2019-2020-2021

The Parliament of the
Commonwealth of Australia

HOUSE OF REPRESENTATIVES

Presented and read a first time

Ransomware Payments Bill 2021

No. , 2021

(Mr Watts)

A Bill for an Act to require the reporting of ransomware payments to the Australian Cyber Security Centre, and for related purposes

Contents

A Bill for an Act to require the reporting of ransomware payments to the Australian Cyber Security Centre, and for related purposes

The Parliament of Australia enacts:

Part 1—Preliminary

1 Short title

This Act is the *Ransomware Payments Act 2021*.

2 Commencement

(1) Each provision of this Act specified in column 1 of the table commences, or is taken to have commenced, in accordance with column 2 of the table. Any other statement in column 2 has effect according to its terms.

Commencement information

Column 1	Column 2	Column 3
Provisions	**Commencement**	**Date/Details**
1. The whole of this Act	A single day to be fixed by Proclamation. However, if the provisions do not commence within the period of 6 months beginning on the day this Act receives the Royal Assent, they commence on the day after the end of that period.	

Note: This table relates only to the provisions of this Act as originally enacted. It will not be amended to deal with any later amendments of this Act.

(2) Any information in column 3 of the table is not part of this Act. Information may be inserted in this column, or information in it may be edited, in any published version of this Act.

3 Definitions

In this Act:

access to data held in a computer has the same meaning as in Part 10.7 of the *Criminal Code*.

attacker: see section 4.

Australian Cyber Security Centre means the part of the Australian Signals Directorate known as the Australian Cyber Security Centre.

civil penalty provision has the same meaning as in the Regulatory Powers Act.

Commonwealth entity has the same meaning as in the *Criminal Code*.

data has the same meaning as in the *Criminal Code*.

data held in a computer has the same meaning as in the *Criminal Code*.

de-identified has the same meaning as in the *Privacy Act 1988*.

electronic communication has the same meaning as in Part 10.7 of the *Criminal Code*.

Federal Circuit Court means the Federal Circuit Court of Australia.

Federal Court means the Federal Court of Australia.

impairment of electronic communication to or from a computer has the same meaning as in Part 10.7 of the *Criminal Code*.

indicator of compromise: see subsection 8(3).

modification, in respect of data held in a computer, has the same meaning as in Part 10.7 of the *Criminal Code*.

personal information has the same meaning as in the *Privacy Act 1988*.

ransomware attack: see section 4.

ransomware payment: see section 4.

Regulatory Powers Act means the *Regulatory Powers (Standard Provisions) Act 2014*.

unauthorised access, modification or impairment has the same meaning as in Part 10.7 of the *Criminal Code*.

4 Meaning of *attacker*, *ransomware attack* and *ransomware payment*

A person (the ***attacker***) engages in a ***ransomware attack*** if:

(a) the person causes, whether directly or indirectly, any of the following by the execution of a function of a computer:
  (i) access to data held in a computer;
  (ii) modification of data held in a computer;
  (iii) the impairment of electronic communication to or from a computer;
  (iv) the impairment of the reliability, security or operation of any data held on a computer disk or other device used to store data by electronic means; and
(b) the person knows the access, modification or impairment is unauthorised; and
(c) in the case of an unauthorised modification or impairment—the modification or impairment:
  (i) restricts access by an authorised person to data held in a computer; or
  (ii) will, or gives an unauthorised person the ability to, modify, damage or destroy data held in a computer or on a computer disk or other device used to store data by electronic means; and
(d) the attacker demands a payment (whether of money or other consideration) (a ***ransomware payment***) to:
  (i) end the unauthorised access, modification or impairment; or
  (ii) prevent publication of any of the data; or
  (iii) end the restriction on access to the data; or
  (iv) prevent damage or destruction of the data; or
  (v) otherwise remediate the impact of the unauthorised access, modification or impairment.

5 Persons and connection with Australia

This Act applies to ransomware payment made by:
(a) a Commonwealth entity; or
(b) a State or Territory or an agency of a State or Territory; or
(c) any other person if:

(i) the person carries on a business (within the meaning of the *Income Tax Assessment Act 1997*) in the income year in which the payment is made; and

(ii) the person is not a small business entity (within the meaning of that Act) for the year; and

(iii) the ransomware payment relates to a ransomware attack against data, a computer, computer disk or other device located in Australia or used by the person in Australia.

Note: For the application of this Act to partnerships, see section 11.

6 Binding the Crown

This Act binds the Crown in each of its capacities.

7 Saving of certain State and Territory laws

It is the intention of the Parliament that this Act is not to affect the operation of a law of a State or of a Territory that:

(a) makes provision with respect to the collection, holding, use, correction or disclosure of information relating to ransomware attacks; and

(b) is capable of operating concurrently with this Act.

Part 2—Notification of ransomware payments

8 Notification of ransomware payments

(1) An entity that makes a ransomware payment must, as soon as practicable, give written notice of the payment to the Australian Cyber Security Centre in accordance with subsection (2).

Civil penalty: 1,000 penalty units.

(2) The notice must set out:

(a) the name and contact details of the entity; and

(b) the identity of the attacker, or what information the entity knows about the identity of the attacker (including information about the purported identity of the attacker); and

(c) a description of the ransomware attack, including:

(i) the cryptocurrency wallet etc. to which the attacker demanded the ransomware payment be made; and

(ii) the amount of the ransomware payment; and

(iii) any indicators of compromise known to the entity.

(3) An ***indicator of compromise*** is technical evidence left by the attacker that indicates the attacker's identity or methods.

Privilege against self-incrimination

(4) An individual is not excused from giving a notice under subsection (1) on the ground that giving the notice might tend to incriminate the individual in relation to an offence.

Note: A body corporate is not entitled to claim the privilege against self-incrimination.

(5) However:

(a) the notice given; and

(b) the giving of the notice; and

(c) any information, document or thing obtained as a direct consequence of the giving of the notice;

are not admissible in evidence against the individual in criminal proceedings other than proceedings for an offence against section 137.1 or 137.2 of the *Criminal Code* that relates to this Act.

9 Australian Cyber Security Centre may use information contained in notifications

(1) This section applies if a person notifies the Australian Cyber Security Centre of a ransomware payment under section 8.

(2) The Australian Cyber Security Centre may disclose any of the information contained in the notification to any person (including the public) for the purpose of informing the person about the current cyber threat environment.

Example: Publication to members of the ACSC Partnership Program through the Centre's threat-sharing platform.

(3) However, the Australian Cyber Security Centre must not disclose personal information under subsection (2) unless the information is first de-identified.

(4) The Australian Cyber Security Centre may disclose any of the information contained in the notification to:

(a) a Commonwealth entity; or

(b) a State or Territory, or an agency of a State or Territory;

for purposes relating to law enforcement.

(5) A person commits an offence if:

(a) information is disclosed to the person under subsection (4); and

(b) the person discloses any of the information.

Penalty: 500 penalty units.

(6) Subsection (4) does not apply if:

(a) the information the person discloses is not personal information; or

(b) the entity that gave the original notification to the Australian Cyber Security Centre consents to the disclosure of the information; or

(c) the Director-General of ASD authorises the disclosure of the information; or

(d) the disclosure is to a court; or

(e) the disclosure is otherwise required or authorised by law.

Note: A defendant bears an evidential burden in relation to the matter in subsection (6): see subsection 13.3(3) of the *Criminal Code*.

Part 3—Miscellaneous

10 Civil penalty provisions

Enforceable civil penalty provisions

(1) Each civil penalty provision of this Act is enforceable under Part 4 of the Regulatory Powers Act.

Note: Part 4 of the Regulatory Powers Act allows a civil penalty provision to be enforced by obtaining an order for a person to pay a pecuniary penalty for the contravention of the provision.

Authorised applicant

(2) For the purposes of Part 4 of the Regulatory Powers Act, the Director-General of ASD is an authorised applicant in relation to the civil penalty provisions of this Act.

(3) An authorised applicant may, in writing, delegate the authorised applicant's powers and functions under Part 4 of the Regulatory Powers Act in relation to the civil penalty provisions of this Act to an SES employee, or acting SES employee, in the Australian Cyber Security Centre.

Relevant court

(4) For the purposes of Part 4 of the Regulatory Powers Act, each of the following courts is a relevant court in relation to the civil penalty provisions of this Act:

(a) the Federal Court;

(b) the Federal Circuit Court.

11 Treatment of partnerships

(1) This Act (other than section 9) applies to a partnership as if it were a person, but with the changes set out in this section.

(2) An obligation that would otherwise be imposed on the partnership by this Act is imposed on each partner instead, but may be discharged by any of the partners.

(3) A contravention of a civil penalty provision of this Act that would otherwise be committed by the partnership is taken to have been committed by each partner.

(4) A partner does not contravene a civil penalty provision because of subsection (3) if the partner:

(a) does not know of the circumstances that constitute the contravention of the provision concerned; or

(b) knows of those circumstances but takes all reasonable steps to correct the contravention as soon as possible after the partner becomes aware of those circumstances.

12 Delegation

The Director-General of ASD may, in writing, delegate all or any of his or her functions or powers under this Act to an SES employee, or acting SES employee, in the Australian Cyber Security Centre.

Note: Sections 34AA to 34A of the *Acts Interpretation Act 1901* contain provisions relating to delegations.