Telecommunications Service Provider (Customer Identity Authentication) Determination 2022

The Australian Communications and Media Authority makes the following determination under subsection 99(1) of the *Telecommunications Act 1997*.

Dated: 1 April 2022

James Cameron
[signed]
Member

Cathy Rainsford
[signed]
~~Member~~/General Manager

Australian Communications and Media Authority

Part 1—Preliminary

1 Name

This is the *Telecommunications Service Provider (Customer Identity Authentication) Determination 2022*.

2 Commencement

This determination commences on 30 June 2022.

3 Authority

This determination is made under subsection 99(1) of the Act.

4 Application

For the purposes of subsection 99(1) of the Act, this determination applies to carriage service providers:

(a) involved in the supply of a telecommunications service; and

(b) when conducting a high-risk customer interaction relating to a customer of a carriage service provider.

but it does not apply to a customer who is an account managed customer or an integrated customer.

5 Objectives

The objectives of this determination are to:

(a) reduce the harm caused to customers when access to their personal information, business information or telecommunications service is targeted by unauthorised persons or entities; and

(b) require carriage service providers to follow effective identity authentication processes to protect the security of high-risk customer interactions.

6 Definitions

(1) In this determination:

access-controlled defence site means defence premises which can only be accessed through a defence access control point.

account information authenticator means a process used to establish that the requesting person is the customer, or is the customer's authorised representative, for the telecommunications service based on the requesting person's knowledge of a piece of the customer's account security information.

account managed customer means a customer of a carriage service provider where the provider assigns one or more of its employees or agents to be a

Authorised Version F2022L00548 registered 06/04/2022

designated contact person for the customer, in relation to all matters relating to the customer's telecommunications services.

account security information means information which is created for the purpose of applying security to an account and which may include one or more of:

(a) an account username or login information which is used to log into the customer's account on the carriage service provider's website or mobile application;

(b) an account number;

(c) an account password;

(d) a personal identification number related to the account; or

(e) the answer to a security question which has been set up for the purposes of identity authentication.

Act means the *Telecommunications Act 1997*.

audio visual link means a facility, including closed-circuit television, that enables reasonably contemporaneous and continuous audio and visual communication between persons at different places.

authorised representative means a person:

(a) who is listed by the customer on their account as having authority from the customer to deal with a carriage service provider on behalf of that customer as their representative; and

(b) whose personal information is recorded on the customer's account.

biometric data means information about any measurable biological or behavioural characteristics of an individual that can be used to verify the identity of the individual, such as their face, fingerprints or voice.

business information means information about a customer who is not an individual.

business to business service request system means a system which is purpose-built for a customer to integrate the customer's information technology systems with the carriage service provider's information technology systems through which transactions relating to the customer's telecommunication service can be conducted using secure methods of communication.

Example: Secure methods of communication include, for example, an application interface which connects the customer's computers or software with the provider's computers prior to which connection, authentication such as IP address ranges or encrypted channels is used.

category A document means a document mentioned in Table 1 in Schedule 1.

category B document means a document mentioned in Table 2 in Schedule 1.

customer means:

(a) an individual who acquires or may acquire a telecommunications service for the primary purpose of personal or domestic use and not for resale; or

Authorised Version F2022L00548 registered 06/04/2022

(b) a business or non-profit organisation which acquires or may acquire one or more telecommunications services which are not for resale and which, at the time it enters into the customer contract:

(i) does not have a genuine and reasonable opportunity to negotiate the terms of the customer contract; and

(ii) has or will have an annual spend with the carriage service provider which is, or is estimated on reasonable grounds by the carriage service provider to be, no greater than $40,000,

and who or which has entered into a customer contract with the carriage service provider.

customer contract means an arrangement or agreement between a carriage service provider and a customer for the supply of a telecommunications service to that customer and includes a standard form of agreement formulated by the carriage service provider for the purposes of section 479 of the Act.

defence access control point and ***defence premises*** have the same meanings as in section 71A of the *Defence Act 1903*.

digital mobile number means a special services number specified in Schedule 5 of the *Telecommunications Numbering Plan 2015* for use with a digital mobile service.

digital mobile service means a public mobile telecommunications service supplied by a network using digital modulation techniques.

emergency means an actual or imminent event (such as fire, flood, storm, earthquake, explosion or terrorist act) that:

(a) causes significant disruption to an individual or business; and

(b) that is perceived to threaten life or property.

foreign military ID card means an identification card:

(a) issued in the name of an individual by a foreign government;

(b) showing a photo of the individual; and

(c) identifying the individual as a current member of the defence forces of that government.

fraud mitigation training means training provided by a carriage service provider to its employees and agents for the purposes of implementing a strategy to detect fraudulent transactions and preventing those transactions from causing financial damage to the customer and carriage service provider.

government-accredited digital identity service means an online service that allows users of that service to verify their identity digitally to relying parties, where that service holds a valid accreditation status, as issued by the relevant government regulator.

Authorised Version F2022L00548 registered 06/04/2022

government document means a document that is issued by the Commonwealth or a State or Territory that is evidence of the person's identity in Australia or use of that identity in Australia.

Note: Examples of government documents include a current driver's licence, Medicare card or Australian passport.

government online document verification service means an online service which allows users of that service to confirm the validity of information recorded on certain identification documents against the databases of the government agency that issued the relevant identification documents, in a manner authorised by that government agency or its representatives.

high-risk customer interaction means an interaction between a carriage service provider and a requesting person, in relation to a customer's telecommunications service, initiated by either the requesting person or by the carriage service provider, during which one or more high-risk customer transactions are requested.

high-risk customer transaction means a transaction that may result in one or more of the following:

(a) a customer losing access to the customer's telecommunications service;

(b) a change to a customer's personal information, business information or account security information held by the carriage service provider relating to the customer's account;

(c) adding or removing a person as a customer's authorised representative;

(d) disclosure to the requesting person of a customer's personal information, business information or account security information held by the carriage service provider relating to the customer's account;

(e) an additional ongoing, or a large one-off charge being applied to a customer's account;

Note: A carriage service provider should determine whether a charge is a large one-off charge with reference to the usual pattern of charges on a customer's account. For example, a one-off charge of $200 may qualify as a large one-off charge for a customer with a regular monthly charge of $15.

but does not include any of the following:

(f) a transfer of title (also known as a change of ownership) where:

(i) the carriage service provider is satisfied that the end-user of a public number, who is not the customer for that number, is affected by domestic or family violence; and

(ii) the terms and conditions in the standard form of agreement, formulated by the carriage service provider for the purposes of section 479 of the Act, permit a transfer of title in those circumstances;

Authorised Version F2022L00548 registered 06/04/2022

(g) a transaction to port a mobile number to which the *Telecommunications (Mobile Number Pre-Porting Identity Verification) Industry Standard 2020* applies; or

(h) a transaction that may result in the disclosure to the requesting person of a customer's personal information, business information or account security information where the information:

(i) is included in a bill or in other correspondence with the customer; or

(ii) is mostly hashed or obscured for the purpose of reminding a customer of the customer's information; or

(iii) is included in notifications relating to a customer's telecommunications service usage.

Note 1: A high-risk customer transaction includes, for example, a SIM swap request, a request to transfer a telecommunications service from being a post-paid carriage service to a pre-paid carriage service, a request for the activation of a telecommunications service where the customer is overseas, a request for a transfer of title (also known as change of ownership), a request to block an International Mobile Equipment Identity or a Permanent Equipment Identifier, a request to purchase an additional mobile communications device, and a request to add an additional carriage service to an account.

Note 2: Carriage service providers have obligations under the *Telecommunications (Mobile Number Pre-Porting Identity Verification) Industry Standard 2020* to confirm that the person requesting the port (within the meaning of that standard) of a mobile service number is the rights of use holder (within the meaning of that standard) for that number. A carriage service provider which must comply with that standard is not required to comply with this determination in relation to a port.

identity authentication process means a process described in subsections 9(1), 9(2), 9(3), 10(2) or 11(2).

integrated customer means a customer who:

(a) uses an integrated service desk provided by the customer's carriage service provider; or

(b) has a business to business service request system with a carriage service provider.

integrated service desk means a service provided to the customer which is tailored to the customer's requirements through which the customer can communicate with the carriage service provider in relation to the customer's telecommunications services via channels dedicated to their account, and may include a dedicated contact number, email mailbox or purpose-built applications.

mobile carriage service provider means a carriage service provider who supplies or arranges for the supply of a public mobile telecommunications service.

mobile service number means a digital mobile number issued by a mobile carriage service provider to a customer in connection with the supply of a public mobile telecommunications service (other than a satellite telephone service).

Authorised Version F2022L00548 registered 06/04/2022

person in vulnerable circumstances means a customer:

(a) who due to their personal circumstances, is experiencing, or is at risk of experiencing, harm, detriment or disadvantage, (including a customer who is overseas who has lost their mobile communications device or a customer who has been impacted by an emergency or domestic or family violence);

(b) who due to the circumstances in (a), cannot access a telecommunication service, device, or cannot provide category A documents or category B documents for the purpose of identity authentication; and

(c) in relation to whom, the carriage service provider is consequently unable to complete the identity authentication processes under section 9(3) or subsection 10(2).

A reference to a customer in this definition, includes their authorised representative.

personal information means information or an opinion about an identified individual, or an individual who is reasonably identifiable, including the customer's name, date of birth, and address:

(a) whether the information or opinion is true or not; and

(b) whether the information or opinion is recorded in a material form or not.

personal information authenticator means a process used to establish that the requesting person is the customer, or is the customer's authorised representative, for the telecommunications service based on their knowledge of a piece of the customer's personal information that is not account security information.

post-paid carriage service means a carriage service that is supplied by a carriage service provider to a person where:

(a) the service may be used fully or in part before payment for the supply of the service is made; and

(b) the person has arranged with the carriage service provider to pay either an amount notified in an invoice issued by the carriage service provider, or instalments of fixed amounts at regular intervals (whether or not, notified in an invoice), for the supply of the service.

pre-paid carriage service means a carriage service that has the following characteristics:

(a) it is a public mobile telecommunications service used in connection with a public number;

(b) the payment for the supply of the service must be made before the service is used, unless the supplier of the service has not required payment for the initial supply of the service; and

(c) it is not a post-paid carriage service.

Authorised Version F2022L00548 registered 06/04/2022

public number means a number specified in the *Telecommunications Numbering Plan 2015* for use in connection with the supply of carriage services to the public in Australia.

requesting person means a person who:

(a) has contacted a carriage service provider; or

(b) has been contacted by a carriage service provider,

in relation to a transaction that results in a high-risk customer interaction.

satellite telephone service means a carriage service with which end-users make calls via a satellite-based facility.

SIM means a subscriber identity module.

SIM swap request means the transfer of a public number connected to a public mobile telecommunications service from one SIM to a new SIM.

SMS message means a message or series of messages sent using a short message service.

special services number has the same meaning as in section 31 of the *Telecommunications Numbering Plan 2015*.

telecommunications service means any of the following carriage services:

(a) standard telephone service;

(b) public mobile telecommunications service;

(c) a carriage service that enables customers to access the internet.

unlisted authorised representative means a person who is authorised by the customer, or by a court or tribunal or any other body legally empowered to represent customers, to act on behalf of the customer, other than an authorised representative.

validated: see subsection (2).

Note: A number of other expressions used in this determination are defined in the Act, including the following:
(a) carriage service;
(b) carriage service provider;
(c) public mobile telecommunications service;
(d) standard telephone service.

(2) An email address, mobile application, device or account (***the contact point***) has been ***validated*** by a customer or authorised representative if the customer or authorised representative has undertaken a security process required by the carriage service provider in relation to the contact point which verifies that the customer or authorised representative has access to the contact point.

Authorised Version F2022L00548 registered 06/04/2022

7 References to other instruments

In this determination, unless the contrary intention appears:

(a) a reference to any other legislative instrument is a reference to that other legislative instrument as in force from time to time; and

(b) a reference to any other kind of instrument is a reference to that other instrument as in force from time to time.

Note 1: For references to Commonwealth Acts, see section 10 of the *Acts Interpretation Act 1901* and subsection 589(1) of the Act, and see also subsection 13(1) of the *Legislation Act 2003* for the application of the *Acts Interpretation Act 1901* to legislative instruments.

Note 2: All Commonwealth Acts and legislative instruments are registered on the Federal Register of Legislation. The Federal Register of Legislation may be accessed free of charge at www.legislation.gov.au.

Part 2—Identity Authentication Requirements

8 Requirement to confirm the requesting person is the customer or the customer's authorised representative

Subject to section 12, prior to undertaking the first high-risk customer transaction in the course of a high-risk customer interaction, a carriage service provider for a telecommunications service must confirm:

(a) the requesting person is the customer, or the customer's authorised representative, for the service by use of the identity authentication process or processes in section 9; or

(b) if section 10 applies – the requesting person is the customer, or the customer's authorised representative, for the service by use of the identity authentication process or processes in section 10; or

(c) if section 11 applies – the requesting person is the customer, or the customer's authorised representative, for the service by use of the identity authentication process or processes in section 11.

9 Multi-factor Authentication Requirements

(1) In a case where the high-risk customer interaction is initiated by the requesting person – a carriage service provider for the telecommunications service must use one of the following identity authentication processes:

(a) at least two account information authenticators; or

(b) at least two personal information authenticators; or

(c) at least:

(i) one account information authenticator; and

(ii) one personal information authenticator;

and must comply with subsection (3).

(2) In a case where the high-risk customer interaction is initiated by the carriage service provider using the public number listed on the customer's account as the contact number for the customer – the provider for the telecommunications service must use at least one personal information authenticator, and must comply with subsection (3).

Authorised Version F2022L00548 registered 06/04/2022

Note: Where a high-risk customer interaction is initiated by the carriage service provider using the public number listed on the customer's account as the contact number for the customer, the carriage service provider will have met the requirement in paragraph (3)(b).

(3) The carriage service provider for the telecommunications service must use at least one of the following identity authentication processes to confirm that the requesting person is the customer, or is the customer's authorised representative, for that service:

(a) subject to subsection (4), confirming the requesting person has direct and immediate access to the telecommunications service; or

Examples:

(a) for a public mobile telecommunications service in a retail environment– personnel representing the carriage service provider call the mobile service number listed on the customer's account while in store and verify that the call has been received by the customer's mobile device used in association with that number while the customer is instore.

(b) in an online environment– personnel representing the carriage service provider receiving confirmation that the customer has received a unique verification code or secure hyperlink.

(b) subject to subsection (4), confirming the requesting person has direct and immediate access to the public number listed on the customer's account as the contact number for the customer; or

Example: For a telecommunications service in a call centre environment, personnel representing the carriage service provider calling back the public number listed on the customer's account to confirm that the requesting person has access to the service used in association with that public number.

(c) use of a unique verification code or secure hyperlink:

(i) which is sent to the customer, or the customer's authorised representative as the case may be (***the relevant person***), by the carriage service provider:

(A) by SMS message to the mobile service number which is listed on the customer's account as the contact number for the customer; or

(B) by email to an email address that has been validated by the relevant person; or

(C) by an in-app message to a carriage service provider's mobile application that has been validated by the relevant person; or

(D) to some other device or account which has been validated by the relevant person; and

(ii) which includes in the message in which the unique verification code or secure hyperlink is sent, a clear statement informing the relevant person:

(A) that a high-risk customer interaction has been initiated in relation to the customer's telecommunications service;

(B) that the code or secure hyperlink should not be shared with any other party except the carriage service provider if the relevant person has initiated the high-risk customer interaction; and

(C) what the relevant person can do if they did not initiate the high-risk customer interaction; and

(iii) after the receipt of which by the relevant person, the carriage service provider receives immediate confirmation from the relevant person that the relevant person has received the unique verification code or secure hyperlink; or

(d) use of one or more forms of biometric data; or

(e) using a category A document via the process described in Schedule 1; or

(f) use of a cryptographic key.

Authorised Version F2022L00548 registered 06/04/2022

(4) When an identity authentication process used to comply with either paragraph (3)(a) or paragraph 3(b) includes the use of a unique verification code or secure hyperlink, the carriage service provider must also comply with paragraph (3)(c).

(5) If, in response to a message sent for the purposes of paragraph (3)(c), the relevant person takes the action referred to in sub-subparagraph (3)(c)(ii)(C):

(a) where one or more high-risk customer transactions have already been completed by the carriage service provider – the provider must:

(i) take steps to immediately reverse or remediate any completed transaction;

(ii) notify the relevant person of steps taken by the carriage service provider under subparagraph (i); and

(iii) notify the relevant person of what they can do to protect the customer's account; and

(b) where a high-risk customer transaction has not yet been undertaken by the carriage service provider – the provider must not undertake a high-risk customer transaction and must:

(i) notify the relevant person that the carriage service provider has not undertaken the high-risk customer transaction; and

(ii) notify the relevant person of what they can do to protect the customer's account.

(6) A carriage service provider may attempt an identity authentication process under subsections (1), (2) and (3) more than once during a high-risk customer interaction.

10 Additional Multi-factor Authentication Requirements

(1) This section applies if:

(a) a high-risk customer interaction is initiated; and

(b) the carriage service provider has taken reasonable steps to use an identity authentication process at subsection 9(3) but has not been able to confirm that the requesting person is the customer, or the customer's authorised representative, for the service.

(2) An employee or agent of the carriage service provider for the telecommunications service, who has completed fraud mitigation training, must use at least one of the following identity authentication processes to confirm that the requesting person is the customer, or the customer's authorised representative, for that service:

(a) using category A documents and/or category B documents via the process described in Schedule 1; or

(b) using a government online document verification service; or

(c) using a government-accredited digital identity service.

Authorised Version F2022L00548 registered 06/04/2022

(3) The carriage service provider is only taken to have confirmed that the requesting person is the customer, or the customer's authorised representative, in accordance with paragraph (2)(b) if:

(a) the requesting person gives the provider:

(i) the identifying number of at least two unique government documents;

(ii) information identifying the State or Territory that issued the government documents, or confirming that the government document was issued by the Commonwealth; and

(iii) if required by the government online document verification service – any dates or other information recorded on the government documents; and

(b) the information given in relation to each of two government documents is verified on a government online document verification service.

Note: The information provided by the requesting person in relation to a government document is matched against the databases held by the agency that issued the document and is either accepted or rejected as matched or not.

(4) The carriage service provider is only taken to have confirmed that the requesting person is the customer, or the customer's authorised representative, in accordance with paragraph (2)(c) if:

(a) the requesting person gives the provider:

(i) the identifying number of at least two unique government documents;

(ii) information identifying the State or Territory that issued the government documents, or confirming that the government document was issued by the Commonwealth; and

(iii) if required by the government online document verification service – any dates or other information recorded on the government documents; and

(b) the information given in relation to each of two government documents is verified on a government-accredited digital identity service.

Note: The information provided by the requesting person in relation to a government document is matched against the databases held by the agency that issued the document and is either accepted or rejected as matched or not.

(5) When the identity authentication process in this section is used, the carriage service provider must, immediately after it has used an identity authentication process for subsection (2), and, either prior to, or immediately after, undertaking the first high-risk customer transaction, send a notification to the customer, or to the customer's authorised representative as the case may be (***the relevant person***):

(a) by SMS message to the mobile service number which is listed on the customer's account as the contact number for the customer; or

(b) by email to an email address that has been validated by the relevant person; or

(c) by an in-app message to a carriage service provider's mobile application that has been validated by the relevant person; or

(d) to some other device or account which has been validated by the relevant person;

which informs the relevant person:

(e) that a high-risk customer interaction has been initiated; and

(f) what the relevant person can do if they did not authorise the interaction.

Authorised Version F2022L00548 registered 06/04/2022

(6) The requirement in subsection (5) does not apply where there is no mobile service number, validated email address, validated mobile application or other validated device or account associated with the customer's account.

(7) The requirement in subsection (5) does not apply where:

(a) the carriage service provider has reasonable grounds to believe that the customer is affected by domestic or family violence; and

(b) the customer has requested that the notification not be sent.

(8) If, in response to a notification sent for the purposes of subsection (5), a relevant person takes the action referred to in paragraph (5)(f):

(a) where one or more high-risk customer transactions have already been completed by the carriage service provider – the provider must:

(i) take steps to immediately reverse or remediate any completed transaction;

(ii) notify the relevant person of steps taken by the carriage service provider under subparagraph (i); and

(iii) notify the relevant person of what they can do to protect the customer's account; and

(b) where a high-risk customer transaction has not yet been undertaken by the carriage service provider – the provider must not undertake a high-risk customer transaction and must:

(i) notify the relevant person that the carriage service provider has not undertaken the high-risk customer transaction; and

(ii) notify the relevant person of what they can do to protect the customer's account.

11 Identity authentication requirements for people in vulnerable circumstances

(1) This section applies if:

(a) a high-risk customer interaction is initiated; and

(b) an employee or agent of the carriage service provider for the telecommunications service who has completed fraud mitigation training, has reasonable grounds to believe that the requesting person is a person in vulnerable circumstances.

(2) An employee or agent of the carriage service provider for the telecommunications service who has completed fraud mitigation training, must use the following identity authentication processes to confirm that the requesting person is the customer, or the customer's authorised representative, for that service:

(a) at least two account information authenticators; or

(b) at least two personal information authenticators; or

(c) at least:

(i) one account information authenticator; and

(ii) one personal information authenticator.

Authorised Version F2022L00548 registered 06/04/2022

(3) If a carriage service provider completes one or more high-risk customer transactions under this section the provider must keep a record of the details of the high-risk customer interaction including:

(a) the identity authentication process used for the purposes of subsection (2);

(b) the basis on which the employee or agent of the provider reasonably believed that the requesting person was a person in vulnerable circumstances; and

(c) any material or supporting evidence that was provided by the requesting person.

(4) When the identity authentication processes in this section are used, the carriage service provider must, immediately after it has used an identity authentication process for subsection (2), and either prior to, or immediately after, undertaking the first high-risk customer transaction, send a notification to the customer, or the customer's authorised representative as the case may be (***the relevant person***):

(a) by SMS message to the mobile service number which is listed on the customer's account as the contact number for the customer; or

(b) by email to an email address that has been validated by the relevant person; or

(c) by an in-app message to a carriage service provider's mobile application that has been validated by the relevant person; or

(d) to some other device or account which has been validated by the relevant person;

which informs the relevant person:

(e) that a high-risk customer interaction has been initiated; and

(f) what the relevant person can do if they did not authorise the interaction.

(5) The requirement in subsection (4) does not apply where there is no mobile service number, validated email address, validated mobile application or other validated device or account associated with the customer's account.

(6) The requirement in subsection (4) does not apply where:

(a) the carriage service provider has reasonable grounds to believe that the customer is affected by domestic or family violence; and

(b) the customer has requested that the notification not be sent.

(7) If, in response to a notification sent for the purposes of subsection 4, a relevant person takes the action referred to in paragraph (4)(f):

(a) where one or more high-risk customer transactions have already been completed by the carriage service provider – the provider must:

(i) take steps to immediately reverse or remediate any completed transaction;

(ii) notify the relevant person of steps taken by the carriage service provider under subparagraph (i); and

(iii) notify the relevant person of what they can do to protect the customer's account; and

(b) where a high-risk customer transaction has not yet been undertaken by the carriage service provider – the provider must not undertake a high-risk customer transaction and must:

Authorised Version F2022L00548 registered 06/04/2022

(i) notify the relevant person that the carriage service provider has not undertaken the high-risk customer transaction; and

(ii) notify the relevant person of what they can do to protect the customer's account.

Part 3—Requirements for unlisted authorised representatives

12 Requirements where an unlisted authorised representative initiates a high-risk customer interaction

(1) This section applies if:

(a) a high-risk customer interaction is initiated; and

(b) the requesting person asserts that they are an unlisted authorised representative in relation to the telecommunications service.

(2) Prior to undertaking the first high-risk customer transaction in the course of a high-risk customer interaction, an employee or agent of the carriage service provider for the telecommunications service who has completed fraud mitigation training must be satisfied that the requesting person is an unlisted authorised representative on the basis of documentary evidence (such as an enduring power of attorney or a financial management order) provided by the requesting person.

(3) If a carriage service provider completes one or more high-risk customer transactions under this section the provider must keep a record of the details of the transaction including:

(a) the basis on which the employee or agent of the provider was satisfied that the requesting person is an unlisted authorised representative; and

(b) any material or supporting evidence that was provided by the requesting person.

(4) If a carriage service provider completes, or is intending to complete, one or more high-risk customer transactions under this section, either prior to, or immediately after, undertaking the first high-risk customer transaction, the provider must send a notification to the customer, or the customer's authorised representative (***the relevant person***):

(a) by SMS message to the mobile service number which is listed on the customer's account as the contact number for the customer; or

(b) by email to an email address that has been validated by the relevant person; or

(c) by an in-app message to a carriage service provider's mobile application that has been validated by the relevant person; or

(d) to some other device or account which has been validated by the relevant person;

which informs the relevant person:

(e) that a high-risk customer interaction has been initiated; and

(f) what the relevant person can do if they did not authorise the transaction.

(5) The requirement in subsection (4) does not apply where there is no mobile service number, validated email address, validated mobile application or other validated device or account associated with the customer's account.

Authorised Version F2022L00548 registered 06/04/2022

(6) The requirement in subsection (4) does not apply where:

(a) the carriage service provider has reasonable grounds to believe that the customer is affected by domestic or family violence; and

(b) the customer has requested that the notification not be sent.

(7) If, in response to a notification sent for the purposes of subsection (4), a relevant person takes the action referred to in paragraph (4)(f):

(a) an employee or agent of the carriage service provider for the telecommunications service who has completed fraud mitigation training must investigate the basis on which the satisfaction required by subsection (2) was attained; and

(b) if the employee or agent is satisfied that there has been fraudulent activity in relation to the high-risk customer interaction,

then:

(c) if one or more high-risk customer transactions have already been completed by the carriage service provider, the provider must:

(i) take steps to immediately reverse or remediate any completed transaction;

(ii) notify the relevant person of steps taken by the carriage service provider under subparagraph (i); and

(iii) notify the relevant person of what they can do to protect the customer's account; or

(d) if a high-risk customer transaction has not yet been undertaken by the carriage service provider, the provider must not undertake a high-risk customer transaction and must:

(i) notify the relevant person that the carriage service provider has not undertaken the high-risk customer transaction; and

(ii) notify the relevant person of what they can do to protect the customer's account.

Part 4—Additional protections requirements

13 Requirements to provide fraud mitigation protections

(1) A carriage service provider must:

(a) have systems in place to identify customers of the carriage service provider who are at risk of fraud in relation to their telecommunications service; and

(b) provide those customers with fraud mitigation protections.

(2) A carriage service provider must, in response to a reasonable request made by a customer of the carriage service provider who believes they are at risk of fraud in relation to their telecommunications services, offer the customer fraud mitigation protections.

Authorised Version F2022L00548 registered 06/04/2022

(3) In subsections (1) and (2), ***fraud mitigation protections*** means additional or tailored measures taken by a carriage service provider which are designed to prevent fraud in relation to the customer's telecommunications service and which may include:

(a) notifying a customer of suspected fraudulent activity;

(b) "flagging" the customer's account as at risk of fraud;

(c) using multi-factor authentication in particular sale channels;

(d) pausing certain high-risk customer transactions on a customer's account; or

(e) sending notifications to a customer's authorised representative.

Part 5—General matters

14 Minimum requirements to publish advice about customer awareness and safeguard information

A carriage service provider must publish information on its website advising customers that:

(a) to protect customers from unauthorised high-risk customer interactions, identity authentication processes will be used to authenticate the identity of the requesting person, prior to the undertaking of a high-risk customer transaction; and

(b) in the event a customer suspects that their telecommunications service or account has been subject to fraud they should immediately report the activity to:

(i) their carriage service provider; and

(ii) their financial services provider.

15 Requirement not to charge a fee for a message or notification

A carriage service provider must not charge a fee to a customer, or a customer's authorised representative, for:

(a) a message sent for the purposes of paragraph 9(3)(c);

(b) a notification sent under subsection 10(5);

(c) a notification sent under subsection 11(4);

(d) a notification sent under subsection 12(4); or

(e) taking an action described in section 13,

except where a customer, or a customer's authorised representative, uses a telecommunications service to initiate a high-risk customer interaction that is not associated with the customer's account.

Authorised Version F2022L00548 registered 06/04/2022

Part 6—Record-keeping

16 Requirement to keep records

A carriage service provider must:

(a) keep records that are sufficient to demonstrate its compliance with the requirements in Parts 2, 3, 4 and 5 of this determination; and

(b) retain the records required to be kept by paragraph (a), subsection 11(3) and subsection 12(3) for a minimum of one year.

Authorised Version F2022L00548 registered 06/04/2022

Schedule 1 – Identity authentication process using category A and category B documents

(Paragraph 9(3)(e) and paragraph 10(2)(a))

(1) This Schedule sets out the identity authentication process which a carriage service provider must use to authenticate the identity of a customer, or a customer's authorised representative, for the purposes of paragraph 9(3)(e) or paragraph 10(2)(a).

(2) Category A documents are those mentioned in Table 1 and category B documents are those mentioned in Table 2.

(3) For paragraph 9(3)(e), and subject to clause (7), a carriage service provider may authenticate that the requesting person is the customer, or is the customer's authorised representative, for a telecommunications service by sighting 1 category A document identifying the customer, or the customer's authorised representative, and which includes a photo of the requesting person.

(4) For clause (3) the carriage service provider must undertake a visual comparison of the requesting person's face against the photo on the category A document either in person or by live audio-visual link.

(5) For paragraph 10(2)(a), and subject to clause (7), a carriage service provider may authenticate that the requesting person is the customer, or is the customer's authorised representative, for a telecommunications service by sighting:

(a) 2 category A documents identifying the customer, or the customer's authorised representative; or

(b) 1 category A document and 2 category B documents, identifying the customer, or the customer's authorised representative.

(6) For clause (5), the same type of document may not be used twice in an identity authentication process.

(7) For the purposes of the identity authentication process described in clauses (3) and (5):

(a) if a document (other than an Australian passport) shown to a carriage service provider includes an expiry date, the carriage service provider must be satisfied that the document has not expired;

(b) if a category A document is a foreign military ID card, the customer must show the document to the carriage service provider in an access-controlled defence site;

(c) if a document shown to a carriage service provider is dated but does not expire, the provider must be reasonably satisfied that the document is recent and accurate;

(d) the name in the category A document or category B document must (subject to paragraph (e)) match the name of the customer, or the customer's authorised representative; and

(e) if the name in the category A document or category B document does not match the name of the requesting person, the document may only be relied upon if the requesting person produces satisfactory documentary evidence of the name change.

Authorised Version F2022L00548 registered 06/04/2022

Table 1 – Category A documents

Item	Description of document
1	Australian State or Territory Driver's Licence issued in the name of the customer by a Commonwealth, State or Territory Department or agency.
2	Australian Passport with an expiry date in the future or no more than 2 years in the past.
3	A birth certificate issued by an Australian State or Territory government.
4	A foreign military ID card.
5	A current foreign passport issued by a foreign government which contains a valid entry stamp or visa issued by the Australian government.
6	Australian citizenship certificate issued by the Commonwealth government.
7	Certificate of identity or Document of identity issued by the Department of Foreign Affairs and Trade (or by any subsequent Commonwealth Department responsible for issuing a like Certificate of identity or Document of identity at the relevant time).
8	Immicard issued by the Department of Home Affairs (or the Commonwealth Government Department responsible for issuing Immicards at the relevant time).
9	Indigenous Community Card issued by Services Australia (or the Commonwealth Government agency or department responsible for issuing Indigenous Community Cards at the relevant time).
10	Firearms licence issued by an Australian State or Territory Police force and which includes the customer's, or the customer's authorised representative's, photo.
11	Aviation Security Identity Card issued by a body which is authorised by the Commonwealth government agency or department responsible for giving an entity authorisation to issue an Aviation Security Identity Card and which includes the customer's, or the customer's authorised representative's, photo.
12	Maritime Security Identity Card issued by a body which is authorised by the Commonwealth government agency or department responsible for giving an entity authorisation to issue a Maritime Security Identity Card and which includes the customer's, or the customer's authorised representative's, photo.
13	Australian Government Issued Photo ID card (employee ID) issued by the relevant Commonwealth, State or Territory government and which includes the customer's, or the customer's authorised representative's, photo.
14	Defence Highly Trusted Token issued by the Australian Department of Defence (or the Commonwealth Government Department responsible for issuing Highly Trusted Tokens at the relevant time).
15	Defence Force identity card issued by the Australian Defence Force and which includes the customer's, or the customer's authorised representative's, photo.
16	Police identity card issued by an Australian State or Territory Police Force and which includes the customer's, or the customer's authorised representative's, photo.

Authorised Version F2022L00548 registered 06/04/2022

17	Prisoner identity card issued by the relevant Australian State or Territory prison authority and which includes the customer's, or the customer's authorised representative's, photo.
18	A trade (work or business) licence issued by an Australian State or Territory government and which includes the customer's, or the customer's authorised representative's, photo (e.g. trade licences, real estate agents, security agents etc.).
19	Tangentyere Community ID card issued by the Tangentyere Council (or an organisation which replaces the Tangentyere Council) and which includes the customer's, or the customer's authorised representative's, photo.
20	Proof-of-Age card issued by an Australian State or Territory government and which includes the customer's, or the customer's authorised representative's, photo.
21	Australia Post Key Pass issued by Australia Post and which includes the customer's, or the customer's authorised representative's, photo.
22	Working with Children/Vulnerable card issued by a State or Territory government and which includes the customer's, or the customer's authorised representative's, photo.

Table 2 – Category B documents

Item	Description of document
1	Bank or financial institution card, passbook or statement issued by a bank, credit union or building society. Card statements or passbooks must cover at least 6 months of financial transactions and be in the individual's name. The individual's signature must be on the card and their current address on the statement or passbook. Documents from foreign banks or institutions are not acceptable.
2	Medicare Card.
3	Post-Paid Telecommunications Billing Record issued by an Australian telecommunications company, which must be a statement of account for a post-paid carriage service issued in the previous 12 months, showing the same name and address given by the customer to the carriage service provider prior to a high-risk customer interaction being initiated.
4	Rates Notice issued by an Australian local government council issued in the previous 12 months, showing the same name and address given by the customer to the carriage service provider prior to a high-risk customer interaction being initiated.
5	Student ID card issued by an Australian tertiary education institution, Australian secondary school, TAFE or registered training organisation.
6	Concession or health care card issued by Services Australia or the subsequent agency or Department responsible for issuing concession and health care cards.
7	Veterans affairs card issued by the Department of Veterans' Affairs.
8	Tenancy agreement or lease being a current formal agreement or lease showing the same name and address given by the customer to the carriage service provider prior to a high-risk customer interaction being initiated.
9	Motor vehicle registration for a vehicle registered in an Australian State or Territory, being current registration papers with the individual's

Authorised Version F2022L00548 registered 06/04/2022

	name, address and proof of payment, showing the same name and address given by the customer to the carriage service provider prior to a high-risk customer interaction being initiated.
10	Electoral enrolment, being proof of electoral enrolment showing the same name and address given by the customer to the carriage service provider prior to a high-risk customer interaction being initiated.
11	Seniors card issued by a State or Territory government to a resident in that State or Territory who is 60 years of age or over.
12	A utility account showing the same name and address given by the customer to the carriage service provider prior to a high-risk customer interaction being initiated.

Authorised Version F2022L00548 registered 06/04/2022