Financial Services Newsletter

2021 . Vol 20 No 2

Contents

Information contained in this newsletter is current as at April 2021

LexisNexis® Butterworths

General Editor's note

Karen Lee *LEGAL KNOW-HOW*

During this summer when many of us are still feeling some impact of COVID-19, a good number of readers told me that they have read a lot. I hope the articles in this issue of the *Financial Services Newsletter* will provide useful knowledge and valuable insights, and you will enjoy reading them. Here's a teaser to get you started.

On 24 February 2021, Australian Securities and Investments Commission (ASIC) issued its first immunity policy. It sets out information on applications for immunity from civil penalty or criminal proceedings for a contravention of a provision in Pt 7.10 of the Corporations Act 2001 (Cth). What is the purpose of the policy? What is its coverage? Who is eligible to apply for immunity, and what does the application process entail? The authors of the first article have all the answers. My thanks to **Felicity Healy**, **Katrina Sleiman** and **Emily Brownlee** (Corrs Chambers Westgarth) for writing this informative piece for our readers. I found their commentary on this policy's implications for corporate entities in the financial services sector particularly relevant and helpful. I am sure you will too.

What comes to your mind when you hear the words "critical infrastructure regulation reform"? Did you know that, in November 2020, the Morrison Government released an exposure draft of the Security Legislation Amendment (Critical Infrastructure) Bill 2020 (Cth)? This Bill proposes to expand the application of the Security of Critical Infrastructure Act 2018 (Cth) to new classes of critical infrastructure sectors, and the financial services is one of them. In his article "Financial services set to be part of Australia's critical infrastructure", **Frank Downes** (Juris IT Services) looks at what financial services lawyers need to know about this law reform.

In their article "The future of data breaches", editorial board member **Andrea Beatty**, **Chelsea Payne** and **Chloe Kim** (Piper Alderman) observe that there may be a shift in the way privacy breaches are currently dealt with, possibly to one which puts the onus on agencies and organisations to comply with data breach requirements or face orders requiring monetary compensation. With recent ASIC actions, such as the commencement of proceedings against Australian Financial Services licence holder RI Advice Group Pty Ltd in August 2020, which was for alleged failure to have adequate cyber security systems, what do we need to know about whether compensation is the way of the future? The authors can shed some light on this for us.

Karen Lee
Principal
Legal Know-How
karen.lee@LegalKnowHow.com.au

Karen Lee is the General Editor of the Australian Banking & Finance Law Bulletin and the Financial Services Newsletter. She also partners with LexisNexis in other capacities, including as Specialist Editor for precedents in banking and finance, mortgages and options, and as contributing author of a number of other publications, including Australian Corporation Finance Law, Halsbury's Laws of Australia and Practical Guidance General Counsel. Karen established her legal consulting practice, Legal Know-How, in 2012. She provides expert advice to firms and businesses on risk management, legal and business process improvement, legal documentation, regulatory compliance and knowledge management. Prior to this, Karen worked extensively in-house, including as Head of Legal for a leading Australasian non-bank lender, as well as in top-tier private practice, including as Counsel at Allen & Overy and Clayton Utz.

ASIC's first immunity policy

***Felicity Healy**, **Katrina Sleiman** and **Emily Brownlee** CORRS CHAMBERS WESTGARTH*

The Australian Securities and Investments Commission (ASIC) has released its first immunity policy[1] to encourage early disclosure of serious financial misconduct. The policy is available to individuals for alleged contraventions of the market misconduct provisions under Pt 7.10 of the Corporations Act 2001 (Cth).

Here we consider how the policy operates, its interaction with the functions of the Australian Competition and Consumer Commission (ACCC), and its implications for corporate entities in the financial services sector.

Purpose of the immunity policy

The immunity policy is designed to encourage self-reporting for serious financial misconduct. Its development aligns with one of ASIC's five regulatory priorities for 2020–21, to continue "to identify, disrupt and deter the most harmful conduct".[2]

ASIC Commissioner Sean Hughes remarked the "Immunity Policy enhances ASIC's ability to identify and take enforcement action against complex markets and financial services contraventions".[3] The policy represents a renewed focus by ASIC on investigating and pursuing serious contraventions of the Corporations Act in contrast to enforcement actions relating to technical breaches.

Coverage of the immunity policy

The immunity policy is available only to individuals who may have contravened a provision in Pt 7.10. The policy is not available to corporate entities.

Part 7.10 deals with serious forms of financial misconduct that are challenging for regulators to detect and investigate, such as:

- market manipulation[4]
- false trading and market rigging[5]
- false or misleading statements in respect of financial products[6]
- dishonest conduct relating to financial products and services[7] and
- insider trading[8]

Contravention of these provisions can give rise to punitive proceedings. Individuals can face up to 15 years in prison and be fined up to the higher of $1.11 million or three times the value of the benefit derived from the contravention.[9]

Under the immunity policy, ASIC is empowered to grant immunity to civil penalty proceedings and to recommend to the Commonwealth Director of Public Prosecutions (CDPP) that immunity from criminal prosecution be granted. The office of the CDPP will be guided by ASIC's recommendation and its own prosecution policy when considering whether to grant immunity.[10]

The immunity policy does not offer an individual immunity from administrative proceedings designed to protect investors and financials consumers (such as actions by ASIC to revoke licences or seek disqualifications) or from an action seeking compensation, including by way of a representative proceeding brought by ASIC on behalf of third party victims of financial misconduct.[11] Theoretically, a successful immunity applicant who assists ASIC, including by giving evidence in court, could still then be subject to proceedings from ASIC seeking non-punitive relief in relation to the same misconduct.

Process of applying for immunity

The grant of immunity requires an individual to go through a three-step process:[12]

- Apply for a "marker" to preserve their position in the queue of people who may also seek immunity in respect of the same misconduct. That application can be made on a hypothetical or anonymous basis, or through legal representatives.
- If you are first in line, make a "proffer" to ASIC disclosing specific information and documents about the misconduct. ASIC may also interview you. If ASIC is satisfied with the assistance provided it can:
  - grant conditional immunity from civil penalty proceedings and
  - recommend to the CDPP that a letter of comfort be issued to the effect that the CDPP intends to grant immunity from criminal prosecution

• Meet all conditions outlined in the immunity policy, subject to which ASIC and the CDPP can then grant final immunity.

Eligibility for conditional immunity

To secure conditional immunity (and a letter of comfort), an individual must provide a satisfactory proffer and comply with nine pre-conditions of eligibility.[13] All pre-conditions are ongoing obligations and immunity can be revoked at any time if they are no longer satisfied. To be eligible an individual must:

- admit they are participating, or have participated, in misconduct that may contravene a provision in Pt 7.10
- not have coerced any other person to engage in the misconduct, though at least one other person must also have engaged in that conduct
- not have been the instigator of the misconduct
- be the first person to apply for immunity (joint requests may be considered in exceptional circumstances)[14]
- apply before any investigation into the relevant misconduct is commenced by ASIC (whether or not that investigation is known to the individual) and
- provide full, frank and truthful disclosure, and undertake to cooperate fully and expeditiously with ASIC, including throughout any investigation and ensuing court proceedings

Eligibility for final immunity

To secure final immunity from civil penalty proceedings, an individual must also:

- maintain confidentiality regarding their status as an immunity applicant (unless otherwise required by law or ASIC provides consent to the disclosure)
- forfeit the profits of any wrongdoing (no guidance has yet been provided as to the mechanism for valuing those profits or whether an exception applies for an individual who is willing but not able to forfeit the profits) and
- if ASIC considers it to be appropriate, make restitution to the victims of any wrongdoing (again, no guidance has been given as to how this will be practically applied by ASIC and what evidentiary thresholds, if any, will be used when determining who is a victim and what an appropriate restitutionary amount is)

Conditions for final immunity from criminal prosecution may also be imposed by the CDPP.

Use of information disclosed under the immunity policy

Admissions and confidentiality

The admissions required to be made in the course of applying for immunity can be used against the individual applicant as follows:

- Information is provided in an application for a marker, and that marker is withdrawn or cancelled. That information can be used by ASIC to further its investigation, including to gather other evidence that could then be used against the individual in punitive proceedings.[15]
- Information is provided in a proffer and ASIC then declines to grant conditional immunity. That information can be used in punitive proceedings.[16]
- ASIC pursues administrative or compensatory proceedings against the individual. The immunity policy does not offer any shields to those actions.
- ASIC is compelled to disclose the admissions to other regulatory agencies (such as the Australian Prudential Regulation Authority)[17] who can use the information to launch their own enforcement proceedings.

Against that background, it is important to ensure an immunity applicant is able to satisfy the conditions of immunity before applying, to avoid a scenario where they are denied immunity and the information they have provided sets off investigations against them (either by ASIC, the CDPP or other regulators).

The requirement to make an admission may also impact any insurance coverage that may be available to the individual — for both current and future investigations and proceedings relating to the admitted misconduct.

Privilege and use immunities

The immunity policy offers no safeguards that would protect an individual from waiving their rights of confidentiality or legal professional privilege over documents they may be asked to produce. The only protections against self-incrimination arise where immunity is granted, or where materials are provided in the course of an application for a marker (though those materials might then be used to gather other incriminating materials).

ASIC has an internal policy[18] which provides a mechanism for legal professional privilege to be maintained, however this is in respect of the regulator's compulsory information gathering powers. Information proffered under the immunity policy could be categorised as "voluntary" as the individual is free to withdraw their application for immunity at any time (albeit the consequence of this would be any information given up to that

point could then be used against them). Adopting the same logic, any use or derivative use immunities that would prevent the disclosed information being used in subsequent non-punitive proceedings would not be available. In the context of punitive proceedings, ASIC may indirectly use information gathered against an individual where their application is withdrawn or immunity is not granted.

Interaction of the immunity policy with the ACCC

The immunity policy is largely modelled off the ACCC's own immunity policy directed to cartel conduct.[19] There are important differences between the policies. The ACCC policy is available for both individuals and corporate entities. It also does not preclude immunity being granted to the person who instigated the misconduct or if an investigation has already commenced.

Interesting questions arise where financial misconduct under Pt 7.10 crosses over with conduct regulated by the ACCC. For example, an immunity applicant could apply under both the ASIC and ACCC immunity policies and be granted immunity for only one of them (say, because they were not first-in-line for the other). In that scenario, whilst the individual would be immune from proceedings from one regulator, the other could still investigate and pursue proceedings against them; potentially using information provided in the course of their immunity applications or through an information sharing protocol between the agencies.

Implications for corporate entities in the financial services sector

Corporate entities should give thought to:

- their process for ensuring timely compliance with their breach reporting obligations under the Corporations Act, particularly given the immunity policy is available only where an ASIC investigation has not already commenced, which encourages individuals to make disclosures at the earliest opportunity — including at a point in time when contraventions are merely suspected
- whether the standard terms of their employment contracts, and the terms of their mandatory whistleblower policies, are sufficiently robust to navigate a scenario in which an employee makes disclosures, reveals internal documents or breaches certain confidentialities in the process of an immunity application
- the implications of any admissions made by an employee, director or officer under the immunity policy on the availability of insurance cover for investigations and proceedings relating to the same misconduct. Particular thought should be given to any exclusions in those policies triggered by admissions in a company's professional indemnity and directors' and officers' liability policies and
- the adequacy of their own detection and investigation mechanisms for financial misconduct in light of ASIC's renewed attention to enforcement in this space

Felicity Healy
Partner
Corrs Chambers Westgarth
felicity.healy@corrs.com.au
corrs.com.au

Katrina Sleiman
Partner
Corrs Chambers Westgarth
katrina.sleiman@corrs.com.au
corrs.com.au

Emily Brownlee
Senior Associate
Corrs Chambers Westgarth
emily.brownlee@corrs.com.au
corrs.com.au

Footnotes

1. Australian Securities and Investments Commission (ASIC) *ASIC immunity policy* (February 2021) https://download.asic.gov.au/media/5988538/asic-immunity-policy-published-24-february-2021.pdf.
2. ASIC, Strategic priorities, 23 October 2020, https://asic.gov.au/about-asic/what-we-do/our-role/strategic-priorities/.
3. ASIC, 21-030MR ASIC launches immunity policy for market misconduct offences, 24 February 2021, https://asic.gov.au/about-asic/news-centre/find-a-media-release/2021-releases/21-030mr-asic-launches-immunity-policy-for-market-misconduct-offences/#:~:text=The%20Immunity%20Policy%20enhances%20ASIC's,is%20available%20on%20its%20website.
4. Corporations Act 2001 (Cth), s 1041A.
5. Above, ss 1041B and 1041C.
6. Above n 4, s 1041E.
7. Above n 4, s 1041G.
8. Above n 4, s 1043A.

9. Treasury Laws Amendment (Strengthening Corporate and Financial Sector Penalties) Act 2019 (Cth); Crimes Act 1914 (Cth).
10. Above n 1, cl 7.
11. Australian Securities and Investments Commission Act 2001 (Cth), s 50.
12. Abov n 1, ss D and E.
13. Above n 1, cl 11.
14. ASIC, ASIC immunity policy: Frequently asked questions, 24 February 2021, https://asic.gov.au/about-asic/dealing-with-asic/asic-immunity-policy/asic-immunity-policy-frequently-asked-questions/#q24
15. Above n 1, cl 38.
16. Above n 1, cl 44.
17. Above n 6, s 122C.
18. ASIC *Claims of legal professional privilege* Information Sheet 165 (December 2012).
19. Australian Competition and Consumer Commission *ACCC immunity and cooperation policy for cartel conduct — a policy document* (October 2019) www.accc.gov.au/system/files/1579_ACCC%20immunity%20%26%20cooperation%20policy%20for%20cartel%20conduct%20-%20October%202019_FA.pdf.

Financial services set to be part of Australia's critical infrastructure

Frank Downes *JURIS IT SERVICES*

The ongoing reform of the laws to ensure Australia's "critical infrastructure assets" and "systems of national significance" are protected has reached another milestone with the Security Legislation Amendment (Critical Infrastructure) Bill 2020 (Cth) (Bill) to amend the Security of Critical Infrastructure Act 2018 (Cth) (SOCI Act) being released at the end of 2020.

The recent spate of cyber breaches involving government departments, media organisations and other prominent Australian institutions highlights the importance of this type of legislation for our national security. Attacks originating from other states and highly sophisticated malicious actors are on the increase and countering these threats will require a centralised and unified effort.

Back in the good old days we only considered the ports and a few locations in the electricity, gas and water sectors to be "critical infrastructure". Not anymore, the SOCI Act is to be expanded to cover 11 sectors, and the assets within them. These are:

- the communication sector
- the financial services and markets sector
- the data storage or processing sector
- the defence industry sector
- the higher education and research sector
- the energy sector
- the food and grocery sector
- the health care and medical sector
- the space technology sector
- the transport sector
- the water and sewerage sector

The Bill introduces a broad definition of "critical infrastructure sector assets", as being "an asset that relates to a critical infrastructure sector".[1] From the perspective of cyber security it is best to consider that the SOCI Act will cover any asset — physical or digital in any defined sector.

It appears the intention of the government is to use the SOCI Act as a net to cover these sectors. The Minister for Home Affairs has a broad power to declare additional assets from the listed sectors as "critical".

Enhanced obligations

There is now a Positive Security Obligation to "embed preparation, prevention and mitigation activities into the business as usual operation of critical infrastructure assets",[2] thereby ensuring the resilience of essential services is strengthened and providing greater situational awareness of threats to critical infrastructure assets.

This positive security obligation consists of three parts:

- *Register of Critical Infrastructure Assets*
  Responsible entities need to provide:
  - *Interest and control information*: details of who owns or controls the asset including the extent of each entities ownership or control of the asset
  - *Operational information*: where the asset is located, what areas and facilities the asset services, details on any entities that operate, or have access to, the asset
- *Critical Infrastructure Risk Management Program*
  Responsible entities must manage and mitigate risks by adopting and maintaining an all-hazards risk management program. The specific matters to be included in a critical infrastructure risk management program will be prescribed in "rules", which will be co-designed between the industry and government. Risk management plans must be reported annually to the Secretary of Home Affairs. The requirements contained in the Bill are "switched on" for a particular sector when a "rule" is made in relation to a critical infrastructure asset or class of infrastructure assets.
- *Mandatory notification of cyber security incidents*
  The government's aim is to create a near-time threat management system. Responsible entities have to report critical cyber incidents to the Australian Signals Directorate within 12 hours of the entity becoming aware that the incident has had, or is having, a significant impact (whether direct or indirect) on the availability of the asset.

This near-time notification requirement demonstrates how serious the government is to strengthen our cyber preparedness and resilience when compared to the existing notification requirements under the Privacy Act 1988 (Cth) and the Australian Prudential Regulation Authority *CPS 234*[3] where entities have up to 30 days to complete a breach assessment for example.

For entities subject to this legislation major improvements in information technology capabilities for the collection and analysis of threat data will be required to enable effective reporting in the new time frames.

It is highly likely that over time, the cyber security requirements in the SOCI Act will become the de-facto baseline that all responsible entities in the defined sectors will have to meet. Critical infrastructure assets can be declared a "system of national significance" which triggers the enhanced cyber security obligations.

With the extensive data processing and storage undertaken by the Banking and Financial Services industry, your clients may have to consider the requirements of the SOCI Act as it applies to the data storage and processing sector also.

The effects of this Bill on your financial sector clients should be considered in respect to the potential impact on loan covenants, materiality reporting requirements and overall compliance requirements.

The government now expects responsible entities to:

- have a critical infrastructure risk management program in place
- comply with the critical infrastructure risk management program
- regularly review the critical infrastructure risk management program
- update the critical infrastructure risk management program
- report annually on the critical infrastructure risk management program
- compliance with requirement to undertake a vulnerability assessment
- compliance with providing a vulnerability assessment report
- compliance with requirement to provide reasonable assistance

Failure to comply with the eight requirements listed above renders the entity subject to fines of between 150 and 200 penalty units.

Criminal penalties

Demonstrating the government's concern in this area, there are now criminal sanctions that can be imposed with goal terms of up to 2 years and fines for staff that do not follow the directions of the Secretary of Home Affairs to create, manage and report on critical infrastructure systems under their control when directed to do so.

That is the stick, however the government has indicated they would prefer to take the carrot approach and have issued the following guidelines:

- will work collaboratively with organisations in the resolution of an incident
- prefers the use of direction powers rather than taking control of a system

Whilst the guidelines are premised around assistance rather than coercion, the government will step in where needed to take control of a system where an organisation is not taking or cannot take the correct steps to rectify a breach or vulnerability.

Of course, as with all legislative requirements with respect to cyber security keep in mind the potential for down-streaming. Your clients should ensure their contracts with suppliers and service providers meet cyber security standards and obligations where there could be a flow on effect in the event of a cyber breach.

For more information:
Protecting Critical Infrastructure and Systems of National Significance (homeaffairs.gov.au)
Explanatory Document — Exposure Draft Security Legislation Amendment (Critical Infrastructure) Bill 2020 (homeaffairs.gov.au)

Frank Downes
CEO
Juris It Services
frankd@jurisit.com.au
jurisit.com.au

About the author
Frank Downes is the CEO of JurisIT, an IT services company that assists law firms with technology, information security, information compliance and successfully implementing, securing and maintaining remote work environments.

Footnotes

1. Security Legislation Amendment (Critical Infrastructure) Bill 2020 (Cth), subs 8E(1).
2. Department of Home Affairs, Positive Security Obligation, 10 December 2020, www.homeaffairs.gov.au/nat-security/Pages/positive-security-obligation.aspx.
3. Australian Prudential Regulation Authority *Prudential Standard CPS 234 Information Security* (July 2019) www.apra.gov.au/sites/default/files/cps_234_july_2019_for_public_release.pdf.

The future of data breaches

***Andrea Beatty**, **Chelsea Payne** and **Chloe Kim** PIPER ALDERMAN*

On 11 January 2021, a determination was made by the Australian Information and Privacy Commission compelling the Australian government agency, Department of Home Affairs to pay compensation to victims of a 2014 data breach. This is the first instance where in a representative action a government body has been ordered to compensate victims for non-economic loss arising from a data breach and sets a unique precedent for the future of data breaches and remediation to victims. In light of the review of the Privacy Act 1988 (Cth) (Privacy Act), it poses a question on whether compensation will become a mandatory requirement for non-economic loss resultant from a privacy data breach.

Breach of detainees' privacy

The data breach saw over a thousand asylum seekers' personal information leaked and exposed online through the mistaken uploading of a report *The Immigration Detention and Community Statistics Summary* on the Department of Home Affairs' website. The report revealed personal information such as names, gender, reason for and location of detainment for 9258 individuals who were in immigration detention.[1] As a result of the data breach, a representative complainant on behalf of the asylum seekers brought proceedings against the Department of Home Affairs which Australian Information Commissioner and Privacy Commissioner Angelene Falk was tasked with determining.

Commissioner Falk determined that the Department of Home Affairs should pay compensation for the non-economic loss suffered by class members as a result of the data breach. The quantity of compensation was measured on a scale of five different categories of loss or damage for non-economic loss, depending on the severity of the breaches' impact.[2]

Based on this tiered system, compensation to data breach victims for non-economic loss will range between $500–$20,000 for 1,297 individuals. As mentioned by Commissioner Falk, this was the first instance of victims to non-economic loss being compensated and monetarily reflects the harmful impact the loss of privacy and unwilling disclosure of personal information can have on individuals. The compensation process is expected to occur over a 12-month period during which individual's compensation will be assessed and disbursed to class members.[3]

Is compensation the way of the future?

The significant data breach incident follows on from other recent government data breaches that took place in 2020. One of the most impactful concerned Service NSW, where a breach of 47 employee email accounts saw the government body being forced to apologise to 25,000 people for the disclosure of their personal information through documents including passports and driver's licences.[4] As a result, 3.8 million documents were investigated in 4 months to establish how the breach had occurred and who it affected. However, despite such personal information being revealed as a result of the cyber attack, victims were not compensated for the loss they incurred.[5]

As Commissioner Falk had adopted the five categories of non-economic loss to assess monetary compensations, perhaps such measures will also be adopted for future government breaches as well. This new way of approaching privacy breaches is aligned with the Office of the Australian Information Commissioner's (OAIC's) proposed overhaul of the Privacy Act to ensure the current privacy framework is able to respond to the new challenges posed to privacy in the digital environment. The OAIC's announcement on 30 October 2020 to review the current Privacy Act will be necessary to ensure privacy protections are relevant and adaptable for the future.[6] The emphasis on ensuring protection of personal information is likely to see amendments to how data breaches are treated by the OAIC and following from the recent compensation ordered on the Department of Home Affairs, may incorporate requirements for compensation or a remediation program for victims. Accordingly, the updated legislation may set the tone for more stringent penalties and remediation steps imposed on companies who fail to meet data breach requirements or do not have sufficient mechanisms in place to initially prevent a breach from occurring.

Data breach litigation

Although in the precedent case *ABC v Lenah Game Meats Pty Ltd*[7] the High Court was cautious in recognising a tort of privacy in Australian law, the recent determination made in favour of the class members seems to signify a shift in thinking. Furthermore, whether a statutory tort for serious invasions of privacy should be

implemented into legislation will be a matter to be considered in the OAIC's review of the Privacy Act.[8]

Recently the first proceedings against an AFSL holder for failing to comply with adequate cyber security obligations were commenced by the Australian Securities and Investments Commission (ASIC) against RI Advice Group Pty Ltd (RI Advice Group). ASIC alleged there had been numerous cyber breach incidents at an authorised representative of RI Advice Group and that they did not have the "adequate policies, systems and resources" reasonable to manage the risk in respect of cybersecurity and cyber resilience.[9] Therefore, ASIC sought declarations that RI Advice Group had contravened the Corporations Act 2001 (Cth), ordered RI Advice Group to pay a civil penalty to be determined by court and for RI Advice Group to implement systems that would be reasonably appropriate to adequately manage risk in respect of cybersecurity and cyber resilience.

The imposition of compensation on a government body and legal proceeding brought by a regulatory agency demonstrates the sincerity in which the government and regulatory agencies are treating privacy breaches and the non-economic loss to individuals consequent from it. Accordingly, it seems there may be a shift in the way privacy breaches are currently dealt with to one which puts the onus on government bodies and companies to comply with data breach requirements or face orders requiring monetary compensation.

Andrea Beatty
Partner
Piper Alderman
abeatty@piperalderman.com.au
www.piperalderman.com.au
www.andreabeatty.com.au

Chelsea Payne
Associate
Piper Alderman
cpayne@piperalderman.com.au
www.piperalderman.com.au

Chloe Kim
Lawyer
Piper Alderman
ckim@piperalderman.com.au
www.piperalderman.com.au

This article was first published in LexisNexis' Privacy Law Bulletin Vol 17 Issue 9 — February 2021.

Footnotes

1. C Knaus "Australian government ordered to pay 1,300 asylum seekers whose details were exposed" *The Guardian* 27 January 2021, www.theguardian.com/australia-news/2021/jan/27/australian-government-ordered-to-pay-1300-asylum-seekers-whose-details-were-exposed.
2. *"WP" and Secretary to the Department of Home Affairs (Privacy)* [2021] AICmr2 (11 January 2021).
3. Above.
4. Service NSW, Service NSW cyber incident, www.service.nsw.gov.au/cyber-incident.
5. Lucy Cormack "Service NSW data breach affected 80,000 fewer people than first thought" *Sydney Morning Herald* 16 December 2020, www.smh.com.au/national/nsw/service-nsw-data-breach-affected-80-000-fewer-people-than-first-thought-20201215-p56np7.html.
6. OAIC, "OAIC welcomes Privacy Act review", media release (30 October 2020) www.oaic.gov.au/updates/news-and-media/oaic-welcomes-privacy-act-review/.
7. *Australian Broadcasting Corp v Lenah Game Meats Pty Ltd* (2001) 208 CLR 199; 185 ALR 1; [2001] HCA 63; BC200107043.
8. Attorney-General's Department, *Terms of Reference*, www.ag.gov.au/system/files/2020-10/privacy-act-review-terms-of-reference.pdf.
9. Federal Court of Australia, *Australian Securities and Investments Commission v RI Advice Group Pty Ltd (ACN 001 774 125)* Statement of Claim (2020), https://download.asic.gov.au/media/5836071/20-191mr-2020-10-26-vid-556-asic-v-ri-soc-filed.pdf.

For editorial enquiries and unsolicited article proposals please contact newsletters@lexisnexis.com.au.
Cite this issue as (2021) 20(2) *FSN*
SUBSCRIPTION INCLUDES: 10 issues per volume plus binder www.lexisnexis.com.au
SYDNEY OFFICE: Locked Bag 2222, Chatswood Delivery Centre NSW 2067
CUSTOMER RELATIONS: 1800 772 772
GENERAL ENQUIRIES: (02) 9422 2222
ISSN: 1035-2155 Print Post Approved PP 25500300764