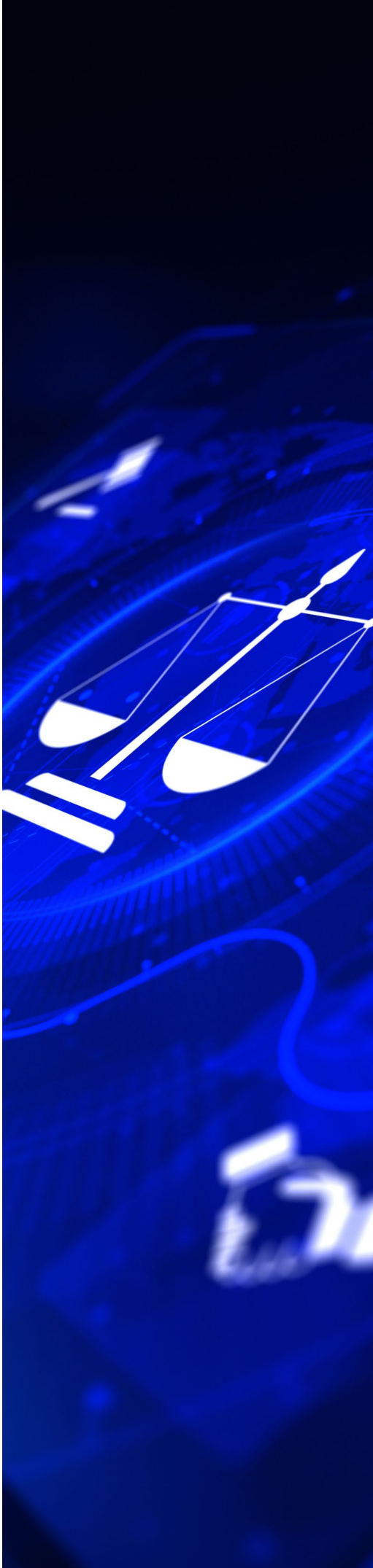
Understanding Customer Authentication

IAA Guidance to members on the:

Telecommunications Service Provider (Customer Identity Authentication) Determination 2022 - ACMA

Internet Association of Australia

Contents



Title: Understanding Customer Authentication, IAA guidance to members
Author: Sophia Joo
Published: May 2022

Executive Summary

IAA's guide to the new Customer Identity rules

On 8 April 2022, the Australian Communications and Media Authority ('ACMA') introduced a new set of rules, the Telecommunications Service Provider (Customer Identity Authentication) Determination 2022 ('Customer Identity Authentication Rules').

These new rules are intended to protect customers from identity fraud scams which occur over telecommunications networks, including unauthorised mobile porting and unauthorised SIM swap scams.

According to ACMA, between 1 January – 30 September 2021, financial losses resulting from fraud resulted in individual victims incurring losses of an average of over $28,000.

This paper seeks to guide members in understanding and implementing these new rules prior to their commencement on 30 June 2022.

NB: This guide will use the term "customers" to refer to both customers, and a customers' authorised representative.

New Rules

Who do they apply to?

Carriage service providers that are:

- Involved in the supply of a telecommunications service; and
- in conducting a high-risk customer interaction relating to a customer of a CSP
- *telecommunications services:* includes "a carriage service that enables customers to access the internet"
- NB: does not apply to an account managed customer or integrated customer (see glossary)

What are the new rules?

Multi-factor Authentication Requirements:

- where a high-risk customer interaction is initiated, the CSP must follow a multi-factor authentication process
- if the customer responds that they did not authorise the interaction, the CSP must take steps to reverse any transactions (if undertaken), and notify the customer of the steps taken by the CSP, and what they can do to protect their account
- Cf. s 9

Additional Multi-Factor Authentication Requirements:

- required where a high-risk customer interaction is initiated and the CSP has not been able to confirm the requesting person is not customer or the authorised representative

New Rules

What are the new rules?

Additional Multi-Factor Authentication Requirements: *(continued)*

- the CSP's employee/agent who has completed fraud mitigation training must follow a further identity authentication process
- Once the identity authentication process is used, the CSP must immediately send a notification to the customer to inform them that a high-risk customer interaction has been initiated; and what they can do if they did not authorise the interaction
- Cf. s 10

Identity Authentication for People in Vulnerable Circumstances:

- Required where a high-risk customer interaction is initiated and the CSP's employee/agent who has completed fraud mitigation training has reasonable grounds to believe that the requesting person is a person in vulnerable circumstances
- the CSP must keep record of high-risk customer interaction for a minimum of one year
- Cf. s 11

New Rules

What are the new rules?

Unlisted Authorised Representative Initiated High-Risk Customer Interaction:

- Required where a high-risk customer interaction is initiated and the requesting person asserts they are an unlisted authorised representative
- the CSP must keep record of the details of the transaction, including the basis on which the CSP was satisfied that the person is an unlisted authorised representative; and any material or supporting evidence provided by requesting person
- once the high-risk customer transaction is completed, the CSP must immediately send a notification to the customer/authorised representative to inform them that a high-risk customer interaction has been initiated; and what they can do if they did not authorise the interaction
- Cf. s 12

Requirement not to Charge a fee:

- The CSP must not charge a fee for messages or notifications sent to customers in relation to the use of an identity authentication process or initiation of high-risk customer interaction
- excludes where customer uses service to initiate a high-risk customer interaction not associated with customer's account
- Cf s. 15

New Rules

What are the new rules?

Requirements to Provide Fraud Mitigation Protections:

- The CSP must have systems in place to identify customers who are at risk of fraud and provide them with fraud mitigation protections
- the CSP must provide fraud mitigation protections in response to reasonable requests made by customers who believe they are at risk of fraud
- fraud mitigation protections: additional or tailored measures designed to prevent fraud in relation to customer's telecommunications service
- Cf. s 13

Minimum Requirements to Publish Advice:

- The CSP must publish information on their websites advising customers that:
- identity authentication processes will be used to authenticate the identity of the requesting person to protect them from unauthorized high-risk customer interactions; and
- in the event that a customer suspects they have been subject to fraud, they should immediately report this to their CSP and their financial services provider
- Cf. s 14

Glossary & Key Terms

- **Account managed customer:** CSP customer where provider assigns 1/+ employees/agents to be designated contact person for the customer
- **high-risk customer interaction:** interaction between CSP and requesting person where one or more high-risk customer transactions are requested
- **high-risk customer transaction:** a transaction which may result in one or more of the following:
  - customer loses access to their telecommunications service
  - a change to customer's personal information, business information, or account security information held by the carriage service provider
  - adding/removing a person as a customer's authorised representative
  - disclosure to requesting person of a customer's personal information, business information, or account security information held by the carriage service provider
  - *does not apply to information which:*
    - is included in a bill or other correspondence with customer;
    - is mostly hashed or obscured for the purpose of reminding a customer of their information;
    - is included in the notifications relating to a customer's telecommunications service usage
    - an additional ongoing, or a large one-off charge being applied to a customer's account

Glossary & Key Terms

- **Integrated customer:** customer who uses an integrated service desk provided by a CSP; or has a business-to-business service request system with a CSP
- **unlisted authorised representative:** person who is authorised by the customer, or a court, tribunal, or any other body legally empowered to represent customers, to act on behalf of the customer; other than an authorised representative
- **person in vulnerable circumstances:** 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 is experiencing the impact of an emergency or domestic or family violence);
  - (b) who due to 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 which, the CSP is consequently unable to complete the identity authentication processes under section 9(3) or subsection 10(2)

What This Means For You

Changes to policy often means changes for you and your business.

Employee training in identity authentication processes and fraud mitigation.

Potentially develop new procedures, software and systems according to identity authenication processes e.g. multi-factor authentication; notificaiton process.

Develop fraud mitigation protections.

Maintain record keeping processes.

Publish relevant advice regarding authentication processes and safeguards on website.

Helpful Contacts

Regulation can be difficult to understand, so talk to people who can help!

Internet Association of Australia Ltd
02 9037 6404
policy@internet.asn.au
www.internet.asn.au

ACMA
1300 850 115
info@acma.gov.au

ACMA Phone Scam Educational Resources: https://www.acma.gov.au/phone-scam-educational-resources

Determination: https://internet.asn.au/wp-content/uploads/2022/04/Telecommunications-Service-Provider-Customer-Identity-Authentication-Determination-2022.pdf

Explanatory Note: https://internet.asn.au/wp-content/uploads/2022/04/TSP-Customer-Identity-Authentication-Determination-2022-Explanatory-Statement.pdf