GIR Global Investigations Review

The Practitioner's Guide to Global Investigations

Volume II: Global Investigations around the World

NINTH EDITION

Editors
Judith Seddon, Eleanor Davison, Christopher J Morvillo†, Luke Tolaini, Celeste Koeleveld, F Joseph Warin and Winston Y Chan

2025

The Practitioner's Guide to Global Investigations

Volume II: Global Investigations around the World

The Practitioner's Guide to Global Investigations

Ninth Edition

Edited by

Judith Seddon

Eleanor Davison

Christopher J Morvillo†

Luke Tolaini

Celeste Koeleveld

F Joseph Warin

Winston Y Chan

Published in the United Kingdom by Law Business Research Ltd
Holborn Gate, 330 High Holborn, London, WC1V 7QT, UK

www.globalinvestigationsreview.com

Enquiries concerning reproduction should be sent to: insight@globalinvestigationsreview.com.
Enquiries concerning editorial content should be directed to the Publisher –
marieke.breijer@lbresearch.com

Printed in Great Britain by
Encompass Print Solutions, Derbyshire
Tel: 0844 2480 112

Acknowledgements

Addleshaw Goddard LLP

Akrivis Law Group, PLLC

A&O Shearman

Anagnostopoulos

Ashurst LLP

Baker McKenzie

BDO USA, PC

Bennett Jones

Bracewell LLP

Campos Mello Advogados (in cooperation with DLA Piper)

Clifford Chance

Cloth Fair Chambers

Cooley LLP

Corker Binning

Cravath, Swaine & Moore LLP

Davis Polk & Wardwell

Debevoise & Plimpton LLP

De Brauw Blackstone Westbroek

Díaz Reus Abogados

DLA Piper

EY Law

Five St Andrew's Hill

Fornari e Associati

Fountain Court Chambers

Fox Williams

Gibson, Dunn & Crutcher LLP

Goodwin Procter LLP

Herbert Smith Freehills

Homburger

Kingsley Napley LLP

Kirkland & Ellis International LLP

Law Offices of Panag and Babu

Linklaters LLP

McDermott Will & Emery UK LLP

Matheson

Meredith Connell

Mori Hamada & Matsumoto

Moroğlu Arseven

Morvillo Abramowitz Grand Iason & Anello PC

Navacelle

Nyman Gibson Miralis

Paul Hastings, LLP

Rebaza, Alcázar & De Las Casas

Robertson Pugh Associates LLP

Sullivan & Cromwell LLP

Travers Smith LLP

Uría Menéndez

Walden Macht Haran & Williams LLP

White & Case

Willkie Farr & Gallagher LLP

Withers LLP

Contents

4

Australia: keeping up to date in a rapidly changing regulatory landscape

Dennis Miralis, Jasmina Ceic, Annabel Wurth, Kartia Zappavigna, Jack Dennis and Harry Sultan

GENERAL CONTEXT, KEY PRINCIPLES AND HOT TOPICS

1 Identify the highest-profile corporate investigation under way in your country, describing and commenting on its most noteworthy aspects.

The highest-profile corporate investigation in Australia in 2024 involves PricewaterhouseCoopers (PWC), a global professional services company that provides accounting and consulting services. The investigation, now in the hands of the Australian Federal Police (AFP), centres on the unauthorised disclosure of confidential government tax strategies by a former partner. The shared information included government plans, meeting agendas and confidential drafts on tax avoidance schemes from the Organisation for Economic Co-operation and Development. This breach enabled commercial exploitation, as PWC formed a global team to leverage these insights for commercial gains. This strategy resulted in approximately A$2.5 million in revenue, as PWC advised 14 companies on how to navigate the new tax laws before they were enacted.

In 2018, the Australian Taxation Office (ATO) first became suspicious and raised its concerns about a confidentiality breach with the AFP; however, due to a lack of detail they could not proceed with an investigation. In 2020, the ATO referred their suspicions to the Tax Practitioners Board (TPB), a government body responsible for regulating the tax advisory industry.

In 2022, the TPB announced that it had suspended the partner's tax licence due to unspecified breaches of integrity standards and ordered PWC to provide training on managing conflicts of interest and provide compliance reports to the TPB for two years. The *Australian Financial Review* broke the story, which prompted the Australian Securities and Investments Commission (ASIC) to ban the former partner from providing financial services for eight years.

In 2023, the Secretary to the Treasury referred the matter to the AFP for criminal investigation. When the story went public in 2023, PWC stated that a single partner was responsible for the breach; however, it was soon revealed that the corruption was widespread, and an internal investigation was launched.

The scandal has prompted widespread regulatory and governmental responses, reflecting Australia's emphasis on corporate accountability and transparency. In August 2023, the federal government announced a crackdown on tax adviser misconduct in response to the scandal. Fines for tax advisers who try to skirt tax laws increased from A$7.8 million to A$780 million. The proposed reforms and structural changes hold the potential to not only prevent the recurrence of these incidents but also to fortify the trust and reliability clients place in these institutions.

2 Outline the legal framework for corporate liability in your country.

The Criminal Code 1995 (Cth) applies to bodies corporate in the same way that it applies to individuals, but with modifications made necessary by the fact that the criminal liability is being imposed on a company rather than an individual. Offences committed by 'a person' will, unless specifically excluded, include a corporation.

Direct liability occurs where both the physical element and the fault element are established. Regarding the physical element, a company is criminally liable when the offence is committed by its directing mind and will. A company can act through its officers or agents, provided they have the requisite authority. Under Section 12.2 of the Criminal Code, when agents have actual or apparent authority, their actions that are within the scope of their authority bind the company.

The fault element, being intention, knowledge or recklessness, may be attributable to a company if the company expressly, tacitly or impliedly authorises or permits the commission of the offence as per Section 12.3 of the Criminal Code. This authorisation or permission of the commission of the offence can be established if, among other things, the corporation's board of directors or high managerial agents intentionally or knowingly engaged in the relevant conduct or there was a corporate culture that directed, encouraged, tolerated or led to non-compliance with the relevant provision.

3 Which law enforcement authorities regulate corporations? How is jurisdiction between the authorities allocated? Do the authorities have policies or protocols relating to the prosecution of corporations?

Australian corporations are mainly regulated at a federal level, with state and territory regulators playing a more limited role, particularly in areas such as fraud, theft and private sector bribery. The following are the primary law enforcement authorities:

- ASIC, which is Australia's corporate regulator and has responsibility for enforcing (including bringing criminal prosecutions under) the Corporations Act 2001 (Cth), the main corporate legislation in Australia. ASIC is authorised to prosecute generally minor regulatory offences, though it will typically refer matters to the Commonwealth Director of Public Prosecutions (CDPP).

- The Australian Competition and Consumer Commission (ACCC), which is responsible for regulating and enforcing the Competition and Consumer Act 2010 (Cth), which regulates the interaction between consumers and businesses. The ACCC can refer matters to the CDPP for prosecution.
- The Australian Criminal Intelligence Commission (ACIC), which has an intelligence mandate, primarily directed at serious organised crime. The ACIC also works extensively with domestic and international partner agencies in the conduct of its investigations.
- ATO, which is responsible for administering Australia's taxation legislation. Under the Tax Administration Act 1953 (Cth), the ATO also prosecutes a range of summary offences and may refer more serious matters to the CDPP to consider prosecution.
- Australian Transaction Reports and Analysis Centre (AUSTRAC), which regulates and enforces cross-border financial transactions.
- The AFP, which is responsible for the investigation of offences under the Criminal Code.
- The CDPP, which is responsible for criminal prosecutions of offences under Commonwealth laws. It does not investigate cases but works collaboratively with government agencies that may refer matters to it for prosecution following investigations. There are also state and territory directors of public prosecutions (DPPs), which pursue prosecutions for offences under state and territory laws.

4 What grounds must the authorities have to initiate an investigation? Is a certain threshold of suspicion necessary to trigger an investigation?

The trigger for an investigation is generally suspicion of a breach of legislation within a regulator's jurisdiction.

For example, ASIC commences an investigation where it has reason to suspect a breach of the Corporations Act. It has wide-ranging investigative powers, including compelling the production of documents and conducting compulsory interviews of persons in relation to its investigations. ASIC can apply for a search warrant under Section 3E of the Crimes Act 1914 (Cth), which is granted where an authorised officer is satisfied that there are reasonable grounds to suspect there is or will be evidential material at the relevant premises.

Additionally, the ATO conducts audits to ensure that businesses and taxpayers are compliant with tax laws, and it has wide investigative powers, which are contained in the Tax Administration Act 1953 (Cth). Where the ATO cannot obtain the documents it requires to support an audit under a cooperative approach or where it suspects tax fraud or tax evasion has occurred, it may use its formal powers to access documents and evidence.

5 How can the lawfulness or scope of a notice or subpoena from an authority be challenged in your country?

In Australia, the lawfulness or scope of a notice or subpoena can be challenged through several legal mechanisms.

A notice or subpoena can be challenged or objected to on several grounds, including that it has been improperly issued, the information sought is not clearly defined and is irrelevant or the request is oppressive or unreasonable in relation to the time for compliance. Additionally, the recipient of a subpoena may refuse to produce documents or information on the basis that it is protected by legal professional privilege, public interest immunity or another form of privilege.

The lawfulness or scope of a notice or subpoena can be challenged to the court that issued it, seeking to have it set aside in whole or in part.

6 Does your country make use of cooperative agreements giving immunity or leniency to individuals who assist or cooperate with authorities?

Australian regulatory authorities have different approaches to granting indemnity.

ASIC's Immunity Policy provides persons with the opportunity to make a request for immunity. ASIC has the power to issue a 'marker' for particular conduct to the first individual who requests immunity. This encourages parties to apply for immunity. However, subsequent applicants will not be eligible for immunity under the Policy, unless the first applicant is not eligible for immunity. Initially, ASIC provides conditional immunity in relation to civil proceedings, and, where relevant, the DPP will issue a letter of comfort for criminal immunity at the same time as civil immunity is granted by ASIC. Conditional civil immunity will become final immunity at the conclusion of any proceedings, including any appeal proceedings, provided that conditions of immunity are not breached and eligibility is maintained under the policy.

The ACCC has the power to grant civil immunity only in relation to cartel conduct. This can be described as a 'first past the post' style policy that provides immunity to the individual or corporation that is first to disclose cartel conduct and cooperate fully with the investigation. One of the criteria for immunity requires the applicant to enter into a cooperation agreement that outlines the initial cooperative steps that the applicant agrees to undertake pursuant to its immunity application.

The DPP or CDPP can grant immunity from prosecution for alleged criminal offences against state, territory or Commonwealth laws. The CDPP and state or territory DPPs have the authority to grant immunity from prosecution to individuals who provide evidence or testimony that is crucial to the prosecution of other offenders. This is typically done under the condition that the individual fully cooperates with law enforcement and the prosecution.

As to leniency, sentencing for criminal conduct is entirely at the discretion of the court.

7 What are the top priorities for your country's law enforcement authorities?

ASIC's enforcement priorities for 2024 include:

- compliance with design and distributor obligations;
- combating greenwashing;

- the superannuation and insurance industries, with enforcement resources to be directed towards addressing:
  - superannuation member services failures and misconduct resulting in the systematic erosion of superannuation balances; and
  - insurer claims handling failures; and
- enforcement action aimed at protecting vulnerable consumers.

Three key themes underpinning the ACCC's 2024–25 compliance and enforcement priorities are sustainability, cost-of-living pressures and the digital economy. Its key priorities include the following:

- consumer, product safety, fair trading, and competition and pricing concerns in relation to environmental claims and sustainability, as well as specifically within the supermarket sector;
- misleading pricing and claims in relation to essential services, with a particular focus on energy and telecommunications; and
- consumer and fair trading issues in the digital economy, with a focus on misleading or deceptive advertising within influencer marketing, online reviews, in-app purchases and price comparison websites.

The ATO has set out its 2024–25 priorities as being incorrectly claimed work-related expenses, inflated claims for rental properties and failure to include all income when lodging tax returns.

AUSTRAC has outlined its strategic priorities for 2024, which aim to ensure that regulated businesses are carrying out the following:

- building and maintaining a culture of anti-money laundering and counterterrorism financing (AML/CTF) compliance and risk management;
- developing and maintaining effective transaction monitoring programmes to identify unusual transactions or suspicious customer interactions; and
- ensuring that any AML/CTF functions that are outsourced to a third party meet legal requirements.

8 To what extent do law enforcement authorities in your jurisdiction place importance on a corporation having an effective compliance programme? What guidance exists (in the form of official guidance, speeches or case law) on what makes an effective compliance programme?

In Australia, law enforcement authorities place importance on corporations having effective compliance programmes. The Australian government and regulatory bodies, such as ASIC, the ACCC and the Australian Prudential Regulation Authority, actively encourage and sometimes mandate the implementation of robust compliance frameworks within corporations. Specific guidance on certain mandatory compliance programmes can be found in regulatory policies of the respective regulatory bodies.

CYBER-RELATED ISSUES

9 Does your country regulate cybersecurity? Describe the approach of local law enforcement authorities to cybersecurity-related failings.

There are both federal and state or territory laws relevant or applicable to cybersecurity. Federally, these include the following laws: the Privacy Act 1988 (Cth), the Crimes Act 1914 (Cth), the Security of Critical Infrastructure Act 2018 (Cth), the Criminal Code, the Telecommunications (Interception and Access) Act 1979 (Cth), the Corporations Act 2001 (Cth) and the Freedom of Information Act 1982. There are also state or territory laws that may be applicable to cybersecurity, including criminal laws (e.g., the Crimes Act 1900 (NSW), Section 308H) and privacy legislation relating to accessing and handling certain information (e.g., health records).

The Australian government is robust in responding to cybersecurity failings, particularly where those failings involve sensitive consumer data being exposed, through the use of civil penalties and other administrative action. In October 2022, Medibank, one of Australia's largest health insurers, was subject to a cyber breach, which involved customer health data being posted on the dark web. Several Australian agencies have acted against Medibank. The Office of the Australian Information Commissioner alleges that from March 2021 to October 2022, Medibank seriously interfered with the privacy of 9.7 million Australians by failing to take reasonable steps to protect their personal information from misuse and unauthorised access or disclosure in breach of the Privacy Act 1988. The Australian Information Commissioner has taken civil penalty proceedings against Medibank in the Australian Federal Court.

10 Does your country regulate cybercrime? What is the approach of law enforcement authorities in your country to cybercrime?

In Australia, data protection and privacy are principally regulated by the Federal Privacy Act 1988, which is currently under review. However, there are a host of laws on a state and federal level that touch on cybersecurity, including the Criminal Code Act 1995, the Telecommunications Sector Security Reforms and the recently amended Security of Critical Infrastructure Act 2018.

The Criminal Code Act 1995 contains various provisions that prohibit activities related to supporting and facilitating cybercrime. These provisions include distribution, sale or the offering for sale of hardware, software or other tools used to commit cybercrime. These are criminalised by Section 478.4 of the Criminal Code, which provides for the offence of 'producing, supplying or obtaining data with intent to commit a computer offence', and Section 478.1 of the Criminal Code, which provides for the offence of 'unauthorised access to, or modification of, restricted data'.

In March 2023, the Australian government announced plans to overhaul the current regime through centralisation and simplification: it will appoint a coordinator for cybersecurity, supported by a new national office within the Department of Home Affairs to ensure a centrally coordinated approach.

CROSS-BORDER ISSUES AND FOREIGN AUTHORITIES

11 Does local criminal law have general extraterritorial effect? To the extent that extraterritorial effect is limited to specific offences, give details.

Australian law makes provision for extraterritorial application at both the federal and state levels. At the federal level, Section 15 of the Criminal Code Act 1995 (Cth) provides for four categories of extraterritorial jurisdiction. To various extents, these categories restrict the application of Australian criminal law depending on the nexus of the offending to Australia, such as whether the crime was committed wholly or partly outside Australia and whether the effects of the relevant conduct occurred wholly or party in Australia. Section 15 also provides for Category D offences, which are criminalised under Australian law regardless of where the offence, or where the effects of the conduct, occur. An example of the application of Category D is to child sex tourism offences under Section 272.

At the state level, Part 1A of the Crimes Act 1900 (NSW) provides for a limited form of extraterritorial application where a geographical nexus exists between the state and the offence, such as whether the crime was committed wholly or partly, or whether the effects of the crime were felt wholly or partly, within the state.

12 Describe the principal challenges that arise in your country in cross-border investigations, and explain whether and how such challenges depend on the other countries involved.

One of the foremost problems facing cross-border investigators is determining the appropriate jurisdiction in which proceedings should be taken. When offences are committed in various countries, or where the offender and victim are located in different places, questions arise as to which jurisdiction should apply.

Issues concerning extradition often arise. Extradition procedures are complex and difficult, making applications costly and slow. Extradition requires not only that an appropriate treaty exists between the two countries concerned, but also that the conduct in question be criminalised in both the requesting and receiving country.

The problem of 'negative international jurisdiction' also arises. This refers to cases that are not investigated because they could be prosecuted in one of many countries, but none want to take action. The reverse can also be a problem, when too many countries want to prosecute a particularly noteworthy cause.

13 Does double jeopardy, or a similar concept, apply to prevent a corporation from facing criminal exposure in your country after it resolves charges on the same core set of facts in another? Is there anything analogous in your jurisdiction to the 'anti-piling on' policy as exists in the United States (the Policy on Coordination of Corporate Resolution Penalties) to prevent multiple authorities seeking to penalise companies for the same conduct?

The prohibition on double jeopardy is a fundamental safeguard in common law. The common law right applies only to subsequent trials within one country, not to a subsequent

trial in a different country to that of the original trial. However, double jeopardy is prohibited under international human rights instruments to which Australia is signatory, and the Australian government would not likely proceed with a criminal prosecution if convictions were secured in another jurisdiction.

14 Are 'global' settlements common in your country? What are the practical considerations?

There are no published examples of Australia engaging in a global settlement agreement for transnational corporate crime.

15 What bearing do the decisions of foreign authorities have on an investigation of the same matter in your country?

Australia conducts investigations independently of foreign authorities. However, Australian law enforcement works cooperatively with international partners and would exercise prosecutorial discretion if the authorities felt an offender had been adequately punished in another jurisdiction.

ECONOMIC SANCTIONS ENFORCEMENT

16 Describe your country's sanctions programme and any recent sanctions imposed by your jurisdiction.

In 2024, Australia has significantly reinforced its sanctions framework, primarily driven by global geopolitical tensions and its commitment to international law. The sanctions target a wide array of issues, including human rights violations, nuclear proliferation and the actions of state and non-state actors involved in destabilising activities.

Iran

Australia has imposed stringent sanctions on Iranian individuals and entities, particularly in response to Iran's missile and unmanned aerial vehicle programmes and its destabilising influence in the Middle East. These sanctions include travel bans and asset freezes against high-ranking officials such as the Defence Minister and key figures within the Islamic Revolutionary Guard Corps. The sanctions also extend to companies involved in military technologies that are seen as threats to regional stability.

Russia and Ukraine conflict

Australia continues to maintain and update sanctions related to Russia's aggression against Ukraine. These sanctions target Russian officials, oligarchs and companies supporting the war effort, including those providing military equipment or financial backing. Australia has also sanctioned Iranian entities for supplying drones to Russia, which are used in the conflict against Ukraine.

Human rights violations

Australia has been active in imposing Magnitsky-style sanctions, targeting individuals and entities responsible for serious human rights abuses. These sanctions have been applied to

officials from various countries, including those involved in the suppression of protests, arbitrary detention and persecution of minorities. For example, Australia imposed sanctions on Iranian officials linked to the death of Mahsa Amini.

Compliance and enforcement

The Australian Sanctions Office is responsible for enforcing these sanctions, working closely with other government agencies such as the Australian Federal Police and the Department of Home Affairs. Breaches of sanctions laws in Australia carry severe penalties, including hefty fines and imprisonment for individuals and corporations involved in unauthorised dealings with sanctioned entities.

17 What is your country's approach to sanctions enforcement? Has there been an increase in sanctions enforcement activity in recent years, for example?

Australia's sanctions regime is closely aligned with those of its international partners, particularly those in the West. This alignment ensures that Australia's sanctions are part of a broader, coordinated effort to address global challenges, such as nuclear non-proliferation and the protection of human rights.

Australia's approach in 2024 highlights its active role in global governance and its commitment to upholding international norms, particularly in regions of strategic importance such as the Middle East and Eastern Europe. The government's actions reflect a broader strategy of leveraging sanctions as a tool for both diplomatic pressure and compliance with international law.

18 Do the authorities responsible for sanctions compliance and enforcement in your country cooperate with their counterparts in other countries for the purposes of enforcement?

Australia's sanctions regime largely mimics the approach taken, often identically, of key international partners such as the US and the UK.

19 Has your country enacted any blocking legislation in relation to the sanctions measures of third countries? Describe how such legislation operates.

The Australian government has not passed any new specific blocking legislation that would impose significant constraints or restrictions on foreign authorities or entities. However, several legislative developments reflect a broader trend of tightening regulations and expanding oversight, particularly in financial and cybersecurity domains.

20 To the extent that your country has enacted any sanctions blocking legislation, how is compliance enforced by local authorities in practice?

There are presently no blocking statutes or other restrictions prohibiting adherence to other jurisdictions' sanctions or embargoes.

BEFORE AN INTERNAL INVESTIGATION

21 How do allegations of misconduct most often come to light in companies in your country?

Allegations of company misconduct have come to light in a variety of ways in Australia. The 2022 Optus data breach is an example of internal audits resulting in misconduct being discovered. In September 2022, telecommunications company Optus suffered a data breach that affected around 10 million current and former customers. The information that was illegally obtained included customers' names, dates of birth, addresses and driving licence details. According to Optus insiders and the Australian government, errors committed by Optus employees caused system vulnerabilities that led to the data breach. Following extensive media reporting and government inquiry, Optus engaged the professional services firm Deloitte to commence an external investigation into the cyberattack. Optus has since apologised for the breach.

INFORMATION GATHERING

22 Does your country have a data protection regime?

In Australia, there is data protection legislation at a state, territory and federal level. At the federal level, the principal data protection legislation is the Privacy Act 1988 (Cth) and the Australian Privacy Principles.

For Australian states and territories, the legislation concerned with data protection includes the Information Privacy Act 2014 (Australian Capital Territory), the Privacy and Personal Information Protection Act 1998 (New South Wales (NSW)), the Information Privacy Act 2009 (Queensland), the Personal Information and Protection Act 2004 (Tasmania) and the Privacy and Data Protection Act 2014 (Victoria (VIC)).

23 To the extent not dealt with above at question 9, how is the data protection regime enforced?

The Office of the Australian Information Commission (OAIC) enforces the data protection regime under the Privacy Act 1988 (Cth). The OAIC has a range of enforcement powers to deal with data protection violations, including issuing infringement notices and accepting enforceable undertakings to applying to court for civil penalty orders where civil penalty provisions have been breached.

The OAIC uses court proceedings for egregious breaches of data privacy. It commenced Federal Court of Australia proceedings against the private health insurance provider Medibank for data breaches in October 2022. The OAIC alleges that Medibank interfered with the privacy of 9.7 million individuals (current and former customers) by failing to take reasonable steps to protect personal information from misuse. Considered one of the most devastating, high-profile data breaches in Australian history, Medibank faces a maximum penalty of A$21.5 trillion. Pursuant to Section 13G of the Privacy Act, the Federal Court can impose a maximum penalty of A$2.22 million for each data

breach of the 9.7 million people. Although this penalty is highly unlikely to be ordered, it demonstrates the magnitude of the privacy breaches. The proceedings are currently subject to administrative directions in the Federal Court.

24 Are there any data protection issues that cause particular concern in internal investigations in your country?

In its 2023–24 corporate plan, the OAIC identified the vulnerabilities associated with online platforms, social media and high-privacy impact technologies as the data protection issues that cause particular concern in internal investigations. Privacy violations can arise from opaque terms and conditions to which individuals agree. Further, another concern is the security of personal information in the finance and health sectors. As the controversies with Medibank data have demonstrated, serious failures by institutions to take reasonable steps to protect personal information remain an ever-present concern.

25 Does your country regulate or otherwise restrict the interception of employees' communications? What are its features and how is the regime enforced?

There is no federal legislation that governs the type of employee monitoring that is permissible or that specifies the circumstances under which it is permitted. This is relegated to the states and territories to regulate. The examples below consider NSW and VIC.

In NSW, the notice requirements that employers must adhere to for compliance are listed in Part 2 of the Workplace Surveillance Act 2005 (NSW). Notably, employees are given a minimum of 14 days' notice prior to surveillance being conducted. The notice will list the circumstances for surveillance being carried out.

In VIC, under Part 2A of the Surveillance Devices Act 1999 (VIC), the surveillance of employees in certain places and circumstances is prohibited.

DAWN RAIDS AND SEARCH WARRANTS

26 Are search warrants or dawn raids on companies a feature of law enforcement in your country? Describe any legal limitations on authorities executing search warrants or dawn raids, and what redress a company has if those limits are exceeded.

Law enforcement and regulatory agencies at both the state and federal levels have the power to execute searches on premises where there is a reasonable suspicion or grounds that an offence was committed or where there is evidence that can be used to prove an offence. Company premises are no exception to this.

There are limitations to search warrants. Both search warrants and dawn raid approvals must be obtained pursuant to orders by judges or magistrates. For Commonwealth search warrants, the High Court reaffirmed in *Smethurst v. Commissioner of the Australian Federal Police* ((2020) 272 CLR 177) that warrants cannot be general and that the offence underlying the warrant must be sufficiently stated.

Companies have redress if search warrant limits are exceeded. Companies can apply to courts for a remedy in the form of orders to have the search warrant set aside and quashed. Consequently, this can prevent prosecutions based on evidence obtained by invalid search warrants.

27 How can privileged material be lawfully protected from seizure during a dawn raid or in response to a search warrant in your country?

The Law Council of Australia and the Australian Federal Police have provided guidelines on how material covered by legal professional privilege can be protected during a search warrant raid. This is of particular use when law offices are raided. According to these guidelines, executing officers should explain the purposes of the search and invite the lawyer to cooperate. Once documents are taken, a list of the general information concerning the nature of the documents should be compiled and then delivered to a third party (such as another lawyer) who then makes a determination on the privilege of the documents in four days. Where privilege appears to apply, the documents are returned to the owner.

28 Under what circumstances may an individual's testimony be compelled in your country? What consequences flow from such compelled testimony? Are there any privileges that would prevent an individual or company from providing testimony?

There are a range of Commonwealth laws that empower federal agencies to conduct investigations that abrogate the right to claim privilege or right against self-incrimination. They are described as 'coercive'. The following are examples of powers that commonly affect companies:

- *Taxation*: Under Section 353-10 of schedule 1 of the Taxation Administration Act 1953 (Cth), the Australian Taxation Office can require a person to give any information required or to attend an examination. This is not balanced against any statutory immunity; however, a court's inherent power to ensure a fair trial could provide protection.
- *Corporate regulation*: Under the Australian Securities and Investments Commission Act 2001, the Australian Securities and Investments Commission has the power to compel people to produce books, attend examinations and answer questions. The privilege against self-incrimination is not applicable, but immunity is available for statements made during criminal proceedings.

WHISTLEBLOWING AND EMPLOYEE RIGHTS

29 Describe the whistleblowing framework in your country. What financial incentive schemes exist for whistleblowers? What legal protections are in place for whistleblowers?

The Corporations Act provides a whistleblowing framework in relation to breaches of the Corporations Act and the Australian Securities and Investments Commission Act 2001

(Cth). In 2019, the Corporations Act was amended to include greater protections for whistleblowers who report the misconduct of companies and company officers. Some of these amendments include:

- the abolition of good faith requirements in whistleblowing. Whistleblowers are only expected to have reasonable grounds for disclosure;
- increased range of people who enjoy protection, which now includes relatives, dependents and spouses of the whistleblower; and
- increased civil penalties for breaching a whistleblower's confidentiality. A body corporate can face a penalty of up to A$16.5 million (as at 1 July 2024), or up to three times the benefit or 10 per cent of the annual company turnover if a court can determine the benefit derived or detriment avoided resulting from the breach.

Australia does not have a financial incentive scheme for whistleblowers.

30 What rights does local employment law confer on employees whose conduct is within the scope of an investigation? Is there any distinction between officers and directors of the company for these purposes?

Employees are entitled to procedural fairness when their conduct is under investigation. Procedural fairness concerns the decision-making process followed or the steps taken by a decision maker rather than the outcome of a decision. There are many forms of procedural fairness. According to the Fair Work Commission, this can include whether an employer follows their own procedures when they dismiss an employee and whether an employee has the opportunity to explain their version of events.

Company officers and directors are not distinct from employees when being investigated. However, pursuant to Section 550 of the Fair Work Act 2009 (Cth), they can face accessorial liability for fair work violations that take place under their management.

31 Do employees' rights under local employment law differ if a person is deemed to have engaged in misconduct? Are there disciplinary or other steps that a company must take when an employee is implicated or suspected of misconduct, such as suspension or in relation to compensation?

An employee under investigation for misconduct may face suspension. An employer has the right to suspend the employee while they undertake an investigation. However, an employer is not obliged to do so. The Federal Court of Australia in *Avenia v. Railway & Transport Health Fund Ltd* ([2017] FCA 859) held that, at common law, employers may temporarily suspend employees in investigating misconduct. However, employees are generally entitled to full pay while suspended and under investigation for misconduct.

32 Can an employee be dismissed for refusing to participate in an internal investigation?

Employees can be dismissed for refusing to participate in an internal investigation. According to the Fair Work Commission in the matter of *Francis v. Patrick Stevedores Holdings Pty Ltd* ([2014] FWC 777), employees generally have a duty to be open, frank

and honest with employers in relation to serious workplace issues. Refusing to answer questions in an internal investigation could be seen as disobeying a lawful direction and thus, in certain circumstances, could be a valid reason for dismissal.

COMMENCING AN INTERNAL INVESTIGATION

33 Is it common practice in your country to prepare a document setting out terms of reference or investigatory scope before commencing an internal investigation? What issues would it cover?

While it is not mandatory, it is common practice in Australia to define the scope of an investigation before it begins. This often includes consideration of any regulatory compliance and reporting obligations. Boards of directors frequently refer internal investigations to external advisers, such as law firms, particularly when there are concerns about litigation or risk management.

This approach can help ensure that the investigation is protected by legal professional privilege. If terms of reference are prepared, they should clearly outline the key issues, information sources and the reporting process.

34 If an issue comes to light prior to the authorities in your country becoming aware or engaged, what internal steps should a company take? Are there internal steps that a company is legally or ethically required to take?

When a company uncovers potential issues, it is crucial to conduct an investigation to determine the scope and nature of any misconduct. The investigation should be set up carefully, with a focus on maintaining confidentiality and legal privilege wherever possible.

The company may need to report certain breaches to regulators or consider self-reporting or seeking immunity. Legal advice is essential before making these decisions, as the consequences can be significant. Steps should also be taken to halt any ongoing misconduct, preserve evidence and manage any disciplinary actions based on legal guidance.

35 What internal steps should a company in your country take if it receives a notice or subpoena from a law enforcement authority seeking the production or preservation of documents or data?

Compliance with compulsory document production notices is essential, as failure to comply without a reasonable excuse constitutes a criminal offence. These notices can be directed at individuals or the company's 'appropriate officer'. While the named individual does not need to coordinate the response, they must be kept informed, as they could be personally liable for non-compliance. Seeking legal advice is recommended to navigate these notices, especially for smaller organisations, to ensure proper handling and to avoid inadvertently waiving any legal rights.

When responding to a notice, companies should adopt a structured approach, ensuring reasonable efforts are made to gather and produce the required materials. This includes identifying data sources, preserving documents and ensuring that original documents and metadata are protected. The same careful approach applies when complying with a subpoena, which mandates document production for court proceedings.

36 At what point must a company in your country publicly disclose the existence of an internal investigation or contact from a law enforcement authority?

If an internal investigation is kept confidential, a company is not required to publicly disclose it. However, disclosure might be necessary if the situation cannot be contained or if there is media or market speculation. For companies under regulatory investigation, disclosure typically depends on the regulator's preferences, and regulators often request that investigations remain private unless agreed otherwise. Publicly listed companies must also consider continuous disclosure obligations. Private companies generally have no legal requirement to disclose internal investigations or law enforcement contact.

37 How are internal investigations viewed by local enforcement bodies in your country?

Local enforcement bodies in Australia generally take a pragmatic approach to internal investigations. These investigations are often seen as a positive step, especially if they demonstrate a company's commitment to addressing potential misconduct proactively. If an internal investigation remains confidential, there is typically no obligation to disclose it publicly unless circumstances require it, such as uncontrollable conduct or market speculation. Disclosure is often guided by the regulator's preferences and they may request confidentiality unless mutually agreed otherwise. However, publicly listed companies need to consider continuous disclosure obligations, which can complicate matters. For private companies, there is generally no legal requirement to disclose internal investigations or contact with law enforcement.

ATTORNEY–CLIENT PRIVILEGE

38 Can the attorney–client privilege be claimed over any aspects of internal investigations in your country? What steps should a company take in your country to protect the privilege or confidentiality of an internal investigation?

Communications made primarily for obtaining or providing legal advice or for the purpose of existing or anticipated litigation can be protected by legal professional privilege (LPP). However, if the communication serves multiple purposes, it may not be privileged. Lawyers' notes during internal investigations usually enjoy LPP, but to maintain this protection, communications should be clearly marked as confidential and privileged. A 2021 Federal Court ruling highlighted the risk of losing privilege when privileged documents are partially shared with regulators, potentially resulting in the loss of privilege for the entire document.

39 Set out the key principles or elements of the attorney–client privilege in your country as it relates to corporations. Who is the holder of the privilege? Are there any differences when the client is an individual?

LPP is held by the client, whether a company or an individual, not by the legal adviser. In some cases, employees may assert common interest or joint privilege if they reasonably believe the lawyer is providing them with legal advice and their interests align with the company. To maintain control over privileged information, companies often instruct lawyers to communicate this distinction, sometimes using a US-style *Upjohn* or corporate *Miranda* warning to ensure employees understand the context of the legal advice being given.

40 Does the attorney–client privilege apply equally to in-house and external counsel in your country?

Yes. The dominant purpose test applies to LPP, whether the lawyer is internal or external. Best practice dictates that in-house counsel should have a current practising certificate and maintain independence. Claims of privilege for advice from in-house counsel are often scrutinised, especially if the counsel also holds a non-legal role or frequently provides commercial advice, which is not covered by privilege. This ensures that the privilege is preserved and not compromised by the nature of the advice or the lawyer's role within the company.

41 Does the attorney–client privilege apply equally to advice sought from foreign lawyers in relation to investigations in your country?

Yes. Australian clients can claim the privilege if the communications are with a qualified lawyer admitted to practising in the foreign country and the communications satisfy the dominant purpose test.

42 To what extent is waiver of the attorney–client privilege regarded as a cooperative step in your country? Are there any contexts where privilege waiver is mandatory or required?

It is common for companies and individuals to assert claims of LPP. Waivers of LPP are typically limited and often occur in cooperation with regulators or when required for immunity agreements. Not claiming LPP can sometimes signal a higher level of cooperation with authorities. However, courts, tribunals or royal commissions may compel the production of documents if LPP claims are deemed invalid. Regulators are increasingly challenging LPP claims, sometimes taking disputes to court when companies withhold documents under the guise of privilege.

43 Does the concept of limited waiver of privilege exist as a concept in your jurisdiction? What is its scope?

Yes. For instance, a party responding to a compulsory notice to produce documents to the Australian Securities and Investments Commission (ASIC) may enter into a voluntary confidential LPP disclosure agreement, which allows the production of the documents to

ASIC, while arguably protecting them from disclosure to third parties. ASIC will undertake to treat the information as confidential and will defer to the privilege holder if ASIC is compelled to produce the documents. These agreements have not been tested by the courts as to whether they will withstand a challenge.

44 If privilege has been waived on a limited basis in another country, can privilege be maintained in your own country?

When considering whether privilege still applies after a waiver, key factors include the context of the waiver (whether it was voluntary or compelled), how the information was used after the waiver and whether, under Australian law, privilege can still be maintained over the information. These considerations are crucial in determining whether the waiver affects the privileged status of the information in future legal contexts.

45 Do common interest privileges exist as concepts in your country? What are the requirements and scope?

Common interest privilege does exist in Australia. For this privilege to apply, the parties involved must share the same, or nearly the same, legal interest, such that they could be represented by the same lawyer. This privilege is not available if the parties have potentially adverse interests. While there is no requirement for a formal agreement or for the parties to declare an intention to claim the privilege at the time of communication, it is advisable to clarify these aspects to solidify the common interest and the extent of the privilege.

46 Can privilege be claimed over the assistance given by third parties to lawyers?

It is not uncommon for lawyers to engage third-party experts to assist in matters related to legal advice. Communications with these experts are typically covered by LPP if they meet the dominant purpose test. However, if a party serves a report or advice from a third party during litigation, all related materials, including briefing documents, generally become discoverable. There are only limited circumstances in which a party can resist the production of these underlying communications.

WITNESS INTERVIEWS

47 Does your country permit the interviewing of witnesses as part of an internal investigation?

In Australia, the interviewing of witnesses as part of an internal investigation is generally permitted and is a common practice in both the public and private sectors.

In fact, interviews may be a mandatory component of an internal investigation ordered at the request of certain bodies, such as the Independent Commission Against Corruption (per the Independent Commission Against Corruption Act 1988 (NSW), Section 54(2)) or be seen as necessary components to properly satisfy other obligations, such as financial reporting obligations.

48 Can a company claim the attorney–client privilege over internal witness interviews or attorney reports?

In Australia, witness interviews and reports prepared by lawyers for the dominant purpose of giving or receiving legal advice or in the preparation of legal proceedings are usually protected by professional privilege.

However, courts will carefully scrutinise the purpose of the interviews and reports in the context of the investigation to determine whether privilege is claimable, as well as whether privilege has been waived.

For example, in *TerraCom Ltd v. Australian Securities and Investments Commission* ([2022] FCA 208), the Federal Court of Australia held that the company waived privilege over a forensic investigation report that was obtained by legal advisers who were advising the company on terminating its commercial general manager, by making public statements that relied on the report's findings. Although reference was only made to part of the report, privilege was waived over the whole report as the Court held that complete waiver was required to provide the necessary context.

Legal professional privilege will not usually attach to notes taken by interviewees or a support person (unless created by the interviewee's appointed legal representative attending to advise the interviewee).

49 When conducting a witness interview of an employee in your country, what legal or ethical requirements or guidance must be adhered to? Are there different requirements when interviewing third parties?

The exact legal requirements applicable in conducting interviews of employees or third parties may vary depending on which state or territory law applies, which may, in turn, depend on other factors such as where the interview is taking place and where the employer carries on its business. Legal requirements may include the following:

- the manner in which the investigation is recorded (for example, in New South Wales, all persons present must consent to an audio recording before one can be taken, per the Surveillance Devices Act 2007 (NSW), Section 7);
- the handling of certain information obtained in interviews (for example, the Privacy Act 1988 (Cth) applies across Australia and regulates the handling of individuals' personal information). This legislation may be in addition to state-specific legislation, such as the Privacy and Personal Information Protection Act 1998 (NSW) for the public sector; and
- confidentiality, protections and prohibitions in relation to whistleblowers, such as the victimisation prohibitions under Section 1317AC of the Corporations Act 2001 (Cth).

Attention may also be best paid to legal requirements and guidance of evidence gathering and use in the litigation context, such as the Evidence Act 1995 (Cth). Further still, proper consideration should be given to the requirements under the Fair Work Act 2009 (Cth) and anti-discrimination laws such as the Sex Discrimination Act 1984 (Cth), the Racial Discrimination Act 1975 (Cth) and the Disability Discrimination Act 1992 (Cth).

It is best practice to ensure that every interview meets basic procedural fairness, including giving the witness a proper opportunity to consider and respond to any questions. The precise ethical guidance would depend on several factors, including the nature and gravity of the issue being investigated and the industry in which it is taking place.

50 How is an internal interview typically conducted in your country? Are documents put to the witness? May or must employees in your country have their own legal representation at the interview?

In Australia, there are no requirements for internal interviews and the manner will depend on several factors, such as the nature and gravity of the situation or allegations being investigated and the industry in which it is taking place.

It is also common practice (but not mandatory) to allow the interviewee the opportunity to have an independent person (whether support or employee representative) attend alongside them.

REPORTING TO THE AUTHORITIES

51 Are there circumstances under which reporting misconduct to law enforcement authorities is mandatory in your country?

Yes, there are several circumstances under which reporting misconduct to law enforcement authorities is mandatory in Australia, which may depend on such things as the industry sector (e.g., financial services), specific characteristics of the entity (e.g., size or revenue) and the circumstances reaching certain thresholds (e.g., seriousness, reasonableness).

Relevant regimes include the following:

- the anti-money laundering or counterterrorism financing regime, which requires regulated entities to report all suspicious matters to the Australian Transaction Reports and Analysis Centre, including when the entity suspects on reasonable grounds that the client is not who they say they are or that the entity has information relevant to tax evasion, criminal offences or proceeds of crime (see the Anti-Money Laundering and Counter-Terrorism Financing Act 2006 (Cth), Section 41);
- licensing regimes, such as obligations on Australian financial and credit licensees to compile a report where there are reasonable grounds to believe there is a 'reportable situation', which includes where a licensee (or representative) has engaged in gross negligence (in providing a financial or credit service) or committed serious fraud (see, e.g., the Corporations Act 2001 (Cth), Section 912D and the National Consumer Credit Protection Act 2009 (Cth), Section 50A);
- workplace safety regimes, such as obligations on persons conducting business to notify the regulator of a death, serious injury or illness, or dangerous incident (see, e.g., the Work Health and Safety Act 2011 (NSW), Part 3); and
- certain criminal regimes, such as the Crimes Act 1900 (ACT), which requires any adult to report to the police information that leads them to reasonably believe that a sexual offence has been committed against a child (see Section 66AA).

There are also reporting obligations that apply generally to entities or are dependent on circumstances beyond 'misconduct' (e.g., statutory requests, such as a Section 19 notice from the Australian Sanctions Office or a Section 353-10 notice from the Australian Taxation Office).

52 In what circumstances might you advise a company to self-report to law enforcement even if it has no legal obligation to do so? In what circumstances would that advice to self-report extend to countries beyond your country?

Where a company becomes aware that misconduct has occurred, factors on whether the entity should report the misconduct, notwithstanding a legal obligation to do so, may include:

- the nature of the misconduct;
- how long ago the misconduct occurred;
- what has occurred since the misconduct; and
- the consequences of the misconduct to date (as well as the prospective consequences).

Self-reporting possible criminal conduct or professional misconduct can have a variety of advantages, including:

- proactively addressing the misconduct;
- establishing a cooperative relationship with the regulator or investigative authority;
- increasing control of the messaging, which may minimise reputational damage;
- limiting liability; and
- maximising sentencing discount.

Whether we would advise to self-report beyond Australia depends on a range of factors, including where the conduct occurred, where the consequences of the conduct unfolded and whether any other country was involved in any respect. It is likely that the advice would require the engagement of foreign lawyers.

53 What are the practical steps needed to self-report to law enforcement in your country?

Depending on the circumstances, practical steps needed to self-report to law enforcement in Australia may include the following:

- adopting an appropriate approach: a company must be prepared to genuinely cooperate;
- conducting an internal investigation: the nature and detail of which will likely depend on the nature of the circumstances at hand;
- communication channels: a company should appoint a point of contact with the law enforcement, determine internal and external communication policies, and consider appointing a project manager (depending on the complexity) with appropriate resources. This should consider privileges;

- data retention and management, which includes identifying the relevant documentary evidence (as well as relevant personnel), protecting this material (or people) from tainting (by personnel or through handling), including protecting backups and ensuring retention policies do not result in loss of evidence, and considering whether a privilege applies, such as legal professional privilege, accounting privilege or self-incrimination. This will likely require reference to how any relevant (domestic or foreign) authorities may expect evidence to be handled;
- employee management: certain employees may need to be moved or suspended, and a company will need to properly allocate resources to ensure employees can genuinely cooperate in any consequences from self-reporting (e.g., investigation);
- business management: there may need to be an immediate response, such as freezing transactions or certain services being provided;
- notifications, such as insurance (to trigger coverage); and
- public relations management: it may be worthwhile considering whether the issue is, or is expected to be, publicly disclosed and whether the entity should release a proactive or reactive public statement, which must be properly considered to avoid undermining the self-reporting.

RESPONDING TO THE AUTHORITIES

54 In practice, how does a company in your country respond to a notice or subpoena from a law enforcement authority? Is it possible to enter into dialogue with the authorities to address their concerns before or even after charges are brought? How?

Corporations must comply with formal notices or subpoenas and law enforcement authorities are under no obligation to enter into a dialogue with the corporation. Nevertheless, enforcement authorities are increasingly open to engaging at the investigation stage. Opening a dialogue with authorities can enable issues such as scope and production time frames to be modified while allowing for greater cooperation, reducing the resources needed on both sides. Generally speaking, it can be sufficient that the corporation reaches out to the authority or authorising officer and asks to discuss compliance with the notice or subpoena.

55 Are ongoing authority investigations subject to challenge before the courts?

There is limited capacity to challenge an ongoing investigation. However specific investigative mechanisms, such as a search warrant, can be challenged through judicial review. Alternatively, a civil action could be brought if there are grounds to show that officers engaged in conduct that was invalid or beyond their power.

56 In the event that authorities in your country and one or more other countries issue separate notices or subpoenas regarding the same facts or allegations, how should the company approach this?

Subpoenas and notices must be complied with. A corporation may reach out to the relevant authorities and seek to negotiate a request consistent in scope or a single response, particularly in instances where the authorities are already working together to investigate the alleged conduct.

57 If a notice or subpoena from the authorities in your country seeks production of material relating to a particular matter that crosses borders, must the company search for and produce material in other countries to satisfy the request? What are the difficulties in that regard?

Corporations must produce material that is in their 'possession, custody or control', irrespective of where it is located. In *Maxi EFX Global AU Pty Ltd v. Australian Securities and Investments Commission* ([2021] FCAFC 59), the Full Federal Court considered whether a corporation was required to produce material said to be in the physical possession of third-party service providers based overseas. The Court held that the corporation was required to produce the material. It noted that the relevant test was concerned less with who was the legal proprietor of the material, than whether the corporation had the practical capacity to access it.

58 Does law enforcement in your country routinely share information or investigative materials with law enforcement in other countries? What framework is in place in your country for cooperation with foreign authorities?

Australian law enforcement agencies regularly share information with law enforcement in other countries through a variety of mechanisms. Law enforcement can formally request the collection and provision of evidence under mutual legal assistance treaties; however, authorities in Australia also regularly exchange information through partnerships and informal information-sharing and intelligence-gathering agreements. For example, the Australian Federal Police and other Australian intelligence agencies are part of the Five Eyes Law Enforcement Group, which is an enforcement partnership with agencies from Canada, the UK and the US, which facilitates intelligence sharing to combat specific crime typologies.

59 Do law enforcement authorities in your country have any confidentiality obligations in relation to information received during an investigation or onward disclosure and use of that information by third parties?

Intelligence information is routinely shared between agencies within limits imposed by statute. For example, the Australian Crime Commission Act 2002 (Cth) limits who

the Australian Criminal Intelligence Commission can share information with. Material intercepted by telecommunications, for example, can only be shared with a small number of listed entities.

60 How would you advise a company that has received a request from a law enforcement authority in your country seeking documents from another country, where production would violate the laws of that other country?

We would advise that the company reaches out to the relevant law enforcement authorities as soon as possible. It may be that the scope of the request can be altered to exclude the information at issue. However, if a company refuses to comply with a formal notice or request, the authority can take enforcement action against the company and the corporation would have to defend its possession in court.

61 Does your country have secrecy or blocking statutes? What related issues arise from compliance with a notice or subpoena?

Australia has blocking statutes under Section 42 of the Foreign Evidence Act 1994 (Cth) and Section 7 of the Foreign Proceedings (Excess of Jurisdiction) Act 1984 (Cth). Under these provisions, the Australian Attorney-General can make an order prohibiting the production of information sought by a foreign state.

62 What are the risks in voluntary production versus compelled production of material to authorities in your country? Is this material discoverable by third parties? Is there any confidentiality attached to productions to law enforcement in your country?

The primary risk in the voluntary production of material compared to compelled production relates to the right against self-incrimination. The Commonwealth laws that enable law enforcement agencies to force the production of information typically also require that the answers or documents are not admissible against the person in criminal or civil proceedings. As a result, while material that could be incriminating must be produced, its subsequent use is restricted. If the material is supplied voluntarily, these limitations do not apply, and the material can be used against the person or corporation that supplied it.

PROSECUTION AND PENALTIES

63 What types of penalties may companies or their directors, officers or employees face for misconduct in your country?

Both individuals and corporations can receive criminal or civil penalties in Australia.

Civil penalties

For breaches of corporate laws, the maximum civil penalty that can be imposed on an individual is the greater of 5,000 penalty units (A$1.565 million) or three times the benefit obtained and detriment avoided. The maximum civil penalty that can be imposed on companies is the greater of:

- 50,000 penalty units (A$15.65 million);
- three times the benefit obtained and detriment avoided; or
- 10 per cent of annual turnover, capped at 2.5 million penalty units (A$782.5 million).

Criminal penalties

The Criminal Code provides a statutory framework for corporate criminal responsibility and prescribes that the Criminal Code applies to corporations in the same way as it applies to individuals. However, only individuals can face imprisonment while both individuals and corporations can incur punitive fines.

Specific offences for directors and company officers

In Australia, company directors and officers can be personally prosecuted for offences related to their corporate responsibilities and conduct. Commonly prosecuted financial crime offences personally applicable to company directors and officers include failing to keep correct financial records, falsifying accounting records, insider trading offences, insolvent trading, fraud and deception, involvement in bribery or corrupt practices, and manipulation of the market in relation to the Australian stock exchange securities trading.

64 Where there is a risk of a corporate's suspension, debarment or other restrictions on continuing business in your country, what options or restrictions apply to a corporate wanting to settle in another country?

At the federal level, Australia does not suspend or disbar corporations as a punitive measure. However, in 2022, the state of Western Australia imposed Australia's first disbarment regime. Under this scheme, businesses that engage in specifically listed conduct can be banned from doing business with Western Australian government agencies for up to five years. The details of the disbarred business are published on a publicly accessible register. Conduct that could result in disbarment includes the following:

- Category A conduct, which includes offences and contraventions of specific provisions of the state and Commonwealth legislation listed in Schedule 1 of the Procurement Act 2020 and Procurement (Debarment of Suppliers) Regulations 2021 (the Regulations), most of which are offences that may lead to a conviction under criminal law;
- Category B conduct, which includes offences and contraventions of the state and Commonwealth legislation listed in Schedule 2 of the Regulations; and
- conduct that is not within Category A or B, but is likely to have a material adverse effect on the integrity of, or public confidence in, government procurement.

65 What do the authorities in your country take into account when fixing penalties?

Penalties under the Criminal Code vary depending on the seriousness of the offence and the offender's degree of knowledge (i.e., intentional or reckless). In 2019, the Treasury Laws Amendment (Strengthening Corporate and Financial Sector Penalties) Act 2019 was introduced, increasing penalties for those who breach corporate laws. This included increasing the maximum prison term to 15 years, which applies for the most serious breaches of directors' duties, as well as false or misleading disclosure and dishonest conduct.

RESOLUTION AND SETTLEMENTS SHORT OF TRIAL

66 Are non-prosecution agreements or deferred prosecution agreements available in your jurisdiction for corporations?

Australia does not have a specific framework for deferred prosecution agreements (DPAs). There have been two attempts to introduce a DPA scheme through the Crimes Legislation Amendment (Combatting Foreign Bribery) Bill, one in 2017 and one in 2019, both of which lapsed.

Without a formal DPA scheme, Australian prosecutors rely on other mechanisms, such as enforceable undertakings or negotiated settlements, to resolve corporate crime cases outside of the courtroom.

67 Does your jurisdiction provide for reporting restrictions or anonymity for corporates that have entered into non-prosecution agreements or deferred prosecution agreements until the conclusion of criminal proceedings in relation to connected individuals to ensure fairness in those proceedings?

Not applicable in this jurisdiction.

68 Prior to any settlement with a law enforcement authority in your country, what considerations should companies be aware of?

Before settling with law enforcement authorities during a government investigation, companies should carefully consider several key factors. First, the settlement should include a non-admission clause to prevent any acknowledgement of liability that could impact future legal proceedings. It is also advisable to negotiate terms to preclude the referral of the matter for criminal prosecution, thereby avoiding further legal complications. Confidentiality and non-dissemination clauses are vital to safeguard the company's reputation by restricting public access to settlement details and investigation outcomes. Additionally, companies should ensure that compliance and remediation requirements are addressed, assess the legal and financial implications, and develop a public relations strategy to manage communications and stakeholder trust effectively.

69 To what extent do law enforcement authorities in your country use external corporate compliance monitors as an enforcement tool?

Australian law enforcement authorities, including the Australian Competition and Consumer Commission and the Australian Securities and Investments Commission (ASIC), do not commonly use external corporate compliance monitors as an enforcement tool. Instead, they favour enforceable undertakings in which companies commit to implementing internal compliance programmes. While these undertakings may involve independent auditors or experts to review and report on compliance, the use of long-term external monitors is not a central feature of the Australian regulatory approach. The focus is on ensuring that companies maintain compliance internally, with oversight provided through regular reporting to the authorities.

70 Are parallel private actions allowed? May private plaintiffs gain access to the authorities' files?

Yes, parallel private actions are allowed in Australia, but a stay of civil proceedings may be warranted if there is a real risk of prejudice to the accused's defence in a criminal trial. However, this risk must be weighed against the potential prejudice caused by staying the civil proceeding (e.g., *Commissioner of Australian Federal Police v. Zhao* ((2015) 255 CLR 46) at [35] and *CFMEU v. ACCC* ([2016] FCAFC 97) at [22]).

Private plaintiffs can gain access to authorities' files by applying for a notice to produce or subpoenas. Alternatively, they may consider freedom of information requests, but the Freedom of Information Act 1982 (Cth) restricts access to documents that could prejudice law enforcement or investigations (Sections 37 and 47E). In some instances, ASIC may exercise the power to provide certain types of information or documents to private litigants, including transcripts of examination and company books, unless the disclosure could potentially compromise an ASIC investigation or enforcement action.

PUBLICITY AND REPUTATIONAL ISSUES

71 Outline the law in your country surrounding publicity of criminal cases at the investigatory stage and once a case is before a court.

During the investigatory stage, publicity is limited to safeguard ongoing investigations and the rights of those involved. Confidentiality may be mandated by statutory obligations; for example, Section 127 of the Australian Securities and Investments Commission Act 2001 requires the confidentiality of information acquired by the Australian Securities and Investments Commission (ASIC) during investigations conducted under Section 25. Additionally, confidentiality may be enforced through potential suppression and non-publication orders by courts, pursuant to Section 37AF of the Federal Court of Australia Act 1976 (Cth). Premature publication can lead to contempt of court and defamation risks.

Once charges are laid and the case is before a court, proceedings are generally public under the principle of open justice. However, restrictions may still apply under the *sub judice* rule or through suppression orders under the Uniform Evidence Acts (the

Evidence Act 1995 (Cth), the Evidence Act 1995 (NSW), etc.) to ensure a fair trial. Media reporting must be accurate to avoid defamation, with some protection afforded by fair reporting privilege.

72 What steps do you take to manage corporate communications in your country? Is it common for companies to use a public relations firm to manage a corporate crisis in your country?

It is crucial that all internal stakeholders, including employees and management, are informed about the investigation and the company's response plan. This includes a review of the statements to avoid self-incrimination or disclosing sensitive information.

It is common for Australian companies to engage public relations firms during a corporate crisis. Public relations firms help manage the company's image, develop strategic messaging and handle media relations to mitigate reputational damage.

73 How is publicity managed when there are ongoing related proceedings?

Publicity regarding ongoing related proceedings may be restricted by court suppression and non-publication orders.

Both the Australian Competition and Consumer Commission (ACCC) and ASIC issue media releases about the commencement and outcomes of court or tribunal proceedings. The ACCC Media Code of Conduct specifically advises against commenting on factual matters during proceedings. The Commonwealth Director of Public Prosecutions adopts a case-by-case approach to media requests for active cases in court.

DUTY TO THE MARKET

74 Is disclosure to the market in circumstances where a settlement has been agreed but not yet made public mandatory?

Under Australian Securities Exchange Listing Rule 3.1, a company must immediately disclose a material settlement that could impact its share price. If the settlement is confidential and pending final negotiations or approvals, disclosure can be deferred under Rule 3.1A. The Australian Securities and Investments Commission advises assessing materiality case by case, meaning disclosure might be required even if the settlement is still pending. Once the settlement is finalised and deemed material, it must be disclosed promptly. Companies should evaluate the settlement's materiality, maintain confidentiality if applicable and be ready to disclose as required.

ENVIRONMENTAL, SOCIAL AND CORPORATE GOVERNANCE

75 Does your country regulate environmental, social and governance matters?

The Australian regulatory landscape for environmental, social and governance (ESG) matters includes both mandatory reporting obligations and quasi-regulation through guidelines.

Corporations Act 2001

Listed companies are required to disclose information that shareholders would reasonably need to assess their operations, financial position and business strategies. This includes climate-related disclosures, where companies must report on how climate risks are integrated into their risk management and financial planning processes. Additionally, the Australian Prudential Regulation Authority has issued guidelines emphasising the importance of considering climate-related financial risks for financial institutions.

National Greenhouse and Energy Reporting Act 2007

Companies that exceed specific thresholds are required to report their greenhouse gas emissions, energy production and energy consumption to the Clean Energy Regulator.

Workplace Gender Equality Act

Private sector organisations with 100 or more employees must file an annual report with the Workplace Gender Equality Agency. This report covers gender equality policies and strategies, actions taken to promote gender equality, work/life balance initiatives and employee support measures, including policies on paid parental leave and gender discrimination.

Modern Slavery Act 2018

Large companies with consolidated revenue of A$100 million or more must publish their annual modern slavery statements in the Australian government's online Modern Slavery Statements Register, to report on the risks of modern slavery within their operations and supply chains, as well as the actions taken to mitigate these risks.

ASX corporate governance principles and recommendations

The Australian Stock Exchange (ASX) provides guidelines recommending that listed companies disclose any material exposure to environmental or social risks and how these risks are managed. The ASX updated these principles in 2019, reinforcing the 'disclose or explain' approach, whereby companies must either follow the recommended practices or provide an explanation for any deviations. This corporate governance statement must be included in the company's annual report or published on its website.

76 Do you expect to see any key regulatory or legislative changes emerge in the next year or so designed to address environmental, social and governance matters?

Significant regulatory changes related to ESG matters, particularly climate reporting, are anticipated in Australia within the next year. The Treasury Laws Amendment (Financial Market Infrastructure and Other Measures) Bill 2024, currently under Senate consideration, is expected to mandate climate-related disclosures for large entities from January 2025. The legislation will be implemented in phases, with Group 1 entities reporting first in FY24–25, followed by Groups 2 and 3 in subsequent years. Disclosures will include governance, emissions data and scenario analyses aligned with the Paris Agreement.

On 11 June 2024, the Modern Slavery Amendment (Australian Anti-Slavery Commissioner) Bill 2023 received royal assent. This Bill amends the Modern Slavery Act 2018 and establishes the Australian Anti-Slavery Commissioner. However, the Law Council of Australia advocates for further amendments to introduce civil penalties for non-compliance with reporting requirements and additional regulatory tools to enhance compliance.

77 Has there been an increase in related litigation, investigations or enforcement activity in recent years in your country?

Australia has seen a marked rise in ESG-related litigation and enforcement in recent years.

Following its review of greenwashing, which concluded in July 2021, the Australian Securities and Investments Commission (ASIC) initiated one civil penalty proceeding, issued 11 infringement notices and secured 23 corrective disclosure outcomes against misleading conduct and unsustainable greenwashing claims between 1 July 2022 and 31 March 2023. As at August 2024, ASIC has commenced three greenwashing proceedings in the Federal Court. Noteworthy cases include victories against Mercer Superannuation (Australia) Limited, Vanguard Investments Australia Ltd and Active Super. ASIC's enforcement priorities for 2024 continue to focus on misleading conduct in sustainable finance, including greenwashing.

The Australian Competition and Consumer Commission (ACCC) first identified environmental and sustainability claims as an enforcement priority in 2022. On 18 April 2024, the ACCC initiated its first greenwashing proceeding against Clorox Australia Pty Ltd, marking the beginning of its greenwashing enforcement actions in the courts.

Additionally, there have been the following private challenges to government actions or inactions:

- *Pabai Pabai v. Commonwealth*: In 2021, Torres Strait Islanders sued the Australian government for failing to reduce carbon emissions, arguing that this inaction threatens their communities with forced migration due to climate change. The Federal Court has yet to make its decision in this matter.

- *Class action against Toyota*: In October 2022, a class action was filed in the Supreme Court of Victoria alleging that Toyota fitted certain vehicles with diesel defeat devices, causing them to emit unlawfully high levels of nitrogen oxide during real-world use, despite passing regulatory tests.
- *Environment Protection Authority v. Sydney Water* ([2023] NSWLEC 2): Filed in December 2022, this case resulted in Sydney Water being fined A$200,000 for environmental harm caused by a sewage spill. The penalty included funding for a local environmental project, reflecting the growing enforcement of environmental regulations and corporate accountability for environmental damage.

ANTICIPATED DEVELOPMENTS

78 Do you expect to see any key regulatory or legislative changes emerge in the next year or so designed to address corporate misconduct?

In 2023, the Australian Law Reform Commission (ALRC) published its final report, 'Confronting Complexity: Reforming Corporations and Financial Services Legislation' (Report 141, 2023), which was tabled in Parliament in 2024. The Report found that legislation governing Australia's financial services industry was difficult to navigate, costly to comply with and difficult to enforce. The ALRC has made 58 recommendations to simplify the law, including a revamped legislative framework for the financial services sector. These reforms aim to reduce costs for service providers and consumers, improve productivity by reducing complexity and provide clarity around compliance requirements and enforcement. Thirteen recommendations made during the inquiry have already been implemented, in full or in part, by legislation passed during 2023. The following recommendations are expected to be implemented in the near future, which will bring legislative change to the financial services sector:

- The Crimes Legislation Amendment (Combatting Foreign Bribery) Bill 2023 introduces expanded foreign bribery offences for corporations, reflecting Australia's dedication to tackling foreign bribery. This legislation aims to simplify the process for prosecutors to take action against corporations involved in these activities. Passed in 2024, the Bill establishes a new offence for corporations that fail to prevent foreign bribery and broadens the existing offence by including a wider range of public officials and types of conduct. However, unlike previous bills, it does not include a deferred prosecution agreement (DPA) regime. The introduction of a DPA scheme has been deferred until after the new measures have been implemented and assessed. A statutory review is scheduled in 18 months, during which Parliament will evaluate whether a DPA regime should be introduced. Given that both the United States and the United Kingdom have DPA regimes in place, future legislative changes could be made for Australia.
- The Banking Executive Accountability Regime (BEAR) and its successor, the Financial Accountability Regime (FAR), are significant regulatory frameworks in Australia designed to improve accountability among senior executives and directors within the financial services industry. FAR is an expansion and enhancement of BEAR, extending the principles of accountability beyond the banking sector to cover a broader range of financial services entities, including insurers, superannuation funds

and other financial institutions. FAR is being introduced gradually, with the aim of eventually covering most financial services industries in Australia from 2025. Unlike BEAR, FAR applies to a broader range of financial entities regulated by both the Australian Prudential Regulation Authority (APRA) and the Australian Securities and Investments Commission (ASIC). This includes general insurers, life insurers, private health insurers, superannuation entities and non-bank lenders. Under FAR, both APRA and ASIC have enforcement powers. The implementation of FAR is expected to have a positive impact on reducing corporate misconduct in Australia's financial services sector.

Acknowledgements

The authors would like to acknowledge the work of Richard Boesel, Thalia Kladis and Doris Lee in the preparation of this chapter.