the collection, sharing, or other use of information when authorised by individuals and organisations that own the information.

This bill would establish the legal basis for a statutory trust framework for digital identity services. The Digital Identity Services Trust Framework seeks to support the provision of secure and trusted digital identity services for individuals and organisations, to give people more control over their information, to support people to prove who they are online, and to make it easier to access online services.

The bill would create an opt-in accreditation scheme for digital identity service providers (TF providers). It is envisioned that the service providers would include government departments, existing identity service providers, and other private sector organisations that verify identities. TF providers would be required to adhere to trust framework rules (TF rules), and would be able to use a mark to identify their accredited services. Users and parties that rely on digital identity services (for example, liquor stores asking for age verification) would not have to be accredited to use the accredited service. The bill would not override any obligations under the Privacy Act 2020.

The trust framework would be governed by the Trust Framework Board (the TF board). The TF board would be responsible for providing guidance about the TF framework, and monitoring the performance and effectiveness of the framework. It would also advise the Minister on the making and updating of the TF rules, including through consultation with interested parties. A Māori Advisory Group would advise the TF board on Māori interests and knowledge as they relate to the trust framework.

A Trust Framework Authority (the TF authority) would also be established to make decisions about accreditations, investigating complaints from the public or issues it identifies, enforcing the TF rules, and granting remedies for breaches.

The bill would come into effect on dates determined by Order in Council, or on 1 January 2024 if not yet in force.

About the public submission process

We received over 4,500 written submissions on this bill. An overwhelming majority of submissions (4,049) were received in the last two days of our six-week public submission period, or after the six-week period ended. This included almost 3,600 between 8:00pm and 11:59pm on the last night alone.[1] We attribute this influx to misinformation campaigns on social media that caused many submitters to believe that the bill related to COVID-19 vaccination passes. We note that submissions on this bill closed at the same time that the COVID-19 Protection Framework (known as the traffic light system) came into effect (11:59pm on 2 December 2021). This was coincidental. The commencement of the COVID-19 Protection Framework required members of the public to present vaccination passes (in digital or paper form) to enter many businesses.[2] The Digital Identity Services Trust Framework Bill has no bearing on vaccination passes. Mandatory vaccination passes have since been phased out.

Many submissions also compared this bill to social credit systems, centralised state control of identity (for example, the removal of physical driver licences), and moving to a cashless society using digital currencies. None of these ideas are related to the content of this bill.

This bill seeks to put a framework in place so that, when New Zealanders choose to disclose their private information to online companies, those companies protect that data appropriately.

The exact text of the bill is publicly available, as is a clause-by-clause analysis detailing exactly how the bill seeks to protect the private data of New Zealanders when they choose to disclose their information.[3] Before introducing the bill, the Department of Internal Affairs conducted targeted consultation with interested stakeholders. We

---

1 Submissions opened on 21 October 2021 and closed at 11:59pm on 2 December 2021.

2 The framework became law through the COVID-19 Public Health Response (Protection Framework) Order 2021.

3 Legislation can be found via the Parliament website and the Legislation website.

encourage people to read about this bill's actual purpose, which we summarised above. We are pleased that advisers from the Department of Internal Affairs have stated that they are reviewing the public communication about this work, to ensure that the purpose and provisions of the bill are made clearer to the public.

Legislative scrutiny

As part of our consideration of the bill, we have examined its consistency with principles of legislative quality. Although advice we received did not directly address the matters we raised in this area, we have no issues regarding the legislation's design to bring to the attention of the House.

Proposed amendments

The rest of this commentary covers the main amendments we recommend to the bill as introduced. We do not discuss minor or technical amendments.

Digital identity services trust framework

Part 2 of the bill sets out the key concepts for the new regime. Clause 8 sets out what the main components of the trust framework would be:

- two administering bodies (the TF board and the TF authority)
- an accreditation regime for digital identity service providers and the digital identity services they provide
- rules and regulations that set requirements for accredited providers and accredited services
- approved marks to identify accreditations.

Tiriti o Waitangi/Treaty of Waitangi

The bill as introduced includes requirements to consult and engage with Māori in decision-making. We recommend inserting clause 8A to consolidate and clarify these requirements, and to explain the ways in which the bill would recognise the Crown's responsibility to give effect to the principles of te Tiriti o Waitangi/the Treaty of Waitangi.

Changing "trust marks" to "accreditation marks", and making them apply only to services

As introduced, clause 12 of the bill provides that TF providers could use trust marks approved by the TF board to identify themselves and which of their services are accredited under the trust framework. Some submitters suggested that where a TF provider provides both accredited and non-accredited services, the bill should require them to make clear which services are accredited and which are not. We agree that it is important that people are clear about which services are accredited. Therefore, we propose that "trust marks" be renamed "accreditation marks" and only be issued for accredited services, and not for TF providers generally. We recommend amending clause 12(1) accordingly.

Trust framework rules

Content of TF rules and who can make them

Clause 17 allows for rules to be made to regulate the operation and administration of the trust framework. The Regulations Review Committee wrote to us about this provision.

As introduced, clause 17 provides that rules could be made either by Order in Council or by the Minister, and both would be known as TF rules. The bill does not specify which matters must be made by Order in Council on the recommendation of the Minister, and which matters can be addressed by rules set by the Minister. We consider that the bill should specify this distinction. The distinction would be based on the proposed content of the rules, which are set out in clause 19 as introduced. We discuss the distinctions below, and note that both rules made by Order in Council and those set by the Minister would have status as secondary legislation.

Matters that should have regulations set by Order in Council

As introduced, clause 19(1)(a) provides that rules could prescribe the types of digital identity services that could be accredited under the bill. We consider that these should more appropriately be prescribed by regulations, which means that they should be made by Order in Council. We note that clause 9 of the bill sets out the meaning of digital identity services. It refers to a service or product that, either alone or together with 1 or more other digital identity services, enables a user to share personal or organisational information in digital form. The clause describes what types of things the service or products might do. We recommend amending clause 19 and inserting clause 9(3) accordingly to provide for the regulation-making power.

Similarly, we consider the matters set out in clause 19(1)(c) should be prescribed by regulations. They relate to self-assessments and reporting requirements for TF providers, compliance and dispute resolution processes, and other matters considered appropriate by the TF board and Minister. We recommend inserting new clause 26A accordingly. We also recommend including the regulation-making power for setting cost-recovery fees in this new clause.

Matters that could be addressed under rules set by the Minister

We understand that the content of the rules set out in clause 19(1)(b) are likely to be technical details. We consider that these matters could appropriately be decided by the Minister under a rule-making power. The matters include setting standards relating to identification management, privacy and confidentiality, information and data management, and the sharing and facilitation of information sharing.

Further clarifications to rule-making power

Clause 18 as introduced sets out that the TF rules could apply to TF providers only to the extent relevant to the provision of accredited services. We recommend making it clear that the rules must not apply to digital identity services that are not accredited services.

We also recommend amending clause 19 to make it clear that:

- if there is inconsistency between a rule made by the Minister and a regulation made by Order in Council, the regulation takes precedence
- the TF rules do not override the Privacy Act 2020.

Consultation before recommending trust framework rules to Minister

Clause 20 sets out the consultation requirements that the TF board must follow before recommending draft TF rules to the Minister. The clause lists who the TF board must invite submissions from. As introduced, subclause (1)(b) would require the TF board to consult "people or groups outside the board with expert knowledge of te ao Māori approaches to identity". We consider that the "people or groups outside the board" should instead be referred to as "tikanga experts who have knowledge of te ao Māori approaches to identity". We consider that this better reflects the level of expertise expected during consultation. We recommend that clause 20(1)(b) be amended accordingly.

Reporting requirements for TF providers

Clause 41 would require TF providers to collect and keep required information about their activities, and give that information to the TF authority on request. The requirement is intended to assist the TF authority to carry out its functions. In practice, we think it would be helpful for there to be periodic reporting so that the TF authority has better oversight of the activities of TF providers. We recommend amending clause 41 to require TF providers to provide information periodically if required to do so, as well as at all reasonable times on request.

Trust Framework Board

Part 4 of the bill would establish the Trust Framework Board (TF board). Clause 42(1) provides that the Trust Framework Board is established to carry out the board's functions as set out in this legislation.

Commitment to principles of the Treaty of Waitangi/te Tiriti o Waitangi

As introduced, Clause 42(2) notes certain clauses applicable to Part 4 that provide a "practical commitment to the principles of the Treaty of Waitangi (te Tiriti o Waitangi) for the governance and operation of the trust framework". The clauses referred to are clauses 20(1)(b), 46(2)(a) and (b), and 50 to 54.

Earlier in our report, we proposed that the bill include a standalone clause (new clause 8A) to list all the ways in which the bill must give effect to the principles of the Treaty of Waitangi/te Tiriti o Waitangi. In light of new clause 8A, clause 42(2) is duplication, and we recommend that it be deleted.

Functions of the Trust Framework Board

Clause 44 sets out the functions of the TF board. They include:

- recommending draft TF rules to the Minister, reviewing the rules, and recommending updates
- recommending regulations to the Minister
- educating and providing guidance to TF providers and the public
- monitoring the effectiveness of the trust framework
- carrying out other functions conferred on it by the bill or the Minister (to achieve the purpose of the bill)
- carrying out incidental functions.

We recommend including an express obligation on the board to engage with Māori in the manner provided for in new clause 52(4A) when performing its functions, in order to provide for Māori interests in the operation of the trust framework. We recommend inserting new clause 44(3) accordingly. We discuss new clause 52(4A) later in our commentary.

Appointment of Trust Framework Board members

Clause 46 sets out the process and requirements for appointing members to the TF board. Subclause (2) lists several areas of expertise that the chief executive must ensure are provided for when selecting the membership of the board. One of the factors listed is experience in engagement with Māori. However, as drafted, it could be interpreted that the experience in engaging with Māori must be in relation to technology and data management. We do not consider this to be the intent of the provision. We recommend redrafting clause 46(2) so that the board's membership must include people with experience in engaging with Māori in a more general sense.

Role of Māori Advisory Group

Clause 52 sets out the role of the Māori Advisory Group. Under clause 52(4), the board and the advisory group would be required to prepare an engagement policy setting out how they will work together. We think that the engagement policy should set out how and when the board and advisory group will consult with iwi and hapū to inform their decision-making and advice. We propose inserting new clause 52(4A) to make it clear that the engagement policy must include this information.

Trust Framework Authority

Part 5 of the bill would establish the Trust Framework Authority (TF authority).

Functions of the TF authority

Clause 59 sets out the functions of the TF authority. The list of functions does not include reference to the intended role of the TF authority to undertake compliance monitoring of TF providers. We suggest this function be included in the list, and recommend inserting subclause (da) accordingly.

Power to require information or documents

Clause 61 sets outs the TF authority's power to require information or documents for the purposes listed in subclause (3). The purposes include assessing or investigating a complaint or investigating compliance. Later in our report, we propose giving the TF authority an express power to lift additional record-keeping and reporting requirements imposed under clause 82. So that it can assess whether those additional requirements should be lifted, we suggest that the TF authority should have a power to require information or documents for that purpose. We recommend inserting paragraph (ba) into clause 61(3) accordingly.

Clause 61(5) sets out the reasons why someone who receives a notice requiring information or documents may refuse to comply with it. The reasons include that the information or document would be privileged in court, or that disclosure would result in a breach of an obligation under another enactment (other than the Privacy Act 2020 or the Official Information Act 1982). We consider that the clause may create uncertainty about how the information-gathering power interacts with other statutory regimes covering the same information. We note that the clause is not intended to override other Acts that deal specifically with access to the information or documents. We recommend that clause 61(5) be amended to provide that a person can refuse to provide information or documents if another Act deals specifically with access to the information or documents.

Complaints, offences, and remedies

Part 6 of the bill sets out provisions that establish processes for dealing with complaints.

Principles for handling complaints under Part 6

Clause 67 sets out the principles that must guide the TF authority when dealing with complaints. One of the principles is having processes for complaints that are fair and accessible, and that have particular regard to tikanga Māori, if the complainant desires. We do not think the complainant should have to request that tikanga Māori be a part of complaints processes. We consider that tikanga should be incorporated into processes as a matter of course for all functions carried out by the TF authority. We recommend amending clause 67(b) accordingly.

How complaints are made

Clause 69 sets out the form and information requirements for a complaint to be made.

The bill as introduced would require a complaint to be made in writing. We acknowledge that this may be unnecessarily restrictive. We propose removing the requirement for a complaint to be in writing, and note that the TF authority would be required under the clause to provide reasonable assistance to a complainant to meet the form and information requirements for a complaint to be made. We recommend amending clause 69(1) accordingly.

Clause 69(1)(c) requires that the complaint identify the relevant rule, regulation, term of use, or provision that is alleged to have been breached. We consider that this requirement is unnecessarily complex, restricting people's access to the complaints process. It should be sufficient for a complaint to describe the alleged breach and state why the complainant believes that a breach has occurred. Accordingly, we recommend that paragraph (c) be deleted.

TF authority may decide not to consider complaint further

Clause 72 sets out the reasons why a TF authority might choose not to consider a complaint. We recommend amending the clause to make it clear that the TF authority could also choose to not consider part of a complaint, for the same reasons.

One of the reasons listed, in subclause (1)(e), is if the complainant knew of the breach or potential breach 6 months or more before they made the complaint. We acknowledge that this timeframe may be overly restrictive, especially given it is a new regulatory regime. We consider that the timing should be extended to 12 months, and recommend amending clause 72 accordingly.

We also think that clause 72(1) should contain an additional reason why the TF authority may decide not to consider a complaint. The option to not consider a complaint, or part of a complaint, should be open to the TF authority if the complaint involves any of the matters set out in clause 75(2). They include:

- matters that may be dealt with under the Privacy Act
- employment disputes that may be dealt with under the Employment Relations Act 2000
- disputes relating to actions that may be prosecuted as offences under the Act
- disputes relating to the carrying out of a Minister's function
- a dispute of a kind prescribed by regulations.

We consider that these matters are best dealt with under the relevant regimes, whether statutory or otherwise prescribed. We recommend inserting clause 72(1)(aa) accordingly.

Referral of complaints to officeholders

Clause 70 sets out how complaints must be dealt with. Clause 71 would allow the TF authority to refer complaints, either in full or in part, to other officeholders if it considers it more appropriate that they deal with them. The other officeholders include the Ombudsman, the Privacy Commissioner, the Inspector-General of Intelligence and Security, or another office holder. If the TF authority refers part of a complaint, we think the bill should specify that the TF authority must continue to make a preliminary assessment of the part of the complaint it has retained, unless it has decided that it does not need to consider it further. We recommend inserting new clause 70(2) accordingly.

Dispute resolution

Clause 75 would enable the TF authority to recommend a dispute resolution service to the Minister. Clause 76 sets out that the Minister could approve a dispute resolution scheme if they were satisfied it provides a means of resolving complaints consistent with the principles set out in the bill, and that it meets regulatory requirements.

We acknowledge that expertise in dispute resolution may need to be sought from external parties. We think it beneficial that the bill make it clear that the chief executive could employ or engage third parties to provide dispute resolution services. We recommend adding clause 75(3), and making a consequential amendment to clause 105, accordingly.

Remedies following a finding of breach

Clause 82 sets out what actions the TF authority could take if it found a breach by a TF provider. The actions include issuing a warning or compliance order, suspending or cancelling an accreditation, or requiring additional record-keeping or reporting requirements.

Under clause 82(1)(b), additional record-keeping or reporting requirements could be set for either a specified period or indefinitely. Submitters suggested that, if additional requirements are imposed on a TF provider, the timeframe that they will apply for should be specified, along with the conditions that, if met, would mean the requirements no longer applied. We think that there could be circumstances where it was appropriate for additional reporting requirements to be imposed for a significant period, for example if there were serious or recidivist breaches. However, we think the bill should expressly allow the TF authority to lift additional requirements earlier than specified if it considered that the requirements were no longer needed. Therefore, we recommend inserting new clause 83A to provide that the TF authority could impose additional record-keeping or reporting requirements for any period that it considered appropriate, but that it could lift those additional requirements earlier, if it considered they were no longer needed.

Suspension or cancellation of accreditations

As introduced, the bill does not provide any consequences for a TF provider if they ignored a compliance order issued by the TF authority issued under clause 82(1)(c). We think that, in such a scenario, the TF authority should have the power to suspend or cancel the accreditation of the provider or the relevant service. Similarly, if a TF provider did not notify the TF authority about its compliance with an order, the TF authority should have the same power. We recommend inserting clause 82(2) accordingly.

Clause 93 sets out other reasons why the TF authority could suspend or cancel accreditations of a provider or service, regardless of whether a breach of the trust framework had occurred. The reasons include matters such as bankruptcy, insolvency, convictions for offences under the Act, or behaviours that the TF authority considered a risk to the integrity or reputation of the framework.

In practice, TF providers are likely to be incorporated entities. We think it is important that the TF authority have an ability to form a view about the suitability of those people involved in an entity, and not just the actions of the entity as a whole. Therefore, we recommend inserting clause 93(6) to make it clear that the reference to TF provider includes those involved in the management of, or employed or contracted by, the TF provider. This would mean that the actions of people involved with a TF provider would be relevant to a TF provider's accreditation status.

Secrecy and immunities under the bill

As introduced, Part 7 of the bill includes provisions relating to obligations to maintain secrecy, and providing immunity to certain persons carrying out functions under the bill.

Removal of secrecy clause

Clause 101 provides that certain persons carrying out functions under the bill would be required to maintain secrecy in respect of all matters that came to their knowledge, unless exceptions were met. Submitters were clear that greater transparency would improve trust in the framework. We consider it unlikely that members of the TF board, the TF authority, or the advisory groups would have access to much sensitive information that would warrant a specific clause. We consider that the persons the clause applies to would be able to manage any sensitive information they handle in accordance with other statutory provisions that already exist, such as those contained in the Official Information Act 1982, the Privacy Act 1993, and the Public Records Act 2005. Therefore, we consider the secrecy provision in clause 101 unnecessary, and recommend it be deleted.

Clarifying the immunity provision for people who are not public service employees

As introduced, clause 102 provides immunity in civil proceedings to members of the TF board, members of the TF authority, members of the Māori Advisory Group, members of any advisory committee, and staff of the board or the authority. The immunity only applies for good-faith actions or omissions when the person was carrying out or intending to carry out their function.

Clause 102 provides that the immunity applies whether those people are public service employees or not. However, public service employees already have immunity from civil proceedings under section 104 of the Public Service Act 2020. Therefore, parts of clause 102 are redundant as they duplicate the immunity already granted to public service employees. For simplicity, we suggest that the immunity granted to public service employees under the Public Service Act should also apply to those persons referred to earlier, but who are not public service employees. We recommend amending clause 102 accordingly.

Immunity for TF providers for actions of users

Clause 103 gives a TF provider immunity from civil liability in relation to harm or damage caused or suffered by a user of their accredited services. The intention is to protect a TF provider from liability as a result of the actions of others where it has acted in good faith. However, a TF provider would not be protected in relation to the alleged harm or damage if they had acted in a manner that constituted bad faith or gross negligence.

Submitters raised concerns that the immunity provisions in clause 103 lack avenues for compensation if a TF provider acted in a way that caused harm. We note that the immunity provided by clause 103(1) would be subject to the proviso in subclause (2) regarding bad faith or gross negligence. However, we acknowledge the point made in submissions that users may be more cautious in using TF providers if normal avenues of redress are unavailable. We consider that the immunity provision in clause 103 should not apply to any proceedings arising under the Privacy Act. We consider that this would give users greater confidence that their privacy rights are protected. We recommend amending clause 103(2) accordingly.

Review of the TF board's operation

Clause 104 requires that, after two years, a review of the TF board's operation be carried out by the responsible department. The clause sets out that the review must include an assessment of the effectiveness of the board in carrying out its functions, and the viability of other models for carrying out the board's functions. We acknowledge stakeholders' views about the effectiveness of governance provisions, privacy standards, and provision for te ao Māori. Therefore, we suggest that the two-year review include an assessment of how other models might better:

- ensure the privacy and security of user information (including Crown-held data) and protect it from unauthorised use
- provide opportunities for Māori engagement in the trust framework.

We recommend amending clause 104 accordingly.

Appendix

Committee process

The Digital Identity Services Trust Framework Bill was referred to the committee on 19 October 2021. We invited the Minister for the Digital Economy and Communications, Hon Dr David Clark, to provide the first oral submission on the bill. He did so on 16 December 2021.

The closing date for submissions on the bill was 2 December 2021. We received and considered about 4,500 submissions from interested groups and individuals. We heard oral evidence from 28 submitters at hearings via videoconference.

We received advice on the bill from the Department of Internal Affairs. The Office of the Clerk provided advice on the bill's legislative quality. The Parliamentary Counsel Office assisted with legal drafting. The Regulations Review Committee reported to us on the powers contained in clauses 17 and 100.

Committee membership

Jamie Strange (Chairperson)

Glen Bennett

Naisi Chen

Hon Judith Collins

Melissa Lee

Key to symbols used in reprinted bill

As reported from a select committee

text inserted unanimously

~~text deleted unanimously~~

Hon Dr David Clark

Digital Identity Services Trust Framework Bill

Government Bill

Contents

The Parliament of New Zealand enacts as follows:

1 Title

This Act is the Digital Identity Services Trust Framework Act **2021**.

2 Commencement

(1) This Act comes into force—

(a) on 1 or more dates set by Order in Council; or

(b) to the extent not brought into force earlier, on **1 January 2024**.

(2) One or more Orders in Council may set different dates for different provisions.

(3) An Order in Council made under this section is secondary legislation (*see* Part 3 of the Legislation Act 2019 for publication requirements).

Part 1
Preliminary provisions

3 Purpose

The purposes of this Act are—

(a) to establish a legal framework for the provision of secure and trusted digital identity services for individuals and organisations:

(b) to establish governance and accreditation functions that are transparent and incorporate te ao Māori approaches to identity.

4 Overview of Act

*Key definitions in **Part 2***

(1) The definition of the digital identity services trust framework is in **section 8** along with a description of the main components of the trust framework. The definition of digital identity service is in **section 9**. The 3 types of trust framework participants are listed in **section 10**.

(1A) The ways in which the Act recognises and respects the Crown's responsibility to give effect to the principles of te Tiriti o Waitangi/the Treaty of Waitangi are listed in **section 8A**.

Other Parts in Act

(2) **Part 3** relates to the TF rules, the accreditation of providers of digital identity services and the services they provide, and record-keeping and reporting by them once they are accredited. **Part 3** also contains provisions relating to the TF register of accredited providers and services.

(3) **Part 4** relates to the TF board, the Māori Advisory Group, and committees of advisers to advise the board.

(4) **Part 5** relates to the TF authority.

(5) **Part 6** relates to complaints and offences. **Part 6** also sets out remedies that may be granted by the TF authority following a finding of breach by a TF provider of the TF rules, regulations, terms of use of ~~trust~~ accreditation marks, or provisions of this Act.

(6) **Part 7** contains a miscellaneous group of provisions relating to regulations, ~~secrecy,~~ immunity from liability, and reviews.

Effect of overview section

(7) This overview is for explanation only and does not affect the meaning of this Act.

5 Interpretation

In this Act, unless the context otherwise requires,—

accreditation mark means an accreditation mark described in **section 12**

accredited digital identity service or **accredited service** means a digital identity service that is accredited by the TF authority to be provided by a particular TF provider (*see also* the definition in **section 32(2)**)

breach has the meaning given in **section 68(2)**

chief executive means the chief executive of the relevant responsible department

department means a public service agency within the meaning given in section 10(a) of the Public Service Act 2020

digital identity service has the meaning given in **section 9**

digital identity service provider means an individual or organisation that provides a digital identity service, whether the provider or service is accredited under this Act or not

digital identity services trust framework or **trust framework** has the meaning given in **section 8**

individual means a natural person

Minister means the Minister of the Crown who, under the authority of any warrant or with the authority of the Prime Minister, is responsible for the administration of this Act

organisation means any organisation, whether public or private, and whether incorporated or not

organisational information means information relating to a particular organisation

participants has the meaning given in **section 10**

personal information has the meaning given in section 7(1) of the Privacy Act 2020

personal or organisational information means—

(a) information that describes the identity of an individual or organisation:

(b) other information about that individual or organisation

public service employee means an employee within the meaning given in section 65 of the Public Service Act 2020

regulations means regulations made under **section 100**

relying party means an individual or an organisation that relies on personal or organisational information shared, in a transaction with a user, through 1 or more accredited digital identity services

responsible department means the department nominated under **section 43 or 58** that is, respectively,—

(a) the department that the TF board sits within:

(b) the department that the TF authority sits within

TF authority or **authority** means the authority established under **section 57**

TF board or **board** means the board established under **section 42**

TF provider means a digital identity service provider that is accredited by the TF authority to provide 1 or more accredited digital identity services (*see also* the definitions in **sections 32(2), 93(6), and 103(3)**)

TF register or **register** means the register of TF providers and accredited services established under **section 32**

TF rules ~~has the meaning given in~~ are the rules made under **section 17**

transaction means a transaction whether online or otherwise

~~**trust mark** means 1 or more of the trust marks referred to in **section 12**~~

user means an individual who—

(a) shares personal or organisational information, in a transaction with a relying party, through 1 or more accredited digital identity services; and

(b) does so for themselves or on behalf of another individual or an organisation.

6 Transitional, savings, and related provisions

The transitional, savings, and related provisions (if any) set out in the **Schedule** have effect according to their terms.

7 Act binds the Crown

This Act binds the Crown.

Part 2
Digital identity services trust framework

8 Trust framework

(1) The **digital identity services trust framework** or **trust framework** means the legal framework established by this Act to regulate the provision of digital identity services for transactions between individuals and organisations.

(2) The main components of the trust framework are—

(a) 2 administering bodies:

(b) an accreditation regime for digital identity service providers and the digital identity services they provide:

(c) rules and regulations that include ~~minimum~~ requirements for accredited providers when providing accredited services:

(d) approved ~~trust~~ accreditation marks to identify ~~accredited providers and~~ accredited services.

(3) The 2 administering bodies for the trust framework are the TF board (*see* **Part 4**) and the TF authority (*see* **Part 5**).

(4) The accreditation regime is run by the authority (*see* **sections 22 to 31**).

(5) The board recommends draft TF rules and regulations to the Minister (*see* **sections 17 and 100**), and the authority is responsible for enforcing the rules (*see* **Part 6**).

8A Tiriti o Waitangi/Treaty of Waitangi

In order to recognise and respect the Crown's responsibility to give effect to the principles of te Tiriti o Waitangi/the Treaty of Waitangi, this Act,—

(a) in **section 20(1)(b)**, requires the TF board to consult and invite submissions from tikanga experts who have knowledge of te ao Māori approaches to identity before it can recommend draft TF rules to the Minister:

(b) in **section 44(3)**, requires the TF board, when performing its functions, to engage with Māori in the manner provided for under **section 52(4A)** to recognise and provide for Māori interests in the operation of the trust framework:

(c) in **section 46(2)(a) and (b)**, requires the chief executive to ensure that members of the TF board include people who have—

(i) expert knowledge of te ao Māori approaches to identity; and

(ii) expert knowledge of the principles of te Tiriti o Waitangi/the Treaty of Waitangi; and

(iii) experience in engaging with Māori:

(d) in **sections 50 to 54**, establishes a Māori Advisory Group to advise the TF board on Māori interests and knowledge, as they relate to the operation of the trust framework:

(e) in **section 52(4A)**, requires the engagement policy between the TF board and the Māori Advisory Group to include details of how and when consultation with iwi and hapū will be undertaken by both the Māori Advisory Group and the board:

(f) in **section 67(a)**, requires the TF authority, when carrying out its functions under **Part 6** (relating to complaints and offences), to be guided by

the principle that processes for complaints should be fair and accessible and have particular regard to tikanga Māori:

(g) in **section 104(3)(c)**, requires a review of the TF board's operation to include an assessment of how other models might better provide opportunities for Māori engagement in the trust framework.

9 Meaning of digital identity service

(1) In this Act, **digital identity service** means a service or product that, either alone or together with 1 or more other digital identity services, enables a user to share personal or organisational information in digital form ~~in a transaction with a relying party~~.

(2) Examples of digital identity services are services or products that—

(a) check the accuracy of personal or organisational information:

(b) check the connection of personal or organisational information to a particular individual or organisation:

(c) provide secure sharing of personal or organisational information between trust framework participants.

(3) The regulations must prescribe the types of digital identity services that may be accredited under this Act.

10 Trust framework participants

(1) The **participants** in the trust framework are—

(a) users:

(b) TF providers:

(c) relying parties.

(2) A single individual or organisation may be 1 or more of the participants listed in **subsection (1)** in the same transaction.

11 Requirements for TF providers dealing with personal or organisational information when providing accredited digital identity services

(1) A TF provider must not collect, use, share, or otherwise deal with personal or organisational information in connection with the provision of an accredited digital identity service unless—

(a) they have reasonable grounds to believe that the collection, use, sharing, or other dealing with the information is authorised by the individual or organisation to which the information relates; and

(b) they do so in accordance with the TF rules and the regulations.

(2) *See* **section 16**, which provides that nothing in this Act overrides the Privacy Act 2020.

12 ~~Trust~~ Accreditation marks

(1) TF providers may use ~~trust~~ accreditation marks approved by the TF board to identify ~~themselves, and~~ the accredited services they provide~~,~~ as being accredited under this Act.

(2) The board ~~must~~ may approve the form and style of ~~trust~~ accreditation marks and may approve different ~~trust~~ accreditation marks to be used ~~by or~~ for different types of ~~providers or~~ services.

(3) The TF authority must set the terms of use of ~~the trust~~ accreditation marks and must publish them on an Internet site maintained by or on behalf of the authority's responsible department.

(4) TF providers must comply with the relevant terms of use when using ~~a trust~~ an accreditation mark.

Digital identity services outside trust framework

13 TF providers may provide both accredited services and services not accredited

(1) A TF provider may provide both accredited services and digital identity services that are not accredited under this Act.

(2) *See* **section 94**, which makes it an offence for a person to knowingly or recklessly represent a digital identity service to be an accredited service when it is not.

14 Digital identity services outside trust framework

(1) An individual or organisation may provide a digital identity service even if they and the service are not accredited under this Act.

(2) *See* **section 94**, which makes it an offence for a person to knowingly or recklessly represent—

(a) themselves to be a TF provider when they are not:

(b) a digital identity service to be an accredited service when it is not.

Relationship with other Acts

15 Relationship with Electronic Identity Verification Act 2012 and Identity Information Confirmation Act 2012

Nothing in this Act limits or otherwise affects the Electronic Identity Verification Act 2012 or the Identity Information Confirmation Act 2012.

16 Application of Privacy Act 2020

Nothing in this Act overrides the Privacy Act 2020.

Part 3
TF rules, accreditation, TF register, and record-keeping and reporting

TF rules

~~17~~ **~~TF rules~~**

~~(1)~~ ~~The Governor-General may, by Order in Council made on the recommendation of the Minister, make rules for the operation and administration of the trust framework.~~

~~(2)~~ ~~The Minister may make rules for the operation and administration of the trust framework.~~

~~(3)~~ ~~Rules made under **subsections (1) and (2)** are together the **TF rules**.~~

~~(4)~~ ~~The TF board may recommend draft TF rules to the Minister for making under **subsection (1) or (2)**.~~

~~(5)~~ ~~The Minister may recommend the making of TF rules or make rules only if satisfied that the requirements for consultation under **section 20** have been met.~~

~~(6)~~ ~~Rules made under this section are secondary legislation (*see* Part 3 of the Legislation Act 2019 for publication requirements).~~

~~Compare: 1994 No 104 ss 36, 36A~~

17 **TF rules**

(1) The Minister may make rules for the matters listed in **section 19**.

(2) The TF board may recommend draft TF rules to the Minister.

(3) The Minister may make rules only if satisfied that the requirements for consultation under **section 20** have been met.

(4) Rules made under this section are secondary legislation (*see* Part 3 of the Legislation Act 2019 for publication requirements).

18 **Who TF rules apply to**

(1) The TF rules apply to TF providers and the accredited services they provide.

(2) The rules ~~may apply to TF providers only to the extent relevant to their provision of accredited services.~~—

(a) may apply to TF providers only to the extent relevant to their provision of accredited services:

(b) must not apply to digital identity services that are not accredited services.

~~19~~ **~~Content of TF rules~~**

~~(1)~~ ~~The TF rules—~~

(a) must identify the types of digital identity services that may be accredited under this Act:

(b) must set minimum requirements for all of the following:

Identification management

(i) determining the accuracy of information, binding that information to the correct individual or organisation, and enabling the secure reuse of the information:

Privacy and confidentiality

(ii) maintaining the privacy and confidentiality of the information of individuals or organisations:

Security and risk

(iii) ensuring that information is secure and protected from unauthorised modification, use, or loss:

Information and data management

(iv) record keeping and format of personal and organisational information, to ensure a common understanding of what is shared:

Sharing and facilitation

(v) the sharing of information with relying parties, including authorisation processes:

(c) may set other requirements for—

(i) periodic self-assessment by TF providers to check their compliance with the TF rules:

(ii) periodic reporting by TF providers about their compliance with the TF rules:

(iii) complaints processes and dispute resolution processes to be operated by TF providers:

(iv) other matters related to the operations of TF providers and the accredited services they provide as the TF board and the Minister think fit.

(2) The TF rules may set different minimum requirements or other requirements for—

(a) different types of TF providers:

(b) TF providers and accredited services:

(c) different types of accredited services:

(d) different levels of assurance for different types of accredited services.

(3) TF rules relating to personal information must be consistent with the Privacy Act 2020 (*see* **section 16**).

19 Content of TF rules

(1) The TF rules must set requirements for all of the following:

Identification management

(a) determining the accuracy of information, binding that information to the correct individual or organisation, and enabling the secure reuse of the information:

Privacy and confidentiality

(b) maintaining the privacy and confidentiality of the information of individuals and organisations:

Security and risk

(c) ensuring that information is secure and protected from unauthorised modification, use, or loss:

Information and data management

(d) record-keeping and format of personal and organisational information, to ensure a common understanding of what is shared:

Sharing and facilitation

(e) the sharing of information with relying parties, including authorisation processes.

(2) The TF rules may set different requirements for the following:

(a) different types of TF providers:

(b) TF providers and accredited services:

(c) different types of accredited services:

(d) different levels of assurance for different types of accredited services.

(3) If a TF rule is inconsistent with the regulations, the regulations prevail.

(4) TF rules relating to personal information must be consistent with the Privacy Act 2020 (*see also* **section 16**).

20 Consultation required before recommending TF rules

(1) Before recommending draft TF rules to the Minister, the TF board must consult and invite submissions from the following on the proposed content of the rules:

(a) the Office of the Privacy Commissioner; and

(b) ~~people or groups outside the board with expert~~ tikanga experts who have knowledge of te ao Māori approaches to identity; and

(c) TF providers; and

(d) people or groups that are likely to have an interest in the TF rules; and

(e) any other individual or organisation that the board considers should be consulted.

(2) The Minister must decide which people or groups the board must consult under **subsection (1)(b)** after taking into account the particular subject matter of the proposed content of rules.

(3) The Minister must also consult the Ministers with portfolio responsibilities that relate to Māori development and Māori-Crown relations before deciding which people or groups will be consulted by the board under **subsection (1)(b)**.

(4) The Minister may decide that consultation under this section is not required if the proposed content of a rule or a proposed change to an existing rule is technical and non-controversial in nature.

21 TF board to report to Minister on consultation

Before recommending draft TF rules to the Minister, the TF board must report to the Minister on the consultation it has undertaken under **section 20**.

Accreditation

22 Application for accreditation

(1) A digital identity service provider may apply to the TF authority to be accredited as a TF provider. That application must be accompanied by an application to have at least 1 digital identity service that they currently provide accredited as an accredited service.

(2) A TF provider may apply at any time to have a digital identity service that is provided by them, and that is not an accredited service, accredited as an accredited service. That service must be in addition to the 1 or more accredited services they already provide.

(3) *See* **section 30** for applications for provisional accreditation of providers and services.

23 Contents of application

(1) An application for accreditation must—

(a) be in the form, and be made in the manner, approved by the TF authority; and

(b) contain—

(i) key information prescribed by the regulations; and

(ii) other information required by the regulations (if any); and

(c) contain the specified information listed in **section 24(1)**; and

(d) be accompanied by the fee prescribed by the regulations (if any).

(2) *See* **section 97**, which makes it an offence to fail to give key information or specified information in an application for accreditation.

(3) The key information referred to in **subsection (1)(b)(i)** and the other information referred to in **subsection (1)(b)(ii)** may differ for—

(a) different types of applications:

(b) different types of digital identity service providers:

(c) TF providers and providers that are not accredited under this Act:

(d) providers and services:

(e) different types of services:

(f) different levels of assurance for different types of services.

(4) The fee referred to in **subsection (1)(d)** may vary in amount to reflect the different costs of processing different types of applications.

24 Specified information

(1) The specified information referred to in **section 23(1)(c)** is whether the applicant (whether already a TF provider or not)—

(a) has been convicted of a criminal offence, whether in New Zealand or overseas:

(b) is being or has been the subject of a formal investigation or proceeding by or taken by the Privacy Commissioner:

(c) has previously—

(i) had an application for accreditation for themselves or a service they provided declined:

(ii) had their accreditation as a TF provider or of a service they provided suspended or cancelled:

(iii) not complied with additional record-keeping or reporting requirements or a compliance order imposed or issued under **section 82**.

(2) In this section, **applicant** means the applicant and (as relevant) their ~~or its~~ officers, and those involved in the management of, employed by, or contracted by, the applicant.

25 ~~Assessment of applications~~ Decision by TF authority

(1) The TF authority may accredit a provider or service if it is satisfied that—

(a) the application meets the requirements of **sections 22 to 24**; and

(b) the application, provider, or service meets any criteria for the assessment of applications, or any other requirements, set by the regulations.

(2) The authority may grant the application in full or in part. However,—

(a) a provider may be accredited only if they will ~~be providing 1 or more accredited services~~ provide at least 1 accredited service:

(b) a service may be accredited only if it will be provided by a TF provider.

(3) An application that meets the requirements of this section may be declined only if the authority is satisfied that the provider's past conduct, or that of a related

individual or organisation, indicates that the provider or a service they provide may pose a risk to—

(a) the security, privacy, confidentiality, or safety of the information of any trust framework participants:

(b) the integrity or reputation of the trust framework.

(4) For the purposes of ~~**subsection (3)**~~ this section, the authority may take into account information that it reasonably believes is likely to be accurate.

26 Notice of decision

(1) The TF authority must give notice of its decision to the applicant and, if it declines the application (whether in full or in part), the authority must also—

(a) set out its reasons for declining the application or part of it; and

(b) tell the applicant of the right under **section 27** to request a reconsideration of the application, if it was declined in full, or of the part that was declined.

(2) If an application is successful in full or in part, the authority must give the applicant the following information along with its decision:

(a) the terms of use of the relevant ~~trust~~ accreditation mark or ~~trust~~ accreditation marks; and

(b) the expiry date that applies to the accreditation of the provider or service~~.~~; and

(c) any requirements set by regulations under **section 26A**.

26A Regulations for accredited providers and services

(1) Regulations may prescribe—

(a) requirements for—

(i) periodic self-assessment by TF providers to check their compliance with the TF rules:

(ii) periodic reporting by TF providers about their compliance with the TF rules:

(iii) complaints processes and dispute resolution processes that must be operated by TF providers:

(b) requirements for other matters related to the operations of TF providers and the accredited services they provide as the TF board and the Minister think fit:

(c) fees for recovering the costs of operating the trust framework.

(2) Regulations referred to in **subsection (1)** may set different requirements or fees for the following:

(a) different types of TF providers:

(aa) in relation to fees, different types of TF providers to reflect the different costs associated with administering the different types:

(b) TF providers and accredited services:

(c) different types of accredited services:

(d) different levels of assurance for different types of accredited services.

27 Reconsideration of application

(1) An applicant may apply to the TF authority for it to reconsider—

(a) an application for accreditation that it declined:

(b) the part of an application that it declined.

(2) The application for reconsideration must—

(a) be in the form, and be made in the manner, approved by the authority; and

(b) be made within 20 working days after receipt of the notice of the decision.

(3) When assessing the application, the authority must consider any new, or additional, relevant information provided by the applicant.

(4) A reconsideration decision by the authority is final. However, this section does not affect the right of an applicant to apply to a court for judicial review of the decision.

(5) Except to the extent that this Act or the regulations set different requirements for applications for reconsideration, **sections 22 to 24** apply to the making of an application under this section as if it were an original application for accreditation.

28 Duration of accreditation

(1) The accreditation of a TF provider or an accredited service commences on the date of the relevant accreditation decision by the TF authority and ends on the earliest of the following:

(a) the date the TF provider tells the authority is the date on which they no longer wish—

(i) to remain accredited as a TF provider; or

(ii) for the service to continue as an accredited service:

(b) the date on which the accreditation of the provider or service is cancelled under **section 82~~(e)~~** or **88**:

(c) the applicable expiry date:

(d) the date on which the accreditation of the service ceases under **subsection (3)**:

(e) the date on which the accreditation of the provider ends under **subsections (4) ~~and (5)~~**.

(2) Under **subsection (1)(c)**, the accreditation of a provider or service expires at the end of the relevant period set by the regulations. The regulations may set different periods for—

(a) different types of TF providers:

(b) TF providers and accredited services:

(c) different types of accredited services:

(d) different levels of assurance for different types of accredited services.

(3) If the accreditation of a TF provider ends under **subsection (1)**, all accredited services provided by that provider cease to be accredited services.

(4) If a TF provider does not provide at least 1 accredited service in a 12-month period or a longer period agreed by the authority (the **applicable period**), their accreditation as a TF provider ends unless ~~within the applicable period they applied for or obtained provisional accreditation for a digital identity service~~ **subsection (5)** applies.

(5) ~~If **subsection (4)** applies~~If a TF provider applies for or obtains provisional accreditation for a digital identity service in the applicable period, their accreditation ~~of a TF provider~~ continues,—

(a) in the case of a TF provider that has applied for provisional accreditation for a service, until the application is refused or, if provisional accreditation is granted, for the duration of that provisional accreditation:

(b) in the case of a TF provider that has obtained provisional accreditation for a service, for the duration of that provisional accreditation.

29 Renewal of accreditation

(1) A TF provider may apply ~~for a renewal of~~ to renew their accreditation or the accreditation of an accredited service they provide.

(2) If a renewal application is made before the accreditation of the provider or service expires, the accreditation continues to have effect until the renewal application is decided by the TF authority.

(3) If the accreditation of a provider or service expires before a renewal application is made, instead of a renewal application, the provider must make a fresh application for accreditation under **section 22**.

(4) A~~n~~ renewal application must be in the form, and be made in the manner, approved by the authority.

(5) Except to the extent that this Act or the regulations set different requirements for renewal applications, **sections 22 to 24** apply to the making of a renewal application as if it were an original application for accreditation.

30 Provisional accreditation

(1) The TF authority may grant provisional accreditation to a digital identity service provider or to a digital identity service.

(2) A digital identity service provider that is not a TF provider may apply to the authority—

(a) for provisional accreditation as a TF provider; and

(b) for provisional accreditation for a service they wish to develop.

(3) An application under **subsection (2)** must be for provisional accreditation for both the provider and at least 1 service they wish to develop.

(4) A TF provider may apply to the authority for provisional accreditation for a service they wish to develop in addition to the 1 or more accredited services they already provide.

(5) An application under this section must be in the form, and be made in the manner, approved by the authority.

(6) Except to the extent that this Act or the regulations set different requirements for applications for provisional accreditation, **sections 22 to 27** apply to the making and deciding of an application under this section with any necessary modifications.

(7) Provisional accreditation expires—

(a) at the end of the 12-month period that begins on the date the provisional accreditation is granted or a longer period agreed by the authority; or

(b) on the date that accreditation is granted for the provider or service ~~following an application~~ under **section 25**.

(8) A provider or service with provisional accreditation is not a TF provider or an accredited service for the purposes of this Act.

31 Obligation to tell TF authority of changes to key information or specified information

(1) If any of the key information referred to in **section 23(1)(b)(i)**, or the specified information listed in **section 24(1)**, changes, the applicant or TF provider must tell the TF authority of the change within 5 working days of the change.

(2) *See* **section 98**, which makes it an offence to fail to tell the authority of a change to key information or specified information.

(3) The obligations under **subsection (1)** apply,—

(a) for an applicant (whether already a TF provider or not), after an application for accreditation has been made and until it is decided by the authority:

(b) for a TF provider, following the accreditation of themselves or a service they provide, from the date of the authority's decision and for the period during which they or the service remains accredited.

(4) The obligations under this section apply even if an applicant or a TF provider has previously failed to give key information or specified information to the authority as required by **sections 23 and 24**.

(5) In this section, **application for accreditation** means—

(a) an application for accreditation under **section 22**:

(b) an application for reconsideration under **section 27**:

(c) an application for renewal of accreditation under **section 29**:

(d) an application for provisional accreditation under **section 30**:

(e) any communication with the authority relating to an application in **paragraphs (a) to (d)**~~, whether in the application itself or made before or after the application is submitted~~ whenever the communication is made.

TF register

32 Register of TF providers and accredited services

(1) The TF authority must establish and maintain a register of TF providers and accredited digital identity services.

(2) In this section and **sections 33 to ~~37~~ 36**,—

accredited digital identity service and **accredited service** include a digital identity service for which accreditation is suspended

TF provider includes an individual or organisation whose accreditation as a TF provider is suspended.

33 Purposes of register

The purposes of the TF register are—

(a) to enable the public to—

(i) determine whether an individual or organisation has been accredited as a TF provider and, if so, the status and history of that accreditation (for example, whether it is current or suspended or has lapsed or been cancelled); and

(ii) determine which of a TF provider's digital identity services have been accredited under this Act and the status and history of those accreditations; and

(iii) choose a suitable TF provider from the list of TF providers; and

(b) to facilitate the administrative, disciplinary, and other functions of the TF authority under this Act.

34 Form of register

The TF register must be kept as an electronic register on a publicly accessible Internet site maintained by or on behalf of the TF authority or its responsible department.

35 Information to be contained in register

(1) The TF register must contain the following information for each TF provider:

(a) the TF provider's full name:

(b) a unique identifier issued by the TF authority (for example, a registration number):

(c) information about the status and history of the TF provider's accreditation as a TF provider, including—

(i) the date on which ~~the TF provider~~ they became accredited; and

(ii) if the accreditation is for a fixed period, the date on which it will expire if not renewed; and

(iii) whether the accreditation is currently suspended and, if it is, the period of the suspension.

(2) For each TF provider, the register must also—

(a) identify ~~any~~ the digital identity services provided by the TF provider that are accredited services; and

(b) include information about the status and history of the accreditation of each of those digital identity services, including—

(i) the date on which the ~~digital identity~~ service became accredited; and

(ii) if the accreditation is for a fixed period, the date on which it will expire if not renewed; and

(iii) whether the accreditation is currently suspended, and, if it is, the period of the suspension.

(3) The register may also contain—

(a) information about former TF providers and former accredited digital identity services, including information about when their accreditation ended; and

(b) any other information that the TF authority considers necessary or desirable for the purposes of the register.

36 Amendments to register

The TF authority may make amendments to the TF register at any time for the purposes set out in **section 33**, including amendments to—

(a) keep the register up to date by reflecting any changes in the information contained in it:

(b) correct an error or omission on the part of the authority or anyone establishing or maintaining the register on the authority's behalf.

~~**37 Search of register**~~

~~Any person may search the TF register, and make copies of parts of it, free of charge, for a purpose set out in **section 33**.~~

Third party assessors

38 ~~TF authority may certify~~ Certification of third party assessors

(1) The TF authority may certify an individual or an organisation as a third party assessor~~s~~ to carry out 1 or more of its functions relating to accreditation of providers or services if permitted by, and in accordance with, the regulations.

(2) ~~Third party assessors do~~ A third party assessor does not have, and nor may the authority delegate to them, the authority's powers under **sections 60 and 61** of this Act.

(3) The regulations may prescribe circumstances under which the authority may suspend or cancel the certification of third party assessors.

39 Accountability and immunity

(1) This section applies to a third party assessor when intending to carry out or carrying out functions under this Act.

Accountability

(2) The Ombudsmen Act 1975 and the Official Information Act 1982 apply to them as if the third party assessor were an organisation named in Schedule 1 of the Ombudsmen Act 1975.

(3) Information they hold is to be treated as also being held by the TF authority for the purposes of the Official Information Act 1982.

Immunity

(4) Section 104 of the Public Service Act 2020 applies to them as if they were a public service employee.

Compare: 2020 No 40 Schedule 6 cl 3(2); 1989 No 24 s 7G

40 Record-keeping and reporting by third party assessors

The regulations may prescribe record-keeping and reporting requirements for third party assessors, including for the collection and keeping of certain information, and for providing information to the TF authority.

Record-keeping and reporting by TF providers

41 Record-keeping and reporting by TF providers

(1) A TF provider must—

(a) collect the required information about its activities; and

(b) keep that information in the required manner and for the required period; and

(c) give that information to the TF authority ~~at all reasonable times on request.~~—

(i) periodically as required:

(ii) at all reasonable times on request.

(2) In this section,—

give, in relation to information, includes—

(a) give access to the information, including by permitting its inspection; and

(b) permit copies of the information to be made

required means required by the regulations.

Part 4
TF board

42 TF board established

(1) The Trust Framework Board is established to carry out the board's functions set out in this Act.

~~(2) **Sections 20(1)(b), 46(2)(a) and (b), and 50 to 54** provide a practical commitment to the principles of the Treaty of Waitangi (te Tiriti o Waitangi) for the governance and operation of the trust framework through the TF board. These provisions relate to consultation by the board before recommending draft TF rules to the Minister, appointment of the members of the board, and the establishment of a Māori Advisory Group to advise the board.~~

43 Responsible department

(1) The Prime Minister must nominate a department to be the responsible department for the TF board.

(2) The board is a body within the responsible department and is accountable to its chief executive.

(3) The responsible department must include in its annual report a description of the board's activities for the period covered by the report.

Compare: 2007 No 15 s 34(1)

TF board's functions and powers

44 Functions of TF board

(1) The TF board's functions are to—

(a) recommend draft TF rules to the Minister, review the rules at reasonable intervals, and recommend updates to them:

(b) recommend regulations to the Minister:

(c) undertake education and publish guidance for TF providers and the public:

(d) monitor the effectiveness of the trust framework:

(e) carry out other functions conferred on the board by this Act or by the Minister to achieve the purposes of this Act:

(f) carry out any functions that are incidental and related to, or consequential on, the functions referred to in **paragraphs (a) to (e)**.

(2) If any functions are conferred on the board by the Minister, this must be done in writing.

(3) When performing its functions, the board must engage with Māori in the manner provided for under **section 52(4A)** to recognise and provide for Māori interests in the operation of the trust framework.

45 General powers of TF board

The TF board has all the powers that are reasonably necessary to carry out its functions under this Act to the extent consistent with **section 43(2)**.

TF board members

46 Appointment of TF board members

(1) The chief executive must appoint the members of the TF board. The members may include public service employees and individuals from outside the public service.

(2) When selecting the board's members, the chief executive must ensure that—

(a) members of the board include people ~~with~~ who have expert knowledge of te ao Māori approaches to identity; and

(b) members of the board include people ~~with expert knowledge of the principles of the Treaty of Waitangi (te Tiriti o Waitangi); and~~ who have—

(i) expert knowledge of the principles of te Tiriti o Waitangi/the Treaty of Waitangi; and

(ii) experience in engaging with Māori; and

(c) the members of the board collectively possess sufficient knowledge and expertise in working with technology and identity data management, including with—

(i) the ethical use of digital information; and

(ii) protecting the privacy and confidentiality of digital information; and

(iii) the secure handling of digital information~~; and~~.

~~(iv) engagement with Māori; and~~

(d) the board has sufficient members to carry out its functions in a timely and efficient manner.

47 Voting rights

Only members of the TF board who are public service employees have voting rights on the board.

48 Removal of TF board members

The chief executive may give written notice to a TF board member removing them from the board if they become bankrupt or neglect their duty, or for misconduct.

49 Remuneration of TF board members

(1) A TF board member who is a public service employee is entitled to be paid by their employer, as if they were undertaking their usual duties, for time reasonably taken by them away from their usual duties to undertake the work of the board.

(2) Other board members are not public service employees as a result of their appointment to the board, and the responsible department must pay fees for their services, and expenses reasonably incurred by them in providing those services, in accordance with the fees framework.

Māori Advisory Group

50 Māori Advisory Group established

The Māori Advisory Group is established to advise the TF board.

Compare: 2020 No 52 s 14

51 Appointment of members of Māori Advisory Group

(1) The Minister must appoint members to the Māori Advisory Group.

(2) The Minister must consult the Ministers with portfolio responsibilities that relate to Māori development and Māori-Crown relations before making any appointments.

(3) The Minister must appoint 1 of the members as chairperson of the Māori Advisory Group.

(4) The Minister must appoint only people who, in the responsible Minister's opinion, have the appropriate knowledge, skills, and experience to assist the Māori Advisory Group to perform its role.

Compare: 2020 No 52 s 15

52 Role of Māori Advisory Group

(1) The role of the Māori Advisory Group is to advise the TF board on Māori interests and knowledge, as they relate to the operation of the trust framework,

and to do so in accordance with the engagement policy and terms of reference referred to in **subsection (4)**.

(2) The board must seek advice from the Māori Advisory Group if a matter the board is dealing with raises matters of tikanga Māori or Māori cultural perspectives.

(3) The board must give effect to the advice of the Māori Advisory Group to the extent that it considers is reasonable and practicable after taking account of other relevant considerations.

(4) The board and the Māori Advisory Group, acting jointly, must—

(a) prepare an engagement policy, setting out how they will work together; and

(b) prepare and agree the terms of reference for the Māori Advisory Group.

(4A) The engagement policy must include details of how and when consultation with iwi and hapū will be undertaken by—

(a) the board:

(b) the board together with the Māori Advisory Group:

(c) the Māori Advisory Group to inform its advice to the board.

(5) The board must publish on an Internet site maintained by or on behalf of the board's responsible department—

(a) the engagement policy and the terms of reference for the Māori Advisory Group; and

(b) all written advice from the Māori Advisory Group to the board, with redactions if needed, to—

(i) protect the privacy of individuals:

(ii) maintain legal professional privilege:

(iii) protect commercially sensitive information.

(6) The board and the Māori Advisory Group, acting jointly, must review both the engagement policy and the terms of reference at intervals of not more than 3 years.

Compare: 2020 No 52 s 17

53 Further provisions relating to Māori Advisory Group

(1) The following provisions of the Crown Entities Act 2004 apply to members of the Māori Advisory Group as if they were members of the board of a Crown agent:

(a) section 28 (method of appointment of members):

(b) section 30 (qualifications of members):

(c) section 31 (requirements before appointment):

(d) section 32 (term of office of members):

(e) section 35 (validity of appointments):

(f) section 43 (no compensation for loss of office):

(g) section 44 (resignation of members):

(h) section 45 (members ceasing to hold office).

(2) The members are entitled to fees for their services, and expenses reasonably incurred by them in providing those services, in accordance with the fees framework.

Compare: 2020 No 52 s 16

54 Removal of Māori Advisory Group members

The Minister may give written notice to a member of the Māori Advisory Group removing them as a member if they become bankrupt or neglect their duty, or for misconduct.

Committees of advisers

55 Appointment and remuneration of committees of advisers

(1) The TF board may establish committees of advisers of public service employees and individuals from outside the public service to give advice and make reports to the board.

(2) An adviser who is a public service employee is entitled to be paid by their employer, as if they were undertaking their usual duties, for time reasonably taken by them away from their usual duties to undertake the work of a committee.

(3) Other advisers are not public service employees as a result of their appointment to a committee, and the board's responsible department must pay fees for their services, and expenses reasonably incurred by them in providing those services, in accordance with the fees framework.

56 Removal of committee members

The TF board may give written notice to a committee member removing them from a committee if they become bankrupt or neglect their duty, or for misconduct.

Part 5
TF authority

57 TF authority established

The Trust Framework Authority is established to carry out the authority's functions set out in this Act.

58 Responsible department

(1) The Prime Minister must nominate a department to be the responsible department for the TF authority.

(2) That department may be the same as the responsible department nominated for the TF board under **section 43**.

(3) The authority is a body within the responsible department and is accountable to its chief executive. However, the authority must act independently in respect of its enforcement functions under **Part 6**.

(4) The responsible department must include in its annual report a description of the authority's activities for the period covered by the report.

Compare: 2007 No 15 s 34(1)

TF authority's functions and powers

59 Functions of TF authority

The TF authority's functions are to—

(a) establish, administer, and maintain an accreditation regime for digital identity service providers and digital identity services:

(b) establish, administer, and maintain a register of TF providers and accredited services:

(c) monitor the performance and effectiveness of the accreditation regime:

(d) ~~establish~~ operate procedures and tests for TF providers to demonstrate their compliance with the TF rules and the regulations:

(da) undertake compliance monitoring of TF providers:

(e) receive and assess complaints:

(f) investigate breaches of the TF rules, the regulations, the terms of use of ~~trust~~ accreditation marks, and this Act:

(g) carry out other functions conferred on the authority by this Act:

(h) carry out any functions that are incidental and related to, or consequential on, the functions referred to in **paragraphs (a) to (g)**.

60 General powers of TF authority

The TF authority has all the powers that are reasonably necessary to carry out its functions under this Act to the extent consistent with **section 58(3)**.

61 Power to require information or documents

(1) The TF authority may, by written notice and without charge, require an individual or organisation to provide to it information or a document in their ~~or its~~ possession or control if satisfied that the information or document is necessary for, and relevant to, 1 or more of the purposes listed in **subsection (3)**.

(2) The notice may set a date by which the information or document must be provided to the authority. This must not be sooner than 5 working days after receipt of the notice by the individual or organisation.

(3) The purposes for which the authority may issue a notice are—

(a) assessing or investigating a complaint under **Part 6**:

(b) investigating compliance— with the TF rules, the regulations, the terms of use of accreditation marks, or this Act:

~~(i) by a TF provider with the TF rules, the regulations, the terms of use of trust marks, or this Act; or~~

~~(ii) by a TF provider with the TF rules relating to an accredited service provided by them:~~

(ba) assessing whether additional record-keeping or reporting requirements imposed under **section 82** should be lifted:

(c) assessing compliance with a compliance order issued under **section 82**:

(d) assessing whether a suspension of accreditation should be lifted.

(4) The individual or organisation that receives a notice must comply with it within the period stated in the notice.

(5) However, an individual or organisation that receives a notice need not comply with it in relation to any information or document if—

(a) it would be privileged in a court:

(aa) another Act deals specifically with access to the information or document:

(b) disclosure would breach an obligation of secrecy or non-disclosure imposed by an enactment (other than the Privacy Act 2020 or the Official Information Act 1982).

(6) The authority must not release any information or document received by it under this section if the information or document is commercially sensitive, unless the release is required by an enactment.

(7) In this section, **information** means any information, whether contained in a document or not.

Compare: 2020 No 31 ss 87-89

62 Extension of time to provide information

(1) An individual or organisation that receives a notice under **section 61** may apply to the TF authority for an extension of time to provide the information or document, and the authority may extend the time for a period it considers to be reasonable in the circumstances.

(2) The application must set out the reasons for requesting the extension of time.

TF authority members

63 Appointment of TF authority members

(1) The chief executive must appoint the members of the TF authority. The members may include public service employees and individuals from outside the public service.

(2) When selecting the authority's members, the chief executive must ensure that the authority has—

(a) members who collectively possess the appropriate skills and experience to carry out its functions; and

(b) sufficient members to carry out its functions in a timely and efficient manner.

64 Removal of TF authority members

The chief executive may give written notice to a member of the TF authority removing them from the authority if they become bankrupt or neglect their duty, or for misconduct.

65 Remuneration of TF authority members

(1) A member of the TF authority who is a public service employee is entitled to be paid by their employer, as if they were undertaking their usual duties, for time reasonably taken by them away from their usual duties to undertake the work of the authority.

(2) Other members of the authority are not public service employees as a result of their appointment to the authority, and the responsible department must pay fees for their services, and expenses reasonably incurred by them in providing those services, in accordance with the fees framework.

Part 6
Complaints and offences

66 Purpose of Part

The purpose of this Part is to promote confidence in the trust framework by establishing processes for dealing with complaints.

67 Principles

In carrying out its functions under this Part (except when granting remedies or prosecuting offences), the TF authority must be guided by the following principles:

(a) processes for complaints should be fair and accessible~~,~~ and have particular regard to tikanga Māori ~~if a complainant desires~~:

(b) complaints should be resolved in a timely and efficient manner:

(c) complaints should be resolved at a level appropriate to the seriousness and nature of the complaint.

Complaints

68 Who may make complaint

(1) Any person may complain to the TF authority if they believe there has been a breach by a TF provider.

(2) ~~In this Part, **breach** means —~~**Breach** means a breach of the TF rules, the regulations, terms of use of accreditation marks, or provisions of this Act.

~~(a) a breach by a TF provider of 1 or more of the TF rules, the regulations, terms of use of trust marks, or provisions of this Act:~~

~~(b) a failure by a TF provider to provide an accredited service in accordance with the TF rules.~~

69 How to make complaint

(1) A complaint must ~~be in writing and —~~

(a) identify the complainant and the TF provider to which the complaint relates; and

(b) describe the alleged breach; and

~~(c) identify the relevant rule, regulation, term of use, or provision; and~~

(d) state why the complainant believes that a breach has occurred; and

(e) comply with other requirements set out in the regulations.

(2) A complainant is entitled to reasonable assistance from the TF authority to meet the requirements of **subsection (1)**.

70 How complaints must be dealt with

(1) As soon as practicable after receiving a complaint, the TF authority must—

(a) tell the complainant in writing that their complaint has been received; and

(b) tell the TF provider in writing about the substance of the complaint; and

(c) give the TF provider a reasonable opportunity to comment; and

(d) consider the complaint and make a preliminary assessment of whether a breach appears to have occurred unless it decides—

(i) to refer the complaint to an office holder under **section 71**; or

(ii) not to consider the complaint further under **section 72**.

(2) If part of a complaint is referred to an office holder, the authority must make a preliminary assessment of the remaining part of the complaint unless it decides not to consider that part of the complaint further under **section 72**.

71 Referral of complaints to office holders

(1) This section applies if the TF authority considers that a complaint (in full or in part) may be more appropriately dealt with by:

(a) the Ombudsman:

(b) the Privacy Commissioner:

(c) the Inspector-General of Intelligence and Security:

(d) another office holder.

(2) The authority must consult the relevant office holder about whether the complaint—

(a) is within their jurisdiction; and

(b) would be more appropriately dealt with by them.

(3) The decision about whether a complaint is within the jurisdiction of an office holder is a matter solely for the relevant office holder.

(4) If the complaint is within the jurisdiction of the office holder and the authority decides that it would be more appropriately dealt with by that office holder, the authority must as soon as practicable—

(a) refer the complaint or the relevant part of it to the relevant office holder; and

(b) tell the complainant and TF provider in writing it has done so.

72 TF authority may decide not to consider complaint further

(1) The TF authority may decide not to consider a complaint or part of a complaint further if it considers—

(a) the complaint does not meet the requirements of **section 69**; or

(aa) the complaint involves any of the matters set out in **section 75(2)**; or

(b) the complainant has not made reasonable efforts to first resolve the complaint directly with the TF provider concerned; or

(c) there is ~~an alternative~~ a dispute resolution scheme or process available to resolve the complaint because of the TF provider's membership of a particular industry and the complainant has not made use of it; or

(d) the complaint appears to largely involve a commercial dispute between 2 or more trust framework participants; or

(e) the complainant knew about the breach or potential breach for ~~6~~12 months or more before they made the complaint; or

(f) the length of time that has elapsed between the date on which the subject of the complaint arose and the date on which the complaint was made means that consideration of the complaint is no longer practicable or desirable; or

(g) the complainant does not have a sufficient personal interest in the subject of the complaint; or

(h) the complaint is frivolous, vexatious, or not made in good faith.

(2) The authority may also decide not to consider a complaint further if, after having regard to all of the circumstances of the case, the authority is of the opinion that considering the complaint further is unnecessary or inappropriate.

(3) If the authority decides~~, in accordance with this section,~~ not to consider a complaint further, it must tell the complainant and TF provider in writing of the decision and give its reasons.

Compare: 2020 No 31 s 74

Preliminary assessment of complaints

73 Procedure for preliminary assessment of complaints

(1) When making a preliminary assessment of a complaint, the TF authority must take into account—

(a) any relevant information and comments received from the complainant; and

(b) any relevant information and comments received from the TF provider; and

(c) any other relevant information that is readily accessible to it.

(2) The authority may, for the purpose of making a preliminary assessment, in its absolute discretion, decide—

(a) to provide information received from the TF provider to the complainant and seek their response:

(b) to obtain information or documents from an individual or organisation under **section 61**.

(3) *See* **section 61(6)**, which limits the release of any information or document that is commercially sensitive. The authority must also not provide any information or document to a complainant that is confidential.

(4) If the authority obtains information or documents under **section 61** from an individual or organisation that is not the TF provider, it must give the TF provider copies and a reasonable opportunity to comment on them.

(5) ~~Except as provided in this Act, t~~The authority may, when making a preliminary assessment, regulate its procedure as it considers appropriate and in a way that is consistent with this Act and the regulations (if any).

74 Notice of preliminary assessment

The TF authority must give the complainant and the TF provider—

(a) written notice of its preliminary assessment including its reasons for the assessment; and

(b) if its assessment is that it appears ~~that~~ a breach has occurred,—

(i) information about the ~~alternative~~ dispute resolution scheme run by the authority; and

(ii) information about the authority's powers of investigation and the remedies it may grant.

~~Alternative d~~Dispute resolution scheme

75 ~~Alternative d~~Dispute resolution scheme

(1) The TF authority may, in accordance with any requirements and criteria prescribed in the regulations, recommend ~~an alternative~~ a dispute resolution scheme for the Minister's approval.

(2) The ~~alternative~~ dispute resolution scheme must not deal with the following ~~disputes~~:

(a) a matter that may be dealt with under the Privacy Act 2020:

(b) an employment dispute that may be dealt with under the Employment Relations Act 2000:

(c) a dispute relating to acts that may be prosecuted as an offence under this Act:

(d) a dispute relating to the carrying out of a Minister's function:

(e) a dispute of a kind prescribed by the regulations.

(3) The chief executive may employ or engage persons or organisations to provide dispute resolution services to support the resolution of complaints under this Part.

76 Ministerial approval of ~~alternative~~ dispute resolution scheme

The Minister may approve ~~an alternative~~ a dispute resolution scheme if satisfied that—

(a) it provides a means of resolving complaints that is consistent with the principles listed in **section 67**; and

(b) it meets any requirements set out in the regulations.

Investigations by TF authority

77 Investigation of breach

The TF authority may commence an investigation—

(a) following a preliminary assessment that a breach that was the subject of a complaint appears to have occurred:

(b) on its own initiative, into any matter that could be the subject of a complaint under this Part.

Compare: 2020 No 31 s 79

78 Commencing investigation

(1) As the first step of an investigation, the TF authority must notify the TF provider that it is commencing an investigation.

(2) A notice given under **subsection (1)** must—

(a) set out the details of—

(i) the alleged breach that was the subject of a complaint; or

(ii) ~~the subject of the investigation~~if the investigation is commenced under **section 77(b)**, the subject of and reasons for the investigation; and

(b) advise the TF provider of their right to provide, within a reasonable time, a written response to the authority.

Compare: 2020 No 31 s 80

79 Conducting investigation

(1) The TF authority must conduct an investigation in a timely manner.

(2) During an investigation, the authority may—

(a) hear and obtain information or documents from any person (*see* **section 61**); and

(b) make any inquiries.

(3) At any time during an investigation, the authority may decide to take no further action on a complaint or matter if it—

(a) is satisfied that any of the matters set out in **section 72(1)** apply; or

(b) after having regard to all of the circumstances of the case, considers that any further action is unnecessary or inappropriate.

(4) As soon as practicable after making a decision under **subsection (3)**, the authority must notify the complainant (if any) and the TF provider of—

(a) that decision; and

(b) the reasons for that decision.

(5) It is not necessary for the authority to hold a hearing, and no person is entitled as of right to be heard by the authority.

(6) Any investigation conducted by the authority must be conducted in private.

Compare: 2020 No 31 s 81

80 TF authority may regulate own procedure

When conducting an investigation, the TF authority may ~~adopt any procedure it~~ regulate its procedure as it considers appropriate ~~that is~~ and in a way that is consistent with this Act and the regulations (if any).

Compare: 2020 No 31 s 82

81 Finding by TF authority

(1) If the TF authority is satisfied, on the balance of probabilities, that a breach has occurred, it must give the complainant (if any) and the TF provider written notice of its decision, including its reasons.

(2) The authority may also grant 1 or more of the remedies listed in **section 82** but must first give the TF provider a reasonable opportunity to make submissions on the issue of remedies.

(3) The authority may find that a breach has occurred even if it is of the view that the breach was unintentional or without negligence on the part of the TF provider. However, the authority must take the conduct of the TF provider into account when deciding what, if any, remedy or remedies to grant.

Compare: 2020 No 31 s 102(3)

Remedies

82 Remedies following finding of breach

(1) If the TF authority finds a breach by a TF provider, it may do 1 or more of the following:

(a) issue a private or public warning:

(b) require the provider to comply with additional record-keeping or reporting requirements either for a specified period or indefinitely:

(c) issue a compliance order:

(d) suspend the provider's accreditation or the accreditation of the relevant service they provide until they take specified steps:

(e) cancel the provider's accreditation or the accreditation of the relevant service they provide.

(2) If the authority is satisfied that a TF provider has failed to comply with a compliance order or give the notice required by **section 87**, it may suspend or cancel the accreditation of the provider or the relevant service.

Public warnings

83 Public warnings

(1) The TF authority may issue a public warning under **section 82(1)(a)** only if it is satisfied on reasonable grounds that—

(a) a public warning is necessary to give users notice that use of a service provided by the TF provider carries a material risk of identity fraud, economic loss, or physical or emotional harm; and

(b) that risk is attributable to the breach by the TF provider; and

(c) the imposition of 1 or more of the other remedies under **section 82** is insufficient to mitigate that risk; and

(d) issuing a public warning will not result in disclosure of a security-related vulnerability of the relevant service that could be exploited by others.

(2) Before making a decision under this section, the authority must—

(a) take reasonable steps to give notice to the TF provider that it is considering issuing a public warning and give them a reasonable opportunity to comment; and

(b) take into account any comments they make.

Additional record-keeping or reporting requirements

83A Additional record-keeping or reporting requirements

The authority may require additional record-keeping or reporting requirements under **section 82(1)(b)** for any period that the authority considers appropriate, but it may lift those additional requirements earlier if satisfied that they are no longer needed.

Compliance orders

84 Issuing compliance order

(1) Before issuing a compliance order under **section 82(1)(c)**, the TF authority must consider all of the following:

(a) whether there is another means under this Act of dealing with the breach that would be more effective than a compliance order:

(b) the seriousness of the breach:

(c) the likelihood of the breach continuing or being repeated:

(d) the number of people who may be or are affected by the breach:

(e) whether the TF provider has been co-operative in all dealings with the authority:

(f) the likely costs to the TF provider of complying with the order.

(2) However, each of those factors need be considered only to the extent that—

(a) it is relevant in the authority's view; and

(b) information about the factor is readily available to the authority.

(3) Before issuing a compliance order, the authority must also—

(a) take reasonable steps to give notice to the TF provider that it is considering issuing a compliance order and give them a reasonable opportunity to comment on—

(i) a draft of the order; and

(ii) a summary of the conclusions reached about the factors in **subsection (1)** that the authority considered; and

(b) take into account any comments they make.

Compare: 2020 No 31 s 124

85 Form of compliance order

(1) A compliance order must—

(a) state the name of the TF provider and describe the relevant accredited service; and

(b) describe the breach, citing the relevant TF rule, regulation, term of use, or provision of this Act; and

(c) require the TF provider to remedy the breach within a specified time that is reasonable in the circumstances; and

(d) require the TF provider to report to the TF authority, within a specified time or times, about—

(i) the steps they have taken to remedy the breach:

(ii) whether the breach has been remedied; and

(e) inform the TF provider that the order may be varied or cancelled under **section 89**; and

(f) contain other information required by the regulations (if any).

(2) A compliance order may also—

(a) require the TF provider to take particular steps to remedy the breach:

(b) contain any other information the authority considers would be useful.

Compare: 2020 No 31 s 125

86 TF provider response to compliance order

(1) A TF provider that is issued with a compliance order must ~~take steps to~~ comply with it, including by taking any particular steps to remedy the breach specified in the order~~, as soon as is reasonably practicable~~.

(2) The TF provider must remedy the breach ~~within the time stated in the order or at a later time if varied by the TF authority.~~,—

(a) if no time is stated in the order, as soon as is reasonably practicable:

(b) within the time stated in the order:

(c) at a later time if varied by the TF authority.

~~(3)~~ ~~**Subsections (1) and (2)** (as relevant) cease to apply on the day after the date an order is varied or cancelled by the authority.~~

Compare: 2020 No 31 s 126

87 TF provider must tell TF authority when compliance order complied with

A TF provider must tell the TF authority when it has complied with a compliance order and must do so within 5 working days of doing so.

88 TF provider may elect to forfeit accreditation

(1) A TF provider that receives a draft compliance order or a compliance order may elect to forfeit their accreditation or the accreditation of the relevant service, whichever is the subject of the draft order or order.

(2) The TF provider must tell the TF authority that it wishes to do so within 5 working days of receiving the draft order or order.

(3) If the authority receives the advice referred to in **subsection (2)** for a draft compliance order, it must cancel the accreditation in place of issuing a compliance order.

(4) If the authority receives the advice after issuing a compliance order, it must cancel both the accreditation and the compliance order.

89 TF authority may vary or cancel compliance order

(1) A TF provider may apply to the TF authority to vary or cancel a compliance order on the ground that there has been an error of fact or law.

(2) The authority may do so on terms it considers appropriate.

Compare: 2020 No 31 s 127

Suspension or cancellation of accreditation following finding of breach

90 Suspension of accreditation

(1) This section applies if the TF authority has suspended the accreditation of a TF provider or a service they provide—

(a) by suspending them or it under **section 82(1)(d)**:

(b) by suspending them or it under **section 82(2)** because the authority is satisfied that a TF provider has failed to comply with a compliance order~~, including because~~ or it has not received notice ~~under~~ required by **section 87**.

(2) The suspension may be for any period the authority considers appropriate, but it may reinstate the accreditation earlier if it is satisfied that—

(a) any steps specified under **section 82(1)(d)** have been taken by the TF provider; and

(b) the TF provider has complied with the compliance order.

(3) However, before making a decision under this section, the authority must—

(a) take reasonable steps to give notice to the TF provider that it is considering suspending the accreditation and give them a reasonable opportunity to comment; and

(b) take into account any comments they make.

91 Cancellation of accreditation

(1) This section applies if the TF authority has cancelled the accreditation of a TF provider or a service they provide—

(a) by cancelling it under **section 82(1)(e)**:

(b) by cancelling it under **section 82(2)** because the authority is satisfied that a TF provider has failed to comply with a compliance order~~, including because~~ or it has not received notice ~~under~~ required by **section 87**.

(2) However, before making a decision under this section, the authority must—

(a) take reasonable steps to give notice to the TF provider that it is considering cancelling the accreditation and give them a reasonable opportunity to comment; and

(b) take into account any comments they make.

92 Suspension or cancellation if breach on 3 or more occasions

(1) If a TF provider is found to have breached any of the following on at least 3 separate occasions in a 12-month period, the TF authority may suspend or cancel their accreditation or the accreditation of the relevant service they provide:

(a) a TF rule:

(b) a regulation:

(c) a term of use of ~~a trust~~ an accreditation mark:

(d) a provision of this Act.

(2) The suspension may be for any period the authority considers appropriate, but it may reinstate the accreditation earlier if it is satisfied the suspension is no longer needed.

(3) The authority must take reasonable steps to give notice to the TF provider of the suspension or cancellation, but need not give them an opportunity to comment before suspending or cancelling the accreditation.

Suspension or cancellation of accreditation for other reasons

93 Suspension or cancellation of accreditation

(1) The accreditation of a TF provider or of a service they provide may be suspended or cancelled by the TF authority if the TF provider—

(a) is convicted of an offence under this Act:

(b) has ceased to operate all or a substantial proportion of their accredited digital identity services:

(c) is declared bankrupt or insolvent, or is unable to pay their debts as they fall due, or enters into an arrangement with creditors as a consequence of defaulting on a payment relating to a debt:

(d) is a director of a company that has been put into receivership or liquidation:

(e) has a receiver appointed for a business through which accredited services are provided:

(f) does something or omits to do something that, in the view of the authority, may pose a risk to—

(i) the security, privacy, confidentiality, or safety of the information of any trust framework participants:

(ii) the integrity or reputation of the trust framework.

(2) This section applies whether or not the authority has found a breach by a TF provider.

(3) The suspension may be for any period the authority considers appropriate, but it may reinstate the accreditation earlier if it is satisfied the suspension is no longer needed.

(4) However, before making a decision under this section, the authority must—

(a) take reasonable steps to give notice to the TF provider that it is considering suspending or cancelling the accreditation and give them a reasonable opportunity to comment; and

(b) take into account any comments they make.

(5) For the purposes of **subsection (1)**, the authority may take into account information that it reasonably believes is likely to be accurate.

(6) In this section, **TF provider** means the TF provider and (as relevant) their officers and those involved in the management of, employed by, or contracted by, the TF provider.

Offences

94 Offence to knowingly or recklessly misrepresent provider to be TF provider or service to be accredited service

(1) A person who knowingly or recklessly represents themselves to be a TF provider when they are not ~~(including using a trust mark when not entitled to do so)~~ commits an offence and is liable on conviction to,—

(a) in the case of an individual, a maximum fine of $50,000:

(b) in the case of a body corporate, a maximum fine of $100,000.

(2) A person who knowingly or recklessly represents a digital identity service to be an accredited service when it is not (including using ~~a trust~~ an accreditation mark when not entitled to do so) commits an offence and is liable on conviction to,—

(a) in the case of an individual, a maximum fine of $50,000:

(b) in the case of a body corporate, a maximum fine of $100,000.

95 Offence to misuse ~~trust~~ accreditation mark

A person who knowingly or recklessly uses ~~a trust~~ an accreditation mark in a manner that is contrary to the terms of use set by the TF authority commits an offence and is liable on conviction to,—

(a) in the case of an individual, a maximum fine of $50,000:

(b) in the case of a body corporate, a maximum fine of $100,000.

96 Offence to knowingly or recklessly give false information to TF authority in application for accreditation

(1) A person who knowingly or recklessly gives false information to the TF authority in an application for accreditation commits an offence and is liable on conviction to,—

(a) in the case of an individual, a maximum fine of $50,000:

(b) in the case of a body corporate, a maximum fine of $100,000.

(2) In this section, **application for accreditation** means—

(a) an application for accreditation under **section 22**:

(b) an application for reconsideration under **section 27**:

(c) an application for renewal of accreditation under **section 29**:

(d) an application for provisional accreditation under **section 30**:

(e) any communication with the authority relating to an application in **paragraphs (a) to (d)**, ~~whether made before or after the application is submitted~~ whenever the communication is made.

97 Offence to fail to give key information or specified information in application for accreditation

(1) A person who makes an application for accreditation and who fails without reasonable excuse to give the TF authority key information or specified information in the application commits an offence and is liable on conviction to,—

(a) in the case of an individual, a maximum fine of $10,000:

(b) in the case of a body corporate, a maximum fine of $20,000.

(2) In this section and **section 98**,—

application for accreditation means—

(a) an application for accreditation under **section 22**:

(b) an application for reconsideration under **section 27**:

(c) an application for renewal of accreditation under **section 29**:

(d) an application for provisional accreditation under **section 30**:

(e) any communication with the authority relating to an application in **paragraphs (a) to (d)**, ~~whether made before or after the application is submitted~~ whenever the communication is made.

key information means the information referred to in **section 23(1)(b)(i)**

specified information means the information listed in **section 24(1)**.

98 Offence to fail to tell TF authority of change to key information or specified information

(1) A person who ~~has made~~ makes an application for accreditation and who fails without reasonable excuse to tell the TF authority of a~~ny~~ change to key information or specified information, as required by **section 31**, commits an offence and is liable on conviction to,—

(a) in the case of an individual, a maximum fine of $10,000:

(b) in the case of a body corporate, a maximum fine of $20,000.

(2) A TF provider that fails without reasonable excuse to tell the TF authority of any change to key information or specified information, as required by **section 31**, commits an offence and is liable on conviction to,—

(a) in the case of an individual, a maximum fine of $10,000:

(b) in the case of a body corporate, a maximum fine of $20,000.

99 Offence to obstruct TF authority

A person who, without reasonable excuse, obstructs the TF authority when it is carrying out its functions or exercising its powers commits an offence and is liable on conviction to,—

(a) in the case of an individual, a maximum fine of $10,000:

(b) in the case of a body corporate, a maximum fine of $20,000.

Part 7
Regulations, ~~secrecy,~~ immunity from civil liability, and reviews

Regulations

100 Regulations

(1) The Governor-General may, on the recommendation of the Minister, by Order in Council, make regulations for 1 or both of the following purposes:

(a) providing for anything this Act says may or must be provided for by regulations:

(b) providing for anything incidental that is necessary for carrying out, or giving full effect to, this Act.

(2) The TF board may recommend draft regulations to the Minister.

(3) Before regulations are made under this section, the Minister must consult the Office of the Privacy Commissioner.

(4) Regulations made under this section are secondary legislation (*see* Part 3 of the Legislation Act 2019 for publication requirements).

Secrecy

101 Members and staff of TF board and TF authority, members of Māori Advisory Group, and members of advisory committees to maintain secrecy

(1) The members of the TF board, members of the TF authority, members of the Māori Advisory Group, members of any advisory committee, and staff of the board or the authority (whether they are public service employees or not) must maintain secrecy in respect of all matters that come to their knowledge in carrying out their functions under this Act.

(2) Despite **subsection (1)**, the members of the board (acting together as the board) and the members of the authority (acting together as the authority) may—

(a) disclose any matters that in their opinion ought to be disclosed for the purpose of giving effect to this Act:

(b) disclose to the Minister or the chief executive of the responsible department matters necessary to be disclosed to them in order for them to carry out their functions under this Act.

(3) Except where necessary for the purposes of a referral under **section 71** or prosecuting an offence under this Act, **subsection (2)** does not extend to—

(a) any disclosure that might prejudice—

(i) any interest protected by section 7 of the Official Information Act 1982:

(ii) the prevention, investigation, or detection of offences:

(b) any matter that might involve the disclosure of the deliberations of Cabinet.

(4) Nothing in this section limits any obligations under the Privacy Act 2020 or the Official Information Act 1982, or any power to gather information under an enactment.

Compare: 2020 No 31 s 206

Immunity from civil liability

102 Immunity for members and staff of TF board and TF authority, members of Māori Advisory Group, and members of advisory committees

(1) The members of the TF board, members of the TF authority, members of the Māori Advisory Group, members of any advisory committee, and staff of the board or the authority (whether they are public service employees or not) are immune from liability in civil proceedings for good-faith actions or omissions when carrying out or intending to carry out their functions.

~~(2) *See also* section 6 of the Crown Proceedings Act 1950.~~

~~Compare: 2020 No 40 s 104~~

102 Immunity for members and staff of TF board and TF authority, members of Māori Advisory Group, and members of advisory committees who are not public service employees

(1) This section applies to a member of the TF board, the TF authority, the Māori Advisory Group, and any advisory committee, and a staff member of the board or the authority, who is not a public service employee.

(2) Section 104 of the Public Service Act 2020 applies to a person listed in **subsection (1)** as if they were a public service employee.

103 Immunity for TF providers for actions of users

(1) A TF provider is immune from liability in civil proceedings for ~~claims~~ a claim that a user, when using an accredited digital identity service provided by the TF provider, has caused harm or damage to an individual or organisation or has themselves suffered harm or damage.

(2) However, **subsection (1)** does not apply ~~if an act or omission by a TF provider relating to the alleged harm or damage constitutes bad faith or gross negligence.~~—

(a) if an act or omission by a TF provider relating to the alleged harm or damage constitutes bad faith or gross negligence:

(b) to proceedings arising from a complaint under the Privacy Act 2020.

(3) In this section,—

TF provider means ~~a~~ the TF provider and (as relevant) their ~~or its~~ officers and those involved in the management of, employed by, or contracted by, the TF provider

using an accredited digital identity service means—

(a) using an accredited service for a transaction with a relying party; or

(b) communicating or interacting with a TF provider in relation to the provision of that service to the user.

Compare: 2012 No 123 s 65(5); 2012 No 124 s 20(3)

Reviews

104 Review of TF board's operation

(1) A review of the TF board's operation must be commenced by its responsible department as soon as practicable after the second anniversary of the commencement of **section 42**.

(2) As soon as practicable after that date, the Minister must set a date for completion of the review.

(3) The review must include—

(a) an assessment of the effectiveness of the board in carrying out its functions; and

(b) an assessment of the viability of other models for carrying out the board's functions.; and

(c) an assessment of how other models might better—

(i) ensure the privacy and security of user information (including Crown-held data) and protect it from unauthorised use; and

(ii) provide opportunities for Māori engagement in the trust framework.

(4) The review may include other matters as the department considers appropriate.

(5) The Minister must present a copy of the review to the House of Representatives as soon as practicable after receiving it from the department.

105 Review of complaints process and ~~alternative~~ dispute resolution scheme

(1) A first review of the complaints process and ~~alternative~~ dispute resolution scheme operated by the TF authority under this Act (including if this is done by persons or organisations under **section 75(3)**) must be undertaken by the TF board as soon as practicable after the second anniversary of,—

(a) in the case of the complaints process, the commencement of **section 68**:

(b) in the case of the ~~alternative~~ dispute resolution scheme, the commencement of **section 75**.

(2) Subsequent reviews of that process and scheme must be undertaken by the authority at 5-yearly intervals from the date on which the first review (in each case) is commenced.

Schedule
Transitional, savings, and related provisions

s 6

Part 1
Provisions relating to this Act as enacted

There are no transitional, savings, or related provisions relating to this Act as enacted.

Legislative history

29 September 2021	Introduction (Bill 78–1)
19 October 2021	First reading and referral to Economic Development, Science and Innovation Committee

Wellington, New Zealand:
Published under the authority of the House of Representatives—2022