15th December 2021

The Manager

Strategy and Projects Section

Australian Communications and Media Authority

Law Courts

Melbourne VIC 8010

**Acceleon** is a leading Melbourne-based Australian data technology company.

**We believe in a future where everyone’s identity is safe, secure, and managed with integrity.**

We have worked with the ACMA since 2011 in our capacity as a public number directory provider under the Telecommunications Act and the IPND scheme. In 2014 Acceleon extended our relationship with Government departments by becoming an ASIC information broker.

Acceleon has since developed a series of products and services that leverage these data assets along with a variety of others to support companies’ efforts to keep their customer information as accurate and current as possible.

Our purpose is to inspire truth, trust, and momentum through the integrity of data, and therefore, we plan to use our data & technology expertise to help fight SIM card fraud theft that is devasting everyday Australians at an alarming rate.

Acceleon thanks the Australian Communication and Media Authority for the opportunity to submit a response to the draft Telecommunications Service Provider (Customer Identity Verification) Determination 2021.

Acceleon is aware of the significant harm Australian Consumers are experiencing due to scammers targeting SIM swap processes.

Our financial services clients are telling us that their existing fraud data triggers are no longer working, so we are determined to help solve this problem.

The only way to keep up with these technologically adept scammers, is to beat them at their own game. We are working on several trials with our clients to use data solutions & technology to better detect fraudulent, unauthorised consumer interactions.

Acceleon will address each of the specific issues for comment:

1. **Effectiveness of the draft determination**

The draft determination sets out a number of customer identity verification requirements for high-risk customer interactions and ways to deal with the specific circumstances affecting customers in vulnerable customers.

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?

Whilst Acceleon supports the additional measures set out in the draft determination, we believe more can and should be done to protect consumers.

We should be striving to do more than what is “adequate” and believe that the telecommunications industry can provide non-PII data to other sectors to help combat the issues on multiple fronts.

There is already precedence set for carriage service providers to capture and send data to a central repository known as the Integrated Public Number Database (IPND). This could be extended, or a similar repository could be created to provide additional mitigation strategies towards Identity Theft and Fraud.

1. **High-risk interactions**

The draft determination defines 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?

Acceleon agrees with the proposed definition. We do not believe there are any specific interactions or class of interactions that should not be considered high-risk. They are all high-risk in our opinion.

1. **Multi-factor verification processes:**

The draft determination sets out processes for customer identity verification but does not intend to limit providers taking additional or innovative actions.

We are specifically interested in how the proposed processes will work where authorised representative arrangements are in place.

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

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?

Yes – a time limit is appropriate to ensure processes are not left open that could be exposed in the future. However, a one-day time limit seems too short for someone to gather the necessary information.

Perhaps an alternative solution would be for interval time limits triggering additional checks. For example, should it take more than 1 day, the carriage service provider may need to re-verify with the consumer via SMS or phone call again before moving beyond the identity verification step.

1. **Identity verification requirements for customers in vulnerable circumstances:**

The draft determination sets out identity verification requirements for people in vulnerable circumstances, such as emergency and family-violence affected individuals.

Are there additional processes that should be considered?

Acceleon believes these people are the ones at most risk of being unable to meet the new identity verification requirements as they may fall outside the general population who have ready access to technology and required services.

These people are those that would be better protected by implementing methods that go beyond what could be considered “adequate” and from solutions that formed by sharing information across different sectors.

1. **Implementation:**

The draft determination is proposed to commence on 5 April 2022.

We welcome feedback on the timing of commencement of the determination, including on any staged transitional arrangements that could be considered so that consumer protections are in place as quickly as possible.

We believe the timing of the commencement could always be sooner as that will benefit the wider public. We also believe there are other means to fight identity theft that should be considered at the same time.

Acceleon believes there is no single solution that can solve this growing problem.

Whilst the draft standard provides additional verification processes, we question if this will have a meaningful impact on unauthorised SIM swaps.

Therefore, Acceleon recommends that the ACMA consider an industry wide approach to the sharing of non PII data provided by the carriage service providers.

Further to Part 4 of Schedule 2 of the Telecommunications Act 1997, these rules could be extended to include Mobile SIM number details and should be managed independently by an accredited data broker (outside the telecommunications industry).

The IPND was initially developed to be a critical source of information for emergency services, law enforcement and national security agencies. We believe what is happening to everyday Australians with SIM card fraud theft is serious enough to consider the expanded use of IPND data or a similar repository of information across commercial industries that deal with the front line of fraud. For example, Financial Services, Email Account providers and any other online account provider.

**How would this data help?**

For example, when a consumer applies for any financial services product, if the service provider detects a high-risk activity attributable to the mobile phone number or sim card, this could trigger additional verification procedures.

**This simple process has just made it harder for a scammer to gain unauthorised services in the name of the potential victim!**

We see many practical use cases for a data set of this sort to help protect consumers from identity theft.

By using data & technology we can outsmart these scammers.

It will take entire industry collaboration, and Acceleon would like the opportunity to discuss our innovative solution with the ACMA in a follow up conversation.

Thank you again for the opportunity to respond.

Please don’t hesitate to contact us should you require clarification or would like further information on our proposed industry approach.

Yours sincerely,

Michelle Cross

Michelle Cross

CEO - Acceleon