Telecommunications Industry Ombudsman

Submission to the ACMA Proposal to make the Telecommunications Service Provider (Customer Identity Verification) Determination

December 2021

Contents

Introduction

Thank you for inviting the Telecommunications Industry Ombudsman to comment on the ACMA's proposed *Telecommunications Service Provider (Customer Identity Verification) Determination 2021* (the **Determination**).

We strongly support regulation requiring telecommunications providers to have more robust identity verification procedures for all high-risk transactions and welcome the draft Determination as it contains important consumer safeguards.

This new regulation is timely, as the advent of the COVID-19 pandemic has coincided with an increase in scams and fraud committed using phone and internet services.[1] As we become increasingly reliant on online platforms to complete every-day tasks, the risks posed by telecommunications-related fraud also increase. In the last financial year, our office received over 500 complaints from consumers who said they had fallen victim to telecommunications-related fraud.[2]

In November 2021, we published a systemic investigation report *Defending phone and internet accounts from fraudsters* (**Systemic Investigation Report**) which highlights the significant harms consumers suffer when their telecommunication accounts are accessed fraudulently. Common kinds of fraudulent activity observed in the report include fraudulent SIM swaps, fraudulent orders for devices like smartphones, and theft of personal information from telecommunications accounts. These fraudulent activities can have devastating impacts for affected consumers, such as theft of significant sums of money, large debts accruing on the victim's telecommunications account, identity theft, and threats to personal safety.

We offer observations on areas in which the Determination could be strengthened or clarified to improve its effectiveness, drawing on our experience in dealing with complaints about telecommunications-related fraud.

Once the Determination comes into effect, our office will continue to handle complaints about fraudulent access of telecommunications accounts. Our office will also continue to monitor emerging trends, conduct systemic investigations, and refer systemic issues to the ACMA when necessary.

[1] See the ACCC's media release, 'Losses reported to Scamwatch exceed $211 million, phone scams exploding', 27 September 2021.

[2] See our systemic investigation report, *Defending phone and internet accounts from fraudsters*, November 2021, page 2.

1. The definition of 'high-risk customer interactions' should be expanded to cover other interactions vulnerable to fraud

We welcome the Determination's broad definition for 'high-risk customer interactions' to which its authentication procedures apply. This definition should cover most of the customer interactions commonly targeted by fraudsters, such as SIM swaps, changing or adding to information listed on a consumer's account, or accessing an account to obtain personal information about a consumer.

The ACMA has invited comment on whether the definition captures all of the interactions targeted by, or vulnerable to, scammers. Our complaints have revealed other customer interactions vulnerable to fraud which are not currently within the scope of the proposed definition. We have identified two areas where the definition of 'high risk customer interactions' could be expanded to ensure the Determination's effectiveness.

1.1. Interactions that add a product or device onto a customer's account

We recommend the definition of 'high-risk customer interaction' be expanded to cover interactions that add a product or device to a consumer's account.

The Determination's definition covers interactions where the provider 'adds or removes a telecommunications service from a customer's account or modifies an existing telecommunications service'. It does not explicitly cover interactions where the provider adds or removes devices or other products from a customer's account.

One common type of fraud we see is where fraudsters access a consumer's account and order new devices such as smartphones. The fraudster directs the provider to send the devices to a new address and sometimes changes the consumer's registered contact details so the consumer does not receive notifications about them. The fraudster takes possession of the devices and the consumer is often left with associated debts.

Case study 1: A fraudster orders multiple mobile handsets on Sam's telco account

Sam* received a call from someone claiming to be from his telco, Bluestone Connect. The person offered to apply a discount to all Sam's services as a special COVID-19 assistance measure.

The person who called Sam knew all of his account details, so Sam was convinced they were calling from Bluestone Connect. The person asked Sam to tell them the confirmation codes he had received by SMS to provide the discount, which Sam did.

Sam received a flood of emails thanking him for upgrading his phone plan, followed by a fraud alert email from Bluestone Connect. He then received a call from Bluestone Connect, checking whether he had upgraded his services and ordered new phones. Sam said he had not ordered anything.

Sam later found out from Bluestone Connect that a fraudster had used his account to order multiple new mobile handsets. He also made a statutory declaration and reported the fraud at a police station.

Sam was charged cancellation fees for the cancelled mobile services and handsets. He disputed the charges with Bluestone Connect, but Bluestone Connect stopped responding to his requests for updates. After Sam complained to us, Bluestone Connect eventually agreed to refund the charges.

** Names of all parties have been changed*

*** This case study first appeared in our Systemic Investigation Report*

1.2. Additional examples of prescribed high-risk customer interactions

We welcome the ACMA's inclusion of a list of prescribed high-risk interactions in the definition. This part of the definition provides clarity for consumers and providers about what interactions are covered and supports consistent application of the Determination between providers.

The ACMA may also wish to provide further examples to the definition's non-exhaustive list, such as adding an authorised representative to a consumer's account and changing the consumer's contact information.

2. The proposed authentication procedures could be strengthened

As we noted in our Systemic Investigation Report, fraudsters are often able to exploit weak identity verification processes to gain access to telecommunications accounts. Further, even where providers have notionally robust authentication processes, their staff do not always follow the processes consistently.

We are pleased sections 8 – 10 of the Determination set out requirements for well-defined multi-factor authentication (MFA) procedures for all high-risk customer interactions. The ACMA has invited comment on whether there are additional examples of account information, personal information and possession-based authenticators that should be covered by these definitions. To maximise their effectiveness, we have identified the following areas where the proposed procedures could be strengthened.

2.1. MFA should not be based on information that may be readily available to fraudsters

The default MFA procedure in section 9 of the Determination partly relies on 'personal information authenticators', and 'account information authenticators'.

We recommend the Determination is drafted to explicitly exclude certain information from being used for these authenticators. MFA procedures should not use information that may be publicly accessible to fraudsters, such as full names, dates of birth, postal addresses and email addresses. As we observed in our Systemic Investigation Report, fraudsters are often able to access this kind of information in the public domain and through social media.[3]

Account information authenticator

An 'account information authenticator' is defined as an authentication process based on the requesting person's knowledge of the customer's account security information. 'Account security

[3] See Finding 1, page 6 of our Systemic Investigation Report.

information' is defined broadly as 'information which is created for the purpose of applying security to an account'.

The definition contains a non-exhaustive list of possible account security information, which includes account login information used to log into a provider's website or mobile application. It is common practice for telecommunications providers to use a registered email address as a username for login purposes. However, email addresses are often widely circulated by consumers and could be easily obtainable by a fraudster.

Personal information authenticator

A 'personal information authenticator' is defined as an authentication process based on the requesting person's 'knowledge of the customer's personal information that is not account security information'. This appears to include processes based on knowledge of information that may be publicly accessible, such as dates of birth.

2.2. The possession authenticator options should be expanded

We welcome the prescribed use of possession authenticators[4] as part of the default identity verification procedure in section 9 of the Determination. Possession authenticators add an additional level of security to authentication procedures because they confirm the person requesting a transaction has direct and immediate possession of the customer's registered device or service.

We recommend expanding the possession authenticator options to include the use of 'public/private' cryptographic keys.[5] These authenticators may not be covered by the range of possession authenticator options available under section 9(2) of the Determination, because they do not require a unique verification code to be sent to the customer by the provider.[6] Instead, we understand the customer's device or app uses its private key to generate a signature or code that can be verified by the provider's IT system.

Secure identity verification using public/private cryptographic keys through a mobile authenticator app or other device is common across the IT and banking sectors. One regularly used example of this kind of authenticator is the Microsoft Authenticator. It is not clear whether this kind of authenticator would be covered by the possession authenticator options in section 9(2).

[4] These authenticators are contained in section 9(2) of the Determination.

[5] Where a consumer uses this form of authenticator, an app on their device generates a secure cryptographic key to be stored secretly on the device (the user does not have visibility of the key). The app also generates public keys, which can be shared with service providers to link a customer's account to the authenticator app. When the consumer wants to access their account, the provider's IT systems communicate with the consumer's app to generate a prompt on the app for the consumer to validate the interaction (for example by pressing a button or entering a PIN on the app). If the consumer validates the interaction, the private key on their device interacts with the public key given to the provider to complete authentication.

[6] Section 9(2)(b)(i)(C)-(D) of the Determination refer to unique verification codes sent by in-app messages to a customer's mobile app or some other device or account, by the provider.

They are a particularly secure form of verification because the customer does not have visibility of the relevant codes, so they are less vulnerable to phishing or social engineering.

2.3. Verification procedures using ID documents are appropriate but could rely on original documents

We support the inclusion of the supplementary verification procedure in section 10, using 'category A' and 'category B' identity documents (mostly government-issued forms of ID). This procedure is a reasonably secure alternative option for authenticating customers who do not have access to a service or device to satisfy the possession authenticators in section 9(2).

We also consider the proposed 24-hour timeframe for providers to complete the supplementary verification process to be appropriate. If a consumer does not have identity documents to hand within the 24-hour timeframe, it will be open to them to reattempt the procedure when they have access to their documents.

The procedure appears to be closely modelled on a similar procedure we supported in the *Telecommunications (Mobile Pre-Porting Additional Identity Verification) Industry Standard 2020* (the **PPV Standard**).[7] In line with our comments to the ACMA's consultation on the PPV Standard, we suggest this supplementary process could be strengthened by requiring providers to sight *original* category A and B documents.

3. Alerts about high-risk interactions are beneficial and should be sent to all consumers

We welcome the proposed requirements for providers to contact consumers during the identity verification process or after a high-risk customer interaction has taken place (**the Alert Requirements**).[8] It is beneficial for consumers to be warned that a high-risk interaction will occur or has occurred and to be advised on what they should do if they did not authorise the interaction.

Complaints to our office show consumers are often unaware fraudulent activity has affected their account until long after the activity has occurred, for example when their application for a home loan is declined because of a default listing resulting from a fraudulent debt.[9] In these circumstances, by the time the consumer reports the fraudulent activity to their provider it is usually too late for the provider to reverse the activity. The Alert Requirements may go some way to addressing this problem.

However, we are concerned the Alert Requirements will only apply where a consumer has a registered mobile number, email address or mobile app with their provider.[10] This would appear to exclude consumers who only have a landline service (a cohort that may include elderly and other vulnerable consumer groups).

[7] See our submission to the ACMA's consultation: *New rules to prevent mobile number porting fraud*, January 2020, page 3.
[8] Section 9(2)(b)(ii), Section 10(4), Section 11(5).
[9] See page 2 of our Systemic Investigation Report.
[10] Section 10(4)-(5), Section 11(5)-(6).

We recommend the Alert Requirements apply to all consumers, irrespective of what contact information they have registered with the provider. Where a consumer only has a landline service, providers could be required to call the consumer to alert them.

4. Flexible verification procedures for consumers in vulnerable circumstances should have an additional guardrail

We support the ACMA's inclusion of flexible verification procedures for consumers in vulnerable circumstances (such as family violence or natural disaster) where they may not reasonably have access to either a device or to identity documents (section 11).

We welcome requirements for training and monitoring

We are pleased to see providers will be required to use staff trained in fraud mitigation to administer the process, and to record why they reasonably believe a customer is in vulnerable circumstances. We also support the requirement for providers to monitor a customer's account for fraudulent activity for 30 days after the process has been completed and contact the customer within 24 hours if they become suspicious of fraudulent activity.

Additional guardrail to strike a better balance between accessibility and security

The ACMA has invited comment on whether there are additional processes that should be considered in relation to the flexible verification procedure.

Our experience dealing with fraud complaints shows flexible authentication procedures are often vulnerable to exploitation by malicious actors. Accordingly, an additional guardrail may be appropriate.

The section 11 procedure is currently available to any person who can persuade a provider they are not able to access category A and B identity documents or a device for MFA because of their vulnerable circumstances. The procedure may expose consumers to the risk that a fraudster will be able to use the less rigorous verification process to authenticate *any* fraudulent high-risk interaction. For example, if a fraudster convinces a provider they satisfy the vulnerability criteria and accesses the procedure, they could use it to authenticate fraudulent orders for a large number of smartphones without any explanation of why the devices are needed.

To avoid this kind of exploitation and limit the risk the procedure presents for consumers, we suggest it be limited only to high-risk interactions that are *reasonably necessary* to address the customer's vulnerable circumstances. This still provides valuable flexibility for consumers experiencing vulnerability because it allows them to authenticate high-risk interactions to address their circumstances when they may not otherwise have been able to do so. For example, a consumer who is in a family violence situation and cannot go back to their family home to collect a device or identity documents without risking physical harm, may be able to use the process to order a new phone service and device they need for safety reasons.

We believe this approach could strike a better balance between accessibility for customers experiencing vulnerability and protecting the security of customer accounts (including those held by customers in vulnerable circumstances).

5. Allowing consumers to request additional verification procedures is welcome but could be clarified

We welcome the requirements for providers to implement additional account security measures on a customer's request (section 12). This includes implementing a customer's 'valid request' to only use a particular identity verification method for future high-risk transactions. These valuable reforms may help to address our finding that fraudsters often exploit providers' delayed responses to breaches of account security.[11]

Our complaint handling experience shows while providers do sometimes agree to implement an additional security measure for a consumer, their staff do not always follow the agreed procedure consistently.

While we support the requirements in section 12, we encourage the ACMA to provide further clarity around how the requirements will interact with the flexible authentication procedure in section 11. It appears unclear which of the two procedures will take precedence if a consumer has made a valid request to limit the authentication procedures available for their account under section 12, but later contacts their provider saying they are in vulnerable circumstances and need to access the procedure in section 11.

Case study 2: Lucien's provider did not follow the additional security measure he requested

Lucien received an SMS from his provider at 11.30pm saying his registered contact details had been changed and to contact his provider as soon as possible if he had not made these changes. Lucien immediately tried to call his provider to report he had not made the changes. Because he called after business hours, Lucien received a recorded message asking him to call back after 9.00am the next day.

When Lucien called his provider the next morning, his provider confirmed Lucien's registered email address had been changed, and agreed to restore the original email address. Because of Lucien's concerns about his account security, his provider placed a password on the account and said Lucien would need to quote the password whenever he wanted to make changes to his account.

One hour later, Lucien's mobile phone lost service and he found the passwords for his email address, internet banking account and myGov account had all been changed.

When we investigated Lucien's complaint, we found his provider had not asked the fraudster to provide Lucien's password on second and subsequent access attempts. It had instead authenticated the fraudster by asking for Lucien's address and account number. The fraudster was able to provide this information and process a SIM swap, giving them access to Lucien's mobile number. They then used their access to the mobile number to complete two factor authentication and reset the passwords on Lucien's other accounts.

** Names of all parties have been changed*

*** This case study first appeared in our submission to Communications Alliance's consultation on the exposure draft of its Existing Customer Authentication Industry Code (C666:2021), in September 2021.*

[11] See Finding 2, page 9 of our Systemic Investigation Report.