20 January 2020

The Manager
Strategy and Projects Section
Australian Communications and Media Authority
Law Courts
Melbourne VIC 8010

The Australian Communications Consumer Action Network (ACCAN) is the peak body that represents all consumers on communications issues including telecommunications, broadband and emerging new services. ACCAN provides a strong unified voice to industry and government as consumers work towards communications services that are trusted, inclusive and available for all.

ACCAN thanks the Australian Communications and Media Authority for the opportunity to make a submission in response to the Draft Telecommunications (Mobile Number Pre-Porting Additional Identity Verification) Industry Standard 2020.

ACCAN is aware of numerous reports by victims of fraudulent number porting which reinforce the need for stronger protections. One Telstra customer reported to ACCAN that he only knew his mobile number had been fraudulently ported after noticing his phone had been on 'SOS only' for 3-4 hours. He received no authentication SMS from Telstra prior to the port taking place, and using stolen credit card and social media information the fraudster reset the customers' email passwords, accessed confidential personal documents saved in his email accounts and activated the customers' stolen credit card. It took the customer four hours to have Telstra reverse the port and add extra security protocols to the account, even after which the fraudster was able to place a diversion on the customer's number without providing extra security information due to lax practices on the part of the retail service provider. This suggests that the current methods of identity verification, including two-factor authentication, are inadequate to prevent fraudulent number porting.

ACCAN will address each of the specific issues for comment.

1. New verification processes

Are there issues in relation to the proposed processes and their utility to meet the objectives?

Two-factor authentication

ACCAN agrees that secure customer identity verification must take place prior to the port of a mobile service number and that the gaining carriage service provider should use two-factor authentication processes to confirm customer approval before a number is ported. However, ACCAN is aware that fraudsters have been able to bypass the use of two-factor authentication in the past, and that it is therefore essential that only strictly secure forms of verification are used to effectively prevent fraudulent number porting.

It is crucial that the forms of identity verification that are used can only be genuinely verified by account holders in order to effectively prevent fraudulent number porting. For example, a two-step authentication process built into an app on a smartphone controlled only by the owner of the mobile phone account, rather than attached to a portable phone number – for example, Authy – would provide a more secure method of authorisation.

ACCAN notes that the wording of 8(2) - that "at least one" of the specified identity verification processes be used by a carriage service provider, in order to confirm the initiating person is the rights of use holder before porting the number – indicates that in fact a single form of identity verification could potentially be used before porting begins. ACCAN is concerned that this process would be inadequate to securely verify an account holder's identity prior to number porting being implemented.

SMS

SMS has been repeatedly reported by consumers to be an insecure method of identity verification, initially adopted by the banks and inappropriate for adoption by telecommunications providers.[1] For example, where two-factor authentication messages are sent via SMS, and phone number porting has already begun without proper authentication and approval of the identity of account holder, the fraudster receives the two-factor authentication SMS message as opposed to the genuine account holder.[2]

Other forms of phishing[3] and spoofing[4] also make it possible for scammers to intercept SMS two-factor authentication, rendering SMS as a form of identity authentication highly ineffective to prevent fraudulent number porting.

To balance the need for an additional factor of authentication with the ease of SMS verification, ACCAN submits that another layer of protection is needed which will not affect a customer's existing user experience. There are several alternatives to SMS two-factor authentication that are worth considering, including:

- Hardware authentication tokens – Hardware authentication relies on a dedicated physical device to grant access. Along with their password, users will also have to input a random token code generated by the device. Logins will fail without the code. The physical nature of this method does have the potential for devices to be lost and stolen but it does address many of the security issues inherent to SMS-based two-factor authentication.

- Software authentication tokens – Software authentication does not require a physical device and token codes are generated with a mobile application. This software does not rely on SMS or the phone network for authentication, eliminating the inherent flaws in SMS-based two-factor authentication.[5]

ACCAN submits that more stringent methods of personal authentication than SMS messages, which are less vulnerable to phishing, spoofing and hacking, need to be used to effectively prevent fraudulent number porting activity.

Biometric

Biometric data offers a highly secure method of identity verification. ACCAN submits that a form of biometric verification should be offered to customers as one of the two forms of

[1] https://accan.org.au/hot-issues/1385-fraudulent-mobile-number-porting-and-identity-theft
[2] https://www.securityweek.com/6-ways-attackers-are-still-bypassing-sms-2-factor-authentication
[3] https://nakedsecurity.sophos.com/2019/10/11/hackers-bypassing-some-types-of-2fa-security-fbi-warns/
[4] https://blog.sucuri.net/2020/01/why-2fa-sms-is-a-bad-idea.html
[5] https://blog.sucuri.net/2020/01/why-2fa-sms-is-a-bad-idea.html

identification used in the two-factor authentication process. However, it is important that use of biometrics should remain optional as it raises significant privacy concerns for some individuals and should not become effectively mandatory.

Documentation

The second tier of verification outlined in 8(3), which allows for documentary evidence to verify the identity of the person seeking to have their mobile service number ported "where the gaining provider is unable to confirm that the initiating person is the rights of use holder", has the potential to undermine the stringency of the verification procedures outlined in 8(2).

ACCAN submits that consideration should be given to situations when confidential documents such as passports and birth certificates have been stored in email accounts by customers, and hackers have secured fraudulent access to those customers' email accounts. In such circumstances, documentary evidence can be fraudulently obtained and used as proof of identity.

In these situations, while documentary evidence might be used as one factor of authentication, the second authentication factor might need to be more secure while still user-friendly – for example, use of hardware or software authentication tokens or biometric data – to prevent fraudulent number porting.

Are there additional processes that should be considered?

ACCAN questions whether the draft standard provides too much flexibility in terms of methods of identity authentication that can be used by mobile carriage service providers to effectively prevent fraudulent number porting.

ACCAN also has concerns about the method by which the test in 8(5) is satisfied – i.e. by what criteria is the "the gaining mobile service provider…satisfied that, in relation to the mobile service number which is the subject of the porting request, the initiating person is the customer for that mobile service number or the authorised representative of that customer."

ACCAN is aware that there have been instances where customers' numbers have been ported even where they have not provided the six digit verification code sent to them via SMS to the gaining mobile service provider.[6] This suggests that the necessary security protocols to verify authentication are not being followed. Imposing penalties for infringement on both the losing and gaining carriage service providers – for example, fines - in cases where rigorous authentication processes have not been followed would act as a deterrent to lax identity verification practices.

Boosted identity checks should be a default obligation on telecommunications providers to prevent fraudulent number porting. This is an option that can be requested by consumers on a case-by-case basis but is often only requested by victims after they have been targeted in a number porting scam.

Although the authentication methods suggested by ACCAN in this submission – for example, a two-step authentication process built into an app on a smartphone, use of hardware and/or software authentication tokens and (optionally) biometric data - offer state-of-the-art solutions to protect customers from fraudulent mobile number porting at this point in time, fraudsters will continue to devise new ways to port numbers if it is to their advantage.

ACCAN notes it is vital that the technology used by mobile carriage service providers to prevent fraudulent mobile number porting is constantly updated to provide gold standard information and cyber security, particularly in the context of the rollout of 5G technology. 5G technology will generate and collect more personal data, enable the proliferation of interconnected devices and increase the risk of exposing personal data to harm.

[6] https://accan.org.au/hot-issues/1385-fraudulent-mobile-number-porting-and-identity-theft

2. Application to customer types

Should some customers have specific processes applied to them? The ACMA is interested in feedback on how the additional identity verification measures proposed will work where authorised representative arrangements are in place.

ACCAN notes that there is a multitude of methods telecommunications companies use in dealing with authorised representatives, and few of them are consistent with the Telecommunications Consumer Protections Code (TCP Code) or ACCC Debt Collection Guidelines. The complications around the issue of authorised representatives acting on behalf of customers demonstrate the need for a uniform and consistent approach to appointing and dealing with authorised representatives.

In the rare circumstances where an authorised representative acting in a professional capacity or a family member might need to port a number on behalf of a customer, ACCAN submits that SMS messaging is not an effective form of identity authentication. In addition to the security limitations of SMS authentication outlined in this submission, an authorised representative will rarely have access to the mobile device attached to a customer's number and so would not receive any SMS authentication message sent by a customer service provider.

ACCAN submits instead that use of hardware or software tokens are an effective second form of identity authentication in this case. First, where an authorised representative contacts a telecommunications carriage service provider and requests that a customers' number be ported, the provider could confirm the identity of the authorised representative by asking some key identity questions (e.g. name of the account, account number, listed address and email address of the representative) which are verified by the authorised representative. Second, a hardware or software token could be used as the next step in two-factor authentication as tokens do not rely on the SMS network.

3. Effectiveness, feasibility and cost

ACCAN submits that any financial and administrative burden imposed on telecommunications carriage service providers would be outweighed by the long-term consumer trust benefits delivered by improved security measures.

Delivering a high quality and secure mobile carriage service will also minimise quantifiable consumer loss at both an individual and broader level. Victims have reported that the disruption to their lives, and time taken to resolve the serious problems triggered by fraudulent number porting, have consumed many hours and days of their time. Consumer losses experienced are exacerbated in the case of small business operators, with up to a week of disruption to business reported to ACCAN as a consequence of fraudulent number porting.

4. Costs to customers

The draft industry standard specifies that providers should not charge customers a fee for an identity verification process. Do you agree with this approach?

ACCAN approves of the provision in 8(3) that "a mobile carriage service provider must not charge a fee to a customer for the completion of an additional identity verification process".

5. Customer information and advice

The draft industry standard sets minimum requirements for consumer awareness and safeguard information. The ACMA is interested in feedback on whether this is warranted and/or whether alternative arrangements should be considered (e.g. inclusion in an industry guidance note).

It is important that the draft industry standard sets minimum requirements for consumer awareness and safeguard information. As mentioned above, ACCAN questions whether the draft standard provides too much flexibility in terms of methods of identity authentication that can be used by mobile carriage service providers to effectively prevent fraudulent number porting. In relation to an industry guidance note, ACCAN's experience is that guidance notes developed by the Communications Alliance are naturally designed to unenforceable favour the interests of the industry, and do not necessarily assist in delivering positive consumer outcomes.

An industry guidance note developed by ACMA which includes consumer awareness and safeguard information with examples of best practice, or inclusion of consumer awareness and safeguard information in the standard itself, would provide firmer guidelines for effective industry implementation of the standard and offer greater protection to consumers.

ACCAN also questions whether the language used in the draft standard is simple enough to be easily understood by consumers. Any industry guidance note drafted by ACMA, or inclusion of consumer awareness and safeguard information in the standard, should contain a requirement for retail service providers to educate customers about the potential dangers of fraudulent mobile number porting and the importance of adhering to safe authentication and security practices. Please do not hesitate to contact us should you require clarification or additional information on any of the issues raised in our submission.

Yours sincerely,

Stephanie Whitelock

Policy Officer