Telecommunications Industry Ombudsman

Submission to Communications Alliance's Existing Customer Authentication Industry Code (C666:2021) Exposure Draft Consultation

September 2021

Introduction

Thank you for the opportunity to comment on Communications Alliance's Exposure Draft for its new *Existing Customer Authentication Industry Code* (C666:2021) ('the Code').

As telecommunications services continue to play an increasingly central role in the management of our everyday lives, fraud committed via telecommunications services poses a significant risk to consumers. We regularly receive complaints about fraud committed using telecommunications services, and the consequences of such fraud for consumers can be severe. This can include theft of money, personal information, and sometimes identity theft. Our experience handling complaints has shown increased customer authentication safeguards are required to protect consumers.

We welcome the development of regulatory safeguards to protect consumers from fraud. To strengthen the Code, Communications Alliance may wish to consider expanding the Code to provide a greater level of detail in key areas, clarifying what providers must do to protect consumers, and ensure consistency of application across the industry.

1. The scope of the Code and use of terminology could be clarified

To ensure the scope of activities to which the Code applies is clear, Communications Alliance could consider clarifying the terminology and definitions used in the Code.

Section 1.3.3 of the draft Code says it applies to the authentication of 'requesting persons' where they seek to conduct a 'transaction on / or to gain access to the information of an account or Telecommunications Service.' However, the Code does not define 'transaction' and it is unclear what is meant by 'information of a Telecommunications Service.' Draft section 1.3.3 is also unclear about whether the Code regulates attempts to access a Telecommunications Service, such as through a SIM swap.[1]

Some terms are used inconsistently throughout the Code, including some capitalised defined terms. For example, the definition of 'Consumer' contained in Part 2 of the draft Code says a Consumer is a 'person who acquires or may acquire Telecommunications Products', but the capitalised term 'Telecommunications Product' is not defined. The remainder of the Code does not refer to Telecommunications Products, but instead uses the term 'Telecommunications Services' as defined in the *Telecommunications Consumer Protections Code*.[2]

The Code could also benefit from the inclusion of further defined terms, such as 'Existing Customer', 'Customer Contract', and 'Customer Facing Customer Service Solution'[3]

[1] We note Communications Alliance's stated intention that the Code address types of fraud that cause consumers to lose access to their telecommunications service.

[2] Section 2.2 of the draft Code; Section 2.1, Telecommunications Consumer Protections Code (C628:2019).

[3] Section 3.2.2 of the draft Code says 'customer facing customer service solutions must ensure appropriate levels of Customer Authentication', but there is no guidance in the Code about what 'customer facing customer service solution' means.

2. The Code could prescribe high risk transaction types for the purposes of Multi Factor Authentication

We welcome the inclusion of general principles for customer authentication in section 3.1 of the draft Code. However, these principles alone may not provide sufficiently robust protections. Section 3.1.4 contemplates each provider will designate the transaction types it considers 'high risk' for the purposes of the Code. This designation is important because 'high risk' transactions are subject to the increased protections of Multi Factor Authentication (MFA) under section 3.3 of the Code.

A framework that allows individual providers to determine what is a high risk transaction may not be appropriate or effective in preventing some common types of fraud.

To ensure consistency for consumers across different providers, Communications Alliance could include a list of transaction types that will always be considered 'high risk' for the purposes of the Code. This may provide a baseline level of protection for transaction types known to be common vectors of telecommunications fraud. The list could include transaction types such as:

- requesting a SIM swap
- adding an Authorised Representative to an account
- changing contact details
- ordering new services or devices
- accessing a provider's online portal.

Case Study 1: A fraudster signed up for devices in Alexis' name

Alexis met John online and formed a romantic relationship with him. John told Alexis he had ordered five mobile phones for his family and was going to get them delivered to Alexis' address. Alexis agreed to receive the phones and send them on to John at his address in Ghana.

Six months later, Alexis received a letter from a debt collector saying she owed her mobile provider around $8,000. Alexis called her provider and was told the debt was for the five mobile phones. Her provider told her she had ordered the phones online and confirmed receipt of them at her home.

It was news to Alexis that the phones had been ordered on her mobile phone account. She had not agreed to pay for the phones, only to receive and forward them to John. She realised John had tricked her and used information he knew about her to order the handsets in her name.

When we investigated Alexis' complaint, her provider told us Alexis had signed up for the mobile devices online and had provided personal information such as her address, email address and mobile number to establish her identity. Alexis' provider was not able to provide any further information showing it had established her identity. We directed Alexis' provider to waive the entire $8,000 debt.

** Names of all parties have been changed.*

3. The Code could provide a procedure for in-store authentication

We support the inclusion of provisions for in-store authentication. This would provide appropriate protections for all consumers, however they choose to transact with their provider.

However, the draft Code is not clear about what providers are required to do to authenticate consumers in-store. Draft section 3.2.2 simply says 'customer facing customer service solutions must ensure appropriate levels of Customer Authentication.'

Communications Alliance could expand on this requirement by including a procedure providers must follow for in-store authentication. The process could be based on the additional identity verification process contained in Schedule 1 to *Telecommunications (Mobile Number Pre-Porting Additional Identity Verification) Industry Standard 2020*.

There should also be an alternative and robust procedure if in-store authentication is not practical or possible for the consumer. There are a variety of circumstances in which consumers may not be able to go to a store, for example for health or mobility reasons.

4. The Code's MFA process could be strengthened

We support the Code's requirement that providers use MFA to authenticate all high risk transactions. However, draft section 3.3 may not provide a sufficiently robust procedure to prevent fraudsters circumventing customer authentication.

To strengthen the MFA process, Communications Alliance may wish to consider making the following changes to section 3.3:

a) **Require that the 'knowledge authenticator' must not be information about a consumer that may be readily available to fraudsters.**

   We often receive complaints where a provider allowed a fraudster to complete customer authentication using information such as the customer's account number, date of birth or full name. To mitigate this risk, Communications Alliance could consider forms of authentication used in other industries, such as banking and financial services.

b) **Exclude the use of email addresses as 'possession authenticators', as this may not provide sufficient protection.**

   Complaints we receive show a fraudster often already has access to a consumer's email address when they attempt to access the consumer's telecommunications account.

c) **Include a prescribed customer authentication process that providers must use when a requesting person says they cannot pass possession or biometric authenticators.**

   Our complaints show that fraudsters are often able to exploit flexible authentication procedures. Communications Alliance could use a procedure similar to the additional identity verification process contained in Schedule 1 to *Telecommunications (Mobile Number Pre-Porting Additional Identity Verification) Industry Standard 2020*.

Case Study 2: Lucien's mobile number and identity were stolen

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*

5. The information standard could require direct provision of information to consumers

We support the addition of information standards in section 3.4 of the draft Code which require providers to publish information on their websites about common kinds of telecommunications fraud and ways of counteracting them.

Communications Alliance could extend the information standard requirements by also requiring providers to supply the same information directly to consumers who contact them to report fraudulent activity. This would ensure the relevant information is readily available to consumers when they suspect their account may have been compromised.

Section 3.4 could also be modified to support the operation of section 3.2.6[1] by requiring providers to publish information on their website saying (where applicable) they will not ask consumers for their personal information as a means of authentication in outbound calls.

[1] Requiring providers to consider whether alternative Customer Authentication processes can be used for outbound communications, rather than asking customers for their security or sensitive information.