Digital Identity Services Trust Framework Bill

Government Bill

Explanatory note

General policy statement

The Digital Identity Services Trust Framework Bill (the **Bill**) establishes a legal framework for the provision of secure and trusted digital identity services for individuals and organisations.

The policy objectives of the Bill are to—

- help drive consistency, trust, and efficiency in the provision of digital identity services:
- support the development of interoperable digital identity services:
- provide people with more control over their personal information and how it is used:
- enable the user-authorised sharing of personal and organisational information digitally to access public and private sector services.

How Bill will achieve policy objectives

To achieve these objectives, the Bill will establish a trust framework (consisting of primary legislation, a set of rules (the **TF rules**), and regulations) for the provision of user-authorised digital identity services in New Zealand (the **trust framework**). It also establishes requirements for accrediting digital identity service providers against those rules. Specific provisions in the Bill will ensure that te ao Māori approaches to identity are considered in trust framework governance and decision making.

Why this approach is needed

Currently, New Zealand lacks consistency in the way personal and organisational information is shared, stored, and used in a digital identity environment. This has led to inconsistencies and inefficiencies in how this information is handled, undermining

trust and confidence in the digital identity system for individuals, government agencies, and the private sector.

This impedes people's ability to access services online, undermines their expectations regarding privacy and security, stifles innovation in service provision, and hinders the realisation of the significant social and economic benefits digital identity services could provide.

Specific measures to achieve policy objectives

Opt-in accreditation scheme for digital identity service providers

The Bill establishes an opt-in accreditation scheme that establishes minimum requirements for handling personal and organisational information that accredited digital identity service providers (**TF providers**) must comply with. Users or consumers of digital identity services will not have to be accredited to use accredited digital identity services.

Opt-in accreditation will allow the digital identity service providers to upgrade their systems to comply with the TF rules at their own pace, before applying for accreditation. The Bill allows accredited providers to use approved trust marks to show their compliance with the TF rules.

These service providers are likely to be organisations such as government departments, existing identity service providers, and other private sector organisations that verify identity. The Bill does not override any obligations under the Privacy Act 2020.

Trust Framework Board

The Bill creates a governance board (the **TF board**), which will undertake education, publish guidance, and monitor the performance and effectiveness of the trust framework. The TF board will also have responsibility for recommending draft TF rules to the Minister and undertaking consultation on the rules before it does so. The TF board members must include people with expert knowledge of te ao Māori approaches to identity, technology, and identity data management.

The TF rules, set by the Minister or by regulation, will support the sustainability of the trust framework by allowing it to be flexible to adapt to changes in the approach to how digital identity services are delivered. To enable transparency of the requirements providers will be accredited against, the rules for the trust framework will be published and accessible to the public.

Before recommending changes to the TF rules, the TF board must consult—

- the Office of the Privacy Commissioner:
- people or groups outside the board with expert knowledge of te ao Māori approaches to identity:
- TF providers:
- people or groups that are likely to have an interest in the TF rules:

- any other individual or organisation that the board considers should be consulted.

In addition, committees of advisers may be established and a Māori Advisory Group will be established to advise the TF board on Māori interests and knowledge as these relate to the trust framework. This will ensure that a wide range of views is considered in the development of the rules.

Trust Framework Authority

To ensure that the TF rules are enforced and to protect the security and privacy of trust framework users, the Bill allows for the establishment of an authority (the **TF authority**) that will be responsible for making decisions on applications for accreditation and renewal of accreditation, conducting investigations following complaints or on its own initiative, and granting remedies for breaches. The authority will also be responsible for maintaining a register of accredited providers.

Complaints and penalties

To protect the integrity of the trust framework and to enforce compliance with the TF rules, the Bill allows for people to submit complaints to the TF authority if they believe a TF provider has breached 1 or more of the TF rules, the regulations, terms of use of trust marks, or the Act. If the TF authority finds that a breach has occurred, it can grant remedies, such as publishing a public warning, suspending a TF provider's accreditation, or cancelling their accreditation. The Bill also contains offences for activities that threaten the integrity of the trust framework, such as falsifying accreditation.

Departmental disclosure statement

The Department of Internal Affairs is required to prepare a disclosure statement to assist with the scrutiny of this Bill. The disclosure statement provides access to information about the policy development of the Bill and identifies any significant or unusual legislative features of the Bill.

A copy of the statement can be found at http://legislation.govt.nz/disclosure.aspx?type=bill&subtype=government&year=2021&no=78

Regulatory impact assessment

The Department of Internal Affairs produced regulatory impact assessments in July 2020, February 2021, and August 2021 to help inform the main policy decisions taken by the Government relating to the contents of this Bill.

Copies of these regulatory impact assessments can be found at—

- https://www.dia.govt.nz/diawebsite.nsf/Files/Proactive-releases/$file/Combined-Digital-Identity-Proactive-Release.pdf (July 2020)
- https://www.dia.govt.nz/diawebsite.nsf/Files/Proactive-releases/$file/proactive-release-digital-identity-trust-framework.pdf (February 2021)

- https://www.dia.govt.nz/Resource-material-Regulatory-Impact-Statements-Index#digital (August 2021)
- http://www.treasury.govt.nz/publications/informationreleases/ria

Clause by clause analysis

Clause 1 is the Title clause.

Clause 2 is the commencement clause. The Bill will come into force on the earlier of 1 or more dates set by Order in Council or 1 January 2024.

Part 1
Preliminary provisions

Clause 3 says that the purposes of the Bill are to establish a legal framework for the provision of secure and trusted digital identity services for individuals and organisations and to establish governance and accreditation functions that are transparent and incorporate te ao Māori approaches to identity.

Clause 4 gives an overview of the Bill.

Clause 5 contains definitions of terms used in the Bill.

Clause 6 is the operative clause for transitional, savings, and related provisions. However, the Bill does not have any of these types of provisions and therefore the *Schedule* referred to in *clause 6* is empty and is inserted for future use only.

Clause 7 says that the Bill binds the Crown.

Part 2
Digital identity services trust framework

Clause 8 contains the definition of digital identity services trust framework. This is the legal framework that will be established by the Bill to regulate the provision of digital identity services for transactions between individuals and organisations. *Clause 8* also sets out the main components of the trust framework. These include a governance board established under *clause 42* (the **TF board**) and an authority established under *clause 57* (the **TF authority**). A major component of the regulatory framework will be the rules made under *clause 17* (the **TF rules**). The board will recommend draft TF rules to the Minister and the authority will enforce the rules.

Clause 9 contains the definition of digital identity service, which is 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. *Clause 9* also gives some examples of digital identity services.

Clause 10 contains the definition of the participants in the trust framework, which are—

- users of digital identity services:

- accredited providers of digital identity services (**TF providers**):
- relying parties.

User is defined in the Bill as an individual who shares personal or organisational information, in a transaction with a relying party, through 1 or more accredited digital identity services. A user can do so for themselves or on behalf of another individual or an organisation. TF provider is defined in the Bill as a digital identity service provider that is accredited by the TF authority to provide 1 or more accredited digital identity services. Relying party is defined in the Bill as an individual or organisation that relies on personal or organisational information shared, in a transaction with a user, through 1 or more accredited digital identity services.

A single individual or organisation can be 1 or more of the participants in a single transaction.

Clause 11 prohibits TF providers from collecting, using, sharing, or otherwise dealing with personal or organisational information unless—

- 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
- they do so in accordance with the TF rules.

Relevant to dealing with personal information, *clause 11* also notes that *clause 16* provides that nothing in the Bill overrides the Privacy Act 2020. Personal information is defined in the Bill as having the meaning given in section 7(1) of that Act.

Clause 12 requires trust marks to be approved by the TF board for use by TF providers to identify both themselves as being accredited TF providers and the accredited services provided by them as being accredited services. The TF authority must set the terms of use of the trust marks and must publish these on the Internet. TF providers must comply with the terms of use of trust marks.

It is an offence to misuse a trust mark (*see clause 95*).

Digital identity services outside trust framework

Clause 13 allows a TF provider to provide both accredited services and digital identity services that are not accredited. *Clause 14* allows individuals and organisations to provide digital identity services even if neither they nor the service are accredited. The effect of both of these clauses is to allow digital identity services to be provided in New Zealand outside of the trust framework.

Relationship with other Acts

Clause 15 says that nothing in the Bill limits or otherwise affects the Electronic Identity Verification Act 2012 or the Identity Information Confirmation Act 2012.

Clause 16 says that nothing in the Bill overrides the Privacy Act 2020.

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

TF rules

Clause 17 allows for the making of the TF rules that will regulate the operation and administration of the trust framework. The rules can be made by Order in Council or by the Minister. The TF board may recommend draft TF rules to the Minister but rules may be made only if the Minister is satisfied that the requirements for consultation under *clause 20* have been met.

Clause 18 says that the TF rules apply to TF providers and the accredited services they provide. TF rules may apply to TF providers only to the extent relevant to their provision of accredited services. (*See clause 13*, which allows a TF provider to provide both accredited services and digital identity services that are not accredited.)

Clause 19 relates to the content of the TF rules. The rules must identify the types of digital identity services that may be accredited services. The rules also must set minimum requirements in the following 5 areas:

- identification management:
- privacy and confidentiality:
- security and risk:
- information and data management:
- sharing and facilitation.

The TF rules may set other requirements for periodic self-assessment and reporting by TF providers for compliance with the rules, complaints and dispute resolution processes to be operated by TF providers, and other matters. The rules may set different minimum or other requirements for different types of providers and services.

The rules must be consistent with the Privacy Act 2020.

Clause 20 requires the TF board to consult and invite submissions on the proposed content of draft TF rules before recommending these to the Minister. Consultation is required with—

- the Office of the Privacy Commissioner; and
- people or groups outside the board with expert knowledge of te ao Māori approaches to identity; and
- TF providers; and
- people or groups that are likely to have an interest in the TF rules; and
- any other individual or organisation that the board considers should be consulted.

However, the Minister has to decide which people or groups the board must consult to satisfy the second requirement. When doing so, the Minister must take into account the particular subject matter of the proposed content of rules. The Minister must also

consult the Ministers with portfolio responsibilities that relate to Māori development and Māori-Crown relations before making that decision.

The Minister may decide that consultation under this clause 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.

Clause 21 requires the TF board to report to the Minister on the consultation it has undertaken before recommending draft TF rules to the Minister.

Accreditation

Clause 22 relates to applications for accreditation. A digital identity service provider can apply to be accredited as a TF provider. That application must be accompanied by an application to have at least 1 digital identity service provided by them accredited as an accredited service. (*See clause 25(2)*, which says a provider may be accredited only if they will be providing 1 or more accredited services and a service may be accredited only if it will be provided by a TF provider.) A TF provider may also apply under *clause 22* to have a digital identity service that is currently provided by them, but that is not an accredited service, accredited as an accredited service. It is an offence to misrepresent a provider to be a TF provider when they are not or a service to be an accredited service when it is not (*see clause 94*).

Clauses 23 and 24 set out requirements for the contents of applications for accreditation. Two key aspects of applications are key information and specified information. Key information will be prescribed by regulations. It can differ for different types of applications, providers, or services. Specified information is listed in *clause 24*. Specified information is any of the information listed about the applicant and those involved in their management or their employees or contractors.

It is an offence to fail to give key information or specified information in an application (*see clause 97*) or to give false information in an application for accreditation (*see clause 96*).

Clause 25 relates to assessment of applications by the TF authority. An application must meet the requirements of *clauses 22 to 24* and any requirements set by regulations. An application may be granted in full or in part, but a provider may be accredited only if they will be providing 1 or more accredited services and a service may be accredited only if it will be provided by a TF provider. An application that meets the requirements of *clause 25* 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—

- the security, privacy, confidentiality, or safety of the information of any trust framework participants:
- the integrity or reputation of the trust framework.

Clause 26 sets out requirements for the notice of the TF authority's decision.

Clause 27 allows for an applicant to apply for a reconsideration of a decision declining an application or part of an application. When assessing an application for recon-

sideration, the TF authority must consider any new, or additional, relevant information provided by the applicant.

Clause 28 sets out circumstances in which the accreditation of a TF provider or an accredited service ends. The end date is the earliest of the following:

- the date the TF provider tells the TF authority is the date on which they no longer wish—
  - to remain accredited as a TF provider; or
  - for the service to continue as an accredited service:
- the date on which the accreditation of the provider or service is cancelled under *clause 82(e)* or *88*:
- the applicable expiry date (which will be set by regulations):
- the date on which the accreditation of any service provided by a TF provider ceases because the accreditation of the TF provider has ended:
- the date on which the accreditation of the TF provider ends because they have not provided at least 1 accredited service in a 12-month period or a longer period agreed by the authority (with 2 specified exceptions).

Clause 29 relates to renewal of accreditation. If a renewal application is made before the accreditation of a provider or service expires, the accreditation continues to have effect until the renewal application is decided by the TF authority. If a renewal application is made after the expiry of the accreditation of a provider or service, a fresh application for accreditation is required.

Clause 30 relates to provisional accreditation of a provider or service to allow the provider to develop a digital identity service before applying for full accreditation. Provisional accreditation is for 12 months or a longer period agreed by the TF authority. A provider or service with provisional accreditation is not a TF provider or an accredited service for the purposes of the Bill.

Clause 31 imposes an obligation on an applicant for accreditation and a TF provider to tell the TF authority of any changes to key information or specified information. For applicants (whether currently a TF provider or not) this obligation continues after they make an application until their application is decided by the authority. For TF providers, following the accreditation of themselves or a service they provide, the obligation continues from the date of the authority's decision and for the period during which they or the service remain accredited. It is an offence to fail to tell the authority of changes to key information or specified information (*see clause 98*).

TF register

Clauses 32 to 37 provide for there to be a register of TF providers and accredited digital identity services (the **TF register**).

Clause 32 requires the TF authority to set up and maintain the TF register.

Clause 33 sets out the purposes of the TF register, which broadly are to—

- enable the public to check the accreditation status of individuals and organisations and any digital identity services offered by them; and
- help the public choose suitable TF providers from the list of providers; and
- help the TF authority carry out its administrative, disciplinary, and other functions.

The register is to be kept on a publicly accessible Internet site (*clause 34*) and contain information about every TF provider (*clause 35*), including—

- the TF provider's name, a unique identifier assigned to them, and the status and history of their accreditation as a TF provider; and
- the accredited services they offer and the status and history of those services' accreditation.

Clause 36 provides for the TF authority to amend the TF register to keep it updated and correct any errors.

Clause 37 enables members of the public to search the TF register, and copy parts of it, for the purposes set out in *clause 33*.

Third party assessors

Clause 38 allows the TF authority to certify persons outside of the authority to carry out 1 or more of its functions relating to accreditation of providers or services if regulations allow for this to happen. Certification must be done in accordance with the regulations. The regulations may prescribe circumstances in which the authority may suspend or cancel the certification of third party assessors. *Clause 38* also says that third party assessors do not have, and nor may the authority delegate to them, its powers under *clauses 60 and 61*.

Clause 39 relates to the accountability of third party assessors and provides immunity for them as if they were public service employees. For accountability, *clause 39* says that the Ombudsmen Act 1975 and the Official Information Act 1982 apply to third party assessors as if they were an organisation named in Schedule 1 of the Ombudsmen Act 1975.

Clause 40 allows regulations to prescribe record-keeping and reporting requirements for third party assessors.

Record keeping and reporting by TF providers

Clause 41 requires TF providers to keep records of their activities and provide the records to the TF authority. The regulations will set out the details of what information must be kept, in what form, and for how long.

Part 4
TF board

Clause 42 establishes the TF board. *Clause 42* also identifies clauses in the Bill 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 through the board. These are *clauses 20(1)(b), 46(2)(a) and (b), and 50 to 54*, which relate to, respectively, 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.

Clause 43 says the Prime Minister must nominate a responsible department for the TF board. The board will sit within that department and is accountable to its chief executive. The annual report of the department must include a description of the board's activities for the relevant period.

TF board's functions and powers

Clause 44 sets out the functions of the TF board.

Clause 45 gives the TF board all the powers that are reasonably necessary to carry out its functions to the extent consistent with the board operating within its responsible department.

TF board members

Clause 46 sets out requirements for the appointment of TF board members by the chief executive of the board's responsible department. The members may include public service employees and individuals outside the public service. The chief executive must ensure that—

- members of the board include people with expert knowledge of te ao Māori approaches to identity; and
- members of the board include people with expert knowledge of the principles of the Treaty of Waitangi (te Tiriti o Waitangi); and
- the members of the board collectively possess sufficient knowledge and expertise in working with technology and identity data management, including—
    - ethical use of digital information; and
    - protecting the privacy and confidentiality of digital information; and
    - secure handling of digital information; and
    - engagement with Māori.

The chief executive must also ensure that the board has sufficient members to carry out its functions in a timely and efficient manner.

Clause 47 says that only TF board members who are public service employees have voting rights.

Clause 48 says that 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.

Clause 49 provides for the remuneration of TF board members.

Māori Advisory Group

Clause 50 establishes the Māori Advisory Group to advise the TF board.

Clause 51 sets out requirements for the appointment of members and a chairperson of the Māori Advisory Group. The Minister must appoint only people who, in the Minister's opinion, have the appropriate knowledge, skills, and experience to assist the Māori Advisory Group to perform its role. Before making any appointments, the Minister must consult the Ministers with portfolio responsibilities that relate to Māori development and Māori-Crown relations.

Clause 52 describes the role of the Māori Advisory Group, which is to advise the TF board on Māori interests and knowledge as they relate to the operation of the trust framework. 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. 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.

Clause 52 also requires the TF board and the Māori Advisory Group, acting jointly, to prepare an engagement policy, setting out how they will work together, and the terms of reference for the group. The Māori Advisory Group must advise the board in accordance with the engagement policy and the terms of reference. Both of these must be reviewed at least every 3 years.

Clause 53 applies certain provisions of the Crown Entities Act 2004 to members of the Māori Advisory Group as if they were members of the board of a Crown agent. *Clause 53* also provides for the remuneration of members of the Māori Advisory Group.

Clause 54 says that the Minister may give written notice to a member of the Māori Advisory Group removing them from the group if they become bankrupt or neglect their duty, or for misconduct.

Committees of advisers

Clause 55 sets out requirements for the appointment of committees of advisers by the TF board and provides for the remuneration of committee members.

Clause 56 says that 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

Clause 57 establishes the TF authority.

Clause 58 says the Prime Minister must nominate a responsible department for the TF authority. The authority will sit within that department and is accountable to its chief executive. However, the authority must act independently in respect of its enforce-

ment functions under *Part 6*. The annual report of the department must include a description of the authority's activities for the relevant period.

TF authority's functions and powers

Clause 59 sets out the functions of the TF authority.

Clause 60 gives the TF authority all the powers that are reasonably necessary to carry out its functions to the extent consistent with the authority operating within its responsible department.

Clause 61 gives the TF authority a power to require information or documents from any individual or organisation for specified purposes. The purposes are—

- assessing or investigating a complaint under *Part 6*:
- investigating compliance by a TF provider with the TF rules, the regulations, the terms of use of trust marks, or provisions of the Bill:
- investigating compliance by a TF provider with the TF rules relating to an accredited service provided by them:
- assessing compliance with a compliance order issued under *clause 82*:
- assessing whether a suspension of accreditation should be lifted.

An individual or organisation need not comply if—

- the information or document would be privileged in a court:
- 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).

The authority must not release any information or document received by it under *clause 61* that is commercially sensitive, unless the release is required by an enactment.

Clause 62 allows the TF authority to extend time to provide information or documents under *clause 61*.

TF authority members

Clause 63 sets out requirements for the appointment of TF authority members by the chief executive of the authority's responsible department. The members may include public service employees and individuals outside the public service. The chief executive must ensure that the authority has—

- members who collectively possess the appropriate skills and experience to carry out its functions; and
- sufficient members to carry out its functions in a timely and efficient manner.

Clause 64 says that the chief executive may give written notice to a TF authority member removing them from the authority if they become bankrupt or neglect their duty, or for misconduct.

Clause 65 provides for the remuneration of TF authority members.

Part 6
Complaints and offences

Clause 66 says that the purpose of *Part 6* is to promote confidence in the trust framework by establishing processes for dealing with complaints.

Clause 67 lists principles to guide the TF authority when carrying out its functions under *Part 6* except when granting remedies or prosecuting offences.

Complaints

Clause 68 allows any person to make a complaint if they believe there has been a breach by a TF provider. A breach is defined as—

- 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 the Bill:
- a failure by a TF provider to provide an accredited service in accordance with the TF rules.

Clause 69 sets out requirements for making a complaint.

Clause 70 sets out requirements for the TF authority when dealing with complaints.

Clause 71 allows the TF authority to refer all or part of a complaint to another office holder (for example, the Privacy Commissioner) and sets out requirements for doing so.

Clause 72 allows the TF authority not to consider a complaint further in specified circumstances.

Preliminary assessment of complaints

Clause 73 sets out requirements and procedures for the TF authority when making a preliminary assessment of a complaint. Except as provided in the Bill, the authority may regulate its procedure as it considers appropriate.

Clause 74 sets out requirements for the TF authority when giving notice of its preliminary assessment to the complainant and the TF provider concerned.

Alternative dispute resolution scheme

Clause 75 allows the TF authority to recommend an alternative dispute resolution scheme to the Minister. The scheme must not deal with specified types of disputes, for example, employment disputes.

Clause 76 allows the Minister to approve an alternative dispute resolution scheme. However, first the Minister must be satisfied that—

- it provides a means of resolving complaints that is consistent with the principles listed in *clause 67*; and
- it meets any requirements set out in the regulations.

Investigations by TF authority

Clause 77 allows the TF authority to commence an investigation—

- following a preliminary assessment that a breach that was the subject of a complaint appears to have occurred:
- on its own initiative, into any matter that could be the subject of a complaint under *Part 6*.

Clause 78 sets the first step for commencing an investigation, which is notifying the TF provider concerned.

Clause 79 sets out requirements and procedures for conducting investigations. *Clause 79* also allows the TF authority to take no further action on a complaint or matter if it is satisfied that any of the circumstances in *clause 72(1)* apply.

Clause 80 allows the TF authority to regulate its own procedure for investigations consistent with the Bill and any regulations.

Clause 81 relates to the finding by the TF authority at the conclusion of an investigation. If the 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. The authority may also grant 1 or more of the remedies in *clause 82*, but must first give the TF provider an opportunity to make submissions on the issue of remedies.

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.

Remedies

Clause 82 lists the remedies available to the TF authority following a finding that a breach has occurred. These are—

- issuing a private or public warning:
- requiring the provider to comply with additional record-keeping or reporting requirements either for a specified period or indefinitely:
- issuing a compliance order:
- suspending the provider's accreditation or the accreditation of the relevant service provided by them until they take specified steps:
- cancelling the provider's accreditation or the accreditation of the relevant service provided by them.

Clauses 83 to 93 set out requirements for and contain further details relating to those remedies.

Public warnings

Clause 83 sets out requirements for the TF authority when considering whether to issue a public warning.

Compliance orders

Clauses 84 to 89 set out requirements for the TF authority when considering whether to issue a compliance order, requirements for the form of an order, and procedures following the issue of an order. A TF provider may elect to forfeit accreditation after receiving a draft order or an order (*see clause 88*). The authority may vary or cancel an order if there has been an error of fact or law (*see clause 89*).

Suspension or cancellation of accreditation following finding of breach

Clauses 90 to 92 set out requirements for suspending or cancelling accreditation following the finding of a breach by a TF provider.

Suspension or cancellation of accreditation for other reasons

Clause 93 sets out requirements for suspending or cancelling accreditation for reasons other than the finding of a breach by a TF provider.

Offences

Clause 94 makes it an offence to knowingly or recklessly misrepresent a digital identity service provider to be a TF provider or a digital identity service to be an accredited service.

Clause 95 makes it an offence to misuse a trust mark in a manner that is contrary to the terms of use set by the TF authority.

Clause 96 makes it an offence to knowingly or recklessly give false information to the TF authority in an application for accreditation.

Clause 97 makes it an offence to fail to give key information or specified information in an application for accreditation.

Clause 98 makes it an offence to fail to tell the TF authority of a change to key information or specified information.

Clause 99 makes it an offence to obstruct the TF authority.

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

Regulations

Clause 100 contains the regulation-making powers. The TF board may recommend draft regulations to the Minister. Before regulations are made, the Minister must consult the Office of the Privacy Commissioner.

Secrecy

Clause 101 says that 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. Some exceptions are provided, for example, nothing in *clause 101* limits any obligations under the Privacy Act 2020 or the Official Information Act 1982, or any power to gather information under an enactment.

Immunity from civil liability

Clause 102 says that 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.

Clause 103 says that a TF provider is immune from liability in civil proceedings for claims that a user, when using an accredited digital identity service provided by the TF provider, has caused harm or damage to any individual or organisation or has themselves suffered harm or damage. However, a TF provider is not protected if they (or those involved in their management or their employees or contractors) act in a manner, relating to the alleged harm or damage, that constitutes bad faith or gross negligence.

Reviews

Clause 104 provides for a review of the TF board's operation as soon as practicable after the second anniversary of the commencement of *clause 42*, which establishes the board.

Clause 105 provides for regular reviews of the complaints process and alternative dispute resolution process operated by the TF authority, beginning as soon as practicable after the second anniversary of the commencement of *clauses 68 and 75*, respectively, and thereafter at 5-yearly intervals.

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**.

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 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,—

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)**)

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) 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 **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 that include minimum requirements for accredited providers when providing accredited services:

(d) approved trust 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 rules to the Minister (*see* **section 17**), and the authority is responsible for enforcing the rules (*see* **Part 6**).

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.

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.

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

12 Trust marks

(1) TF providers may use trust 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 approve the form and style of trust marks and may approve different trust 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 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 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

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.

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**).

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 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.

(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 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 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:

(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)**, 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 mark or trust marks; and

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

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.

(5) If **subsection (4)** applies, the 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 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, the provider must make a fresh application for accreditation under **section 22**.

(4) An 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.

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**,—

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 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 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 third party assessors

(1) The TF authority may certify third party assessors 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 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.

(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:

(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.

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 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

(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.

(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 procedures and tests for TF providers to demonstrate their compliance with the TF rules:

(e) receive and assess complaints:

(f) investigate breaches of the TF rules, the regulations, the terms of use of trust 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—

(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:

(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:

(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—

(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

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**.

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 further if it considers—

(a) the complaint does not meet the requirements of **section 69**; 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 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 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 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, the authority may, when making a preliminary assessment, regulate its procedure as it considers appropriate.

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 dispute resolution scheme

75 Alternative dispute resolution scheme

(1) The TF authority may, in accordance with any requirements and criteria prescribed in the regulations, recommend an alternative 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.

76 Ministerial approval of alternative dispute resolution scheme

The Minister may approve an alternative 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; 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) 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 considers appropriate 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 pro-

vider. 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

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.

Public warnings

83 Public warnings

(1) The TF authority may issue a public warning under **section 82(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.

Compliance orders

84 Issuing compliance order

(1) Before issuing a compliance order under **section 82(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 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.

(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 it under **section 82(d)**:

(b) because the authority is satisfied that a TF provider has failed to comply with a compliance order, including because it has not received notice under **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(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(e)**:

(b) because the authority is satisfied that a TF provider has failed to comply with a compliance order, including because it has not received notice under **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 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.

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 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 mark

A person who knowingly or recklessly uses a trust 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.

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

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 an application for accreditation and who 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.

(2) A TF provider that fails without reasonable excuse to tell the 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

103 Immunity for TF providers for actions of users

(1) A TF provider is immune from liability in civil proceedings for claims 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.

(3) In this section,—

TF provider means a 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.

(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 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 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.

Wellington, New Zealand:
Published under the authority of the New Zealand Government—2021