Australian Government
Digital Transformation Agency

Fraud Control Requirements

Trusted Digital Identity Framework
February 2018, version 1.0

dta

Digital Transformation Agency

Licence

Use of the Coat of Arms

The terms under which the Coat of Arms can be used are detailed on the It's an Honour website (http://www.itsanhonour.gov.au)

Contact us

Digital Transformation Agency is committed to providing web accessible content wherever possible. If you are having difficulties with accessing this document, or have questions or comments regarding this document please email the Director, Trusted Digital Identity Framework at identity@dta.gov.au.

Document Management

This document has been reviewed and endorsed by the following groups.

Endorsement

Group	Endorsement date
Director, Trusted Digital Identity Framework	Jan 2018
Commonwealth GovPass Design Authority	Feb 2018

Change log

Version	Date	Author	Description of the changes
0.01	Sept 2017	PH	Initial version
0.02	Jan 2018	PH	Feedback incorporated from public consultation
1.0	Feb 2018		Endorsed by the Commonwealth GovPass Authority

Conventions

The following conventions[1] are used in this document.

- **MUST** – means an absolute requirement of this document.
- **MUST NOT** means an absolute prohibition of this document.
- **SHOULD** means that there may exist valid reasons in particular circumstances to ignore a particular item of this document, but the full implications need to be understood and before choosing a different course.
- **MAY** – means truly optional.

[1] These conventions are taken from Request for Comments 2119 (RFC2119) – Keywords for use in RFCs to indicate requirements levels

Contents

1 Introduction

The Digital Transformation Agency (DTA), in collaboration with other government agencies and key private sector bodies, is leading the development of a national federated identity 'eco-system' (the 'identity federation'). Implementation and operation of the identity federation is underpinned by the Trusted Digital Identity Framework (TDIF). This document should be read in conjunction with the *Trust Framework: Overview and Glossary*, which provides a high-level overview of the TDIF including its scope and objectives, the relationship between its various documents and the definition of key terms.

This document lists the TDIF Fraud Control Requirements (FCRs) which are applicable to an Applicant's identity service but not its broader organisational or agency activity. For example, the FCRs apply to an organisation or agency's identity service if it is accredited as an Identity Service Provider but it does not apply to the other functions such HR, finance, or other business services.

This document comprises two parts:

- Part one - Fraud control requirements that Applicants are required to implement for their identity service.
- Part two - Fraud control guidance which Applicants can use to satisfy the requirements of part one.

The intended audience for this document includes:

- Accredited Providers.
- Applicants.
- Authorised Assessors.
- Relying Parties.
- Trust Framework Accreditation Authority.

2 Part one: Fraud control requirements

2.1 Fraud control responsibilities

Applicants **MUST**:

- Conduct fraud risk assessments annually, when there is a substantial change in their structure, functions or activities AND when there are significant changes in technological capabilities which impacts on the service or services provided. Further information on Risks that **MUST** be considered are listed at *Annex A: Potential Sources of Risk*, in the *Risk Management Requirements*.
- Develop a fraud control plan that clearly delineates between process, architecture and technology-based risks as soon as practicable after conducting a risk assessment. This plan **MUST** include an appropriate system of internal controls over internal processes, technological processes, technologies, victim support and access to sensitive data to reduce the scope for internal fraud.
- Ensure that fraud control arrangements identified in the fraud control plan are implemented as soon as practicable.
- Develop governance that promotes the proper use and management of identity and related information, functions and the financial sustainability of their processes.
- Store and protect information in accordance with the *Privacy Requirements* and the *Protective Security Requirements*.
- Establish and maintain an appropriate system of fraud risk oversight and management for each Trust Framework-related service as described in the *Risk Management Requirements*.
- Provide an appropriate system of internal controls, including implementation measures directed at Personnel and third-party service providers in accordance with the *Privacy Requirements* and the *Protective Security Requirements*.
- Not improperly use their position or the information they have access to.

2.2 Fraud prevention

Applicants **MUST**:

- Have in place appropriate processes, technologies and mechanisms for preventing fraud, ensuring that:
    - They develop and deliver targeted fraud control training.
    - They document instructions and procedures to assist personnel and third-party providers to prevent, detect and deal with fraud in a Fraud Control Procedures Manual.
    - Personnel and third-party providers are made aware of what constitutes fraud for the Applicant service prior to commencing their roles.
    - The risk of fraud is taken into account in accordance with the Applicant's Fraud Risk Assessment and Fraud Control Plan.
    - Employ technologies to assist in the prevention of fraud.
    - Only employ trusted third-party service providers.
- Conduct vetting of personnel, third party providers and systems as described in the *Protective Security Requirements*.
- Monitor and limit as appropriate, Personnel and third-party provider access to sensitive user information as described in the *Protective Security Requirements*.

2.2.1 Aptitude and training

Applicants **MUST** ensure that all personnel and third-party service providers undertaking facial recognition and matching tasks have been completed and have passed:

- A range of facial recognition aptitude testing provided by recognised and reputable tertiary institutions recognised by the Trust Framework Accreditation Authority.
- Facial recognition and matching training and eLearning approved by the Department of Home Affairs (DOHA).

Applicants **MUST**:

- Ensure personnel and third-party providers primarily engaged in fraud control activities possess or attain relevant qualifications or training to effectively carry out their duties;
- Use fraud information gathered to update and tighten security and fraud control capabilities based on fraud incidents, investigations, reports and analytical data.

- Conduct performance testing and monitoring of technology supporting Trust Framework solutions.

Where a data breach as described in the *Privacy Requirements* occurs, the applicant **MUST** notify all data owners of the potential that their data may be used to commit fraud and assist potential victims to secure their digital identities and credentials.

2.3 Fraud detection

Fraud may be detected at a number of touchpoints throughout the identity life-cycle. The greatest opportunities to detect fraud arise during the initial enrolment of an individual with an Identity Service Provider (IdP), Credential Service Provider (CSP) or Attribute Provider, during authentications or transactions and through reporting by Relying Parties and Users

Applicants **MUST** have in place appropriate mechanisms for detecting incidents of fraud or suspected fraud, including a process for IdP personnel and users to report suspected fraud confidentially.

Applicants **SHOULD** undertake fraud monitoring activities based on available data. Information **SHOULD** be analysed by trained members of staff using rule based or diagnostic tools.

Where a suspected fraud incident is detected by or reported to an Applicant, it **MUST** be assessed, actioned and the appropriate stakeholders notified as soon as possible.

2.4 Fraud investigations

Applicants are responsible for investigating instances of fraud or suspected fraud against it including investigating disciplinary matters, unless the matter is referred to and accepted by the Australian Federal Police (AFP) or another law enforcement agency. Applicants **MAY** seek guidance on the criteria for serious and complex crimes from the AFP.

Applicants **MUST** ensure that they are aware of their fraud control roles and responsibilities as per these FRCs.

If criminal activity is identified in an investigation the Applicant **MUST** where permissible, notify the affected parties, ensuring that no information is shared inappropriately.

Applicants **MUST**:

- Have in place appropriate mechanisms, procedures and personnel or third-party providers for investigating or otherwise dealing with incidents of fraud or suspected fraud.
- Ensure that staff involved in, and responsible for undertaking fraud investigation or resolution of suspected or known incidents of fraud, are appropriately trained and skilled in the area of fraud investigations as required by the Australian Government Investigation Standards (AGIS).
- Have in place investigation and referral processes and procedures that are consistent with the AGIS and the current edition of the Australian Government Information Security Manual (ISM).
- Resolve fraud matters in accordance with relevant internal and external requirements where a law enforcement agency has declined a referral.
- Document decision criteria at critical stages in managing a suspected fraud incident.
- Resolve fraud investigations when they occur and advise stakeholders (particularly affected individuals, identity federation participants) of the investigation outcome.
- Appropriately document decisions to use civil, administrative or disciplinary procedures, or to take no further action in response to a suspected fraud incident.

2.5 Reporting fraudulent activity

Where fraud is found to have occurred, Applicants **MUST**:

- Have appropriate mechanisms within their user records to flag incidents of fraud and a repository or database for recording and reporting identities or credentials of concern against which all new user registrations are matched.
- Conduct fraud reporting as required in annual compliance audits.

Where an investigation discloses potential criminal activity involving another entity's activities or programs, Applicants **MUST** report the matter to that entity to the extent possible subject to relevant requirements of any Australian law.

2.6 Fraud victim support

Applicants **MUST**:

- Have in place processes and services including online, face to face and telephone services, to assist users whose identities or authentication credentials have been compromised.
- Enable victims to advise the Applicant when they become aware of any fraudulent activities using their digital identity.
- Prevent continued fraudulent use of user accounts when fraud has been reported or where it appears highly likely that fraudulent activity is occurring based on available data.
- Where the Applicant identifies likely fraudulent activity, verify with the potential victim whether those activities are fraudulent.
- Where possible, advise parties within the identity eco-system of compromised or fraudulent identities.
- Ensure that identity attributes are re-proofed when a fraud victim is identified.

3 Part two: Fraud control guidance

3.1 Fraud control responsibilities

Many of the FCRs are tied to the requirements of other Trust Framework requirements documents. The TDIF FCRs fall into two categories:

- General responsibilities for all Applicants.
- Role-based responsibilities.

Table 1: Applicant's Fraud Control Responsibilities

What	Responsibility
Governance	Applicants are required to develop governance that promotes the proper use and management of identity and related information, functions and the financial sustainability of their processes.
Information Management	Applicants are required to collect, store and protect all information in accordance with the *Trust Framework Core Privacy Requirements*, the *Trust Framework Core Security Requirements* and the *Australian Government Information Security Manual* to reduce the risk of Fraudulent access or use of this information. Applicants can only collect and use information for the purposes described in the *Privacy Requirements* and the Fraud Control Requirements (this document). Applicants and personnel **MUST NOT** use their position to improperly gain access to, sell or share personal data. E.g. using data collected for market research. Information can be used for the purposes for which it was collected under the TDIF and as prescribed by legislation relevant to the Applicant.
Fraud Risk Oversight	If there is an intention for an applicant to operate more than one service under the TDIF, the Applicant will be required to develop separate systems of fraud risk oversight including Fraud Risk Assessments and Fraud Control Plans for each TDIF accredited service. E.g. if an Applicant operates both as an IdP and Attribute Provider, it **MUST** develop and maintain an appropriate system of fraud risk oversight for an IdP and separately for its operation as an Attribute Provider. Requirements for fraud risk oversight and management are listed in the *Risk Management Requirements*.
Personnel	The following documents set the requirements for personnel and third-party providers working for the Applicant: • *Privacy Requirements.* • *Protective Security Requirements.* • Commonwealth Fraud Control Framework 2017. • Current edition of the Australian Government Information Security Manual

The table below identifies the responsibilities of Applicants accredited against the TDIF. While effective fraud control requires the commitment of all personnel, third-party providers and individual users of a service, the primary responsibility for fraud control rests with Applicants.

The Trust Framework Accreditation Process apply to the first two categories listed in the table below, however Applicants are required to demonstrate how and when they made Relying Parties aware of their responsibilities under the Trust Framework.

Table 2: Role-based fraud control responsibilities

Role	Responsibility
IdPs, CSPs, Attribute Providers	• Develops Fraud Risk Assessment and Fraud Control Plan. • Collects, verifies and stores appropriate user information. • Educates users on how to safeguard their identity information within the IdP. • Ensures that information collected is accurate and up to date. • Issues digital identities and/or authentication credentials. • When authorised by the user, enables verification of digital identity with Relying Party. • Provides fraud reporting channels to users, Relying Parties and appropriate law enforcement agencies. • Advises the Identity Exchange of fraud-related transactions within the IdP. • Investigates reports of identity fraud within its user base. • Maintains records of identity fraud within its user base. • Assists victims of digital identity theft to regain control of their digital identity.
Identity Exchange	• Develops Fraud Risk Assessment and Fraud Control Plan. • Ensures the privacy of the user within the identity eco-system is protected. • Advises IdPs, CSPs and Attribute Providers of fraud-related transactions reported by the Relying Party. • Advises Relying party of fraud-related transactions reported by the IdP, CSPs and Attribute Providers.
Relying Party	• Verifies user identity using services provided by the Accredited Provider. • Ensures where necessary through their own means of information collection, that enrolling users are unique in the context of their system. • Collects user information relating to determining eligibility for Relying Party purposes. • Detects and report identity fraud and credential fraud-related transactions to the Identity Exchange.

Role	Responsibility
User	• Provides accurate identity information. • Corrects or update identity information with Document Issuers as identity information such as name changes. • Does not share account or identity information with third parties. • Reports unauthorised use of their digital identity or authentication credential to both the Accredited Provider and the Relying Party as soon as they become aware of it.

3.1.1 Fraud Risk Assessment

Further Guidance on fraud risk assessments can be found in *Risk Management Requirements*.

Table 3: Fraud Risk Assessments

What	Description
Frequency	All Applicants **MUST** conduct annual risk assessments for each of their services under the Trust Framework and a risk assessment when there is a significant change in technological capabilities which impact on the service or services provided. e.g. If the IdP implements its own face to passport chip matching technology in preference to using the Facial Verification Service, a review of the risk assessment would be required.
Fraud Risks	Applicants **MUST** demonstrate in their Fraud Risk Assessments that they have considered, mitigated and/or managed these Fraud risks and any additional risks which may arise as a result of their service solution. Fraud risks within the program are listed in *Annex A: Potential Sources of Risk*, of the *Risk Management Requirements*.

3.1.2 Fraud Control Plan

Further guidance on the development of Fraud Control Plans and Fraud Control Procedures Manuals is provided by the Australian Commission for Law Enforcement Integrity and can be found at www.aclei.gov.au.

Table 4: Fraud Control Plan Requirements

Factors	Description
Separation of types of fraud risk	Process, architecture and technology-based fraud risks must be identified and mitigated or addressed individually. Fraud control plans must differentiate between these risks and their mitigation, management and treatment. A process-based fraud risk is a risk arising due to a fraud opportunity within a process. E.g. if an agency official is not trained or is unable to differentiate between faces but makes binding decisions for individuals presenting in person after an online biometric process was unsuccessful. An architecture-based fraud risk is a risk arising due to the way information is stored, shared or interpreted. E.g. no check with an issuing source that a document has been issued. A technology-based fraud risk is a risk arising due to technological gaps, for example if a facial recognition tool had the acceptance threshold set too low, resulting a higher number of potential false positive matches at the binding stage.
System of internal controls	A system of internal controls is required for the following: • Internal processes - identify leaving personal information in a location accessible to others without a need to know as an opportunity for future identity fraud. Educate staff regarding the management of personal data. • Technological processes - identifying gaps in the way that technologies used by the applicant interact with each other. • Technologies - identifying gaps and mitigations based on the technologies used by the applicant • Access to sensitive data - identifying the fraud risk of access to sensitive personal data, restrict personnel access to a need to know basis for personal data and set up system records
Implementation timeframe	Fraud control arrangements must be in place when the service commences or if identified after the service has commenced, as soon as practicable after identification. For example, if an IdP commences operations, all fraud control arrangements identified **MUST** be implemented e.g. staff training must have taken place prior to an Applicant's commencement as an IdP. If a fraud control measure is identified subsequent to commencement as an IdP, e.g. the solution to a newly identified issue is developed, it **MUST** be put in place as soon as practicable.
Governance	Applicants **MUST** develop a Fraud Control Plan that clearly identifies responsibilities for managing and investigating different levels of fraud.

3.2 Fraud prevention

Preventing fraud is more efficient and less costly than detecting and managing fraud downstream. Fraud can be prevented in the following ways:

- By using technologies such as the Document Verification Service (DVS) which check at source with the issuing agency whether a document has been validly issued.
- Through enrolment processes flows that prevent a user from with the IdP using identity information that is not theirs. E.g. if a potential fraudster wants to sign up for a digital identity using a stolen binding document, they will need to pass a DVS check, followed by an FVS or face to passport RFID chip check to verify that they are the person that the document was issued to.
- Through education of personnel and third-party providers to assist them to understand the definition of fraud in their environment, identify areas and sources of fraud and prevent fraud from occurring especially for personnel in customer-facing roles.
- Through education of users who are applying for or already have a digital identity or credential with the Applicant to prevent them from sharing information with individuals or businesses falsely claiming to represent the IdP.

3.3 Personnel and third-party requirements

3.3.1 Training

The Applicant **MUST** develop and deliver fraud control training to personnel and third-party providers based on:

- What constitutes fraud for the Applicant's identity service.
- Level of access to personal information and systems.
- Fraud Risk Assessment.
- Fraud Control Plan.
- Section 10 of the Public Governance, Performance and Accountability Rule 2014.

This training can be delivered in a number of ways including online and classroom learning. Training recipients need to demonstrate understanding of this training prior to commencing work on the applicant service or having access to user information.

Fraud Control Training must be summarised in a Fraud Control Procedures Manual in a user-friendly and accessible format for personnel and third-party providers.

Applicants **MUST** update the Fraud Control Procedures Manual as new types of fraud are detected and new mitigations and controls are developed.

In addition to general IdP fraud training, personnel and third-party providers working in specialised roles will need to undertake specialised training.

3.3.2 Facial recognition aptitude and training

Staff responsible for making binding decisions (facial verification to link an individual to their document without the assistance of a biometric system) providing face to face services online or over the counter **MUST** demonstrate proficiency in facial recognition and face matching. Studies have shown that 1 in 10 people are capable of facial recognition of unknown faces (i.e. faces that they have not seen before) and facial comparisons. It is therefore important that Applicants only employ persons who have demonstrated aptitude in this field, to make binding decisions.

The DOHA is currently developing facial recognition and match training, which will be made available to users of the FVS. Several international universities have made free online facial recognition aptitude tests available. All persons making binding decisions **SHOULD** pass all tests they are given.

3.3.3 Fraud investigation training

Training requirements for personnel primarily engaged in fraud control activities are required to possess or obtain relevant qualifications to effectively carry out their duties. The qualifications required to carry out fraud investigations are contained in the AGIS and the Commonwealth Fraud Control Framework.

3.3.4 Vetting

The Applicant **MUST** ensure that personnel and third-party providers do not have a history of misconduct and do not have ties to organised crime. Security and integrity of systems should be conducted as described in the *Protective Security Requirements* to prevent cyber security incidents.

3.3.5 Monitoring

The *Protective Security Requirements* provides information relating to monitoring personnel access to information. Where user information has been compromised as a result of access by personnel or third-party providers, the Applicant **MUST** investigate and take appropriate action against personnel and third party involved.

3.3.6 User training and information

Applicants **MUST** develop and deliver a communications package to assist users to safeguard their identities under the TDIF. Where scams are detected, Applicants **MUST** provide advice to all current users. Applicants **MAY** choose hire a specialised third party such as IDCARE to assist in this activity.

Where a data breach as described in the *Privacy Requirements* occurs, Applicants **MUST** follow the *Protective Security Requirements* and **MUST**, where possible, provide potential fraud victims with instructions on impact minimisation and set up a helpline to answer any additional queries from affected users.

3.4 Fraud detection

Fraud may be detected at a number of touch points throughout the identity life-cycle. Under the TDIF, the greatest opportunities to detect fraud arise during the initial enrolment of an individual with an IdP or CSP, during authentications or transactions and through reporting by Relying Parties and Users.

Table 5: Non-exhaustive list of possible mechanisms to detect fraud

Fraud Type	Mechanism	Purpose
Document Fraud	Document Verification Service	Verifying that the document was issued by the source agency. E.g. verifying that a passport with those details was issued by the Australian Passports office

Fraud Type	Mechanism	Purpose
Impostor (not the real owner of the binding document)	The Binding step described in the Identity Proofing Requirements. Comprising: Face Verification Service Face to passport RFID chip check and Passive liveness detection	Checking whether the person whose photograph was taken is alive and whether they are the same person that a binding document was issued to.
Credential Fraud	Identity Proofing the Credential Owner	Verifying that the credential belongs to a particular user.

Applicants **MUST** use fraud monitoring tools and analytics set up by a qualified or experienced data analyst.

Based on the assessed risk associated with a transaction, a Relying Party **MAY** request that aspects of an identity are re-proofed when a user attempts to gain access to a service, this re-proofing might involve a request that the binding process is repeated at the time of the transaction. E.g. A user might apply for a Tax File Number. Due to the level of risk associated with the request, the Australian Taxation Office might request re-proofing involving a facial verification.

Where Applicants are advised of or become aware of specific types of fraud such as compromised batches of documents or identities, they **SHOULD** engage in rules-based fraud prevention - e.g. if advice is received by the applicant from an issuing agency or a reliable source (e.g. IDCare), that certain batches of documents cannot be trusted or used, both the system and personnel **SHOULD** take this into account before enabling users holding such documents to enrol.

Where fraud or suspected fraud is reported or detected, the Applicant **MUST** assess the incident and ensure that appropriate stakeholders are notified as soon as possible. E.g. if a User reports that their identity has been used without the knowledge or permission, the IdP **MUST** advise the Identity Exchange of the instances of inappropriate use of a digital identity so that the Identity Exchange can notify the relevant Relying Parties.

When an incident of fraud is confirmed, the Applicant **MUST** take the actions specified in the Fraud Control Plan and Fraud Risk Management plan to manage the fraud.

3.5 Fraud investigations

3.5.1 Sources of guidance and requirements for conducting fraud investigations

Information on fraud investigation requirements are documented in the following acts:

- Crimes Act 1914.
- Freedom of Information Act 1982.
- Privacy Act 1988.
- Archives Act 1983.

And the following policies, frameworks, standards and manuals

- Prosecution Policy of the Commonwealth.
- The Protective Security Policy Framework.
- The Commonwealth Fraud Control Framework 2017.
- AGIS.
- The current edition of the ISM.

The Australian Federal Police (AFP) and Attorney General's Department (AGD) also provide guidance on the requirements for fraud investigations.

Applicants **MUST** ensure that they meet all of the requirements for conducting fraud investigations. If anything recorded in these documents contravenes these FCRs, Applicants **SHOULD** make the Trust Framework Accreditation Authority aware of the situation as soon as possible.

3.5.2 Fraud investigation requirements

Applicants **MUST** investigate all instances of fraud or suspected fraud against them unless the matter is referred to and accepted by the AFP.

Law enforcement agencies may not always have the capacity to investigate fraud. Where a law enforcement agency has declined a referral, the Applicant **MUST** undertake the investigation and bring the investigation to a conclusion within a reasonable timeframe. It is acceptable for the Applicant to outsource the investigative

function to a reliable Australian-based third party such as IDCare, provided that the requirements of the AGIS and ISM are met.

3.5.3 Information sharing

The Applicant **SHOULD**, where permissible, where fraudulent or criminal activity is detected, share this information with other participants under the TDIF. For example, where an Applicant detects a possible or known fraudulent identity, they **SHOULD** share the details of the fraudulent identity with other participants in the identity federation.

Where a legitimate identity has been compromised and a victim was able to demonstrate ownership of the identity, the victim and all other parties notified by the Applicant **MUST** be advised of the outcome of the investigation.

Where an investigation discloses potential criminal activity involving another entity's activities or programs, Applicants **MUST** report the matter to that entity or agencies managing fraud on the behalf of that entity to the extent possible subject to relevant requirements of any Australian law.

3.5.4 Fraud and investigation monitoring tools

Applicants **MUST** report on instances of fraud and the outcomes of fraud investigations. To support this, the Applicant **MUST** have in place systems or mechanisms in which potential fraud can be flagged and decision criteria are recorded and workflow and allocations of work are visible. E.g. A case management system for suspected fraud and fraud investigations.

This system will need to be capable of inputting information in accordance with the decision criteria in the Fraud Control Plan, the Fraud Risk Management Guide and the Fraud Control Procedures Manual. This **MAY** include but is not limited to criteria such as:

- When an incident is first identified.
- What type of fraud has been identified.
- The impacts on the identity.

- Frequency of use of the identity, location it was used etc.
- The outcome of the investigation.

The system will be used to appropriately document decisions to use civil, administrative or disciplinary procedures or to take no further action in response to a suspected or confirmed fraud incident.

3.6 Fraud reporting

Further to the fraud reporting tool described under '*Fraud and Investigations Monitoring Tools*' section above, where fraud is found to have occurred, Applicants **MUST** have appropriate mechanisms to flag incidents of fraud and suspected fraud in their user database, and should also maintain a database or list of identities or credentials of concern, against which all new user registrations are matched.

Applicants **MUST** follow the fraud reporting requirements in the TDIF *Annual Review* and the Commonwealth Fraud Control Framework 2017.

3.7 Fraud victim support

3.7.1 Communications channels for fraud victims

When a users' details have been compromised, the user **MUST** be able to immediately notify the Applicant using a variety of communications channels. The Applicant **MUST** have in place processes such as appropriate identification of a user whose identity has been compromised and appropriate technologies to enable the Applicant to flag the identity as compromised.

The Applicant **MUST** have sufficient trained and qualified personnel managing online, face-to-face and telephone channels to provide victim support services within a reasonable timeframe. A third-party service provider such as IDCARE may be able to provide this type of assistance.

Staff providing telephone and face to face services **SHOULD** be based in Australia and that the Applicant **MUST** have mechanisms in place to prevent client information from being inappropriately shared or used by third party providers.

3.7.2 Managing the identities of fraud victims

When a victim of fraud is identified or self-identifies, their identity **MUST** be re-proofed. This **SHOULD** be done using the face-to-face channel.

For identities at IP 3 and above[2], a face to document image match by appropriately qualified personnel and a machine-based biometric match **SHOULD** be conducted using the binding document image.

Where the fraud victim's identity documents have been compromised, the victim should where possible, be able to use other documents to verify their identity or request that their digital identity is re-proofed using the binding step whenever the identity is used until the issue is resolved.

Where a fraud victim's identity has been compromised, the Applicant **SHOULD** supply evidence of the compromised identity to the victim, to assist in the management of their identity going forward. This evidence **SHOULD** include where possible:

- The shareable details of the applicant.
- The date that the compromise commenced (if known).
- The date that the Applicant became aware of the compromise.

The Victim **SHOULD** be able to obtain a list of transactions that occurred for the period during which their identity was compromised to assist the victim to regain control of their identity.

The Applicant **MUST** assist the victim to investigate when the fraud commenced and advise Relying Parties through the Identity Exchange, of suspected fraudulent transactions.

Where the quality of a claim that an identity is fraudulent has been checked and Applicants are authorised by legislation or where there is consent from the victim,

[2] See the *Identity Proofing Requirements* for further information on IP levels

Applicants **MUST** advise other parties operating under the TDIF of any compromised or fraudulent identities they encounter.

3.7.3 Management of unusual account transactions

Where unusual account transactions are detected e.g. new device in different geolocation is used to change personal details, the Applicant **MUST** verify with the owner of the identity, using a combination of verification or validation tools, that the account is under the control of the owner of the identity or authentication credential.

4 References

The following information sources have been used in developing this document.

1. Attorney-General's Department, Commonwealth Fraud Control Framework, 2017, https://www.ag.gov.au/CrimeAndCorruption/FraudControl/Pages/FraudControlFramework.aspx
2. Australian Government Investigations Standards
3. Australian Signals Directorate, 2017, '*2017 Australian Government Information Security Manual: Controls (ISM)',* Australian Government, Canberra. https://www.asd.gov.au/infosec/ism/
4. Crimes Act 1914 (Cwth)
5. Criminal Code 1995 (Cwth)
6. Department of Finance, 2014, '*Commonwealth Risk Management Policy*', Australian Government, Canberra.http://www.finance.gov.au/comcover/risk-management/the-commonwealth-risk-management-policy/
7. Public Governance, Performance and Accountability Act 2013 (Cwth)
8. Public Governance, Performance and Accountability Rule 2014 (Cwth)
9. Proceeds of Crime Act 2002 and the Proceeds of Crime Regulations 2002 (Cwth)
10. Public Service Act 1999 (Cwth)