



AGL Energy Limited
T 02 9921 2999 Level 24, 200 George St
F 02 9921 2552 Sydney NSW 2000
agl.com.au Locked Bag 1837
ABN: 74 115 061 375 St Leonards NSW 2065

15 December 2021

The Manager
Telecommunication Performance and Regulation Section
Australian Communications and Media Authority
PO Box 13112
Law Courts
MELBOURNE VIC 8010

Submitted via website: <https://www.acma.gov.au/have-your-say>

New rules to prevent fraud from unauthorised customer interactions with telecommunications providers

AGL Energy (**AGL**) welcomes the opportunity to provide feedback to the Australian Communications and Media Authority (the **ACMA**) consultation on proposed new rules to prevent fraud from unauthorised customer interactions with telecommunication providers, dated 17 November 2021.

Following the purchase of the Southern Phone Company in 2019, AGL entered the telecommunications industry to become one of Australia's largest energy-led multi-product retailers, providing over 4.2 million electricity, gas and telco services to residential, small, and large businesses, and wholesale customers. AGL believes that carriage services providers (**CSPs**) have a central role to play in protecting customers from unauthorised access and fraudulent activity in relation to their telco services.

AGL supports the introduction of additional verification processes to protect customers from harmful unauthorised transactions, recognising that two-factor authentication can be a highly effective tool for preventing fraud. However, the draft determination is overly prescriptive with respect to the verification requirements while the breadth of the defined terms in the draft determination could result in outcomes not intended by the ACMA. Specifically, in its current form, the draft determination captures the overwhelming majority of all customer-CSP interactions, requiring additional verification processes to be undertaken by the customer. We believe the ACMA should better balance protecting consumers against unauthorised transactions without restricting access or creating barriers to accessing the telco services.

AGL recommends a more targeted scope for the application of the new rules to capture those transactions which have the highest propensity to harm consumers if initiated fraudulently. Specifically, these are sim swap transactions, call forwarding, blocking, and diversion as well as requests to transfer from post-paid to pre-paid services.

AGL provides responses to the ACMA's consultation questions below:



1. Draft Effectiveness

Are these requirements adequate to achieve the objectives of the draft determination to reduce consumer harm and protect the security of high-risk customer interactions?

Two-factor authentication is an effective way to protect customers from harmful, fraudulent transactions and AGL supports the requirement that interactions with a high risk of harm should require additional steps to verify the identity of the person making the request.

However, it may not always be straightforward for customers to comply with additional verification requirements. Many individuals face challenges in their day-to-day lives such as not having access to technology and the internet, or may have limited literacy, numeracy, and digital skills which can make engaging with the telco services a difficult task. For customers experiencing vulnerability due to a sudden unexpected change in circumstances such as illness, displacement from their usual place of residence or some other circumstance, these challenges can compound and greatly impact the way that customers engage with their service providers. In implementing additional verification requirements, the ACMA should assess how access to telco services for customers in vulnerable circumstances (beyond those defined in the draft determination) could be adversely impacted.

The ACMA should be cognisant that the introduction of additional verification requirements to simple transactions may create or exacerbate barriers to participating in the telco market. The current definition of “high-risk interaction” which, in addition to adding, removing, or modifying a telecommunications service, includes any changes to, or disclosure of, personal or account information. This approach is extremely broad and likely to capture most customer-CSP interactions, creating a disjointed and highly interrupted experience for routine transactions. Customers with basic billing and payment enquiries, as well as those requiring payment support options such as establishing a payment plan will be required to undertake onerous verification requirements each time they interact with their CSP. AGL recommends the ACMA adopt a more risk-based approach to the draft determination which targets high-risk interactions such as sim swaps, call diversion, forwarding and blocking, as well as requests to transfer from post to pre-paid services. Narrowing the scope of the determination to these types of high-risk interactions will provide the highest level of protection, foster ongoing participation, ensure an improved customer experience while keeping industry costs for implementation and management at a reasonable level.

We also note that additional verification measures may not be effective in every scenario (such as lost or stolen devices, have no other contact methods etc.), therefore, two-factor authentication has limited value in these circumstances.

[Further clarity required on key concepts in the Determination](#)

The proposed draft introduces a number of new concepts, some of which are defined within the draft determination while others are more ambiguous. Key concepts should be defined by the ACMA to provide certainty for CSPs when developing business processes, agent training and IT systems. The ACMA should clearly define:

Suspects: Appearing under Part 11 and Part 12 of the Act, in the event the CSP “suspects” a customer’s account has been subject of fraudulent activity, then a number of proactive obligations apply. AGL notes that



regulatory obligations which arise from CSP forming a suspicion were not previously incorporated under the PPV Standard.

AGL does not support the inclusion of obligations which place an onus on the CSP to identify fraud and relies on the CSP forming a state of mind, particularly where there is no clear definition as to which elements the CSP must have regard. For example, irregular/high data usage, calls/SMS made, additional handset purchase, changes to payment method or personal information, frequent contact with the CSP, etc. In the majority of cases, the presence of any one or more of these elements does not necessarily indicate that fraudulent activity has taken place, however, the lack of clarity around these obligations makes compliance difficult, onerous on the CSP, and almost impossible to achieve. Without specific 'triggers', CSPs could be contacting their customers frequently causing unnecessary stress to customers.

AGL recommends that this term be more clearly defined and linked directly to where law enforcement is involved, on advice from the ACMA, the customer and/or the customer's financial institution. Alternatively, AGL recommends that this term be removed from the draft determination where it creates a proactive obligation on the CSP.

Fraudulent Activity: AGL notes that the concept of the CSP suspecting "fraudulent activity" was also not part of the PPV Standards and the ACMA has not provided any further information on how these obligations are to be met by CSPs. As such, AGL seeks more clarity from the ACMA as to what "indications of fraudulent activity" the CSP must have regard to when reviewing the customer's account.

2. High-risk customer interactions

Will this definition capture all of the interactions targeted by, or vulnerable to, scammers? If not, what are the other interactions?

Are there any specific interactions or class of interactions that should not be considered high-risk, and why?

The broad definition of "high-risk interaction" which includes adding, removing and modifying a service, or changing and disclosing personal or account information, will have the effect of capturing most, if not all everyday customer interactions, including simple payment-related queries which will create complexity for regular, day-to-day contact from customers.

While we understand the ACMA may be reluctant to provide detailed information about emerging scams, the statement in the draft determination about "emerging harms as scammers target other interactions....to facilitate identify and financial theft" is not supported by any data or statistics to demonstrate how the proposed wide-reaching regulatory reform will prevent these types of harms.¹ In our experience, other than phone porting, fraudulent sim swap requests, call forwarding, diversion and barring have a high potential to harm consumers and therefore should require the customer to undertake additional verification processes.

The risk of widespread harms resulting from other interactions such as the disclosure of non-sensitive account information has not been fully explained to substantiate additional verification requirements for everyday customer transactions. We recommend a risk-based framework be adopted in assessing which

¹ Australian Communications and Media Authority, *New rules to prevent fraud from unauthorised customer interactions with telecommunications providers, Proposal to make the Telecommunications Service Provider (Customer Identity Verification) Determination 2021*, November 2021, p4.



transactions require an uplift in authentication and verification. The framework should aim to better balance the objective to protect customers from increasing fraudulent transactions while also ensuring a positive customer experience, and accessibility to telco services by defining the types of “high-risk interaction” to mean:

An interaction in relation to a customer’s telecommunications service, instigated by either the requesting person or by the carriage service provider, where the carriage service provider does all or any of the following:

Initiates or completes a SIM swap request, a call diversion or forwarding request, a request to transfer a telecommunications service from being a post-paid carriage service to a pre-paid carriage service and a call barring request but does not include a transaction to port a mobile number to which the *Telecommunications (Mobile Number Pre-Porting Identity Verification) Industry Standard 2020* applies.

3. Multi-factor identity verification processes

Are there additional examples of account information, personal information or possession-based authenticators that should be covered by these definitions?

The ACMA should provide clarity on the relationship between the verification requirements under Section 9(1) of the Act and existing obligations under the Privacy Act to verify the identity of the individual, and whether the ACMA intended for Section 9(1) to complement or replace standard privacy obligations.² The proposed definitions for “account information authenticator” and “personal information authenticator” are narrow and may further exacerbate challenges for individuals to complete the verification process. Further, the definitions and the requirement under Section 9(1) relating to personal information are duplicative of those under Privacy Act.

The draft determination imposes a time limit of one day for multi-factor identity verification to be completed using identity documents. Is a time limit required and, if so, is this period appropriate?

Time sensitive verification requirements can increase barriers to accessing telecommunication services and may disadvantage customers who have a limited ability to produce documents digitally or in person, as well as those customers who do not have verifiable documents readily available due to circumstances outside of their control.

It is important that the telco services remain inclusive of all customers and do not create harms or barriers to participation due to regulatory intervention. We encourage the ACMA to balance consumer safety while also avoiding introducing unnecessarily higher barriers to timely access by imposing onerous additional verification requirements, or the timeframe within which the identity documents must be produced. These requirements could adversely affect customers who require access to their telco services but:

- Do not have access to a device, email account, app, or have any other way to comply with additional verification requirements e.g., lost, or stolen devices.

² *Telecommunications Service Provider (Customer Identity Verification) Determination 2021*, Section 9(1): A carriage service provider for the telecommunications service must use either of the following identity verification processes: (a) at least two account information authenticators; or (b) at least: (i) one account information authenticator; and (ii) one personal information authenticator.



- Do not wish to disclose their personal circumstances to CSP agents or may not identify as experiencing vulnerable circumstances.
- Are located in a rural or remote community for the purposes of physically presenting documentation.
- Have no access to the internet or other electronic services or are otherwise unable to produce documents electronically.
- Do not have a representative such a caregiver, family member, friend or financial counsellor who can advocate on the customer's behalf.

The ACMA should clearly outline how CSPs should treat these types of customers as we do not believe the draft determination intends for these circumstances to fall under the vulnerable customer exemption from undertaking the additional verification processes. In AGL's view, applying a more targeted scope for the definition of "high-risk interaction" as put forward in the response to Question 2 above, could reduce barriers for these customer cohorts, as the additional verification requirements would apply only to the transactions with the highest risk, rather than affecting day-to-day transactions, such as establishing a payment plan or changing the method of payment.

4. Identity verification requirements for customers in vulnerable circumstances

Are there additional processes that should be considered?

Notwithstanding AGL's endorsement of outcomes-based regulation, there is substantial ambiguity in the draft determination on how to treat to customers with limited capacity to satisfy the additional verification requirements. These include customers with no access to valid documentation, identification number of unique government documents as well as customers who cannot produce these documents in a way that can be "confirmed by the CSP that the requesting person is the customer for that service."

Requirement to record basis for reasonably believing the customer is in vulnerable circumstances

AGL does not support the introduction of Section 11(3)(a)(ii) which requires that the CSP record "the basis on which the provider reasonably believed that the requesting person was a customer in vulnerable circumstances".

AGL believes that all individuals should have right to determine whether or not they wish for this type of information to be recorded against their account. There may also be interactions where the customer is not forthcoming or does not want to disclose their circumstances to the CSP, meaning that CSP agents would need to either decline to service the customer or be unable to meet the requirements of this provision.

With respect to customers affected by family violence, no action should be taken, or any information recorded on the account unless explicitly instructed by the customer so as to not compromise their safety. In this context, agents would be required to proactively ask the customer if they are permitted to record the basis for believing the customer is in vulnerable circumstances, which could be intrusive and unwelcome. If the customer declines to have this information recorded, the CSP will be unable to comply with this requirement.

Further, where the customer is a customer is affected by an emergency, if the emergency is related to medical reasons, recording this information triggers a number of obligations under the Privacy Act on how to collect and use sensitive information, including capturing the customer's explicit informed consent to do so.

We do not believe that recording sensitive information or capturing "the basis for believe the customer is in vulnerable circumstances" will assist in preventing fraudulent activity or promote better protections for customers in vulnerable circumstances. AGL recommends that this provision be removed.



5. Implementation

In setting an appropriate implementation date, the ACMA should have consideration to the need to protect consumers from high-risk fraudulent transactions balanced against the substantial effort required to operationalise the changes in their current state. Broadly, CSPs would be required to:

- Develop and build the systems architecture required to support the scope of the proposed changes, including new instantaneous SMS/Email/App notifications as well as preparing telephony systems for 2-way SMS functionality, noting some of this is already required under the PPV Standard.
- Establishing new business processes and agent training for customer verification requirements across all types of interactions and transactions.
- Creating verification processes for online MyAccount services and applications where the customer can modify personal and/or account information.
- Establishing new processes to receive and verify category A and B documents and online government verification services.

Given the breadth of the proposed definition of “high-risk interaction” and that the final determination is not known (and is unlikely to be final until end of February 2022), an implementation date of 5 April 2022 is not sufficient where changes are of this magnitude in Service Centres, digital channels, and retail environments (including training) could take many months to implement.

The ACMA will be aware that the Consumer Data Right (CDR) is proposed to commence in the telco industry sometime in 2023. We believe some of the elements from the draft determination can be staggered to coincide with the CDR arrangements.

AGL’s recommendation is that:

1. The definition of “high-risk interaction” be narrowed to mean interactions those referred to in our response to Question 2, with the ACMA extending the implementation timeframe until later in the next financial year;
2. A transitional arrangement where CSPs can accept alternative methods of customer verification while CSP build systems and processes to accept and verify category A and B documents be put in place for a period of three to six months; and
3. Additional verification methods for all other interactions captured by the current definition could be staggered or coincide with the CDR coming into effect. This approach will also allow the ACMA to assess data and trends relating to fraudulent activity and assess the effectiveness of the new rules in further preventing fraud and identify other opportunities as they are identified.

6. Other Matters

5 business days to produce documents to the ACMA

AGL has extensive experience in responding to regulatory requests to produce documentation and information in the energy and telecommunications industries, including from various commissions, regulators, ombudsman schemes and government departments across Australia. AGL notes the importance of responding to such requests and the need to cooperate regulators on such requests. Therefore, we do not believe it is necessary to impose a five-business day timeframe within which the CSP must provide documentation in response to the ACMA under these rules.



We consider that the ACMA should determine the appropriate timeframe for each request on a case-by-case basis, having consideration to the nature and cause of the alleged conduct, the number of customers affected, the complexity of complying with the request to produce documentation (for example, where data is stored across multiple IT systems) and the sophistication of the alleged fraudulent activities (such as where a crime syndicate is identified).

Alternatively, and consistent with longer timeframes generally provided for information requests under section 521 of the *Telecommunications Act 1997*, we believe that 10 working days can be complied with which will accommodate more detailed and comprehensive requests.

If you would like to discuss any aspect of AGL's submission, please contact Valeriya Kalpakidis at vkalpakidis@agl.com.au.

Yours sincerely,

A handwritten signature in blue ink, appearing to read 'Elizabeth Molyneux', is written over a faint, light blue circular watermark.

Elizabeth Molyneux
General Manager, Policy and Energy Markets Regulation
AGL Energy