Telecommunications Industry Ombudsman

TIO submission to the Australian Communications and Media Authority -

Consultation on proposal to vary the Telecommunications Service Provider (Customer Identity Authentication) Determination 2022

February 2025

Table of Contents

Introduction

Thank you for the opportunity to comment on the Australian Communications and Media Authority's (**ACMA**) proposal to vary the *Telecommunications Service Provider (Customer Identity Authentication) Determination 2022* (**Determination**).

Our office strongly supported the Determination when the ACMA consulted on its original exposure draft in December 2021.[1] We continue to support the ACMA's multifactor authentication (**MFA**) rules as an important safeguard for consumers against unauthorised account access and telecommunications fraud.

While we support the Determination, we also know some consumers have difficulty completing the MFA processes their telcos put in place to comply with its security requirements. While the Determination may allow for flexible MFA options, we see complaints where telcos do not offer them. From our complaints we can see that inflexible MFA approaches can have a very real impact on some of the most vulnerable consumer cohorts. Telecommunications are an essential service, and the community has a reasonable expectation that telcos will offer a variety of secure authentication methods to meet diverse consumer needs.

In general, we support the ACMA's proposed variations to the Determination, as they will allow for more flexibility in telcos' MFA processes, and for the use of more secure MFA processes in some areas. We particularly support the proposed inclusion of passkeys as an alternative primary authentication process in subsection 9(1). We understand passkeys are more secure than account information authenticators and personal information authenticators because they do not rely on a requesting person's knowledge of information. Passkeys are therefore less vulnerable to phishing attacks than passwords or PINs. They may also provide a suitable authentication option for consumers who have difficulty remembering security credentials.

The current consultation process is a valuable opportunity for the ACMA to strengthen the Determination's authentication requirements and reevaluate areas of its drafting that may have presented difficulty for telcos and consumers. Going forward, it is critical the Determination strikes the right balance between requiring robust, secure authentication procedures and allowing flexibility in those procedures for the benefit of consumers.

We offer the following additional commentary on the ACMA's proposed amendments, and on the Determination more broadly, based on our experience dealing with telecommunications complaints.

1 Consumers would benefit from positive obligations for telcos to offer the flexible authentication methods available under the Determination

The drafting of the Determination has had unintended consequences for consumers who require flexibility in authentication methods. This includes consumers experiencing vulnerabilities that make it impossible or impractical for them to use their telco's preferred (or default) MFA method.

1.1 The Determination does not contain clear obligations for telcos to offer flexible MFA methods

The current structure of the Determination outlines a variety of permitted MFA methods, including (among others) methods based on possession of devices and on access to mobile and landline

[1] See our submission to the ACMA's consultation on its 2021 proposal to make the *Telecommunications Service Provider (Customer Identity Verification) Determination*.

telephone numbers, email addresses, and identity documents. It also includes a flexible procedure in section 11 to help consumers in vulnerable circumstances complete authentication.

The Determination does not contain any clear, direct obligations for telcos to offer any particular authentication methods that are permitted under its rules. Instead, the Determination prohibits carriage service providers (**CSPs**) from processing high-risk customer transactions unless the requesting person has first completed one of the permitted forms of MFA. The Determination gives CSPs the discretion to determine which of the MFA methods they will use to authorise high-risk transactions.

1.2 We receive complaints from consumers experiencing difficulty completing their telco's MFA process

Since the Determination came into force in June 2022, our office has observed a trend in complaints about the accessibility of the authentication methods CSPs have used to comply with its MFA requirements. Affected consumers say they were not able to successfully complete MFA because their telco required them to use an authentication method that was not accessible for them. Many of these complaints have occurred in circumstances where there was likely an alternative and more suitable form of MFA available under the Determination, but the telco did not make that method available.

Systemic Investigation Case Study: Telcos using inflexible MFA methods after the Determination came into force

In late 2022 and 2023, we investigated the customer authentication practices of several large telcos. We were concerned the telcos were not consistently offering MFA options that were accessible and suitable for individual consumers' circumstances, even though flexible options were permitted under the Determination.

Common issues we identified included telcos insisting their customers complete MFA using a one-time code (**OTC**) sent to a registered mobile number rather than a registered email address (or vice-versa) or requiring them to complete MFA for interactions that were not considered 'high-risk' under the Determination (such as troubleshooting). In some instances, telcos required consumers to complete MFA using OTCs when the consumer had a landline number on their account and could not receive an OTC, for example because they did not have a mobile or internet service. Several of these consumers could likely have completed MFA by the telco calling them back on their landline to confirm their access to the number, had their telco offered them that option.

Where a consumer was unable to complete their telco's preferred MFA process, generally the telco directed them to complete MFA at a physical store with their identity documents. In some cases, this was not accessible for the consumer, often because they had limited mobility or lived a long distance from the nearest store.

Another common issue we identified was that telcos were not consistently recognising the authority of listed and unlisted authorised representatives (such as those with power of attorney or guardianship orders authorising them to represent a customer) when completing MFA. In some cases, the telco insisted they speak with an account holder directly or that the account holder needed to complete MFA themselves, even where this was not appropriate

because the consumer did not have legal capacity or was distressed by the contact from their telco.

Generally, telcos responded to our investigations by agreeing to implement improvements to make their authentication processes more accessible. Improvements telcos agreed to make included introducing additional MFA methods to their processes, and running extra training for staff on their MFA policies and the Determination's requirements.

While the telcos made improvements to their processes, we still receive complaints about consumers impacted by inflexible MFA practices. We remain concerned about the consistency and accessibility of the authentication practices used across the industry.

Consumers affected by these issues often find themselves unable to review their accounts or change important details such as payment information. Others are unable to cancel unwanted services or accounts. Where a telco takes an inflexible approach to the authentication methods it provides under the Determination's rules, consumers often encounter difficulty because the telco's preferred MFA method relies on incorrect or out-of-date contact information for the consumer. We sometimes see complaints where a telco does not offer the consumer any alternatives to its preferred MFA method in the first instance, and only helps them complete authentication (using a different MFA method) after they lodge a complaint with our office.

Case Study 1: Kaname's telco did not give her adequate assistance to complete its identity verification process*

Kaname decided to cancel her mobile service with Propeller Net, as it no longer met her needs. After cancelling the service, Kaname received a notice from Propeller Net saying she would need to pay around $800 for remaining charges on her mobile handset. Kaname was unsure whether this amount was correct and thought she might have been overcharged.

Kaname called Propeller Net to ask about the notice, but Propeller Net refused to discuss it with her. Propeller Net said it needed to identify Kaname by SMSing a code to her phone, but Kaname had changed her mobile number and was not able to receive the code. Kaname explained this, but the Propeller Net representative did not help her to identify herself in a different way. Instead, the representative told Kaname they could not help her and ended the call.

After we referred Kaname's complaint to Propeller Net, it helped her to complete its identity authentication process and resolved her complaint.

**Names of all parties have been changed. A version of this case study first appeared in our November 2023 submission to Treasury's consultation on its Unfair Trading Practices Consultation Regulation Impact Statement.*

It is typical for telcos to use OTCs as their preferred form of primary MFA under subsection 9(3) of the Determination. In some instances, consumers are told they need to receive OTCs using a contact method (mobile phone or email) that is not suitable for their circumstances. This can be particularly problematic for consumers experiencing vulnerability, who often have reduced capacity

to afford an otherwise unwanted or impractical mobile or internet service.

Case Study 2: Russell's telco changed its authentication requirements, leaving him unable to complete MFA*

Russell is a pensioner and needs to manage his finances carefully. He has a landline service and a low-cost internet service with Brik Tel. The internet service is prepaid, and Russell needs to log into his online account with Brik Tel to manage the service and purchase new recharges for it as required. Before contacting our office, Russell was accustomed to completing MFA and logging into his online account with Brik Tel by entering an OTC Brik Tel sent to his email address.

One day, Russell tried to log into his account but found the option to send an OTC to his email address was no longer available. When Russell called Brik Tel to enquire, it told him it had changed its process and would now only send OTCs to a registered mobile number. This was a problem for Russell because he did not have a mobile phone and did not want to use one. He also knew the mobile coverage at his home was not reliable. Russell felt he had no choice but to buy a new mobile phone so he could log into his account, but was concerned he would not be able to afford one.

After we referred Russell's concerns to Brik Tel's dispute resolution area, it resolved his complaint by covering the cost of a mobile phone and prepaid mobile service for him to use when completing MFA to access his online account.

**Names of all parties have been changed.*

Case Study 3: Hilda was not able to read OTCs sent by SMS because of her low vision*

Hilda contacted our office after she encountered difficulty updating her direct debit payment information with her telco, Pebbletel. Hilda's debit card had expired, and she needed to update her banking information so her next payment for her services would be processed correctly.

When Hilda contacted Pebbletel, it told her she needed to complete authentication by reading back an OTC Pebbletel had sent to her mobile number. Hilda has poor eyesight, and was not able to read the OTC. Even though she explained this to Pebbletel, it insisted she complete MFA using the OTC sent to her mobile. Pebbletel did not help Hilda authenticate her identity using any other method, and did not update her payment information.

Instead, Pebbletel told Hilda it would disconnect her services for non-payment.

**Names of all parties have been changed.*

Case Study 4: Thorn Net did not allow Jacques' representative to help him report a fault *

Jacques is elderly and lives with a disability. A local community group supports him to live independently in the community. A member of the community group contacted our office after they had difficulty reporting a fault affecting Jacques' landline to Thorn Net, on his behalf.

Jacques' landline is his only means of contacting the outside world, and his representative was concerned the fault could prevent him calling for help in an emergency. Jacques' representative had tried to report the fault to Thorn Net several times, including by accompanying Jacques to a Thorn Net store.

Despite this, Thorn Net refused to accept the representative's fault report, because it claimed Jacques needed to complete MFA using an OTC sent to a mobile phone. Jacques did not have a mobile phone, and his representative explained he would not be able to use one even if he did. Because of his circumstances, Jacques did not have photo identity documents either.

Although Jacques' circumstances would likely have allowed Thorn Net to use the flexible section 11 MFA procedure for persons in vulnerable circumstances, Thorn Net did not use the procedure to help him complete authentication. It is also unlikely the Determination required Thorn Net to complete MFA before accepting the fault report (reporting faults is not a high-risk customer transaction).

**Names of all parties have been changed.*

In some cases, we see that a CSP requires consumers to undergo a particular form of authentication before they can complete certain kinds of high-risk transactions. In these cases, the telco may be willing to use a more accessible form of MFA for some transactions, but not the transaction the consumer wants to complete. Authentication processes that require the consumer to upload their identity documents, photographs or videos of themselves are common drivers of complaints, as many consumers do not feel comfortable providing this information online.

1.3 Positive obligations for CSPs to offer a variety of accessible MFA methods would improve the accessibility of the Determination's processes

Changes to the Determination are necessary to support consumers with diverse needs and circumstances when completing authentication. Our experience dealing with complaints about MFA accessibility has shown that a 'one-size-fits-all' approach to customer authentication is not appropriate for all consumers, and does not reflect the essential nature of telecommunications services. It is not appropriate (for example) for a CSP to offer only one form of primary authentication under subsection 9(3), and require all its customers to use that process.

Recommendation: Mandatory baseline authentication methods

We would support changes to the Determination so it obliges CSPs to offer a baseline number of flexible authentication methods to their customers. The mandatory authentication methods could include (at a minimum) primary authentication methods (under subsection 9(3)) that rely on OTCs sent by SMS, call-backs to registered mobile *and* landline numbers, and authentication based on identity documents.

Recommendation: Clarify that CSPs must offer section 10 and section 11 authentication processes

The Determination could also clarify that CSPs are obliged to offer authentication under the section 10 secondary process, and the section 11 process for consumers in vulnerable circumstances, when the criteria for using those processes are satisfied. That is, it could clarify that a CSP does not comply with the Determination by refusing to process a high-risk customer transaction, if the section 10 or section 11 process is applicable to the consumer's circumstances and the CSP has not attempted to complete authentication under that process.

Recommendation: Require CSPs to proactively discuss MFA options and account for consumer preferences about MFA

An additional approach could be to create positive obligations for CSPs to proactively discuss MFA options with a consumer when they first sign up for services with that CSP. These obligations could require CSPs to outline the MFA methods they offer and ask the consumer to nominate their preferred method. CSPs could then be required to take reasonable steps to accommodate the consumer's preferred MFA method when authenticating their identity.

This approach would improve the accessibility of MFA by giving consumers more choice in the MFA methods they use. It would also have the benefit of raising consumer awareness about a CSP's MFA options, and prompting consumers to give CSPs the information they need to complete MFA easily and efficiently. For example, it could help to avoid situations where a CSP cannot complete MFA based on OTCs because they do not have the consumer's current mobile number registered as their contact telephone number.

2 The Determination should not allow CSPs to require consumers to use a government-accredited digital identity service against their wishes

We support the ACMA's proposal to make the use of government-accredited digital identity services a primary form of authentication under subsection 9(3). Government-accredited digital

identity services may provide an effective and secure form of primary MFA for those who wish to use them.

However, while we support the broader availability of MFA using government-accredited digital identity services, these services may not be suitable for all consumers. They may be particularly inappropriate for elderly consumers or those who are not comfortable with technology. Other consumers may not feel comfortable providing their personal information to a third-party digital identity provider, even if that provider has been accredited by government.

As highlighted above, we receive complaints where consumers report their telco did not offer a form of MFA that was suitable or accessible for them, even though more appropriate methods were likely available under the Determination. In this context, we are concerned that under the current proposal some CSPs may elect to offer a government-accredited digital identity service as their *only* form of primary MFA under subsection 9(3). Some CSPs may view government-accredited digital identity services as the most convenient and secure form of primary authentication available to them.

This will likely result in an increased number of consumers experiencing accessibility problems when dealing with their telco, and an increased number of complaints to our office.

Recommendation: Ensure CSPs cannot require consumers to use government-accredited digital identity services

We encourage the ACMA to ensure rules are in place so that a CSP cannot require consumers to complete MFA using a government-accredited digital identity service as the only form of primary MFA that CSP offers.

3 We support completely removing biometrics-based authentication from the Determination

We support changes to the Determination to remove authentication processes based on biometric data collected by a CSP or third-party. In our view, the risks associated with a CSP or third-party collecting information as sensitive as a consumer's biometric data outweigh the benefits biometrics may have as a means of completing identity authentication.

The Australian public is increasingly aware of the risks associated with giving their personal information (including sensitive information) to service providers where this is not necessary for the provider to supply the relevant service.[2] We agree with the ACMA's observation that there are significant risks associated with the use of biometric information, as it cannot be replaced if it is stolen or disclosed in a data breach.

In our experience, few CSPs use MFA processes that rely on the consumer giving their biometric data to a CSP or third-party. The use of biometric information for authentication may be more typical in the context of device-based authentication functions such as Apple's Face ID. For example, a consumer might use a face recognition technology to unlock their device or their provider's app, so they can respond to an in-app authentication prompt. Where this occurs, we understand the biometric information is generally stored securely on the user's device, and is not

[2] See, eg, the Office of the Australian Information Commissioner's report on its 2023 Australian Community Attitudes to Privacy Survey, page 26.

sent to a service provider or any third-parties.

Recommendation: Remove authentication processes based on giving biometric information to a CSP or third-party

Removing processes from the Determination that rely on supplying biometric data to a CSP or third-party would appropriately protect consumers from the risks associated with giving their biometric information to their telco. The ACMA could provide stronger protections by explicitly prohibiting CSPs from using authentication processes that rely on biometric data supplied to the CSP or to a third-party.

Should the ACMA decide not to remove authentication processes based on biometric data from the Determination, we would in the alternative support the ACMA's currently proposed changes. These would restrict the circumstances in which biometric data can be used to complete MFA under the Determination. They would also ensure biometric information is collected only with the requesting person's consent, and is stored securely.

4 The proposed changes to the Determination's record keeping rules will make it more difficult to determine whether a CSP has complied with its MFA obligations

The ACMA's proposed amendments to paragraphs 11(3)(c) and 12(3)(b) would change the Determination's record keeping requirements. The changes would mean CSPs are only required to record information about *the type* of material or supporting evidence a requesting person supplies to establish they are a 'person in vulnerable circumstances' or a customer's unlisted authorised representative.

We appreciate the amendments have been proposed to reduce the need for telcos to store personal information and documents, in a manner consistent with the National Strategy for ID Resilience. However, we are concerned to ensure that the approach taken to this issue allows regulators, consumers and our office to effectively verify whether a CSP has appropriately complied with the section 11 and 12 authentication processes.[3]

4.1 It is important CSPs retain sufficient information to verify their compliance with the section 11 and section 12 procedures

The section 11 and 12 MFA processes are the most flexible of the Determination's authentication procedures. The flexibility of these procedures means they do not rely on 'possession factors' such as access to a verified mobile number or email address, or on identity documents showing the requesting person is the CSP's customer. It is important the Determination includes the section 11 and 12 procedures to support consumers who require them (generally those experiencing some kind of vulnerability).

[3] Section 11 provides a flexible authentication procedure for persons in vulnerable circumstances who, because of their vulnerable circumstances, are unable to complete the primary MFA procedure under section 9 or the secondary 'back-up' procedure under section 10. Section 12 provides a procedure for authenticating a customer's 'unlisted authorised representative', such as a person with power of attorney to represent the customer.

However, the flexibility of the procedures also makes them less secure than the Determination's other MFA processes. As a result, when fraudsters target a consumer's telco account, they are likely to attempt to exploit the section 11 and 12 procedures. In this context, it is important that when a CSP completes customer authentication based on the section 11 procedure or the section 12 procedure, it retains sufficient information to establish that it complied with its obligations.

Recommendation: Consider what records will be needed to enforce the section 11 and section 12 requirements

In our view, the Determination should require CSPs to retain records about more than just the type of supporting material or evidence requesting persons provide in relation to the section 11 and section 12 procedures. This would not necessarily mean CSPs need to retain copies of documents requesting persons provide. Depending on the type of supporting material or evidence a requesting person supplies, there may be information such as a reference number or date of issue that could help a regulator verify that the material was in fact sighted by the CSP, at a later date for enforcement purposes. It may also be beneficial for CSPs to record the content of documentary material or evidence, even if they do not retain copies of the documents themselves.

When determining the final form of these amendments, we encourage the ACMA to consider what evidence it would require to support enforcement action against a CSP for non-compliance with the section 11 or section 12 processes.

5 We have identified areas where the proposed amendments may present additional security risks

While we support changes to the Determination to improve the accessibility of its processes, it is important these are balanced appropriately to avoid undue risks to consumers.

Recommendation: Consider how security risks arising from the proposed amendments could be minimised

We ask the ACMA to review our observations about each of the areas outlined below and to consider how any potential risks could be minimised, when deciding its amendments to the Determination.

5.1 The proposed changes to provisions for reviewing category A and B identity documents

We note the ACMA has sought feedback from CSPs about whether they have encountered difficulty authenticating customers under clause 4 of Schedule 1 to the Determination. Clause 4 of Schedule 1 lays out the Determination's procedure for comparing a requesting person's face to category A and category B identity documents. The procedure is used for the purposes of verifying

that the requesting person is a customer (or a customer's authorised representative) under paragraph 9(3)(e) or paragraph 10(2)(a).

We understand the ACMA has requested feedback on this issue with a view to potentially making changes to allow CSPs to undertake the comparison of a requesting person's face with identity documents in a manner other than in person or via video link. We encourage the ACMA to take the utmost care to ensure that any changes to these procedures do not expose consumers to increased risk of fraud.

The real-time nature of comparisons undertaken in person and via video link is an important part of what makes those processes secure. It helps to mitigate the risk that fraudsters may use stolen or manipulated videos and images to successfully pass authentication. With the increasing availability of AI tools that can generate photo and video 'deep fakes', it is critical that the process contained in clause 4 of Schedule 1 accounts for these risks.

5.2 The proposal to allow OTCs to be sent to mobile numbers other than the number registered as the consumer's contact number

The ACMA's proposed new sub-paragraph 9(3)(c)(i)(B) would apply when a customer does not have a mobile service number listed on their account as their contact number. Where the sub-paragraph applies, it would allow a CSP to send authentication OTCs and secure hyperlinks to 'the mobile service number of the customer', which need not be registered on the customer's account as their contact number.

We appreciate the intent of this proposal is to improve the accessibility of MFA processes. It would allow consumers to authenticate using OTCs sent by SMS, even where they do not have their current mobile number listed on their account as their contact number. This could occur in circumstances where a consumer has not explicitly advised their CSP that their mobile number is their contact number, or where the consumer has a landline number listed as their contact number.

We understand the proposal would in effect allow CSPs to authenticate a customer by sending an OTC or secure hyperlink to *any* mobile number connected under or otherwise listed on the customer's account. It is not unusual for fraud to be committed by a person known to the victim. The current proposal could therefore create material security risks in circumstances where a consumer has a mobile number connected under their account that is used by a different person.

For example, it is not uncommon for a consumer to have mobile services connected under their own account that are used by their partner or children. There may be increased risks for small business consumers, whose accounts sometimes include mobile services used by their employees.

Any changes to the rules governing the mobile numbers that can be used to receive OTCs and secure hyperlinks under subsection 9(3) should account for these risks. Ideally, the rules in this space would ensure the consumer knows what mobile number will be used for the purposes of authentication (and has approved the use of that number) before it is used for MFA. One option could be to allow OTCs to be sent to a mobile number that is registered on the customer's account as the number to be used *for the purposes of completing customer authentication*, rather than as the contact number for the customer. This could allow a consumer to nominate a mobile number for the purposes of MFA, even if their preferred contact number is a landline number.

5.3 The proposal to expand the exceptions to requirements for sending notifications about high-risk customer transactions

The ACMA's proposed provisions in subsections 10(8), 11(6), and 12(7) expand the existing exceptions to the requirement to send notifications about high-risk customer transactions where a CSP has reasonable grounds for believing a customer is affected by domestic or family violence (**DFV**) and the customer requests that the notification not be sent. The proposed changes would mean this exception applies to authorised representatives as well as customers, where the CSP has reasonable grounds for believing the customer or authorised representative is affected by DFV.

We support measures to help consumers experiencing DFV protect their safety. However, as outlined above, the Determination's more flexible MFA procedures (including the section 11 procedure) are likely to be targeted by fraudsters. Where fraudsters do target these procedures, a notification about a pending high-risk customer transaction may be the only way the victim is alerted to the fraudulent activity in time to successfully reverse it.

Expanding the exceptions to cover authorised representatives as well as customers may result in increased security risks. We encourage the ACMA to take this into account when deciding the final form of these amendments. If the ACMA implements the proposed amendments in subsections 10(8), 11(6), and 12(7), we would support further amendments to clarify who can ask for notifications not to be sent to a particular class of 'relevant person'. In the current draft, it may not be clear whether an authorised representative who is affected by DFV can ask for a notification not to be sent to a customer (or vice-versa).

5.4 The proposal to explicitly include references to the use of a government death notification system as documentary evidence in section 12

The proposed change to subsection 12(2) includes an explicit reference to the use of a government death notification system as an example of documentary evidence a requesting person could provide to show they are an unlisted authorised representative.

We receive complaints from consumers who are experiencing delays and other difficulties dealing with bereavement issues. Typically, these consumers come to us for assistance in cancelling their deceased relative's services and ensuring any remaining charges are finalised. Occasionally, consumers want to transfer the deceased relative's services into their own name or organise for a credit balance on their account to be refunded.

We support the aim of making it easier for the relatives of deceased customers to deal with bereavement issues. The proposed inclusion in subsection 12(2) of a reference to use of a government death notification system as documentary evidence may assist bereaved consumers to deal with these issues more easily and efficiently.

However, we query whether government death notification systems are set up to fully verify whether a notifying person is authorised to represent a deceased person's estate. We understand the role of the Australian Death Notification Service (whose website is linked in the ACMA's consultation paper) is to facilitate the notification of a person's death only, rather than to verify any representative status of the person notifying about the death. The 'help centre' page on the Australian Death Notification Service's website says organisations notified of a person's death will likely need more information from the notifying person to validate their role in handling the deceased person's affairs.[4]

[4] See https://deathnotification.gov.au/help-centre, under a tab titled 'Will organisations ask me for more information?'.

Depending on how CSPs interpret the proposed amendments to subsection 12(2) there may be a risk they will accept instructions from a person who is not authorised to represent a deceased customer's estate. In the typical case where a relative only wants to cancel the deceased person's services and finalise the account, we expect the risk to the estate would likely be minimal. Where a bereavement request involves the refunding of credit balances or the transfer of services or accounts into another person's name, there may be heightened risks. We ask the ACMA to be mindful of these risks when considering the proposed amendments.

6 The privacy protections in proposed section 16 should be made generally applicable to all CSPs covered by the Determination

We welcome the proposed new section 16 of the Determination, which will provide privacy protection obligations for CSPs that are not covered by the requirements of the *Privacy Act 1988* (**Privacy Act**). These provisions will provide robust protections for consumers' personal information. They should ensure CSPs will use the personal information they collect as part of their MFA processes only for the purpose of complying with the Determination, and will not disclose that information to third-parties except in one of the circumstances laid out in subsection 16(a). They will also require the secure destruction of the information when it is no longer required under the Determination or other applicable laws.

Recommendation: Section 16 should apply to all CSPs covered by the Determination

We understand the intention of section 16 is that it will provide similar privacy protections to those contained in the *Australian Privacy Principles* (**APPs**), for customers of those CSPs that are not required to comply with the APPs under the Privacy Act. However, in our view the new section 16 should apply to all CSPs covered by the Determination (including those required to comply with the APPs). This will ensure robust protections are applied consistently across the industry.

6.1 The section 16 requirements provide clearer and more targeted protections than APPs 6 and 11

While section 16 broadly mirrors the requirements of APPs 6 and 11, it takes a more prescriptive approach to the way CSPs are required to deal with personal information. This means it will likely provide clearer and more robust protections for the personal information used in MFA processes than the APPs do. Unlike the APPs, section 16 explicitly defines the circumstances in which CSPs are permitted to disclose the information to third-parties. APP 6 notionally permits disclosure of the information in a broader range of circumstances, including for any related secondary purpose the individual would reasonably expect the CSP to disclose the information for.[5]

Proposed section 16 also explicitly requires CSPs to destroy personal information when it is no longer required 'under [the Determination] or any other applicable laws'. By contrast, APP 11.2 only requires CSPs to take reasonable steps to destroy or de-identify personal information where they no longer need it for any purpose for which the information may be used or disclosed under the APPs.

[5] See APP 6.1 - 6.2.

6.2 Applying section 16 only to CSPs not bound by the Privacy Act will cause unnecessary complexity and confusion when applying the rules

In our view, making section 16 apply only to CSPs that are not bound by the Privacy Act will introduce unnecessary complexity in the rules, and may cause confusion as to which rules apply in particular circumstances. The Privacy Act is complex, and it may not always be clear whether a CSP is bound by the Privacy Act and the APPs. Given the more prescriptive requirements contained in section 16, making it apply only to CSPs not bound by the Privacy Act may also have the perverse effect of imposing stricter rules on CSPs not bound by the APPs than on those that are bound by them.

While there would be significant overlap between proposed section 16 and the requirements of APPs 6 and 11 (for those CSPs bound by the APPs), this is not necessarily undesirable. It is unlikely the requirements of section 16 would be inconsistent with CSPs complying with APPs 6 and 11. Making the requirements of section 16 apply universally to all CSPs covered by the Determination (including those bound by the APPs) would ensure consistency of approach between CSPs and clarity in the interpretation of the rules.

7 We encourage the ACMA to consult further on its proposed guidance for industry

We support the ACMA's proposal to develop guidance for industry on best practices and compliance with the revised Determination. Through our complaints we have seen inconsistency in telcos' understanding of and approach to the obligations in the Determination. It would be beneficial for all stakeholders for the ACMA to provide additional clarity on how the Determination should be applied.

Recommendation: Consult broadly on future guidance for industry, including with the TIO and other non-industry stakeholders

Our experience handling complaints about telecommunications fraud and unauthorised account access gives us a valuable perspective on the practical implications of different approaches to the Determination's rules. We encourage the ACMA to consult broadly on any future guidance for industry on the Determination, including with our office and other non-industry stakeholders, before the guidance is finalised.