EXPLANATORY STATEMENT

Approved by Authority of the Minister for Communications

Telecommunications Act 1997

Telecommunications Amendment (Disclosure of Information for the Purpose of Cyber Security) Regulations 2022

Purpose and operation of the Instrument

The purpose of the *Telecommunications Amendment (Disclosure of Information for the Purpose of Cyber Security) Regulations 2022* (the Instrument) is to amend the *Telecommunications Regulations 2021* (the Regulations) to prescribe two new circumstances for the purposes of section 292 of the *Telecommunications Act 1997* (the Act).

The Instrument is made by the Governor-General under section 594 of the Act, which allows the Governor-General to make regulations prescribing matters required or permitted to be prescribed by the Act, or necessary or convenient to be prescribed for carrying out or giving effect to the Act.

Subsection 33(3) of the *Acts Interpretation Act 1901* relevantly provides that where an Act confers a power to make an instrument of a legislative character (including regulations) the power shall be construed as including a power exercisable in the like manner and subject to the like conditions to repeal, rescind, revoke, amend, or vary any such instrument.

Section 276 of the Act provides a general prohibition on carriers and carriage service providers disclosing customer information to third parties. Subsection 292(1) empowers regulations to be made that create exceptions from the section 276 prohibition.

The purpose of the amendments to the Regulations is to remove legal barriers faced by carriers and carriage services providers in disclosing certain customer data in limited circumstances.

The amendment to the Regulations would permit carriers and carriage service providers to securely disclose government identifiers such as drivers licence and passport numbers to financial services entities (covering entities like Australian banks) and government agencies. If specified by the Minister, other information that relates to the identification of an individual that relates to the carriers and carriage service providers existing and past customers may also be securely disclosed. In addition, other related financial services entities or supporting bodies can be approved by the Minister. This secure disclosure would help to protect the customers of the particular carrier or carriage service provider in the event of a cyber security incident, fraud, scam, identity theft or malicious cyber activity.

Without the amendment to the Regulations, carriers and carriage service providers would continue to be subject to the general prohibition on disclosing the information in accordance with section 276 of the Act unless another secondary disclosure exception under Part 13 of the Act was applicable. Disclosures of personal information by carriers and carriage service providers in the circumstances described in either section 15A or section 15B of the Regulations (being a disclosure permitted by Division 3 of Part 13 of the Act) will be deemed disclosures authorised by law for the purposes of the *Privacy Act 1988* or a registered Australian Privacy Principles (APP) code, and therefore, a permitted secondary disclosure under APP 6.2(b).

Commonwealth entities and State authorities that intend to make requests under section 15B of the Regulations would develop internal procedures for these purposes, including establishing a register or rule for the persons authorised to make such requests.

A provision-by-provision description of the Instrument is set out in the notes at Attachment A.

The Instrument is a disallowable legislative instrument for the purposes of the *Legislation Act 2003*.

Documents incorporated by reference

The Instrument does incorporate a document by reference (namely, the *Prudential Standard CPS 234 Information Security* (at subparagraph 15A(2)(g)) and this is done in reliance on section 589 of the Act.

Consultation

Given the urgent and sensitive nature of the amendment to the Regulations, the Department of Infrastructure, Transport, Regional Development, Communications and the Arts did not conduct a public consultation. A range of relevant stakeholders were consulted, including the Department of Prime Minister and Cabinet, Department of Home Affairs, Treasury, Attorney-General's Department, the Australian Government Solicitor, Office of the Australian Information Commissioner, the Australian Signals Directorate, , the ACCC, the Australian Communications and Media Authority, Services Australia, APRA, Optus and the Australian Banking Association.

Regulatory impact assessment

The Office of Best Practice Regulation has advised a RIS is not required (OBPR22-03455).

Statement of compatibility with human rights

Subsection 9(1) of the *Human Rights (Parliamentary Scrutiny) Act 2011* requires the rule-maker in relation to a legislative instrument to which section 42 (disallowance) of the *Legislation Act 2003* applies to cause a statement of compatibility with human rights to be prepared in respect of that legislative instrument.

The statement of compatibility set out below has been prepared to meet that requirement.

Human rights implications

The Instrument engages the Right to Privacy in Article 17 of the *International Covenant on Civil and Political Rights.* Article 17 provides for the right to protection against arbitrary and unlawful interferences with privacy.

Article 17 prohibits arbitrary or unlawful interference with an individual's privacy, family, home or correspondence. Non-arbitrary interference, and some limitations provided by law, are permissible. In order for limitations to be deemed non-arbitrary, there must be a legitimate objective and it must be reasonable, necessary and proportionate.

The purpose of the Instrument is to allow carriers and carriage service providers to disclose certain personal information to financial services entities (including via entities approved by the Minister), Commonwealth entities and State authorities (which includes by definition various Territory entities) and other financial services entities approved by the Minister for the purposes of preventing, responding to, or responding to the consequences of cyber security incidents, frauds, scams, instances of identity theft or malicious cyber activity. The Instrument does not permit the disclosure of the personal information for other purposes.

The Instrument incorporates a number of safeguards across the whole process, including who has access to relevant information, the manner in which requests are made and information transmitted, and how information needs to be handled.

The Instrument restricts entities that have access to the data from carriers and carriage service providers to:

- financial services entities that are regulated by APRA. This class of potential entities includes Australian Authorised Deposit taking Institutions, general insurers, life insurers, registerable superannuation entities and their licensees, and private health insurers. The class can also be extended by the Minister in writing to cover a narrow set of additional financial services entities. This could include entities that are trusted portals for exchanging information that would receive data from the carrier or carriage service provider, and then provide other financial services entities with access to this data directed at a sole permitted purpose.
- Commonwealth entities as defined in the *Public Governance, Performance and Accountability Act 2013*, and 'State authorities' (as defined in the *Intelligence Services Act 2001,* which covers various State and Territory entities).

Financial services entities will be required to provide the ACCC with written commitments confirming they will comply with the following steps when accessing carrier or carriage service provider information:

- access, use, and sharing of information by APRA-regulated financial services entities with associates is limited to the sole purposes specified in the relevant circumstances;
- information or data cannot be shared with third parties (unless that third party is approved by the Minister and is directly related to or supports the provision of services to a financial services entity for a sole permitted purpose – see note above on trusted portals for exchanging information);
- entities must comply with requirements under the *Privacy Act 1988* in relation to any access, use or disclosure;
- entities must store the information in a way that prevents unauthorised access, disclosure, or loss to information received;
- entities must review whether the information still needs to be retained at least once every 12 months;
- information received must be destroyed once it is no longer required;
- entities have appropriate written procedures covering how they handle information received; and
- entities obtain similar written commitments from associate entities, apart from employees, who also need access to information received.

Copies of these written commitments provided to the ACCC will be forwarded on to relevant carriers and carriage service providers. A failure by a financial services entity to fulfil any of the positive written commitments given in favour of the ACCC may constitute misleading and deceptive conduct pursuant to subsection 18(1) of the *Australian Consumer Law*, and the ACCC could take appropriate enforcement action.

Additionally, APRA-regulated financial services entities will also be required to provide APRA with an attestation signed by an authorised officer, confirming they are complying with *Prudential Standard CPS 234 – Information Security* as in force from time to time. In the event that the Minister were to consider approving an additional financial services entity to which a carrier or carriage service provider would be permitted to disclose information, the information security credentials of that financial services entity would be considered by the Minister, based on advice from relevant government agencies.

The Instrument only allows for government identifiers, such as driver licences and passports, or other information that can identify individuals as approved by the Minister, to be released by carriers and carriage service providers to financial services entities and government entities.

The Instrument is temporary, and the new sections it inserts into the amendments to the Regulations will be automatically repealed 12 months after they come into effect.

Conclusion

The Legislative Instrument is compatible with human rights. To the extent that it may limit human rights, those limitations are reasonable, necessary and proportionate.

Attachment A

Notes to the *Telecommunications Amendment (Disclosure of Information for the Purpose of Cyber Security) Regulations 2022*

Section 1 - Name of Regulations

The section provides that the name of the Instrument is the *Telecommunications Amendment (Disclosure of Information for the Purpose of Cyber Security) Regulations 2022.*

Section 2 - Commencement

The section provides for the Instrument to commence on the day after the Instrument is registered.

Section 3 - Authority

The section provides that the Instrument is made under the *Telecommunications Act 1997* (the Act).

Section 4 - Schedules

The section provides that each instrument that is specified in a Schedule to the Instrument is amended or repealed as set out in the applicable items in the Schedule concerned, and any other item in a Schedule to the Instrument has effect according to its terms. There is only one Schedule to the Instrument.

Schedule 1 - Amendments

Item 1 to Schedule 1 inserts two new sections, 15A and 15B, into the *Telecommunications Regulations 2021* after the existing section 15.

Section 15A addresses disclosures to financial services entities for the specific sole purposes of preventing, responding to, or addressing cyber security incidents, fraud, scam activity, identity theft or malicious cyber activity. Section 15B addresses disclosures to the Commonwealth and States authorities (which includes various Territory bodies) for those same purposes.

New section 15A - Disclosures to financial services entities for the purpose of cyber security and identity fraud

Subsection 15A(1) creates an exception to the general prohibition under section 276 of the Act to enable carriers and carriage service providers to disclose certain information and documents to financial service entities, if all circumstances in subsection 15A(2) are met.

Subsection 15A(2) sets out circumstances that would have to be satisfied for the exception to the prohibition under section 276 of the Act to apply.

Paragraph 15A(2)(a) states the first condition that must be met is that the information or document in question is 'specified information' (defined in subsection 15A(6)) or a 'specified document' (defined in subsection 15A(6)), in relation to the carrier or carriage service provider. This narrows the class of documents or information that come within the scope of section 15A to documents or information held by the carrier or carriage service provider to the following two:

- government related identifiers of individuals who are existing or were past customers; and
- a form of 'personal information' of existing or past customers as specified by the Minister in a notifiable instrument under subsection 15A(5)(a) or (b).

For the first class, the term 'government identifier' has the same meaning as within section 6 of the *Privacy Act 1988* and covers an identifier of individuals that have been assigned by a range of Commonwealth entities, such as a Commonwealth body, agency, department, or an eligible hearing service provider; the service operator under the *Healthcare Identifiers Act 2010*, or a State or Territory authority; an agent of an agency, or a State or Territory authority acting in its capacity as an agent. Examples of commonly issued government identifiers are Medicare, driver licence and passport numbers.

For the second class, the type of information that is capable of being specified by the Minister is limited to 'personal information' as defined in the *Privacy Act 1988*. This covers a range of information about an individual such as names, addresses and date of birth.

The power for the Minister to extend the class of information that is permitted to be disclosed by a carrier or carriage service provider in reliance on the circumstance for the purposes of section 292 of the Act (being a secondary disclosure provision under Part 13 of the Act) must be in the form of a notifiable instrument. It is intended that this power is held in reserve and only used in compelling circumstances such as a cyber-attack where a carrier or carriage service provider's customer records are compromised and the nature of threatened cyber incidents, fraud, scam activity, identity theft, or malicious cyber activity that could emerge from the attack warrants a high level of class of disclosure of particular kinds of personal information. The creation of new accounts using compromised government identifiers is the major source of risk arising from a cyber security attack that involves the compromise of customer data, such as the one recently experienced by Optus, and knowledge of compromised government identities by the financial institutions will allow countermeasures to directly target the source of this risk.

Paragraph 15A(2)(b) sets out the condition that the carrier or carriage service provider has received a written request from an officer of a financial services entity for the particular 'specified information' and/or 'specified document'.

Paragraph 15A(2)(c) sets out a further condition about the particulars of the request, namely that the entity is seeking the information or document for a particular sole purpose of enabling the entity:

- to take steps to prevent a cyber security incident, fraud, scam activity or identity theft; or
- to take steps to respond to a cyber security incident, fraud, scam activity or identity theft; or
- to take steps to respond to the consequences of a cyber security incident, fraud, scam activity or identity theft; or
- to take steps to address malicious cyber activity.

The information or documents obtained by the carrier or carriage service provider cannot and must not be used for commercial purposes.

The concept of 'fraud', is intended to be interpreted broadly and cover acts on behalf of a person that is deceptive or deceitful in some way, in that, it causes them to receive a benefit that they are not entitled to. With the advent of online services and the internet, fraud can be committed in a range of ways.

The concept of 'scam activity' can overlap in some ways with the concept of fraud, and is more commonly understood as a dishonest scheme or trick used to cheat someone out of something, usually money.

The concept of 'identity theft' is intended to have its usual meaning under various laws.

The term 'cyber security incident' is defined under subsection 15A(6) to have the same meaning as in the *Security of Critical Infrastructure Act 2018*. It is an unwarranted or unexpected cyber security event or series of such events that has a significant probability of compromising business operations.

Subsection 15A(2)(d) sets out that the authorised officer must state in the request that, in their opinion, the disclosure of the relevant customer information or document is necessary and proportionate to deal with the cyber security incident, fraud, scam activity, identity theft or malicious cyber activity mentioned in paragraph 15A(2)(c). This is framed to ensure that financial services entities only request information they truly need, consistent with best practice privacy design. For example, if only the disclosure of one type of government identifier (for example, driver licence) is necessary and proportionate to a particular entity taking steps to preventing a scam activity or identity theft, then the entity should only request that type.

As the Regulation is unable to impose offences directly on the receiving entity, the circumstance in paragraph 15A(2)(e) sets out a comprehensive condition that before the relevant customer data can be disclosed to the financial services entity, that entity must have given the Australian Competition and Consumer Commission (ACCC) a written commitment (on terms acceptable to the ACCC) as to various matters: refer subparagraphs 15A(2)(e)(i) – (x). Entities must also obtain a written commitment in the same terms as that set out in paragraph (e) from another financial services entity, and their associates before sharing the information or document with that person. At law, a company is usually responsible for the actions of its employees, officers and agents, and in this way the financial services entity must ensure it has procedures and controls in place to ensure that its

employees, officers and agents adhere to the commitments given. However, neither employees of a financial services entity nor employees of an associate need to give a written commitment directly; the exclusion of employees in sub-paragraph (ix) can apply multiple times in a recursive way.

A failure by a financial services entity to fulfil any of the positive written commitments given to the ACCC may constitute misleading and deceptive conduct pursuant to subsection 18(1) of the *Australian Consumer Law*, and the ACCC could take appropriate enforcement actions.

Paragraph 15A(2)(f) sets out the condition dealing with the transmittal of the specified information or specified document. The document of information must be disclosed in a secure or trusted manner in all cases. Carriers and carriage service providers are all regulated by the *Privacy Act 1988* and are expected to have appropriate written procedures and system controls in place to ensure the data is handled appropriately and in accordance with the regulation (including procedures around use, access and security and that the data is not used for secondary purposes).

There is a reserve ability for the Minister to approve a particular manner of disclosure under subsection 15A(3). This is intended to keep in reserve the ability for the Minister to specify a particular method of disclosure if needed at a future date. The effect of the Minister's power under subsection 15A(3) is to approve a manner of disclosure of the information or document, and therefore comes within the exclusion at item 5 of the table accompanying section 6 of the *Legislation (Exemptions and Other Matters) Regulation 2015.* It is not a legislative instrument.

Paragraph 15A(2)(g) requires the authorised officer of a financial services entity regulated by the Australian Prudential and Regulation Authority (APRA) to have given a particular attestation to the APRA that it meets and will meet the principles and requirements of *Prudential Standards CPS 234 Information Security* (CPS) as in force from time to time in relation to the information or document requested from the carrier or carriage service provider. The incorporation by reference of CPS as in force from time to time is done in reliance on subsection 589(1) of the Act. The CPS aims to ensure that APRA-regulated entities take measures to be resilient against information security attacks (including cyber-attacks) by maintaining an information security capability commensurate with information security vulnerabilities and threats.

Subsection 15A(3) sets out that the Minister may, in writing, approve the manner in which a carrier or carriage service provider must disclose information or a document.

Subsection 15A(4) contains a reserve power for the Minister to approve in writing a body for the purposes of paragraph (c) of the definition of 'financial services entity' in subsection 15A(6). To prevent the introduction of integrity and other security risks, the identity of a body that is approved as a financial services entity to receive a specified document or specified information would not be required to be published.

The Minister may only approve a body to be a 'financial services entity' if it provides services that are either:

- directly related to, or support, the provision of services by an entity of a type set out in paragraphs (a) and (b) of the definition of financial services entity; or
- directly related to or support the provision of services to one of those types of entities, and the services provided are directly related to or support the purposes outlined in subsection 15A(2)(c), that is, responding to a cyber security incident, fraud, scam activity, identity theft or malicious cyber activity.

In the event that the Minister were to consider approving an additional financial services entity to which a carrier or carriage service provider would be permitted to disclose information, the information security credentials of that financial services entity would be considered by the Minister, based on advice from relevant government agencies.

The Minister's approval of particular bodies comes within the legislative instrument exception at item 4 of the table accompanying section 6 of the *Legislation (Exemptions and Other Matters) Regulation 2015*.

Subsection 15A(5) sets out that the Minister may, by notifiable instrument, specify additional kinds of information and documents, however, this specification would be limited to personal information (within the meaning of the *Privacy Act 1988*) about one or more individuals who are, or were, customers of the carrier or carriage service provider. The intention is that the Minister would specify information and documents that relate to the identification of an individual. The nature of the Minister's power under subsection 15A(5) is considered to be administrative in nature and the scope of this power is narrowly fixed by the express limit prescribed in the provision (namely, personal identifying information of a past or existing customer of a carrier or carriage service provider). Subsection 13(3) of the *Legislation Act 2003* permits determinations by notifiable instrument to be made on a class basis.

Subsection 15A(6) sets out relevant definitions for the section 15A, namely, 'ADI ', 'associate ', 'cyber security incident ', 'financial services entity ', 'officer ', 'specified document ', and 'specified information '.

The term 'associate ' is defined in a relational way, by reference to an entity (which, under section 64A of the *Corporations Act 2001* (Corp Act)), captures natural persons, body corporates (other than an exempt public authority), partnership or trusts (and trustees of trusts). In order for a person to be considered an associate of a financial services entity, it must be one of the following:

- an employee of the entity;
- where the entity is a body corporate:
    - a related body corporate (within the meaning of the Corp Act) of the entity; or
    - an employee of the related body corporate;
- a contractor of the entity (the concept of 'contractor' is intended to have a broad meaning and cover individuals, partnerships, body corporates that are contracted to

provide goods or services to the financial services entity. By way of example, the concept of 'contractor' in section 15A could capture a software company contracted by a bank to update the bank's fraud control system to prevent fraud. It could also capture an individual who is contracted to provide services to a bank).

Subsection 15A(7) clarifies that the section 15A applies to information or a document held by a carrier or carriage service provider before, on or after the section commences.

Subsection 15A(8) sets out that section 15A will be repealed 12 months after it commences.

New section 15B - Disclosures to government entities for the purpose of cyber security and identity fraud

Subsection 15B(1) creates an exception to the general prohibition under section 276 of the Act and enable carriers and carriage service providers to disclose information and documents to government entities if all circumstances in subsection 15B(2) are met.

Subsection 15B(2) contains circumstances that would have to be satisfied for the exception to the prohibition under section 276 of the Act to apply.

Paragraph 15B(2)(a) sets out that the first condition that must be met is that the particular carrier or carriage service provider has received a written request from an official of the Commonwealth entity or State authority for the information or the document.

Paragraph 15B(2)(b) sets out the second condition that the request must state that the information or document is required for the sole purpose of enabling the Commonwealth entity or State authority to take steps to:

- prevent a cyber security incident, fraud, scam activity or identity theft; or
- respond to a cyber security incident, fraud, scam activity or identity theft; or
- respond to the consequences of a cyber security incident, fraud, scam activity or identity theft; or
- address malicious cyber activity.

A disclosure that is requested for a purpose in sub-paragraph (i), (ii), (iii) or (iv), depending on the circumstances and entity seeking help as is reasonably necessary from a carrier or carriage service provider, may also come within the scope of one of the purposes listed in subsection 313(3) of the Act.

Paragraph 15B(2)(c) sets out the that the officer of the Commonwealth entity or State authority must record in the request, their opinion that the disclosure of the information or document is necessary and proportionate to deal with the purpose mentioned in paragraph 15B(2)(b) for which the information or document is required.

Consistent with data minimisation practice, a Commonwealth entity or State authority should not request information or documents containing data that is not necessary and proportionate to deal with the sole purpose outlined in the Regulations.

Paragraph 15B(2)(d) sets out that government related identifiers or personal information (within the meaning of the *Privacy Act 1988*) as specified by the Minister in a notifiable instrument under paragraph 15B(2)(e) may be disclosed to a Commonwealth entity or State authority. The nature of the Minister's power under subsection 15B(2)(e) is considered to be administrative power in nature and the scope of this power is narrowly fixed by the express limit prescribed in the provision (namely, personal identifying information of a past or existing customer of a carrier or carriage service provider). Subsection 13(3) of the *Legislation Act 2003* permits determinations by notifiable instrument to be made on a class basis.

Paragraph 15B(2)(e) sets out that information and documents must be transferred in a secured and trusted manner.

A note accompanies subsection 15B(2) in recognition that carriers and carriage service providers have a duty to provide reasonable necessary assistance to officials and authorities of the Commonwealth and of States and Territories for purposes specified at subsection 313(3) of the Act. The note explains that subsection 15B(2) does not limit a carrier, or carriage service provider's obligations under subsection 313(3) of the Act to help such officers and authorities.

Additionally, there may be other laws that permit the relevant information or document to be disclosed by a carrier or carriage service provider to a Commonwealth entity in reliance on section 280 of the Act because the disclosure is as required or authorised by a law (for example, section 86E of the *Crimes Act 1914* (Cth)), and section 15B is not intended to interfere with the operation of those laws.

Subsection 15B(3) empowers the Minister to approve additional kinds of information that can be disclosed via notifiable instrument.

Definitions

Subsection 15B(4) sets out relevant definitions for the section, namely, 'Commonwealth entity ', 'cyber security incident ', 'official ', and 'State authority '.

The term, 'Commonwealth entity' is defined by reference to the meaning given for that term in *Public Governance, Performance and Accountability Act 2013*. Specifically, it includes a Department of State; a body corporate that is established by a law of the Commonwealth (but this excludes Commonwealth companies).

The term 'State authority ' defined by reference to the meaning given for that term in the *Intelligence Services Act 2001* and includes: a Department of State of a State or Territory or a Department of the Public Service of a State or Territory; and a body established, or continued in existence, for a public purpose by or under a law of a State or Territory; and a body corporate in which a State, Territory or a body referred to in paragraph (b) has a controlling interest.

Whilst the term 'official ' includes any member of staff, or officer or employee, of a Commonwealth entity or State authority, it is envisaged that only officials of appropriate

seniority of each Commonwealth entity (e.g. SES Level) and equivalent senior levels in State authorities would actually request a carrier or carriage service provider to disclose information or a document in reliance on subsection 15B(2) and be the proper persons to give their opinion that the disclosure of that information/document is necessary and proportionate (as required under paragraph 15B(2)(c)).

Similar to financial services entities, the Commonwealth entities and the Norfolk Island administration are regulated by the *Privacy Act 1988*. Most Australian states and territory have equivalent legislation that covers their public sector agencies and a limited number of state authorities and instrumentalities are also bound by the *Privacy Act 1988*. The use, handling, and dealing by such entities will be regulated and those entities will also be constrained in how they can use the information or documents they receive from a carrier or carriage service provider under section 15B. In many cases, there will be Commonwealth or State/Territory laws setting out protections for the information received.

Application

Subsection 15B(5) clarifies that section 15B applies to information or a document held before, on or after the section commenced.

Sunsetting information

Subsection 15B(6) sets out that section 15B will be repealed 12 months after the section commences.