Telecommunications Industry Ombudsman

Submission to the ACMA New rules to prevent mobile number porting fraud

January 2020

Introduction from the Ombudsman, Judi Jones

Thank you for inviting me to comment on the ACMA's proposed *Telecommunications (Mobile Number Pre-Porting Additional Identity Verification) Industry Standard 2020* (Standard).

The proposed Standard is a positive step towards safeguarding mobile customers from fraudsters and generally strikes the right balance between accessibility and security.

The telecommunications industry has worked hard over the last year to address the security risks associated with mobile number theft. As noted in the ACMA's consultation paper, the Telecommunications Industry Ombudsman and the ACMA have contributed to this work.[1]

It is important that mobile pre-porting procedures keep up with evolving technological risks and consistent requirements apply across the industry.

Once the Standard comes into effect, my office will continue to handle complaints about the unauthorised porting of mobile service numbers in accordance with my Terms of Reference. My office will also continue to monitor emerging trends, conduct systemic investigations and refer systemic issues to the ACMA when necessary.

This submission offers observations about four of the issues on which the ACMA has invited comment:

1. Areas for improvement in new verification processes
2. Specific processes for small businesses
3. Pre-port verification process should be free to customers
4. There should be minimum requirements for customer information and advice.

1. Areas for improvement in new verification processes

We have identified some areas for improvement where the new verification processes could still leave customers vulnerable.

1.1. Access to a mobile device

The proposed Standard suggests gaining service providers confirm the initiating person has direct and immediate access to a mobile device used in association with the mobile service number to be ported.

It is important providers do not over rely on the customer having access to the device, as a fraudster could impersonate a customer if they have stolen their device. A SIM card can also be inserted and used in almost any device, as the number is linked to the SIM card, not the device.

Providers should ensure, as noted in the Standard, they do not proceed with the port before being satisfied the initiation person is also the customer, or authorised representative, of the mobile number to be ported.

[1] In 2018, my office identified a trend of complaints about mobile service providers who had a low bar for customer identity verification and worked with these providers to improve their practices. We published our Systemic Spotlight Report: *Reducing fraudster's theft of mobile numbers* which raised awareness about how customers' mobile numbers can be stolen by a fraudulent third party.

1.2. Unique verification codes

We have received complaints which show the unique verification codes can sometimes be exploited by fraudsters.

To reduce the opportunity for exploitation, the ACMA may wish to consider shortening the 30-day timeframe in which a code remains valid.

1.3. Multi-factor authentication

The proposed Standard allows providers to choose "some other verification process which is a multi-factor authentication process". "Multi-factor authentication process" is defined as a process that uses two or more authentication factors, with at least one factor being access to the mobile device associated with the mobile service number to be ported.

Without a minimum threshold for the other authentication factor, some providers may use information that is easily obtained by fraudsters. This could particularly impact customers who are experiencing family violence, and whose personal information, such as date of birth or address, would be commonly known by the perpetrator of the violence.

1.4. Use of biometric data

Providers should be aware the use of biometric data could be subject to higher privacy obligations. This is because biometric data is classified as "sensitive information" under the *Privacy Act 1988*.

1.5. Alternative verification process using identity documents

It is important to ensure there are secure alternatives for customers to verify their identity if their mobile device is lost, stolen, or broken. Our complaints show fraudsters have already obtained pieces of the customer's personal information before stealing their mobile number. Often, the customer's mobile number is the last piece of information the fraudster needs.

The proposed Standard provides for this by providing an alternative verification process in Schedule 1. The Standard could go further by making it clear the gaining provider is required to sight *original* Category A and B documents as part of the verification process.

Case study 1: Fraudster used stolen mobile number to fraudulently withdraw funds from a customer bank account

The customer's mobile number was stolen by a fraudster impersonating the customer via online chat. The fraudster had already obtained the customer's personal information and was able to pass identity checks by using this. After the customer's mobile number was ported, $17,500 was withdrawn from their bank account. The customer says they did not receive any notification before their number was ported.

2. Specific processes for small businesses

We agree there should be pre-port verification processes in place for all customers. However, there may need to be different processes for residential and small business customers.

Small businesses often rely on authorised representatives, which may change from time to time. In a situation where a small business is required to undertake alternative identity verification using the documents and process described in Schedule 1 of the proposed Standard, it may be difficult for the small business to produce the relevant documents, especially if the authorised representative has changed.

Small businesses may also be vulnerable to overreliance on authorised representatives. A different process, such as password, may be more appropriate for small business customers.

3. Pre-port verification process should be free to customers

We strongly support fee-free pre-port verification processes, because fees would add an increased barrier to customers' ability to port their number.

However, there may be situations where there is a cost to the customer because they must take pre-port identification steps using their losing provider's service. This could occur if the customer is required to have credit to send a return SMS or mobile data to access a weblink. This could be an issue for some particularly vulnerable customers.

The proposed Standard states the obligation to provide free of charge verification is only applicable to the gaining provider.

Case study 2: Small business' number stolen by authorised representative

This small business' number was ported to another provider by an ex-employee. The ex-employee contacted the small business' provider via online chat and asked to be added as an authority on the account.

After the ex-employee was added as an authorised representative, without the small business' knowledge or consent, the ex-employee ported the business number away for their own use.

4. There should be minimum requirements for customer information and advice

We strongly support minimum requirements for customer awareness and safeguard information as currently proposed in the Standard.

For more details based on a recent systemic issues investigation, please see the **Confidential Annexure** to this submission.