Financial institutions
Energy
Infrastructure, mining and commodities
Transport
Technology and innovation
Life sciences and healthcare

NORTON ROSE FULBRIGHT

cdbp Complete Data Breach Protection

Complete data breach protection

Assisting insurers and their insureds manage data breaches and cyber incidents across Australia, the Asia Pacific region and globally.

An increasingly complex web of national and international laws govern the treatment of data in Australia and around the world. With its unmatched global network, Norton Rose Fulbright is ideally placed to advise on complex cyber incidents. We are strong across the key industry sectors: Financial Institutions; Energy; Infrastructure, Mining and Commodities; Transport; Technology and Innovation; and Life Sciences and Healthcare. We provide an end-to-end service offering which covers both the advisory and contentious stages of the data breach lifecycle including:

Protect

We have dedicated privacy, IT and IP lawyers who advise organisations on their data security and privacy obligations and potential cyber security risk exposures including:

- conducting digital risk audits – advising on the best way to collect, store and dispose of data
- incident response readiness – preparing organisations for data breach incidents includingdeveloping tailored incident response plans
- cross-border data flows – advising on cross-border data transfers
- IT vendor risks – advising on third party contractual arrangements including IT outsourcing, cloudcomputing and data analytics
- regulatory risks – advising on regulatory obligations, risks and penalties.

Respond

As ‘breach coach’ we work with you to provide a streamlined incident response service across a range of incident types, including data breach and network interruption.

We coordinate the entire response by assessing the size and nature of the incident, taking steps to contain it, coordinating our panel of carefully selected third party vendors, all the while managing stakeholders’ interests and mitigating potential loss.

Our early involvement and establishment of legal professional privilege protects you to the maximum extent possible as far as sensitive communications are concerned.

Recover

Following containment of an incident, we take steps to reduce potential harm and respond to any fallout.

We help you manage notification to affected parties, law enforcement and regulatory bodies; coordinate credit monitoring and ID protection services; and respond to any media coverage.

We can also act in defence of your organisation and its directors and officers in third party liability claims and regulatory or PCI investigations. Our end-to-end capabilities mean we are best placed to understand how the breach, investigation, response, remediation and notification aspects will impact on litigation. We also advise on recovery options.

Cyber Experience at a Glance

Some of our recent Australian experience includes:

US-based e-retail company – data breach notification	Advised a US-based e-retail company on its disclosure obligations after its Australian customer database was compromised. Managed and co-ordinated notifications to Australian and New Zealand customers, regulators and law enforcement bodies, and negotiated credit monitoring and ID protection services for impacted customers.
Australian e-retail company – incident response	Providing incident response services to an Australian e-retail company while it was suffering a live Distributed Denial of Services attack to its website, including managing the company's third party data storage provider which was providing IT response services. Advising the company on its recovery options, and on strengthening its contractual position with the data storage provider in order to better protect its interests in any future incidents.
Large superannuation company - data breach	Advising a large superannuation company regarding a data breach in respect of its customer portal, which allowed improper disclosure of personal information.
Data breach by employee - notification to regulator and police investigation	Advised a major Australian business following theft of data by an employee, including notification to the regulator and a police investigation.
Major department store - data breach notification and extortion	Advised a major department store about the unauthorised copying of customer records by a hacker, and the store's notification obligations. This event involved an extortion threat by a hacker who stole 3,000 customer records, and demand for ransom payment, and received widespread media coverage.
Leading data centre provider - data breach notification and extortion	Advised a leading data centre provider about a data breach after a hacker obtained personal information of the customers of its financial institution clients. Advised on notification obligations, potential risks including loss of reputation, as well as extortion response.
Large international footwear manufacturer – global data breach notification	Advising a large international footwear manufacturer in relation to its mandatory data breach disclosure obligations in Australia and, with our other offices, various Asian jurisdictions in response to a data breach incident, including assisting with the forensic investigation and notification obligations.
Hacktivist shutdown – liability advice	Advising on liability issues under an ISR policy, following a Distributed Denial of Services attack where a 'hacktivist' shut down our client's server mainframe, causing it significant business interruption losses.
Major Australian bank – regulatory obligations	Advising an Australian bank in respect of 2,100 customer records inadvertently emailed to the wrong financial advisers. Advice included advice on liability under the Privacy Act 1988 (Cth) and obligations to notify customers and the Australian Privacy Commissioner.

Major Australian bank - privacy notification	Advising a major Australian insurer on its incident response obligations and preparing a comprehensive data breach / IT incident response plan.
Major cloud provider – security breach	Assisting a provider of cloud data storage and processing services dealing with security breach discovered by a privacy activist and potential claims by affected customers.
One of Australia's largest web hosting companies - network interruption and extortion	Advised one of Australia's largest web hosting companies about its proposed response to an extortion threat made against it by a hacking group Armada Collective, and provided on-call assistance throughout the resulting Distributed Denial of Services attack.
Major public health charity - one of the largest data breaches in Australian history	We advised a major public health charity about the legal risks and issues arising from this significant data breach. We provided advice in respect of the management of IT service providers, forensic investigation of the data breach, responses to the Australian Privacy Commissioner and key regulatory risks. The handling of the matter required rapid and strategic responses in order to reduce public concern and to manage the risks in respect of potential privacy breaches.
Microsoft Google - personal information and regulatory advice	Advising Microsoft about the privacy implications associated with Google's collection of personal information through the Google Toolbar. Also advising Microsoft on technology and telecommunications regulatory issues arising from its proposed implementation of web and telephone based business services in Australia.
Accounting firm - ransomware	Providing data breach incident response services to an accounting firm following a crypto-locker attack and resulting ransom demand.
One of Australia's largest food franchisors - ransomware	Advising one of Australia's largest food franchisors in respect of legal issues arising from a Cryptolocker ransomware attack, that had encrypted the documents on its systems.
A not-for-profit government contractor - ransomware	Providing data breach incident response services to a not-for-profit government contractor following a ransomware attack. We advised the client and insurers on the potential data breach, business interruption, third party claim and recovery implications of the event.
A travel agency group - regulator inquiry	Advised a travel agency group following inadvertent e-mail disclosure of a spreadsheet containing names, addresses and contact details, including responding to the Privacy Commissioner in relation to a complaint made and preparing an apology letter to affected recipients
An educational institution - unauthorised collection	Advised an educational institution on a data breach regarding inappropriate retention of student personal information and credit card details.

CDBP Key Australian Contacts

Tricia Hobson
Partner and Chairman, Head of Insurance for Asia Pacific
Sydney
Tel +61 2 9330 8609
tricia.hobson@nortonrosefulbright.com

Jacques Jacobs
Partner, Insurance
Sydney
Tel +61 2 9330 8156
jacques.jacobs@nortonrosefulbright.com

Nick Abrahams
Partner, Global Head of Technology & Innovation
Sydney
Tel +61 2 9330 8312
nick.abrahams@nortonrosefulbright.com

Matthew Ellis
Partner, Insurance
Melbourne
Tel +61 3 8686 6329
matt.ellis@nortonrosefulbright.com

Bernard O'Shea
Partner, Technology
Melbourne
Tel +61 3 8686 6573
bernard.oshea@nortonrosefulbright.com

Jim Lennon
Special Counsel, Technology
Sydney
Tel +61 2 9330 8426
jim.lennon@nortonrosefulbright.com

As part of our Complete Data Breach Protection service offering, we have developed two global best practice cyber risk management packages to help organisations address cyber risks, and prepare for and respond to incidents. Contact us for further details.

Norton Rose Fulbright

Norton Rose Fulbright is a global law firm. We provide the world's preeminent corporations and financial institutions with a full business law service. We have more than 4000 lawyers and other legal staff based in more than 50 cities across Europe, the United States, Canada, Latin America, Asia, Australia, the Middle East and Africa.

Recognized for our industry focus, we are strong across all the key industry sectors: financial institutions; energy; infrastructure, mining and commodities; transport; technology and innovation; and life sciences and healthcare. Through our global risk advisory group, we leverage our industry experience with our knowledge of legal, regulatory, compliance and governance issues to provide our clients with practical solutions to the legal and regulatory risks facing their businesses.

Wherever we are, we operate in accordance with our global business principles of quality, unity and integrity. We aim to provide the highest possible standard of legal service in each of our offices and to maintain that level of quality at every point of contact.