Our reference: s47E(d)/s47G

Thank you for your statement notifying the Information Commissioner of a data breach.

If you have not done so already, please provide a copy of the notification that you have sent to affected individuals to databreaches@oaic.gov.au. This will assist our staff when assessing your notification.

If we require any further information, we will be in contact. If we receive a complaint from individuals affected by the incident, we will deal with that complaint on its merits.

Further resources

Entities covered by the *Privacy Act 1988* (Cth) have obligations under Australian Privacy Principle (APP) 11 to take reasonable steps to protect the personal information they hold from misuse, interference and loss, and unauthorised access, modification or disclosure. APP 6 also limits the circumstances in which an APP entity is permitted to disclose the personal information it holds. Please visit our website for more information on the APPs.

The OAIC's *Guide to securing personal information* contains information about reasonable steps APP entities should consider taking to protect the personal information as required by APP 11 of the Privacy Act.

You may also find the OAIC's *Data breach preparation and response: a guide to managing data breaches in accordance with the Privacy Act 1988 (Cth)* useful in preparing for and responding to future data breaches.

If the breach you have reported is a cyber-security incident, you could also report it to the Australian Cyber Security Centre (ACSC). The ACSC can provide advice to organisations that have experienced a data breach, and reports to the ACSC help build the Australian Government's understanding of the cyber threat environment.

Yours sincerely

Office of the Australian Information Commissioner

6 December 2023

Our reference: s47E(d)/s47G

Thank you for your statement notifying the Information Commissioner of a data breach.

If you have not done so already, please provide a copy of the notification that you have sent to affected individuals to databreaches@oaic.gov.au. This will assist our staff when assessing your notification.

If we require any further information, we will be in contact. If we receive a complaint from individuals affected by the incident, we will deal with that complaint on its merits.

Further resources

Entities covered by the *Privacy Act 1988* (Cth) have obligations under Australian Privacy Principle (APP) 11 to take reasonable steps to protect the personal information they hold from misuse, interference and loss, and unauthorised access, modification or disclosure. APP 6 also limits the circumstances in which an APP entity is permitted to disclose the personal information it holds. Please visit our website for more information on the APPs.

The OAIC's *Guide to securing personal information* contains information about reasonable steps APP entities should consider taking to protect the personal information as required by APP 11 of the Privacy Act.

You may also find the OAIC's *Data breach preparation and response: a guide to managing data breaches in accordance with the Privacy Act 1988 (Cth)* useful in preparing for and responding to future data breaches.

If the breach you have reported is a cyber-security incident, you could also report it to the Australian Cyber Security Centre (ACSC). The ACSC can provide advice to organisations that have experienced a data breach, and reports to the ACSC help build the Australian Government's understanding of the cyber threat environment.

Yours sincerely

Office of the Australian Information Commissioner

17 October 2023

Our reference: s47E(d)/s47G

Thank you for your statement notifying the Information Commissioner of a data breach.

If you have not done so already, please provide a copy of the notification that you have sent to affected individuals to databreaches@oaic.gov.au. This will assist our staff when assessing your notification.

If we require any further information, we will be in contact. If we receive a complaint from individuals affected by the incident, we will deal with that complaint on its merits.

Further resources

Entities covered by the *Privacy Act 1988* (Cth) have obligations under Australian Privacy Principle (APP) 11 to take reasonable steps to protect the personal information they hold from misuse, interference and loss, and unauthorised access, modification or disclosure. APP 6 also limits the circumstances in which an APP entity is permitted to disclose the personal information it holds. Please visit our website for more information on the APPs.

The OAIC's *Guide to securing personal information* contains information about reasonable steps APP entities should consider taking to protect the personal information as required by APP 11 of the Privacy Act.

You may also find the OAIC's *Data breach preparation and response: a guide to managing data breaches in accordance with the Privacy Act 1988 (Cth)* useful in preparing for and responding to future data breaches.

If the breach you have reported is a cyber-security incident, you could also report it to the Australian Cyber Security Centre (ACSC). The ACSC can provide advice to organisations that have experienced a data breach, and reports to the ACSC help build the Australian Government's understanding of the cyber threat environment.

Yours sincerely

Office of the Australian Information Commissioner

13 October 2023

Our reference: s47E(d)/s47G

Thank you for your statement notifying the Information Commissioner of a data breach.

If you have not done so already, please provide a copy of the notification that you have sent to affected individuals to databreaches@oaic.gov.au. This will assist our staff when assessing your notification.

If we require any further information, we will be in contact. If we receive a complaint from individuals affected by the incident, we will deal with that complaint on its merits.

Further resources

Entities covered by the *Privacy Act 1988* (Cth) have obligations under Australian Privacy Principle (APP) 11 to take reasonable steps to protect the personal information they hold from misuse, interference and loss, and unauthorised access, modification or disclosure. APP 6 also limits the circumstances in which an APP entity is permitted to disclose the personal information it holds. Please visit our website for more information on the APPs.

The OAIC's *Guide to securing personal information* contains information about reasonable steps APP entities should consider taking to protect the personal information as required by APP 11 of the Privacy Act.

You may also find the OAIC's *Data breach preparation and response: a guide to managing data breaches in accordance with the Privacy Act 1988 (Cth)* useful in preparing for and responding to future data breaches.

If the breach you have reported is a cyber-security incident, you could also report it to the Australian Cyber Security Centre (ACSC). The ACSC can provide advice to organisations that have experienced a data breach, and reports to the ACSC help build the Australian Government's understanding of the cyber threat environment.

Yours sincerely

Office of the Australian Information Commissioner

12 October 2023

Our reference: s47E(d)/s47G

Thank you for your statement notifying the Information Commissioner of a data breach.

If you have not done so already, please provide a copy of the notification that you have sent to affected individuals to databreaches@oaic.gov.au. This will assist our staff when assessing your notification.

If we require any further information, we will be in contact. If we receive a complaint from individuals affected by the incident, we will deal with that complaint on its merits.

Further resources

Entities covered by the *Privacy Act 1988* (Cth) have obligations under Australian Privacy Principle (APP) 11 to take reasonable steps to protect the personal information they hold from misuse, interference and loss, and unauthorised access, modification or disclosure. APP 6 also limits the circumstances in which an APP entity is permitted to disclose the personal information it holds. Please visit our website for more information on the APPs.

The OAIC's *Guide to securing personal information* contains information about reasonable steps APP entities should consider taking to protect the personal information as required by APP 11 of the Privacy Act.

You may also find the OAIC's *Data breach preparation and response: a guide to managing data breaches in accordance with the Privacy Act 1988 (Cth)* useful in preparing for and responding to future data breaches.

If the breach you have reported is a cyber-security incident, you could also report it to the Australian Cyber Security Centre (ACSC). The ACSC can provide advice to organisations that have experienced a data breach, and reports to the ACSC help build the Australian Government's understanding of the cyber threat environment.

Yours sincerely

Office of the Australian Information Commissioner

9 October 2023

Our reference: s47E(d)/s47G

Thank you for your statement notifying the Information Commissioner of a data breach.

If you have not done so already, please provide a copy of the notification that you have sent to affected individuals to databreaches@oaic.gov.au. This will assist our staff when assessing your notification.

If we require any further information, we will be in contact. If we receive a complaint from individuals affected by the incident, we will deal with that complaint on its merits.

Further resources

Entities covered by the *Privacy Act 1988* (Cth) have obligations under Australian Privacy Principle (APP) 11 to take reasonable steps to protect the personal information they hold from misuse, interference and loss, and unauthorised access, modification or disclosure. APP 6 also limits the circumstances in which an APP entity is permitted to disclose the personal information it holds. Please visit our website for more information on the APPs.

The OAIC's *Guide to securing personal information* contains information about reasonable steps APP entities should consider taking to protect the personal information as required by APP 11 of the Privacy Act.

You may also find the OAIC's *Data breach preparation and response: a guide to managing data breaches in accordance with the Privacy Act 1988 (Cth)* useful in preparing for and responding to future data breaches.

If the breach you have reported is a cyber-security incident, you could also report it to the Australian Cyber Security Centre (ACSC). The ACSC can provide advice to organisations that have experienced a data breach, and reports to the ACSC help build the Australian Government's understanding of the cyber threat environment.

Yours sincerely

Office of the Australian Information Commissioner

5 October 2023

Our reference: s47E(d)/s47G

Thank you for your statement notifying the Information Commissioner of a data breach.

If you have not done so already, please provide a copy of the notification that you have sent to affected individuals to databreaches@oaic.gov.au. This will assist our staff when assessing your notification.

If we require any further information, we will be in contact. If we receive a complaint from individuals affected by the incident, we will deal with that complaint on its merits.

Further resources

Entities covered by the *Privacy Act 1988* (Cth) have obligations under Australian Privacy Principle (APP) 11 to take reasonable steps to protect the personal information they hold from misuse, interference and loss, and unauthorised access, modification or disclosure. APP 6 also limits the circumstances in which an APP entity is permitted to disclose the personal information it holds. Please visit our website for more information on the APPs.

The OAIC's *Guide to securing personal information* contains information about reasonable steps APP entities should consider taking to protect the personal information as required by APP 11 of the Privacy Act.

You may also find the OAIC's *Data breach preparation and response: a guide to managing data breaches in accordance with the Privacy Act 1988 (Cth)* useful in preparing for and responding to future data breaches.

If the breach you have reported is a cyber-security incident, you could also report it to the Australian Cyber Security Centre (ACSC). The ACSC can provide advice to organisations that have experienced a data breach, and reports to the ACSC help build the Australian Government's understanding of the cyber threat environment.

Yours sincerely

Office of the Australian Information Commissioner

3 October 2023

Our reference: s47E(d)/s47G

Thank you for your statement notifying the Information Commissioner of a data breach.

If you have not done so already, please provide a copy of the notification that you have sent to affected individuals to databreaches@oaic.gov.au. This will assist our staff when assessing your notification.

If we require any further information, we will be in contact. If we receive a complaint from individuals affected by the incident, we will deal with that complaint on its merits.

Further resources

Entities covered by the *Privacy Act 1988* (Cth) have obligations under Australian Privacy Principle (APP) 11 to take reasonable steps to protect the personal information they hold from misuse, interference and loss, and unauthorised access, modification or disclosure. APP 6 also limits the circumstances in which an APP entity is permitted to disclose the personal information it holds. Please visit our website for more information on the APPs.

The OAIC's *Guide to securing personal information* contains information about reasonable steps APP entities should consider taking to protect the personal information as required by APP 11 of the Privacy Act.

You may also find the OAIC's *Data breach preparation and response: a guide to managing data breaches in accordance with the Privacy Act 1988 (Cth)* useful in preparing for and responding to future data breaches.

If the breach you have reported is a cyber-security incident, you could also report it to the Australian Cyber Security Centre (ACSC). The ACSC can provide advice to organisations that have experienced a data breach, and reports to the ACSC help build the Australian Government's understanding of the cyber threat environment.

Yours sincerely

Office of the Australian Information Commissioner

1 October 2023

s 47E(d)/s 47G	Respondent Sector	s 47E(d)/s 47G	Source of Breach	Source of Breach Level 2	Source of Breach Level 3	DBN NDB Global number of people affec
	Health service providers		Human error	PI sent to wrong recipient (email)		1
	Retail		Malicious or criminal attack	Cyber incident	Malware	1001 - 5 000
	QLD Government		Malicious or criminal attack	Cyber incident	Phishing (compromised credentials)	1
	Health service providers		Human error	PI sent to wrong recipient (email)		1
	Mining & Manufacturing		Malicious or criminal attack	Cyber incident	Ransomware	25001 - 50000
	Finance (incl. superannuation)		Human error	PI sent to wrong recipient (email)		2 - 10
	Education		Human error	Unauthorised disclosure (failure to redact)		2 - 10
	Health service providers		Malicious or criminal attack	Cyber incident	Ransomware	10001 - 25000
	Insurance		Human error	Unauthorised disclosure (verbal)		1
	Health service providers		Human error	Loss of paperwork / data storage device		1001 - 5 000
	Personal services (incl employment, child car		Malicious or criminal attack	Rogue employee / insider threat		11 - 100
	Health service providers		Human error	PI sent to wrong recipient (email)		1
	Travel & Hospitality industry		Malicious or criminal attack	Rogue employee / insider threat		1
	Insurance		Human error	Unauthorised disclosure (unintended release or public		1
	Finance (incl. superannuation)		Human error	Unauthorised disclosure (unintended release or public		1
	Education		Human error	Loss of paperwork / data storage device		11 - 100
	Health service providers		Malicious or criminal attack	Cyber incident	Ransomware	1 000 001 - 10 000 000
	Australian Government		Malicious or criminal attack	Social engineering / impersonation		11 - 100
	Health service providers		System fault	Unintended access		1
	Insurance		Human error	Unauthorised disclosure (unintended release or public		1
	Retail		Malicious or criminal attack	Cyber incident	Phishing (compromised credentials)	11 - 100
	Health service providers		Human error	Unauthorised disclosure (unintended release or public		11 - 100
	Health service providers		Human error	Unauthorised disclosure (verbal)		1
	Education		Human error	Unauthorised disclosure (unintended release or public		1
	Australian Government		Human error	Unauthorised disclosure (unintended release or public		1
	Property/construction/Architects/surveyors		Malicious or criminal attack	Rogue employee / insider threat		2 - 10
	Finance (incl. superannuation)		Malicious or criminal attack	Social engineering / impersonation		1
	Religious organisations		Malicious or criminal attack	Theft of paperwork or data storage device		11 - 100
	Mining & Manufacturing		Malicious or criminal attack	Theft of paperwork or data storage device		2 - 10
	Legal, accounting & management services		Malicious or criminal attack	Cyber incident	Phishing (compromised credentials)	11 - 100
	Insurance		Malicious or criminal attack	Social engineering / impersonation		2 - 10
	Retail		Malicious or criminal attack	Cyber incident	Hacking	5 0001 - 10 0000
	Education		Human error	Unauthorised disclosure (unintended release or public		11 - 100
	Mining & Manufacturing		Malicious or criminal attack	Cyber incident	Phishing (compromised credentials)	11 - 100
	Education		Malicious or criminal attack	Cyber incident	Hacking	500 001 - 1 000 000
	Retail		Malicious or criminal attack	Rogue employee / insider threat		11 - 100
	Health service providers		Human error	Unauthorised disclosure (verbal)		1
	Australian Government		Human error	PI sent to wrong recipient (mail)		2 - 10
	Travel & Hospitality industry		Malicious or criminal attack	Cyber incident	Phishing (compromised credentials)	11 - 100
	Health service providers		Malicious or criminal attack	Social engineering / impersonation		1
	Finance (incl. superannuation)		Malicious or criminal attack	Rogue employee / insider threat		2 - 10
	Property/construction/Architects/surveyors		Malicious or criminal attack	Cyber incident	Phishing (compromised credentials)	11 - 100
	Finance (incl. superannuation)		Malicious or criminal attack	Cyber incident	Phishing (compromised credentials)	2 - 10
	Health service providers		Human error	PI sent to wrong recipient (mail)		1
	Retail		Malicious or criminal attack	Cyber incident	Ransomware	2 - 10
	Information Technology		Malicious or criminal attack	Cyber incident	Ransomware	100 001 - 250 000
	Retail		Human error	Unauthorised disclosure (verbal)		1
	Personal services (incl employment, child car		Human error	PI sent to wrong recipient (email)		1
	Australian Government		Human error	PI sent to wrong recipient (email)		1
	Australian Government		Human error	PI sent to wrong recipient (mail)		1
	Recruitment Agencies		Malicious or criminal attack	Social engineering / impersonation		11 - 100
	Information Technology		Malicious or criminal attack	Cyber incident	Compromised or stolen credentials (method unk	11 - 100
	Recruitment Agencies		Malicious or criminal attack	Social engineering / impersonation		11 - 100
	Finance (incl. superannuation)		Malicious or criminal attack	Social engineering / impersonation		1
	Charities		Malicious or criminal attack	Theft of paperwork or data storage device		11 - 100
	Travel & Hospitality industry		System fault	Unintended access		2 - 10
	Insurance		System fault	Unintended release or publication		1
	Insurance		Human error	Unauthorised disclosure (unintended release or public		1
	Insurance		Human error	Unauthorised disclosure (verbal)		1
	Health service providers		Human error	Loss of paperwork / data storage device		2 - 10
	VIC Government		Malicious or criminal attack	Cyber incident	Hacking	5001 - 10000
	Retail		Malicious or criminal attack	Cyber incident	Ransomware	5001 - 10000
	Retail		Malicious or criminal attack	Cyber incident	Malware	2 - 10
	Retail		Malicious or criminal attack	Cyber incident	Ransomware	101 - 1000
	Mining & Manufacturing		Malicious or criminal attack	Cyber incident	Ransomware	101 - 1000
	Legal, accounting & management services		Malicious or criminal attack	Cyber incident	Phishing (compromised credentials)	101 - 1000
	Legal, accounting & management services		Malicious or criminal attack	Cyber incident	Compromised or stolen credentials (method unk	1
	Finance (incl. superannuation)		Malicious or criminal attack	Cyber incident	Phishing (compromised credentials)	11 - 100
	Charities		Malicious or criminal attack	Cyber incident	Compromised or stolen credentials (method unk	Unknown
	Business/Professional Associations		Malicious or criminal attack	Cyber incident	Hacking	11 - 100
	Insurance		Malicious or criminal attack	Cyber incident	Compromised or stolen credentials (method unk	1
	Insurance		Malicious or criminal attack	Cyber incident	Compromised or stolen credentials (method unk	1
	Insurance		Malicious or criminal attack	Cyber incident	Compromised or stolen credentials (method unk	1
	Insurance		Malicious or criminal attack	Cyber incident	Compromised or stolen credentials (method unk	1
	Insurance		Malicious or criminal attack	Cyber incident	Compromised or stolen credentials (method unk	1
	Insurance		Malicious or criminal attack	Cyber incident	Compromised or stolen credentials (method unk	1
	Health service providers		Malicious or criminal attack	Social engineering / impersonation		1
	Health service providers		Human error	PI sent to wrong recipient (mail)		1
	Australian Government		Human error	Unauthorised disclosure (verbal)		1
	Retail		Malicious or criminal attack	Cyber incident	Ransomware	1001 - 5 000
	Recruitment Agencies		Malicious or criminal attack	Social engineering / impersonation		101 - 1000
	Postal & courier		Malicious or criminal attack	Cyber incident	Compromised or stolen credentials (method unk	1
	Personal services (incl employment, child car		Malicious or criminal attack	Cyber incident	Compromised or stolen credentials (method unk	101 - 1000
	Legal, accounting & management services		Malicious or criminal attack	Cyber incident	Phishing (compromised credentials)	101 - 1000
	Health service providers		Malicious or criminal attack	Theft of paperwork or data storage device		11 - 100
	Finance (incl. superannuation)		Malicious or criminal attack	Social engineering / impersonation		1
	Australian Government		Malicious or criminal attack	Social engineering / impersonation		11 - 100
	Unions		Malicious or criminal attack	Cyber incident	Hacking	1001 - 5 000
	Personal services (incl employment, child car		Human error	PI sent to wrong recipient (mail)		1
	Insurance		Human error	Unauthorised disclosure (failure to redact)		1
	Finance (incl. superannuation)		Human error	PI sent to wrong recipient (email)		1
	Utilities		Malicious or criminal attack	Cyber incident	Phishing (compromised credentials)	101 - 1000
	Travel & Hospitality industry		Malicious or criminal attack	Cyber incident	Compromised or stolen credentials (method unk	1001 - 5 000
	Insurance		Malicious or criminal attack	Social engineering / impersonation		1
	Finance (incl. superannuation)		Malicious or criminal attack	Theft of paperwork or data storage device		2 - 10

s 47E(d)/s 47G	Australian Government	s 47E(d)/s 47G	Malicious or criminal attack	Social engineering / impersonation		2 - 10
	Health service providers		Human error	Failure to use BCC when sending email		101 - 1000
	Mining & Manufacturing		Malicious or criminal attack	Cyber incident	Malware	101 - 1000
	Finance (incl. superannuation)		Malicious or criminal attack	Social engineering / impersonation		1
	Australian Government		Malicious or criminal attack	Rogue employee / insider threat		1
	Insurance		System fault	Unintended release or publication		11 - 100
	Health service providers		Human error	Unauthorised disclosure (failure to redact)		2 - 10
	Finance (incl. superannuation)		Human error	PI sent to wrong recipient (email)		1
	Australian Government		Human error	Unauthorised disclosure (failure to redact)		1
	Marketing and market research		Malicious or criminal attack	Cyber incident	Ransomware	1001 - 5 000
	Legal, accounting & management services		Malicious or criminal attack	Cyber incident	Malware	2 - 10
	Information Technology		Malicious or criminal attack	Cyber incident	Ransomware	101 - 1000
	Health service providers		Human error	Failure to use BCC when sending email		101 - 1000
	Utilities		Malicious or criminal attack	Social engineering / impersonation		11 - 100
	Health service providers		Malicious or criminal attack	Cyber incident	Phishing (compromised credentials)	5001 - 10000
	Retail		Human error	Failure to use BCC when sending email		101 - 1000
	Insurance		Human error	PI sent to wrong recipient (email)		1
	Health service providers		Human error	PI sent to wrong recipient (email)		101 - 1000
	Retail		Malicious or criminal attack	Cyber incident	Ransomware	101 - 1000
	Education		Human error	Unauthorised disclosure (unintended release or public		1001 - 5 000
	Australian Government		Human error	Loss of paperwork / data storage device		1
	Retail		Malicious or criminal attack	Social engineering / impersonation		1001 - 5 000
	Property/construction/Architects/surveyors		Malicious or criminal attack	Cyber incident	Ransomware	101 - 1000
	Personal services (incl employment, child car		Malicious or criminal attack	Rogue employee / insider threat		11 - 100
	Mining & Manufacturing		Malicious or criminal attack	Cyber incident	Compromised or stolen credentials (method unk	101 - 1000
	Health service providers		System fault	Unintended access		11 - 100
	Australian Government		Malicious or criminal attack	Social engineering / impersonation		101 - 1000
	Business/Professional Associations		Human error	PI sent to wrong recipient (email)		11 - 100
	Online services		Malicious or criminal attack	Cyber incident	Phishing (compromised credentials)	5 0001 - 10 0000
	Health service providers		Malicious or criminal attack	Cyber incident	Phishing (compromised credentials)	11 - 100
	Insurance		Human error	Unauthorised disclosure (verbal)		1
	Education		Human error	Unauthorised disclosure (unintended release or public		11 - 100
	Retail		Malicious or criminal attack	Cyber incident	Ransomware	5 0001 - 10 0000
	Legal, accounting & management services		Malicious or criminal attack	Cyber incident	Phishing (compromised credentials)	101 - 1000
	Personal services (incl employment, child car		Human error	Failure to use BCC when sending email		11 - 100
	Australian Government		Human error	PI sent to wrong recipient (mail)		1
	SA Government		Malicious or criminal attack	Cyber incident	Compromised or stolen credentials (method unk	2 - 10
	Retail		Malicious or criminal attack	Cyber incident	Compromised or stolen credentials (method unk	5001 - 10000
	Insurance		Malicious or criminal attack	Social engineering / impersonation		2 - 10
	Health service providers		Malicious or criminal attack	Cyber incident	Compromised or stolen credentials (method unk	101 - 1000
	Finance (incl. superannuation)		Malicious or criminal attack	Cyber incident	Compromised or stolen credentials (method unk	1
	Australian Government		Malicious or criminal attack	Rogue employee / insider threat		25001 - 50000
	Australian Government		Human error	Unauthorised disclosure (unintended release or public		1
	Travel & Hospitality industry		Malicious or criminal attack	Theft of paperwork or data storage device		11 - 100
	Legal, accounting & management services		Malicious or criminal attack	Theft of paperwork or data storage device		11 - 100
	Insurance		Malicious or criminal attack	Cyber incident	Compromised or stolen credentials (method unk	1
	Personal services (incl employment, child car		Malicious or criminal attack	Cyber incident	Hacking	1001 - 5 000
	Health service providers		Malicious or criminal attack	Cyber incident	Compromised or stolen credentials (method unk	1001 - 5 000
	Education		Human error	PI sent to wrong recipient (other)		1
	Property/construction/Architects/surveyors		Malicious or criminal attack	Cyber incident	Phishing (compromised credentials)	11 - 100
	Legal, accounting & management services		Malicious or criminal attack	Theft of paperwork or data storage device		101 - 1000
	Health service providers		Malicious or criminal attack	Cyber incident	Phishing (compromised credentials)	101 - 1000
	Australian Government		Malicious or criminal attack	Social engineering / impersonation		101 - 1000
	Finance (incl. superannuation)		Human error	PI sent to wrong recipient (mail)		1
	Insurance		Malicious or criminal attack	Cyber incident	Ransomware	11 - 100
	Finance (incl. superannuation)		Malicious or criminal attack	Cyber incident	Compromised or stolen credentials (method unk	2 - 10
	Health service providers		Human error	PI sent to wrong recipient (email)		1
	Utilities		Malicious or criminal attack	Cyber incident	Brute-force attack (compromised credentials)	11 - 100
	Finance (incl. superannuation)		Malicious or criminal attack	Rogue employee / insider threat		2 - 10
	Travel & Hospitality industry		Malicious or criminal attack	Cyber incident	Phishing (compromised credentials)	101 - 1000
	Health service providers		Malicious or criminal attack	Theft of paperwork or data storage device		101 - 1000
	Finance (incl. superannuation)		Malicious or criminal attack	Cyber incident	Ransomware	101 - 1000
	Political / Lobby & Clubs / Interest Groups		Human error	Unauthorised disclosure (unintended release or public		101 - 1000
	Insurance		Human error	PI sent to wrong recipient (email)		1
	Finance (incl. superannuation)		Human error	PI sent to wrong recipient (email)		1
	Agriculture, Forestry, Fisheries		Human error	Failure to use BCC when sending email		11 - 100
	Retail		Malicious or criminal attack	Cyber incident	Compromised or stolen credentials (method unk	1
	Health service providers		Malicious or criminal attack	Cyber incident	Ransomware	1001 - 5 000
	Health service providers		Human error	PI sent to wrong recipient (mail)		1
	Recruitment Agencies		Malicious or criminal attack	Social engineering / impersonation		11 - 100
	Health service providers		Malicious or criminal attack	Cyber incident	Phishing (compromised credentials)	11 - 100
	Health service providers		Malicious or criminal attack	Rogue employee / insider threat		1
	Finance (incl. superannuation)		Human error	Unauthorised disclosure (unintended release or public		101 - 1000
	Travel & Hospitality industry		Malicious or criminal attack	Rogue employee / insider threat		1
	Health service providers		Malicious or criminal attack	Social engineering / impersonation		101 - 1000
	Finance (incl. superannuation)		System fault	Unintended release or publication		101 - 1000
	Transport		Malicious or criminal attack	Cyber incident	Hacking	101 - 1000
	Legal, accounting & management services		Malicious or criminal attack	Cyber incident	Malware	11 - 100
	Insurance		Malicious or criminal attack	Social engineering / impersonation		2 - 10
	Health service providers		Malicious or criminal attack	Social engineering / impersonation		11 - 100
	Charities		Malicious or criminal attack	Rogue employee / insider threat		1
	Health service providers		Human error	PI sent to wrong recipient (email)		101 - 1000
	Mining & Manufacturing		Malicious or criminal attack	Cyber incident	Ransomware	1001 - 5 000
	Legal, accounting & management services		Malicious or criminal attack	Cyber incident	Phishing (compromised credentials)	1001 - 5 000
	Interest groups/theatre/sports		Malicious or criminal attack	Rogue employee / insider threat		101 - 1000
	Insurance		Human error	PI sent to wrong recipient (mail)		2 - 10
	Real estate agents		Malicious or criminal attack	Cyber incident	Phishing (compromised credentials)	11 - 100
	Insurance		Malicious or criminal attack	Social engineering / impersonation		1
	Finance (incl. superannuation)		Human error	Insecure disposal		2 - 10
	Australian Government		Human error	Unauthorised disclosure (verbal)		1
	Health service providers		Malicious or criminal attack	Rogue employee / insider threat		1
	Property/construction/Architects/surveyors		Malicious or criminal attack	Cyber incident	Ransomware	101 - 1000
	Property/construction/Architects/surveyors		Malicious or criminal attack	Cyber incident	Ransomware	11 - 100
	Health service providers		Malicious or criminal attack	Theft of paperwork or data storage device		2 - 10
	Transport		Malicious or criminal attack	Cyber incident	Compromised or stolen credentials (method unk	25001 - 50000
	Recruitment Agencies		Malicious or criminal attack	Social engineering / impersonation		2 - 10

s 47E(d)/s 47G	Mining & Manufacturing	s 47E(d)/s 47G	Malicious or criminal attack	Cyber incident	Ransomware	101 - 1000
	Mining & Manufacturing		Malicious or criminal attack	Cyber incident	Phishing (compromised credentials)	2 - 10
	Charities		Malicious or criminal attack	Rogue employee / insider threat		1
	Agriculture, Forestry, Fisheries		Malicious or criminal attack	Cyber incident	Compromised or stolen credentials (method unk	11 - 100
	Health service providers		Malicious or criminal attack	Rogue employee / insider threat		2 - 10
	Australian Government		Malicious or criminal attack	Social engineering / impersonation		101 - 1000
	Insurance		System fault	Unintended release or publication		1
	Australian Government		Human error	PI sent to wrong recipient (email)		1
	Travel & Hospitality industry		Malicious or criminal attack	Rogue employee / insider threat		1
	Finance (incl. superannuation)		System fault	Unintended release or publication		11 - 100
	Legal, accounting & management services		Malicious or criminal attack	Cyber incident	Compromised or stolen credentials (method unk	11 - 100
	Health service providers		Malicious or criminal attack	Cyber incident	Compromised or stolen credentials (method unk	101 - 1000
	Health service providers		Malicious or criminal attack	Cyber incident	Phishing (compromised credentials)	101 - 1000
	Finance (incl. superannuation)		Malicious or criminal attack	Cyber incident	Brute-force attack (compromised credentials)	11 - 100
	Recruitment Agencies		Malicious or criminal attack	Social engineering / impersonation		2 - 10
	Personal services (incl employment, child care		Malicious or criminal attack	Rogue employee / insider threat		11 - 100
	Mining & Manufacturing		Malicious or criminal attack	Cyber incident	Hacking	101 - 1000
	Health service providers		Malicious or criminal attack	Cyber incident	Phishing (compromised credentials)	2 - 10
	Finance (incl. superannuation)		Malicious or criminal attack	Cyber incident	Ransomware	25001 - 50000
	Australian Government		Human error	Unauthorised disclosure (failure to redact)		1
	Australian Government		Human error	PI sent to wrong recipient (email)		11 - 100
	Australian Government		Human error	PI sent to wrong recipient (email)		2 - 10
	Mining & Manufacturing		Malicious or criminal attack	Cyber incident	Ransomware	1001 - 5 000
	Australian Government		Malicious or criminal attack	Theft of paperwork or data storage device		2 - 10
	Travel & Hospitality industry		Human error	Unauthorised disclosure (unintended release or public		101 - 1000
	Health service providers		Human error	Loss of paperwork / data storage device		1
	Telecommunications		Malicious or criminal attack	Cyber incident	Compromised or stolen credentials (method unk	1001 - 5 000
	Health service providers		Malicious or criminal attack	Cyber incident	Ransomware	11 - 100
	Retail		Malicious or criminal attack	Cyber incident	Hacking	5001 - 10000
	Retail		Malicious or criminal attack	Cyber incident	Malware	101 - 1000
	Mining & Manufacturing		Malicious or criminal attack	Cyber incident	Phishing (compromised credentials)	1001 - 5 000
	Utilities		Human error	Unauthorised disclosure (failure to redact)		11 - 100
	Personal services (incl employment, child care		Human error	PI sent to wrong recipient (mail)		2 - 10
	Finance (incl. superannuation)		Human error	PI sent to wrong recipient (email)		1
	Travel & Hospitality industry		Malicious or criminal attack	Cyber incident	Phishing (compromised credentials)	101 - 1000
	Religious organisations		Malicious or criminal attack	Social engineering / impersonation		101 - 1000
	Mining & Manufacturing		Malicious or criminal attack	Cyber incident	Phishing (compromised credentials)	101 - 1000
	Insurance		Malicious or criminal attack	Cyber incident	Compromised or stolen credentials (method unk	1
	Insurance		Malicious or criminal attack	Cyber incident	Compromised or stolen credentials (method unk	1
	Health service providers		Malicious or criminal attack	Cyber incident	Phishing (compromised credentials)	10001 - 25000
	Health service providers		Malicious or criminal attack	Cyber incident	Phishing (compromised credentials)	11 - 100
	Finance (incl. superannuation)		Malicious or criminal attack	Cyber incident	Phishing (compromised credentials)	1
	Education		Malicious or criminal attack	Cyber incident	Malware	2 - 10
	Religious organisations		Human error	PI sent to wrong recipient (email)		1
	Insurance		Human error	Unauthorised disclosure (unintended release or public		1
	Health service providers		Human error	PI sent to wrong recipient (other)		1
	Health service providers		Human error	PI sent to wrong recipient (email)		2 - 10
	Health service providers		Human error	Failure to use BCC when sending email		11 - 100
	Australian Government		Human error	Unauthorised disclosure (unintended release or public		1
	Retail		Malicious or criminal attack	Cyber incident	Ransomware	1001 - 5 000
	Legal, accounting & management services		Malicious or criminal attack	Rogue employee / insider threat		5001 - 10000
	Insurance		Malicious or criminal attack	Social engineering / impersonation		2 - 10
	Education		Malicious or criminal attack	Social engineering / impersonation		11 - 100
	Education		Human error	PI sent to wrong recipient (email)		1
	Australian Government		Human error	PI sent to wrong recipient (other)		1
	Retail		Malicious or criminal attack	Cyber incident	Compromised or stolen credentials (method unk	1 000 001 - 10 000 000
	Property/construction/Architects/surveyors		Malicious or criminal attack	Cyber incident	Ransomware	11 - 100
	Health service providers		Malicious or criminal attack	Cyber incident	Phishing (compromised credentials)	11 - 100
	Insurance		Human error	PI sent to wrong recipient (mail)		25001 - 50000
	Finance (incl. superannuation)		Human error	PI sent to wrong recipient (other)		1
	Retail		Malicious or criminal attack	Theft of paperwork or data storage device		11 - 100
	Postal & courier		Malicious or criminal attack	Cyber incident	Ransomware	10001 - 25000
	Personal services (incl employment, child care		Malicious or criminal attack	Cyber incident	Phishing (compromised credentials)	2 - 10
	Mining & Manufacturing		Malicious or criminal attack	Cyber incident	Ransomware	101 - 1000
	Interest groups/theatre/sports		Malicious or criminal attack	Cyber incident	Brute-force attack (compromised credentials)	2 - 10
	Insurance		Malicious or criminal attack	Cyber incident	Compromised or stolen credentials (method unk	1
	Health service providers		Malicious or criminal attack	Theft of paperwork or data storage device		101 - 1000
	Education		Malicious or criminal attack	Rogue employee / insider threat		101 - 1000
	Health service providers		Human error	Unauthorised disclosure (unintended release or public		1
	Property/construction/Architects/surveyors		Malicious or criminal attack	Cyber incident	Ransomware	11 - 100
	Legal, accounting & management services		Malicious or criminal attack	Cyber incident	Ransomware	11 - 100
	Interest groups/theatre/sports		Malicious or criminal attack	Cyber incident	Compromised or stolen credentials (method unk	1
	Insurance		Malicious or criminal attack	Cyber incident	Compromised or stolen credentials (method unk	1
	Finance (incl. superannuation)		Malicious or criminal attack	Social engineering / impersonation		1
	Property/construction/Architects/surveyors		Malicious or criminal attack	Cyber incident	Phishing (compromised credentials)	2 - 10
	Personal services (incl employment, child care		Malicious or criminal attack	Cyber incident	Brute-force attack (compromised credentials)	1 000 001 - 10 000 000
	Finance (incl. superannuation)		Malicious or criminal attack	Cyber incident	Ransomware	2 - 10
	Health service providers		Malicious or criminal attack	Cyber incident	Ransomware	1001 - 5 000
	Retail		Malicious or criminal attack	Cyber incident	Phishing (compromised credentials)	11 - 100
	Personal services (incl employment, child care		Malicious or criminal attack	Rogue employee / insider threat		2 - 10
	Personal services (incl employment, child care		Malicious or criminal attack	Cyber incident	Ransomware	1001 - 5 000
	Education		Malicious or criminal attack	Cyber incident	Brute-force attack (compromised credentials)	101 - 1000
	Personal services (incl employment, child care		Human error	PI sent to wrong recipient (email)		1
	Personal services (incl employment, child care		Malicious or criminal attack	Theft of paperwork or data storage device		11 - 100
	Health service providers		Malicious or criminal attack	Rogue employee / insider threat		1
	Mining & Manufacturing		Malicious or criminal attack	Cyber incident	Ransomware	2 - 10
	Insurance		Malicious or criminal attack	Cyber incident	Ransomware	11 - 100
	Insurance		Malicious or criminal attack	Cyber incident	Ransomware	11 - 100
	Health service providers		Malicious or criminal attack	Cyber incident	Compromised or stolen credentials (method unk	101 - 1000
	Finance (incl. superannuation)		Malicious or criminal attack	Cyber incident	Ransomware	11 - 100
	Finance (incl. superannuation)		Malicious or criminal attack	Cyber incident	Ransomware	2 - 10
	Charities		Malicious or criminal attack	Cyber incident	Ransomware	10001 - 25000
	Information Technology		Malicious or criminal attack	Cyber incident	Ransomware	11 - 100
	Finance (incl. superannuation)		Malicious or criminal attack	Cyber incident	Ransomware	11 - 100
	Health service providers		Malicious or criminal attack	Cyber incident	Ransomware	101 - 1000
	Mining & Manufacturing		Malicious or criminal attack	Cyber incident	Ransomware	2 - 10

s 47E(d)/s 47G	Insurance	s 47E(d)/s 47G	Malicious or criminal attack	Cyber incident	Ransomware	101 - 1000
	Finance (incl. superannuation)		Malicious or criminal attack	Cyber incident	Ransomware	11 - 100
	Australian Government		Malicious or criminal attack	Cyber incident	Ransomware	2 - 10
	Agriculture, Forestry, Fisheries		Malicious or criminal attack	Cyber incident	Ransomware	2 - 10
	Health service providers		Malicious or criminal attack	Cyber incident	Compromised or stolen credentials (method unk	1001 - 5 000
	Travel & Hospitality industry		Malicious or criminal attack	Cyber incident	Ransomware	1
	Insurance		Malicious or criminal attack	Cyber incident	Ransomware	11 - 100
	SA Government		Malicious or criminal attack	Cyber incident	Ransomware	101 - 1000
	Charities		Malicious or criminal attack	Cyber incident	Ransomware	1001 - 5 000
	Legal, accounting & management services		Malicious or criminal attack	Cyber incident	Ransomware	2 - 10
	Finance (incl. superannuation)		Malicious or criminal attack	Cyber incident	Ransomware	1
	Charities		Malicious or criminal attack	Cyber incident	Ransomware	25001 - 50000
	Transport		Malicious or criminal attack	Cyber incident	Ransomware	1
	Health service providers		Malicious or criminal attack	Cyber incident	Ransomware	5001 - 10000
	Travel & Hospitality industry		Malicious or criminal attack	Cyber incident	Ransomware	11 - 100
	Legal, accounting & management services		Malicious or criminal attack	Cyber incident	Ransomware	11 - 100
	Insurance		Malicious or criminal attack	Cyber incident	Ransomware	2 - 10
	Charities		Malicious or criminal attack	Cyber incident	Ransomware	5 0001 - 10 0000
	Health service providers		Malicious or criminal attack	Cyber incident	Hacking	2 - 10
	Health service providers		Malicious or criminal attack	Cyber incident	Ransomware	1001 - 5 000
	Business/Professional Associations		Malicious or criminal attack	Cyber incident	Ransomware	101 - 1000
	Mining & Manufacturing		Malicious or criminal attack	Cyber incident	Hacking	5001 - 10000
	WA Government		Malicious or criminal attack	Cyber incident	Ransomware	11 - 100
	Charities		Malicious or criminal attack	Cyber incident	Ransomware	101 - 1000
	Insurance		Malicious or criminal attack	Cyber incident	Ransomware	2 - 10
	Health service providers		Malicious or criminal attack	Cyber incident	Ransomware	2 - 10
	Information Technology		Malicious or criminal attack	Cyber incident	Ransomware	101 - 1000
	Health service providers		Malicious or criminal attack	Cyber incident	Compromised or stolen credentials (method unk	25001 - 50000
	Mining & Manufacturing		Malicious or criminal attack	Cyber incident	Hacking	5001 - 10000