



ACCC submission to the Australian Communications and Media Authority

Telecommunications Service Provider (Customer Identity Verification) Determination

IFC 39/2021

December 2021

1. Introduction

The Australian Competition and Consumer Commission (**ACCC**) welcomes the opportunity to provide comments to the Australian Communications and Media Authority (**ACMA**) on the Telecommunications Service Provider (Customer Identity Verification) Determination 2021 (**the Draft Determination**).

Scammers often use access to a consumer's phone number as the first step to accessing bank and other services. For this reason, the ACCC strongly supports the introduction of the additional safeguards proposed in the Draft Determination.

The ACCC is the economy-wide competition and consumer regulator responsible for enforcing the *Competition and Consumer Act 2010* (**CCA**). The objective of the CCA is to enhance the welfare of Australians through the promotion of competition and fair trading and provision for consumer protection. The ACCC also runs the Scamwatch website (www.scamwatch.gov.au) and educates the community about how to recognise, avoid and report scams.

The ACCC welcomes the new rules to prevent fraud from unauthorised customer interactions with telecommunications providers. The Draft Determination complements safeguards in the Telecommunications (Mobile Pre-Porting Additional Identity Verification) Industry Standard 2020 (**the PPV Standard**) to improve identity verification processes by mobile carriage service providers.

Phone scams are a major and increasing threat to Australian consumers. They frequently result in both financial and personal information loss and often ongoing psychological harm. There has been an increase in losses to phone scams reported to Scamwatch of over 160% over the past 5 years.

Between 1 January and 14 November 2021, Scamwatch has received over 135,500 reports of phone scams, with reported losses of over \$77.6 million (an 86% increase compared to the same period in 2020). Scamwatch has also received over 61,000 reports of text message scams for this period, with associated loss of \$9.7 million (more than 300% increase compared to the same period in 2020). The ACCC notes that scam losses are under reported with only 12% of victims reporting to the ACCC. These figures are therefore represent a small portion of the real impact on the Australian community.

In 2018 the ACCC published its submission¹ to the *Review of the national arrangements for the protection and management identity information*. In that submission the ACCC advocated for better identity verification for mobile porting and has been pleased to see that the implementation of the PPV Standard has resulted in a decrease of mobile porting fraud. The ACCC continues to advocate for improved identify verification processes across all sectors.

Since that time the ACCC has worked in partnership with the ACMA on the Scam Technology Project and is a member of the Scams Telecommunications Action Taskforce. The ACCC also works with telecommunications providers to understand how they are meeting their requirements under the current standard. The ACCC provides regular reports of telephone numbers that have been reported to Scamwatch to a number of Communications Alliance members, including Telstra, Vodafone, Optus, Vocus, Pivotal, Aussie Broadband, MNF Group and NetSip.

In addition to the scam disruption work being undertaken by the ACMA, ACCC and other

¹ ACCC [Submission](#) to the *Review of national arrangements for the protection and management of identity information* (November 2018).

organisations, the ACCC considers it is imperative that there are enforceable regulations in place to help combat phone scams and supports the enhancements proposed in the Draft Determination.

In October 2021, the ACCC provided comment on Communications Alliance's proposed Industry Code DR C666:2021 "Existing Customer Authentication" (the Code). A copy of ACCC's submission can be found in **Attachment 1**. Communications Alliance is yet to finalise the proposed industry code.

The ACCC agrees with ACMA that it is an unusual approach to have two processes running concurrently, one being an industry developed voluntary code, the other being a regulatory instrument. The ACCC is of the view that a Determination will be more effective than a voluntary code self-governed by industry. A Determination will provide meaningful and enforceable obligations on the telecommunications industry. We make this consideration based on the demonstrable impact the PPV Standard has achieved in reducing fraudulent number porting.

Further, the ACCC considers it appropriate that the ACMA be granted a broad range of immediately available enforcement powers to address industry non-compliance.

The ACCC's comments on the Draft Determination are set out below.

2. Telecommunications Service Provider (Customer Identity Verification) Determination

The ACCC strongly supports the prohibition against high-risk interactions without the mandatory verification processes taking place (section 8). Further, the ACCC is pleased to see the following important consumer protections included in the Draft Determination:

- clear obligations on service providers to undertake multi factor identity verification to confirm that the requesting person has direct and immediate access to the telecommunications service (Part 9).
- obligations on service providers to provide additional protections when specifically requested by the customer (section 12).
- a requirement to provide the customer with a contextual explanation of why a unique verification code has been provided in identity verification, and advise the customer not to share the code with other parties (section 9(2)(b)(ii)). This is a standard that the ACCC supports for all One-Time-Pins.

Additional protections would be useful in five key areas:

i. SIM swapping as a 'high-risk customer interaction'

While SIM swap requests are included in the definition of '*high-risk customer interaction*', the Draft Determination should qualify explicitly in the definition that 'a SIM swap request is considered a modification of a customer's account associated with the telecommunications service'. This may help ensure that SIM swaps, which can result in the loss of individuals' entire bank accounts, are always captured by provisions placing higher requirements on these interactions, such as the multi-factor identity verification requirements in section 9 of the Draft Determination. Having SIM swaps considered in this way may assist external arbiters such as the Telecommunication Industry Ombudsman when reviewing cases involving alleged breaches of section 10 involving SIM swaps.

ii. Mandatory delay period for SIM swap requests

Section 10 of the Draft Determination should include a mandatory delay period for all SIM swap requests that is sufficient for a legitimate customer to be able to respond and inform the carriage service provider that there has been an unauthorised high-risk transaction attempt.

Many SIM swap reports to Scamwatch note a loss of service either overnight or when distracted for multiple hours in a row. This is often intentionally timed by the scammer to coincide with the victim's sleeping hours. A SIM swap without some form of mandated wait does not provide sufficient time for consumers to intervene and means a subsequent bank or email account compromise is more likely.

The ACCC appreciates that a balance between customer experience and consumer protection is required and suggests a mandatory delay period of 10 hours on this basis. We note that this time would delay the swap process. The consumer would continue to have an active phone service during this delay. The 10 hour delay period would not need to apply to a customer who attends in person with a Category A document and their identity can be compared directly with their photograph.

iii. Identity verification where no response received 24 hours after instigation of high-risk interaction

The ACCC considers that current document check processes for the purposes of identity verification could be improved significantly in the telecommunications sector.

The ACCC recommends that the ACMA review the processes outlined in section 10 to provide more robust protection to customers where the provider has not been able to confirm that the requesting person is the customer for the service within the 24 hour period. The ACCC suggests that a provider should be required to send a further warning to the customers mobile service and if provided an email address prior to relying on the use of Category A and/or B documents or the government verification service (sections 10 (2)(a) and (b)).

The ACCC notes that the use of the government online verification service will only confirm that documents match, this means that scammers who have access to personal information or documents can provide that information or document in an attempt to take over a mobile phone account. If the provider verifies that the documents match and sends a further request to the customer which does not receive a response (as per section 10(4)), the ACCC suggests the Draft Determination should make it clear to providers that the request should not proceed or should not proceed until a further 24 hours has lapsed.

Current document check processes in the sector simply confirm that the information provided to the telecommunications provider matches what they have on file. This does not prevent scammers from using this (stolen) information to access customers' accounts.

The ACCC continues to advocate for enhanced security measures around identity verification and driver licences. The ACCC has been working with the Department of Home Affairs to ensure the Document Verification Service (**DVS**) processes are robust. Specifically, we have been seeking agreement with state/territory driver licence authorities on a nationwide solution that will enable the use of a unique identifier number (**UID**) on each new driver licence issued. The UID will be in addition to a driver licence number. The Department of Home Affairs have been working to add this additional layer of security, the UID field, to the DVS and on the National Exchange of Vehicle and Driver Information System (**NEVDIS**). Most states and territories have uploaded the UID data into NEVDIS. An additional feature of the updated NEVDIS system will be the ability to flag stolen or lost driver licences. NSW has made it

mandatory that by mid-2022 only the most recent driver licences (with the UID) will be validated in NEVDIS. Home Affairs is working with other states to ensure similar mandatory feature is implemented.

Telecommunication providers, as users of DVS, should make system changes to ensure they are able to input and verify the driver licence UID field when performing an identity verification check. This check will ensure the customers' most recent driver licence is being used and that it has not been flagged as lost or stolen. The Draft Determination should include a provision that states that where a Category A document is being used the provider should undertake a process to verify that a driver licence is not lost or stolen where that feature is available.

iv. Identity Verification with reference to Category A documents

The ACCC is concerned about the reliance on photo documentation from Category A (section 10(2) of the Draft Determination) without a corresponding comparison of customers' physical appearance.

Category A documents are generally considered a stronger authentication method because they contain a photo. In Australia, modern identity theft occurs less often with forged documents (though we acknowledge synthetic identity use is prevented by the verification suggested in the Draft Determination) and more commonly with stolen credentials obtained through:

- Physical mailbox compromise
- Email compromise
- Requests for driver licences in electronic marketplace sales to 'verify' the victim's identity.

There are many existing compromised Category A documents already in the hands of scammers. The Draft Determination should mandate a physical comparison with the customer; by (phone or computer) video, or through physically appearing in front of staff. Ideally more than a still camera shot would be required, but this would still be a significant additional safeguard compared with the current requirement.

v. Customers in vulnerable circumstances

In November 2021, the ACCC released its publication [Consumer vulnerability: A business guide to the Australian Consumer Law](#). This publication is designed to help businesses understand their key responsibilities under the Australian Consumer Law and how to engage with consumers experiencing vulnerability. We also note ACMA's current consultation process on its Statement of Expectations on Consumer Vulnerability.

In addition to the definition of 'customers in vulnerable circumstances' in section 6, the Draft Determination should reference guidance material to assist providers in understanding the broad range of circumstances that can increase vulnerability.

The ACCC understands that there may be some situations where consumers experiencing vulnerability who don't have direct access to their device may have difficulty providing information required in the Draft Determination. The ACCC recommends that some flexibility should be considered for vulnerable consumers who have accessibility requirements, but there needs to be sufficient obligations in place to ensure that vulnerable consumers are not more exposed to fraud and scams. It is often vulnerable consumers who are disproportionately impacted by scams so the ACCC expects that these consumers also

receive an appropriate level of protection.

3. Case studies

The following case studies are reports to Scamwatch from the public which illustrate how entire individual and/or business bank accounts can be stolen as a result of a sim swap or any other process that enables the takeover of a phone. The reports are modified to protect the privacy of the reporters.²

Case Study 1- \$800,00 lost

David's wife found her phone in SOS status around 9pm on 23 October 2021. David thought it was just because of a bad signal. He asked his wife to restart her phone. David then attended a ZOOM meeting from 9 to 10pm. He then found that his ANZ and Westpac online banking accounts had all been locked. When he went to call ANZ he found his phone was also in SOS status. David used another number to call ANZ who told him that 2 transactions had been made. While the bank was able to stop one of them the other remained to be dealt with.

David then called Westpac and they said that all of his accounts had been suspended so David did not know what was going on in his Westpac accounts. David had about \$800 000 in that account. Then David logged into his Liberty online account where he found that there was a transaction of \$2 300 made by someone else (the scammer) to the scammers account. David did not make the transaction. David called Liberty but they were out of business hours and he could not reach them. Not knowing what to do David called 000 and they told him to report to Scamwatch. David reported that the scammer got his information and access via the fraud SIM card.

Case Study 2 - \$77,000 lost

Sarah received messages from Optus around 8am Friday morning saying her password had been changed. She had been noticing a lot of scam text messages around that time and thought the message from Optus was another of those. A short time later her phone had no signal and she was no longer able to make phone calls.

She went to Optus and discovered that someone had access to all her personal details and was able to call up Optus and request a new sim transfer. While Sarah was trying to sort out the phone through Optus she started to notice in her emails that a lot of her accounts had password change activations. She then noticed that Coinspot had a withdrawal request and the scammer was even replying via her email account. Sarah messaged Coinspot straight away and asked them to suspend the account as it had been accessed. Coinspot called her later that day and said her account had been wiped. Coinspot explained that they spoke to the scammer and the scammer was able to verify all of Sarah's details so they processed the transaction.

² Reports are reproduced largely as reported by the consumer, however small edits are made to improve readability, fix errors, remove personal information or reduce content.

**Attachment to Certificate of mandatory consultation on
an industry code under Part 6 of the
*Telecommunications Act 1997***

Comments from ACCC:

This Code applies to the authentication of existing customers (so not new customers). Its objective is to prevent unauthorised access or unauthorised actions on their accounts. In terms of scams we know that inadequate verification processes can lead to phone porting fraud, SIM swapping fraud and the ordering of additional handsets or other alterations to a customer plan. We note phone porting has its own Industry Standard so the application to porting here is limited.

The dangers of SIM swapping are the same as for phone porting however this proposed Code appears to have lower requirements for verification than those in the *Telecommunications (Mobile Number Pre-Porting Additional Identity Verification) Industry Standard 2020*. At the very least the requirements should be the same. In addition, we remain concerned about the telecommunications industry not mandating the visual comparison of photographic identification with the person.

Customer Authentication Measures are vague and unenforceable (clause 3.1)

We are concerned that section 3.1 'Customer Authentication Measures' prioritises the level of Customer Authentication required based on the value and potential risk of harm to the Customer of the transaction. We don't think it's appropriate to leave this up to the CSP – from a consumer protection perspective this means there will be different levels of protection for different situations with different CSPs. The potential for harm arising from SIM swapping is significant and therefore should always attract the highest level of verification.

***Clause 3.1.2** A CSP must designate High-Risk Transactions based on whether the transaction relates to a Consumer or Large Business Customer, and what will be the impact of the associated transaction and the potential risk of harm to the Customer of the transaction.*

***Clause 3.1.3** A CSP must ensure that the Customer Authentication measures, or security practices are commensurate with the value and potential risk of harm to the Customer of the transaction.*

Clause 3.1.2 and 3.1.3 as drafted are open to wide interpretation, subjective and likely unenforceable. We recommend changing the definition of High Risk Transaction to ensure it provides a list of transactions (such as SIM swapping; changes to any identity or contact information held by the CSP) that **must** be considered high risk transactions.

Clause 3.2.2 (outlined below) is vague and potentially unenforceable. Specifically, the reference to 'appropriate' provides too much discretion.

Section 3.2.2

CSPs must ensure that customer facing service solutions implement appropriate levels of Customer Authentication, which may include electronic forms of authentication, or verifying the identity of the Requesting Person by viewing either;

- *1 Category A Document (identifying the Customer); or*
 - *2 Category B Documents, each of a different kind (identifying the Customer).*
- Scammers often have access to a wide range of personal information about individuals and we are concerned by any move toward purely oral authentication for transactions that may result in the compromise of a consumer's bank account.

- We are concerned by the permissive use of 'may' and would suggest 'must' with a caveat for exceptional circumstances or impossibility.

Identity verification standard should not be lower than the standards that are set out in the Telecommunications (Mobile Number Pre-Porting Additional Identity Verification) Industry Standard 2020

- The dangers of phone porting are nearly identical to those in SIM-swapping.
- It is concerning that the document verification in the equivalent code for 'mobile porting' mandates the use of 2 Category A documents, or a combination of 1 Category A document and 2 Category B documents.
- The Code should not provide a lower standard of a single Category A document, or no Category A document and 2 Category B documents.
- Photo identification is crucial in the modern context of identity thieves targeting physical mailboxes and electronic mailboxes to obtain category B documentation such as bills.
- The Code should mandate the provision of a Category A document and a visual comparison with the applicant (see below).

Photo identification should be used in conjunction with a visual comparison of the applicant

- ACCC feedback on this point is similar to that provided to the Telecommunications (Mobile Number Pre-Porting Additional Identity Verification) Industry Standard 2020.
- Under 3.2.2, the CSP can ask the customer to provide identity verification using 1 category A documents, or 2 category B documents.
 - A scammer could provide a stolen or deceptively obtained category A document such as: a Driver's License, or Proof of Age Card.
- Transaction processing should require in-person in-store matching with the category A (photographic) identity document, or live-online-webcam matching with the category A (photographic) identification.
 - This is the standard with mobile dating applications and online cryptocurrency exchanges.
 - Both of these environments present lower security risks than sim swapping, noting the potential for bank account compromise.
- The Code's documentation requirements should match those in the Telecommunications (Mobile Number Pre-Porting Additional Identity Verification) Industry Standard 2020 to ensure the use of photo identification. I.e. 2 Category A documents or 1 Category A document and 2 Category B documents.

Multi Factor Authentication is not a substitute for a visual comparison of a photographic identification document

- We support the inclusion of mandatory Multi Factor Authentication in instances for High Risk Transactions and consider Section 3.3 to provide useful additional protections.
- As stated above, we consider that all SIM-swapping transactions should be considered High Risk by default.

As with our submission in relation to Mobile Phone Pre-Porting Verification, we reiterate that existing data leaks and dedicated identity thieves' access to documentation necessitates a response that includes a visual comparison of any applicant and a photographic identification document.