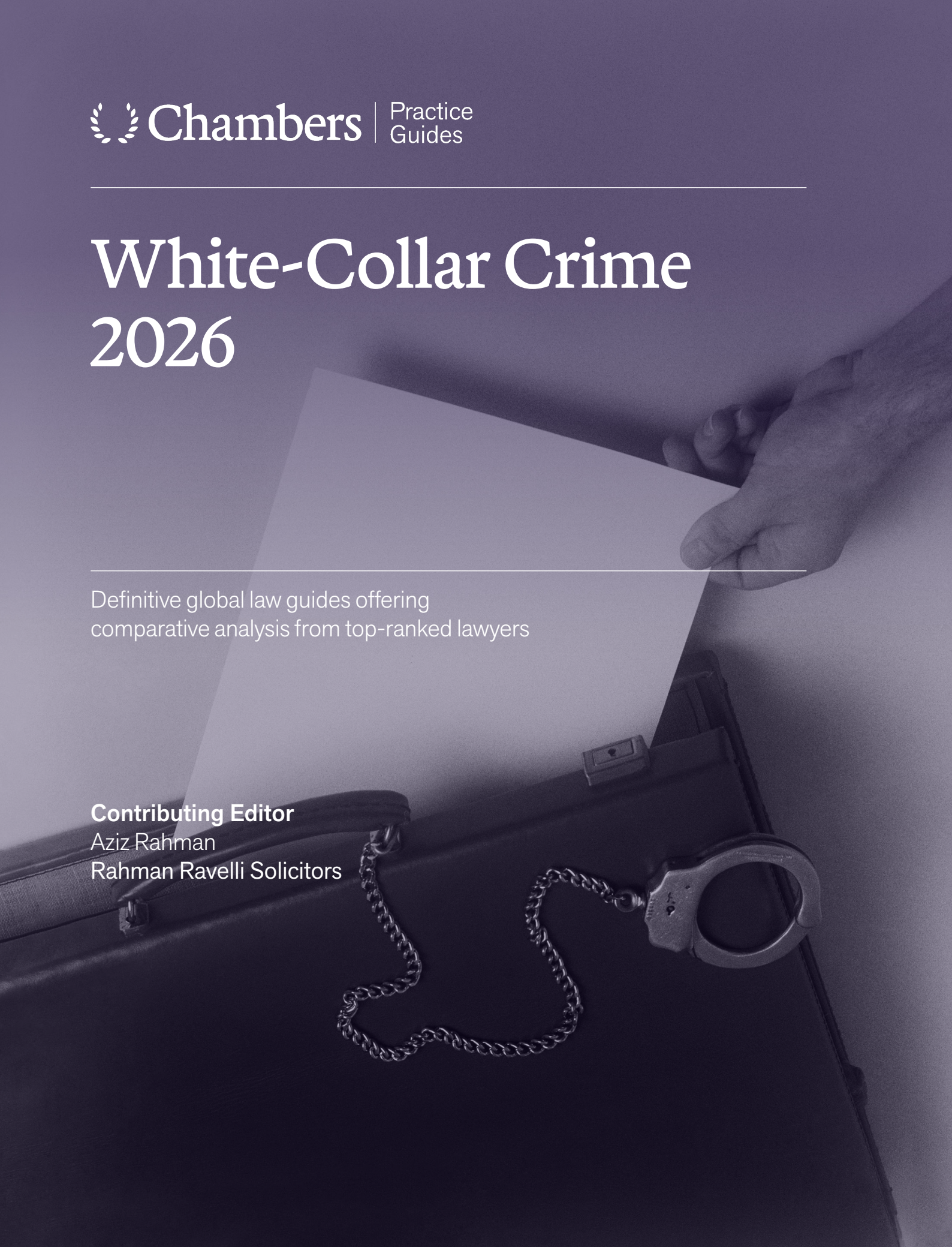
Chambers | Practice Guides

White-Collar Crime 2026



Definitive global law guides offering comparative analysis from top-ranked lawyers

Contributing Editor
Aziz Rahman
Rahman Ravelli Solicitors

AUSTRALIA



Law and Practice

Contributed by:
Dennis Miralis, Kartia Zappavigna, Jessica Semsarian and Olivia McDonald
Nyman Gibson Miralis

Contents

1. Criminal Law P.11
1.1 Criminal Offences p.11
1.2 Burden of Proof p.11
1.3 Statute of Limitations p.11
1.4 Extraterritorial Reach and Cross-Border Co-Operation p.12
1.5 Corporate and Personal Liability p.12
1.6 Sentencing and Penalties p.13
1.7 Damages and Compensation p.13

2. Enforcement P.13
2.1 White-Collar Enforcement Authorities p.13
2.2 Initiating an Investigation p.14
2.3 Powers of Investigation p.14
2.4 Use of Technology in Investigations p.15
2.5 Internal Investigations p.15
2.6 Prosecution p.15
2.7 Deferred Prosecution p.16

3. White-Collar Offences P.16
3.1 Criminal Company Law and Corporate Fraud p.16
3.2 Bribery, Influence Peddling and Related Offences p.16
3.3 Anti-Bribery Regulation p.17
3.4 Insider Dealing, Market Abuse and Criminal Banking Law p.17
3.5 Tax Fraud p.18
3.6 Financial Record-Keeping p.18
3.7 Cartels and Criminal Competition Law p.19
3.8 Consumer Criminal Law p.19
3.9 Cybercrimes, Computer Fraud and Protection of Company Secrets p.20
3.10 Financial/Trade/Customs Sanctions p.20
3.11 Concealment p.21
3.12 Aiding and Abetting p.21
3.13 Money Laundering p.22
3.14 ESG-Related Offences p.22
3.15 Artificial Intelligence and Automation Misuse p.22
3.16 Crypto-Assets and Digital Currency Crimes p.23

4. Pleas and Defences P.23
4.1 White-Collar Defences p.23
4.2 De Minimis p.24
4.3 Plea Agreements, Co-Operation, Self-Disclosure and Leniency p.24
4.4 Whistle-Blower Protection p.24
4.5 Cross-Border Defence Strategies p.24

5. Key Trends and Future Outlook P.25
5.1 The Year Ahead p.25

Nyman Gibson Miralis is an international, award-winning criminal defence law firm based in Sydney, Australia. For more than 55 years, the firm has been leading the market in all aspects of general, complex and international crime and is widely recognised for its involvement in some of Australia's most significant criminal cases. Nyman Gibson Miralis' international law practice focuses on white-collar and corporate crime, transnational financial crime, international sanctions, bribery and corruption, international money laundering, cybercrime, international asset freezing/forfeiture, extradition and mutual assistance law. The team strategically advises and appears in matters where cross-border investigations and prosecutions are conducted in parallel jurisdictions, involving some of the largest law enforcement agencies and financial regulators worldwide. Working with the firm's international partners, Nyman Gibson Miralis has advised and acted in investigations involving the USA, Canada, UK, EU, China, Hong Kong, Singapore, Taiwan, Macao, Vietnam, Cambodia, Russia, Mexico, South Korea, British Virgin Islands, New Zealand and South Africa.

Authors



Dennis Miralis of Nyman Gibson Miralis is a leading Australian defence lawyer who specialises in international criminal law, with a focus on complex multi-jurisdictional regulatory investigations and prosecutions. His areas of expertise include international sanctions, cybercrime, global investigations, proceeds of crime, bribery and corruption, AML, worldwide freezing orders, national security law, INTERPOL Red Notices, extradition and mutual legal assistance law. Dennis advises individuals and companies under investigation for economic crimes both locally and internationally. He has extensive experience in dealing with all major Australian and international investigative agencies.



Kartia Zappavigna is an international criminal lawyer whose practice focuses on AML/CTF, UN and Australian sanctions compliance, anti-bribery and corruption, whistleblower protections, the Foreign Influence Transparency Scheme, AUSTRAC registration, notifiable data breach reporting and human rights and fair trials.



Jessica Semsarian is a defence lawyer assisting the white-collar crime team at Nyman Gibson Miralis. She has previous experience in financial services and corporate law, where she developed expertise in anti-money laundering and counter-terrorism financing compliance, financial services regulation and general corporate law. Jessica holds a LLB (First Class Honours) and a BA in international security studies from the Australian National University, specialising in international and comparative law.



Olivia McDonald is a solicitor in the white-collar crime team where she assists in complex tax and business crime investigations. Olivia has also previously worked on serious offences, including Trials, Sentences and Special Hearings in both the District and Supreme Court. She holds a LLB from the University of Technology Sydney.

Nyman Gibson Miralis

Level 9
299 Elizabeth Street
Sydney
NSW 2000
Australia

Tel: +61 292 648 884
Email: dm@ngm.com.au
Web: www.ngm.com.au

1. Criminal Law

1.1 Criminal Offences

Australia is a federal system. Commonwealth, state and territory laws legislate criminal offences and penalties, with different rules and procedures applying depending on the jurisdiction. Across these jurisdictions, offences are classified as either summary or indictable, with summary offences being considered less serious than indictable offences.

The jurisdictions treat this classification differently. At the Commonwealth level, the maximum penalty determines whether the offence is summary or indictable. Summary offences carry a maximum imprisonment of no more than a year whilst indictable offences carry imprisonment over a year (see the Crimes Act 1914 (Cth), Section 4H; and the Crimes Act 1914 (Cth), Section 4G).

Generally, an accused person is convicted only if the prosecution proves beyond reasonable doubt both the physical and mental elements (actus reus and mens rea, respectively) of the offence. The required mental element depends on the offence and may be intention, knowledge, recklessness or negligence. However, with strict or absolute liability offences, the prosecution does not need to prove the mental element. In Australia, the prosecution need not prove motive; it is primarily a sentencing factor.

Both Australian common law and statute recognise several forms of extended criminal liability. The Commonwealth Criminal Code Act 1995 (the "Criminal Code") sets out specific provisions for attempt, complicity, innocent agency, incitement and conspiracy. Someone found guilty under attempt, complicity, innocent agency or conspiracy "is taken to have committed that offence and is punishable accordingly". Only "incitement" entails a lesser degree of punishment.

1.2 Burden of Proof

As in any other criminal prosecution in Australia, the accused in white-collar proceedings is presumed innocent until proven guilty. To secure a conviction, the prosecution must prove each element of the alleged offence beyond a reasonable doubt, in law and in fact. The accused can raise a positive defence but must discharge only an evidential burden on the balance of probabilities, which the prosecution must refute beyond a reasonable doubt.

1.3 Statute of Limitations

Under Section 15B of the Crimes Act 1914 (Cth), Commonwealth offences with a maximum penalty of less than six months' imprisonment have a 12-month limitation period and those with a maximum penalty of more than six months' imprisonment have no limitation period. Offences that attract only a pecuniary (financial) penalty and no term of imprisonment, have a 12-month limitation period.

In New South Wales (NSW), offences with penalties of under two years' imprisonment have a six-month limitation period. However, under the Fines Act 1996 (NSW), Section 37A(2), an individual can be issued a penalty notice fine up to 12 months after the offence. NSW has no limitation period for indictable offences.

No specific statute of limitation addresses the concealment of offences or continuing offences. This is likely because the statute of limitations for criminal prosecutions applies only to minor offences.

1.4 Extraterritorial Reach and Cross-Border Co-Operation

Australian law makes provisions for the extraterritorial application of criminal jurisdiction at the federal level. "Standard geographical jurisdiction" applies when either the conduct or the result of the offence took place wholly or partially in Australia (Division 14 of the Criminal Code). "Extended geographical jurisdiction" is set out under Division 15 of the Criminal Code and provides for four categories.

- Category A: The person charged was either an Australian citizen or a body corporate incorporated under Australian law at the time of the offence.
- Category B: The person charged was an Australian resident at the time of the offence.
- Category C: Unrestricted extraterritoriality on the person charged – this applies whether or not the conduct or the result of the conduct constituting the alleged offence occurs in Australia. However, a defence may be available depending on the law of the foreign country where the conduct occurs.
- Category D: Unrestricted extraterritoriality but with no foreign law defence.

Extended geographical jurisdiction applies to several white-collar offences including money laundering, fraud and offences involving the use of carriage services.

At the state level, Part 1A of the Crimes Act 1900 (NSW) provides for a limited extension of geographical jurisdiction, which requires a nexus between the state and the offence. The crime must be committed wholly or partly in the state or the effects of the crime must be felt wholly or partly within the state.

Mutual Legal Assistance and Extradition

Australia's mutual assistance system and extradition regime are governed by the Mutual Assistance in Criminal Matters Act 1987 (Cth) and the Extradition Act 1988 (Cth), which set out the procedures for issuing and receiving assistance requests to and from Australia. The International Crime Cooperation Central Authority within the Attorney General's Department handles requests under these Acts, which treat white-collar offences the same as other offences.

1.5 Corporate and Personal Liability

Both individuals and bodies corporate can be criminally liable in Australia and be prosecuted jointly or separately. **2.5 Internal Investigations** sets out the way offences can be attributed to a corporation:

- the physical element of an offence can be attributed to a body corporate if the element is committed by an employee, agent or officer of a body corporate acting within the actual or apparent scope of their employment or authority; and
- the fault or mental element may be attributable to a company if the company expressly, tacitly or impliedly authorises or permits the commission of the offence under 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
- a corporate culture directed, encouraged, tolerated or led to non-compliance with the relevant provision.

Internal investigations can be expressly displaced by specific statutory provisions, for example, the "failure to prevent foreign bribery", discussed below.

No formal policy establishes a preference for prosecuting an individual over a company or vice versa. Ultimately, the Office of the Commonwealth Director of Public Prosecutions (CDPP) would determine this decision by exercising its prosecutorial discretion and considering the range of factors articulated in the Prosecution Policy of the Commonwealth.

In terms of penalties, many offences set out specific penalty provisions for corporations. In addition, Section 4B of the Crimes Act 1914 (Cth) allows a fine to be imposed for offences that specify only imprisonment as a penalty.

1.6 Sentencing and Penalties

Sentencing Principles and Guidance

Australia has no specific sentencing principles or guidelines for white-collar offences, nor formal sentencing guidelines for any criminal offence. Rather, the sentencing process is informed by the general principles set out in the Crimes Act 1914 (Cth), including:

- the nature and circumstances of the offence;
- any injury, loss or damage resulting from the offence; and
- the degree to which the person has co-operated with law enforcement agencies in the investigation of the offence or of other offences.

The CDPP has published Sentencing of Federal Offenders in Australia: A Guide for Practitioners, which is updated annually and provides detailed consideration of relevant sentencing factors and case law.

In NSW, the Sentencing Bench Book provides commentary on the relevant principles and practices applicable to the sentencing process and the law relating to it: the Crimes (Sentencing Procedure) Act 1999 and the relevant common law.

Factors relevant to the sentencing of both NSW and Commonwealth fraud offences include:

- the amount of money involved;
- the scale and complexity of the offence;
- the level of sophistication and planning involved;
- the length of time over which the offences were committed;
- the offender's role, particularly any accompanying breach of trust;
- the impact on public confidence and the victim; and
- general deterrence.

No Deferred Prosecution Agreements and Plea Agreements

Presently, Australia does not provide for deferred prosecution agreements (DPAs); however, it does allow plea agreements (see **4.3 Plea Agreements, Co-Operation, Self-Disclosure and Leniency**).

1.7 Damages and Compensation

There is legislation at both the federal and state level that enables victims to bring compensation claims in respect of injury or loss arising from criminal conduct. However, these can be limited. For example, the Victims Rights and Support Act 2013 (NSW) only provides for victims of violent crimes, acts of modern slavery and road crime and does not extend to most white-collar offences. By comparison, under Commonwealth law (Crimes Act 1914 (Cth), Section 21B), the court can order an offender to pay reparation to a victim for any loss suffered or expense incurred as a result of a Commonwealth offence. This can include financial loss for financial offences.

2. Enforcement

2.1 White-Collar Enforcement Authorities

The Australian Federal Police (AFP) and the CDPP are the two main authorities responsible for the investigation and prosecution of Commonwealth offences in Australia. Several regulatory authorities also have the power to investigate and prosecute white-collar offences.

AFP

The AFP is Australia's national policing agency and is responsible for investigating federal offences under the Criminal Code. These include white-collar offences related to bribery, insider trading, money laundering and fraud.

CDPP

The CDPP is Australia's federal prosecution service. It initiates and prosecutes offences under Commonwealth law. The CDPP operates a commercial, financial and corruption practice group responsible for prosecuting serious financial and white-collar crimes.

Australian Taxation Office (ATO)

The ATO is the Australian government's principal revenue collection agency. It also plays an active role in investigating and enforcing white-collar crime offences relating to tax avoidance and fraud under the Tax Administration Act 1953 (Cth).

Australian Transaction Reports and Analysis Centre (AUSTRAC)

AUSTRAC is Australia's financial intelligence unit and anti-money laundering and counter-terrorism financing (AML/CTF) regulator. It administers the Anti-Money Laundering and Counter-Terrorism Financing Act 2006 (Cth) (AML/CTF Act) and Anti-Money Laundering and Counter-Terrorism Financing Rules Instrument 2007 (No 1).

Australian Competition and Consumer Commission (ACCC)

The ACCC is an independent statutory authority responsible for fair trading, consumer protection and competition by enforcing the Competition and Consumer Act 2011 (Cth).

Australian Securities and Investments Commission (ASIC)

ASIC is Australia's corporate, markets, financial services and consumer credit regulator. ASIC is primarily responsible for administering the Corporations Act 2001 (Cth).

2.2 Initiating an Investigation

White-collar investigations typically begin in response to reports of misconduct from those impacted or through the agency's own monitoring. An authority's individual internal policy will determine when escalation to investigation is appropriate. Three examples are set out in the following.

AFP investigations are typically instigated in response to:

- a report from the public or Parliament;
- intelligence received through its systems and networks;
- an operational activity; or
- findings from an earlier or related investigation.

ASIC initiates investigations in response to reports of misconduct by members of the public or through AUSTRAC's monitoring and surveillance work or information received from other agencies and regulators. In deciding whether or not to initiate a formal investigation, ASIC will consider the following factors:

- areas of significant harm;
- broader public benefit;
- issues specific to the case; and
- alternatives to formal investigation.

The ACCC can initiate an investigation in response to a report from parliamentarians, the public or other agencies or from ASIC's own monitoring activities, intelligence gathering or market studies. Whether an investigation will be initiated will be decided with regard to the issues and priority areas outlined in the ACCC Compliance and Enforcement Policy. This includes whether the conduct:

- results in substantial consumer or small business detriment;
- has a significant impact on the cost of living;
- disproportionately targets consumers experiencing vulnerability or disadvantage; or
- is of significant public interest or concern.

2.3 Powers of Investigation

The AFP has a wide range of statutory powers enabling it to investigate serious white-collar crime in Australia. These powers include the authority to issue warrants, conduct searches and interviews and seize evidence. However, several regulators also have wide-reaching powers, some of which go beyond the AFP's.

ASIC has the power to:

- require the production or inspection of documents;
- compel individuals and entities to attend examinations;
- compel reasonable assistance to an investigation;
- apply for and execute search warrants to secure essential documents; and
- conduct general surveillance.

The ATO has the power to:

- issue notices requiring the provision of information or the production of documents;
- issue notices requiring attendance before the Commissioner to give evidence; and
- access land, premises or places to inspect or copy documents or information.

Alongside its original powers to request information, in 2025 AUSTRAC acquired a range of new investigative powers and can now:

- issue a notice compelling a person to produce information or documents;
- authorise a person to share information with AUSTRAC without violating other privacy or confidentiality laws; and
- compel a person to attend compulsory examinations to give evidence or produce documents.

Notably, the compulsory interview powers of several relevant regulatory authorities, including the three listed in the 2025 amendments, require individuals to answer questions regardless of whether the answer may incriminate them. However, information obtained in this manner cannot then be used in criminal proceedings. Failure to comply with a regulator's requests/demands can also expose an individual or company to criminal sanction.

2.4 Use of Technology in Investigations

In Australia, certain law enforcement authorities and regulators, including the AFP, AUSTRAC, ATO, ACCC and ASIC, are adopting AI to help manage and process large amounts of data and improve operational efficiency. The Policy for the responsible use of AI in government (2025) requires most non-corporate agencies to publish transparency statements explaining how they deploy AI.

Notably, the AFP's current use of AI focuses on managing data to improve human efficiency when processing the increasingly large volumes of data that characterise the AFP's complex investigations.

The AFP has stated that machine-produced material must be subject to human review and judgement before it can be used in any operational decision-making. According to the AFP, this means that AI will not replace the requirement for personal accountability for any decision that impacts on an individual's rights.

AUSTRAC uses generative AI tools to undertake research and discovery and for workplace productivity purposes. AUSTRAC has not yet deployed any use of AI that directly interacts with the public or supports decision-making and administrative action without human intervention. However, AUSTRAC uses statistical, rules-based AI modelling and machine learning to support non-sensitive research and basic secretariat support, identify indicators of money laundering, terrorism financing or financially enabled crime and generate actionable financial intelligence for its partners.

2.5 Internal Investigations

Internal investigations in Australia are usually voluntary. Corporate entities may initiate an internal investigation in response to the results of an internal audit, on the advice of in-house counsel in relation to allegations of misconduct or in response to the identification of a breach by a regulator.

However, an internal investigation may also be initiated on the compulsory instruction of a regulator. For example, AUSTRAC's enforcement powers include "remedial directions", in which AUSTRAC can direct a company in writing to take specific actions to comply with certain parts of the AML/CTF Act. In the past, this has included directions to appoint an auditor to conduct money laundering and terrorism financing risk assessments.

2.6 Prosecution

While regulators such as ASIC, the ATO and the ACCC have the authority to initiate criminal proceedings within their respective areas of regulation, the CDPP is typically briefed to handle the prosecution of most white-collar crime cases. The CDPP's dedicated commercial, financial and corruption practice group prosecutes offences related to corporations, financial markets and services, large-scale tax fraud, criminal cartel behaviour and money laundering, as well as bribery and corruption involving Commonwealth and foreign officials.

As referenced in **1.5 Corporate and Personal Liability**, the CDPP decides whether to initiate a prosecution in accordance with the Prosecution Policy of the Commonwealth. A prosecution will commence only when there are reasonable prospects of securing a conviction and if it is in the public interest to pursue a prosecution. Other factors that can be taken into account include:

- the seriousness of the offence, including mitigating or aggravating circumstances;
- the prevalence of the alleged offence and the need for deterrence; and
- alternatives to prosecution.

2.7 Deferred Prosecution

Australia does not provide for DPAs. However, there are several mechanisms for providing immunity from prosecution in exchange for co-operation with the regulator; these are discussed in **4. Pleas and Defences**.

The CDPP, under Section 9 (6D) of the Director of Public Prosecutions Act 1983 (Cth), can make a formal undertaking to a person that they will not be prosecuted in respect of specified acts or omissions ("an indemnity"). An indemnity will only be given if:

- the evidence that the individual can give is necessary to secure the conviction of another defendant or is essential to disclose the nature and scope of the offending fully and that evidence is not available from other sources; and
- the individual can reasonably be regarded as significantly less culpable than the other defendant.

The CDPP's Legal Direction states that indemnities will only be provided in "exceptional circumstances".

3. White-Collar Offences

3.1 Criminal Company Law and Corporate Fraud

Australian criminal law applies to companies and individuals alike (see **1.5 Corporate and Personal Liability**) and there are a range of offences applicable only to companies and their officers.

Companies can be punished for fraud through ordinary fraud offences. For example, under the Criminal Code, fraud is criminalised against government entities:

- Sections 134.2 and 135.2 – obtaining a financial advantage by deception from a Commonwealth entity;
- Section 135.1 (3) – dishonestly causing a loss to the Commonwealth; and
- Sections 145.1 and 145.2 – using or possessing a forged document with the intention to dishonestly obtain a gain, cause a loss or influence the exercise of a public duty or function.

Other examples of corporate fraud offences include insider trading, market manipulation (see **3.4 Insider Dealing, Market Abuse and Criminal Banking Law**) and money laundering (see **3.13 Money Laundering**).

3.2 Bribery, Influence Peddling and Related Offences

Bribery

Australian bribery offences fit into three categories.

Domestic government bribery

The Criminal Code, Sections 141.1 and 142.1 prohibit both active (giver) and passive (receiver) domestic bribery involving Commonwealth officials. The maximum penalty depends on the entity type. For individuals, the penalty is 10 years' imprisonment and a fine of AUD3.64 million (10,000 penalty units); for corporations, it is a fine of AUD36.4 million (100,000 penalty units), three times the value of the benefit obtained or 10% of annual turnover.

Foreign government bribery

Section 70.2 of the Criminal Code prohibits providing, offering or promising a benefit to a foreign public official with the intention of securing or retaining a personal or business advantage. The two unique defences are that the conduct was legal in the foreign country or that it was a facilitation payment meeting certain requirements. The maximum penalty is the same as for domestic bribery.

Private bribery

Various legislation prohibits certain forms of private bribery, including company officers accepting bribes (Corporations Act, Section 184) and agents corruptly receiving bribes in relation to the principal's affairs or business (Crimes Act 1900 (NSW), Section 249B). The penalties vary.

Influence Peddling

Influence peddling and covert foreign interference are prohibited by Part 5.2 of the Criminal Code, particularly Sections 92.2–92.8, which criminalise covert, deceptive or undisclosed conduct undertaken on behalf of a foreign principal to influence political or governmental processes. These offences attract penalties of up to 20 years' imprisonment.

3.3 Anti-Bribery Regulation

As of September 2024, Section 70.5A of the Criminal Code has addressed the offence of failing to prevent foreign bribery.

A company commits an offence if an "associate" engages in foreign bribery for the corporation's profit or gain, unless the company can demonstrate it had "adequate procedures" designed to prevent such conduct.

This "adequate procedures" requirement is essentially an anti-bribery "compliance programme" for foreign bribery offences. The Australian Attorney General's Department guidance suggests an "adequate procedure" should address:

- the fostering of a control environment proportionate to the operational circumstances;
- top-level management's involvement in the development, implementation and promotion of the compliance programme;
- risk assessments, including the mitigation measures of non-controlled associates (eg, third-party service providers);
- communication and training, including how to respond to solicitation;
- reporting processes, including whistle-blower protections; and
- monitoring and reviewing (regularly and when required; eg, when entering a new market).

Australian law does not require a compliance programme for domestic bribery offences.

3.4 Insider Dealing, Market Abuse and Criminal Banking Law

Insider Dealing

Insider dealing (or "insider trading" in Australia) is prohibited under Section 1043A of the Corporations Act. Section 1043A prohibits a person from acquiring, disposing or entering into an agreement to acquire or dispose of "Division 3 financial products" where they possess "insider information". It also covers procuring other persons to do so or tipping off others who would undertake such transactions.

"Division 3 financial products" includes securities, derivatives, debentures, stocks, managed investment scheme interests and certain superannuation products, while "inside information" is defined as information not generally available – and where, if it were generally available, it would expectedly have a material effect on the product's value or price. Various exceptions and defences apply, including where an effective "Chinese wall arrangement" was established.

Penalties can be civil or criminal and vary by entity type. For individuals, the maximum criminal penalty is 15 years' imprisonment and/or a fine, being the greater of AUD1,820,000 (5,000 penalty units) and three times the benefit derived or detriment avoided; for corporations, it is AUD1,820,000 (50,000 penalty units), three times the benefit or detriment avoided or 10% of its annual turnover capped.

Market Abuse

Market abuse is prohibited in various forms under the Corporations Act:

- Section 1041A – transacting to have the effect of creating an "artificial price" for financial products or maintaining the financial product's price at an artificial level;
- Section 1041B – doing (or omitting to do) an act that has the effect of creating a false or misleading appearance of active trading, market or price of financial products; and
- Section 1041C – a fictitious or artificial transaction or device resulting in the maintenance, inflation, depression or "fluctuations" of a financial product's price.

There are also offences concerning the dissemination of information relevant to the foregoing transactions, false or misleading statements, trading to influence a financial benchmark and other dishonest conduct. The maximum penalty for individuals is 15 years' imprisonment.

Criminal Banking Law

The Banking Act 1959 (Cth) and the Financial Accountability Regime Act 2023 (Cth) regulate various banking offences. The primary offence is carrying on a banking business in Australia without authorisation from the Australian Prudential Regulation Authority. The penalty is AUD72,800 for individuals and five times that for companies. An offence occurs each day the company carries out the business.

3.5 Tax Fraud

Tax fraud and related conduct is criminalised by the Criminal Code and the Taxation Administration Act 1953 (Cth) (TAA) and prosecuted by the CDPP or the ATO.

Serious tax fraud is typically prosecuted by the CDPP pursuant to the offences under the Criminal Code (see **3.1 Criminal Company Law and Corporate Fraud**).

The ATO typically prosecutes certain types of fraud-related conduct such as making false or misleading statements to the ATO or keeping incorrect records with the intention to deceive or mislead the ATO, as well as omissions such as a failure to lodge tax returns, business activity statements (BAS) or fringe benefits tax (FBT) or to respond to an information-gathering notice. According to the most recent statistics, in 2024-25, the ATO prosecuted 369 cases in total, with 343 convictions, reparation orders of AUD25,386 and fines of over AUD5.18 million.

Separate from offences, fraudulent conduct in tax affairs is relevant to other aspects of tax processes:

- there is no time limit on the ATO amending a taxpayer's assessment where there is evasion or fraud; and
- an administrative penalty of 75% of a tax shortfall is imposed where a taxpayer (or their agent) has intentionally disregarded a taxation law in making a statement that is misleading or false in a material particular.

Relatedly, the Tax Agent Services Act 2009 (Cth) prohibits tax practitioners from marketing tax avoidance schemes and imposes civil penalties for contraventions.

Penalties for tax fraud vary by offence type, including a maximum of ten years' imprisonment. Australia does not impose an explicit obligation to prevent tax evasion.

3.6 Financial Record-Keeping

Australia imposes strict financial record-keeping obligations on corporations and individuals under the Corporations Act and the TAA. Failure to meet these obligations can result in civil and criminal penalties under their respective statutes and the Criminal Code.

Key offences include:

- under the Corporations Act, failing to keep financial records that correctly explain transactions that enable "true and fair" financial statements to be prepared, as well as sustainability records, punishable by up to two years' imprisonment;
- under the Criminal Code, making, altering, destroying or concealing accounting documents to facilitate, conceal or disguise illegitimate benefits or illegitimate losses, punishable for individuals by ten years imprisonment or an AUD3.64 million fine – and for corporations by a fine equal to the greatest of AUD36.4 million, three times the value of any benefit the corporation obtained from the offence and 10% of the corporation's annual turnover; and
- under the TAA, not keeping accounts or records that correctly record and explain matters, transactions, acts or operations as required by taxation law.

To prove a criminal record-keeping offence, authorities must show that a person knowingly or recklessly failed to keep proper books, intentionally falsified records or destroyed documents to mislead or obstruct the Commissioner or a particular taxation officer.

Penalties vary significantly depending on the severity of the conduct. Intentional false dealing with accounting documents, an offence under the Criminal Code, is punishable by up to ten years' imprisonment and a fine of up to 10,000 penalty units when committed by an individual.

Reckless false dealing with accounting documents carries a maximum penalty of five years' imprisonment and a fine of up to 5,000 penalty units. Civil penalties under the Corporations Act may also be substantial and individuals may be disqualified from managing corporations if their conduct demonstrates unfitness, improper governance or involvement in contraventions.

3.7 Cartels and Criminal Competition Law

Australia maintains a dual civil-criminal regime for cartel conduct under Part IV of the Competition and Consumer Act 2010 (Cth) (CCA).

Sections 45AF–45AG criminalise corporations making or giving effect to a contract, arrangement or understanding that contains a cartel provision. A cartel provision arises where competitors agree to:

- price fixing;
- restricting outputs in production and supply chains;
- allocating customers, suppliers or territories; or
- engage in bid rigging.

Under criminal penalties, corporations may be fined the greater of AUD100 million, three times the total benefit obtained or 30% of their annual turnover. Additionally, an individual who attempts to contravene, aid, abet, counsel, procure or induce or is "concerned in" the contravention or conspires to contravene the foregoing provisions, may be punished with up to ten years' imprisonment and/or a fine of AUD728,000 (2,000 penalty units).

In 2022, Australia saw the first custodial sentence for cartel conduct in *CDPP v Vina Money Transfer Pty Ltd* [2022] FCA 665. The latest sentence came in February 2024: Mr Tartak and Mr Roussakis were sentenced to two terms of 18 months' imprisonment (served concurrently) and 18 months' imprisonment, respectively, for price-fixing arrangements for demolition waste services in Sydney. The two companies involved were fined AUD30 million and AUD3.5 million.

3.8 Consumer Criminal Law

The criminal and administrative offences relating to consumer law are primarily governed by the Australian Consumer Law (ACL), found in Schedule 2 of the CCA.

Key offences include:

- false or misleading representations about goods or services (including testimonials for which the accused must provide evidence that the testimonial is true) or about the sale of land;
- conduct liable to mislead persons seeking employment as to any matter relating to employment that is actually or possibly being offered;
- falsely offering rebates, gifts, prizes or other free items in trade or commerce; and
- accepting payment for goods and services without intention to supply (or being reckless as to whether the goods or services would be supplied).

Other offences related to bait advertising, pyramid schemes, referral selling, harassment and coercion in business exist.

Generally, penalties under the ACL fit into two categories:

- for the offences listed in the foregoing (and more), individuals are punishable by a fine of AUD2.5 million, while corporations are punishable by a fine not more than the greater of AUD100 million, three times the value of the benefit and 30% of annual turnover; and
- certain other offences are punishable by lesser amounts – for example, breaching rules around negotiating unsolicited consumer agreements are punishable for individuals and corporations by a fine of AUD10,000 and AUD50,000, respectively.

No offences under the ACL are punishable by imprisonment. Civil penalties can apply concurrently (eg, fines, banning orders, injunctions, compensation) and companies may be ordered to implement compliance programmes or corrective advertising.

3.9 Cybercrimes, Computer Fraud and Protection of Company Secrets

Cybercrimes

Both federal and state legislation criminalises cybercrimes and computer fraud.

Under federal law, the key provisions include Part 10.7 (Computer Offences) of the Criminal Code, namely:

- Section 478.1 – unauthorised access to or modification of, data held in a computer to which access is restricted by an "access control system" (eg, a password);
- Section 477.3 – unauthorised impairment of electronic communication;
- Section 474.17 – using a carriage service to menace, harass or cause offence; and
- Sections 478.3 and 478.4 – anticipatory offences, such as possessing, controlling, producing, supplying or obtaining data with the intent to commit a computer offence (even where the anticipated offence is impossible).

States also have similar computer-specific crimes, such as Part 6 of the Crimes Act 1900 (NSW). The offences covered above carry penalties ranging from two to ten years of imprisonment.

Protection of Company Secrets

Civil penalties and criminal offences specifically address dishonestly obtaining or using company information and secrets.

- Part 10.8 (Financial information offences) of the Criminal Code covers dishonestly obtaining or dealing with "personal financial information" without the consent of the person to whom the information relates. The penalty is up to five years' imprisonment.
- Section 184 (2) of the Corporations Act criminalises using information obtained by a director, officer or employee of a corporation to gain an advantage for themselves or another or to cause detriment to the corporation. For the conduct to amount to an offence, the person must have used their position dishonestly and acted intentionally or recklessly.

Beyond criminal law, Australian law provides additional protections for company secrets, including Section 183 of the Corporations Act and equitable principles (eg, fiduciary duties owed by an employee to an employer).

3.10 Financial/Trade/Customs Sanctions

The Australian sanctions and customs regimes are covered by a set of legislation, including:

- the Charter of the United Nations Act 1945 (Cth) (COTUNA), implementing internationally mandated sanctions;
- the Autonomous Sanctions Act 2011 (Cth) (the "Sanctions Act"), implementing Australia's autonomous sanctions;
- the Customs Act 1901 (Cth) and the Customs (Prohibited Exports) Regulations 1958 (Cth), imposing controls for the import and export of most goods; and
- Defence Trade Controls Act 2012 (Cth) (the "DTC Act") and the Defence and Strategic Goods List 2024 (DSGL), imposing controls on the transfer of defence and strategic goods, technologies and services (including dual-use).

The Australian Sanctions Office within the Department of Foreign Affairs and Trade regulates the sanctions regimes, while other agencies regulate customs and trade laws.

Key offences in these areas of law include the following.

- Sanctions Act, Section 16: Engaging in conduct (by acting or omitting to act) that contravenes either a sanctions law or conditions of authorisation under sanctions law. The elements depend on the sanctions law or authorisation in question and on whether the offender is an individual (requiring proof of intent) or a body corporate (strict liability, meaning no proof of intent is required). Punishment depends on the offender type:
  (a) for individuals – up to ten years maximum imprisonment, a fine of up to (the higher of) three times any relevant transaction(s) involved or AUD910,000 or both; and
  (b) for bodies corporate, a fine of up to (the higher

of) three times any relevant transaction(s) or AUD3.64 million.
- Customs Act, Section 33: Moving, altering or interfering with goods that are "subject to customs control", a term that depends on the types of goods being imported into (and to an extent, exported from) Australia. For example, all goods onboard a ship or aircraft from outside Australia are subject to customs control while within an Australian port or airport. Penalties vary depending on the conduct, but can include a fine of up to AUD182,000.
- DTC Act, Sections 10, 10A and 10B: The supply of certain technology and goods on the DSGL to a place or person outside Australia or to a foreign person, where the supplies are not properly authorised. This offence has technical elements and is subject to certain exceptions. Punishment for this offence is ten years' imprisonment, a fine up to AUD910,000 or both. There is a similar offence for the provision of DSGL-listed services outside Australia.

Although the relevant agency primarily handles breaches of these statutes administratively, prosecutions for the foregoing offences can and have occurred. For example, in 2024–25, the CDPP dealt with two offences under the DTC Act and 115 offences under the Customs Act. Prosecutions under Australian sanctions laws are rarer, with the only recent case being in 2021, R v Choi (No 10) [2021] NSWSC 891, in which Mr Choi pleaded guilty to brokering "sanctioned services" to entities in North Korea in 2017 in breach of both COTUNA and the Autonomous Sanctions Act. He was sentenced to three years and six months' imprisonment.

3.11 Concealment

Concealment of a crime is an offence under both Australian federal and state laws. These offences range from active steps to conceal a crime to merely not informing authorities of information.

- Section 149.1 of the Criminal Code prohibits a person from hindering a Commonwealth public official in the performance of their functions. The penalty is a maximum of two years' imprisonment.
- The Corporations Act, Section 1101E prohibits a person from concealing certain business records, while Section 1310 prohibits individuals (without lawful excuse) from hindering ASIC in its functions or powers. Penalties depend on the type of entity (person or corporate), including two-year imprisonment for either offence.
- The Crimes Act 1900 (NSW), Section 316 (1) criminalises someone failing to inform authorities when they have information "that might be of material assistance" to apprehend, prosecute or convict an offender "without reasonable excuse". The maximum penalty is five years' imprisonment where the predicate offence is punishable by 20 years' imprisonment or more.

Various concealment and augmented offences also appear throughout legislation. For example, under the Criminal Code, Section 91.6, it is an aggravated offence to commit espionage and conceal the security classification of a record or article. Depending on the level of involvement, concealing a crime could also mean a person may be liable for it as a principal, aider/abetter or otherwise (see **3.12 Aiding and Abetting**).

3.12 Aiding and Abetting

In Australia, there are various modes of liability. The Criminal Code is the key federal statute, under which a person can be taken to have committed an offence if they:

- intentionally or recklessly aided, abetted, counselled or procured its commission (Section 11.2);
- agreed to commit the offence or any other offence committed in the course of carrying out such an agreement (Section 11.2A); or
- conspired with another to commit the offence, so long as a person has committed "an overt act pursuant to the agreement" – and the underlying offence is punishable by at least 12 months imprisonment or a 200 penalty unit fine (Section 11.5).

A person can be found guilty under Sections 11.2 and 11.2A, even if another person has not been prosecuted or convicted; similarly, Section 11.5 can apply even if all other parties cannot be criminally responsible or have been acquitted.

Additional modes of liability include commission by proxy (Section 11.3) and incitement (Section 11.4).

There are also other specific conspiracy offences, such as conspiracy to defraud a Commonwealth entity (eg, the ATO for tax fraud) under Section 135.4 of the Criminal Code.

Each state and territory also has its own modes of liability, often included as a separate offence rather than rendering an individual liable for the underlying offence; for example, aiding, abetting, counselling, procuring, soliciting and inciting under the Crimes Act 1900 (NSW), Section 249F.

3.13 Money Laundering

Australia has no specific obligation to prevent money laundering. However, the criminal and regulatory regime prohibits money laundering and requires certain entities to monitor and report suspicious conduct.

Money laundering offences are primarily contained in three instruments.

- The Criminal Code, specifically Chapter 10, Part 10.2, Division 400, defines and captures 19 money laundering offences. These offences relate to "dealing" with "money or other property" reasonably believed to be the proceeds of crime. These penalties increase in severity based on the quantum involved and the offender's state of mind (eg, intentional, reckless or negligent). For example, for money or property worth AUD10 million or more, individuals may face up to life imprisonment or a fine of 2,000 penalty units (AUD728,000), while a corporation may receive a fine of 10,000 penalty units (AUD3.6 million).
- The AML/CTF Act, enforced by AUSTRAC, requires regulated entities to have a programme to identify, mitigate and manage risks posed to the business by money laundering and terrorism financing and to notify authorities of suspicious matters.
- Australian states and territories' criminal laws – for example, Part 4AC of the Crimes Act 1900 (NSW) – prohibit dealing with property while knowing or being reckless as to whether the relevant property is proceeds of crime or where there are reasonable grounds to suspect this.

In addition to criminal prosecution, the Proceeds of Crime Act 2002 (Cth) allows the AFP to seek freezing, restraining or forfeiture orders for property suspected to be proceeds of crime or instruments of crime, even before conviction.

For federal money laundering and proceeds of crime offences, the CDPP is the primary government agency responsible. Each state and territory's public prosecution office is responsible for prosecuting money laundering offences that breach state/territory laws.

3.14 ESG-Related Offences

Key ESG-related offences have been outlined below.

- The Corporations Act, Section 286A, criminalises companies (that are "large entities") failing to prepare annual sustainability reports and retain records for seven years. The maximum penalty is two years' imprisonment or 60 penalty units.
- The Environment Protection and Biodiversity Conservation Act 1999 (Cth) (the "EPBC Act"), Section 18, prohibits taking an action that has, will have or is likely to have a significant impact on matters of national environmental significance (eg, on threatened species, ecological communities or heritage values). The maximum penalty is 5,000 penalty units for individuals and 50,000 penalty units for companies.
- State-based offences, such as the Protection of the Environment Operations Act 1997 (NSW), Chapter 5, criminalise various types of conduct, including certain forms of water, air, noise and land pollution.

On 28 November 2025, the federal government passed seven acts amending the EPBC Act, increasing penalties, establishing a new National Environment Protection Agency with enhanced compliance and enforcement powers and introducing new criminal offences concerning environmental auditors and audits.

3.15 Artificial Intelligence and Automation Misuse

Australia has no specific criminal offences targeting AI misuse, algorithmic trading or automated decision-making. Instead, regulators such as ASIC and the Office of the Australian Information Commissioner (OAIC) apply existing laws to address misuse under broader categories such as market manipulation, mis-

leading conduct or privacy breaches. The penalties range from fines to imprisonment, depending on the statute.

For example, the Corporations Act, Section 1041A (see **3.4 Insider Dealing, Market Abuse and Criminal Banking Law**) can be used to prosecute:

- use of trading algorithms that cause false or misleading market appearances (eg, "spoofing" or "layering"); and/or
- the misuse of AI (eg, creating deepfakes of CEO announcements to influence share prices).

Deepfakes also pose a serious threat to AML/CTF compliance in Australia. Misuse of AI in this way can lead to criminal liability for individuals (fraud, money laundering, terrorism financing) and also civil sanctions for financial institutions that fail to take sufficient steps to mitigate the risk (AUSTRAC penalties, enforceable undertakings).

3.16 Crypto-Assets and Digital Currency Crimes

Criminal Offences

Australia does not have specific crypto-crimes. Australian law currently treats crypto-assets as property and their misuse can constitute criminal offences such as fraud, money laundering, unauthorised access, tax evasion and terrorism funding. Examples include the convictions of Boliang Liu and Tao Zhou, as well as the charges against ACCE Australia Pty Ltd's ex-CEO, Grant Colthup.

The Proceeds of Crime Act 2002 (Cth), Section 228A allows for the seizure of digital assets during the execution of search warrants. For example, an executing officer may use any electronic equipment found during a search and, if necessary, copy, delete or alter data for the purpose of seizing a digital asset.

Civil Regulation

"Virtual asset" providers are regulated under the AML/CTF Act if they meet the geographical nexus requirement (see **3.13 Money Laundering**). The new definition, which came into force on 1 March 2026, captures a broad range of entities that: exchange or make arrangements for the exchange of virtual assets, facilitate transfers of virtual assets, provide virtual asset safekeeping services or provide financial services in connection with the offer or sale of a virtual asset.

ASIC and the Corporations Act primarily regulate crypto-assets to the extent that they involve financial products or financial services. Such service providers must hold an Australian Financial Services licence or operate as an authorised representative of a licence holder. Criminal penalties can be up to five years' imprisonment or AUD218,400 in fines (600 penalty units) for individuals and AUD2.2 million in fines (6,000 penalty units) for corporations.

4. Pleas and Defences

4.1 White-Collar Defences

Common Defences

In Australia, defendants in white-collar cases usually rely on the general criminal law rules about fault and defences. They may argue that they did not intend to do anything wrong, that they did not know the relevant facts or that they made an honest mistake about those facts. Many white-collar offences require the prosecution to prove a particular state of mind, such as dishonesty, so showing that the person acted openly, followed procedures or believed they were complying with the law can be very important.

Role of Professional Advice

Reliance on professional advice is not a standalone defence. However, evidence that a defendant sought and followed expert advice may help explain their state of mind, support a claim of good faith or be considered a mitigating factor during sentencing or regulatory assessments.

Compliance Programmes

Generally, the existence of a compliance programme is not a standalone defence. The major new exception is the "failure to prevent foreign bribery" offence introduced in 2024. A company can avoid liability if it had adequate procedures designed to prevent bribery by its associates (see **3.3 Anti-Bribery Regulation**).

For other offences, the strength or weakness of a company's compliance systems is highly relevant to regulatory enforcement and penalties.

4.2 De Minimis

Australia does not have a general "de minimis" principle that excuses small-scale or low-value white-collar misconduct. There are also no broad exemptions for particular industries, professions or categories of transactions. Certain regulatory regimes do include narrow, offence-specific carve-outs that operate only in limited circumstances – for example, an exception that permits underwriters to acquire securities under an underwriting obligation without breaching insider trading prohibitions.

Although the law does not excuse conduct simply because it is minor, enforcement agencies and prosecutors may consider it when deciding whether to commence proceedings.

4.3 Plea Agreements, Co-Operation, Self-Disclosure and Leniency

Plea Discussions and Charge Negotiation

Australia allows charge negotiation. An accused may agree to plead guilty to some or different charges and in return the prosecution may drop other charges or accept a narrower set of facts, but only if this still reflects the evidence and serves the public interest. The court is not bound by the agreement.

Self-Disclosure, Co-Operation and Leniency

Courts treat early guilty pleas, genuine remorse, assistance to authorities and voluntary disclosure as important mitigating factors in sentencing.

Regulators maintain their own co-operation frameworks; ASIC has the power to grant immunity from civil proceedings or recommend immunity from criminal proceedings for contraventions of the Corporations Act where an individual admits to the misconduct and intends to co-operate with ASIC in an investigation. This is only available for individuals, not corporations.

Similarly, the ACCC has the power to grant civil immunity in relation to cartel conduct. Immunity can be provided to the individual or corporation that is first to disclose the conduct and co-operate fully with the investigation. The applicant must enter into a co-operation agreement with the ACC that outlines the co-operative steps that the applicant agrees to undertake.

Self-reporting is also important in the tax context. The ATO operates a long-standing voluntary disclosure regime, under which taxpayers who proactively disclose contraventions before detection can receive substantial reductions in administrative penalties.

4.4 Whistle-Blower Protection

Australia's whistle-blower protection framework spans multiple federal and state statutes.

Key features of whistle-blower protections under the Corporations Act and TAA include the ability to make anonymous disclosures, protection from civil, criminal and administrative liability, reinstatement rights where employment detriment occurs and restrictions on using protected disclosure material in criminal penalty proceedings. Victimisation of whistle-blowers is also prohibited and can constitute a civil penalty or criminal offence.

For public-sector whistle-blowers, the Public Interest Disclosure Act 2013 (Cth) was updated by the Public Interest Disclosure Amendment (Review) Act 2022 (Cth), which expanded reprisal protections to capture indirect threats and strengthened investigatory obligations across government agencies.

4.5 Cross-Border Defence Strategies

White-collar matters often cross borders – for example, foreign bribery, sanctions, tax fraud and money laundering involving funds or communications that move through multiple countries. Different jurisdictions have different rules on privilege, self-incrimination, data privacy, document production and corporate liability. This can create real tension for defence teams trying to respond consistently to regulators in several countries at once.

Lawyers must anticipate how information provided to an Australian regulator may later be shared abroad, manage privilege and confidentiality risks across differing legal systems and co-ordinate the sequencing of interviews and document productions to ensure consistency. Blocking statutes, which seek to limit for-

eign law enforcement's ability to prosecute its nationals under extraterritorial legislation, can equally limit defence lawyers' ability to obtain evidence in aid of their client.

5. Key Trends and Future Outlook

5.1 The Year Ahead

Looking ahead, key dates, potential reforms and new enforcement priorities are set to propel investigation lawyers, businesses and Australia into 2027.

Key Legislative Dates in 2027

There are already several key calendar dates to note in the white-collar investigations and crime landscape:

- The Customs Legislation Amendment (False Trade Marks Infringement Notices) Act 2026 introduces a new strict liability offence of importing goods with false trademarks into Australia. The provisions commence on the earlier of Proclamation or 20 November 2026. The offence carries a maximum penalty of 60 penalty units or AUD21,840.
- The Corporations Amendment (Digital Assets Framework) Act 2026 commences on 9 April 2027, including digital asset platforms and tokenised custody platforms as categories of financial products subject to the Corporations Act and the Australian financial services licensing regime.
- The first tranche of reforms introduced by the Australian Government's 2026-2027 Budget Tax Reforms will come into effect from 1 July 2027, which includes replacing the 50% capital gains tax discount with a discount based on inflation, the introduction of a 30% minimum tax rate on capital gains and limiting negative gearing for residential property investments to new builds only.

Looking ahead, increased investigations and enforcement actions to punish and combat offences will continue into 2027 and 2028, with regulators and courts pursuing and imposing tougher penalties for breaches of the law. AI-enabled corporate crime will likely remain a key focus as technology becomes more sophisticated and is increasingly used to facilitate corporate crime.

Enforcement Priorities in 2026

Key regulators have released new enforcement priorities, as outlined below.

- ASIC's 2026-2027 Corporate Plan reveals that scam prevention and disruption will remain a key enforcement priority, along with the impact and use of AI, the regulation of digital asset platforms, financial reporting, valuations and auditing and ensuring directors are accountable for misconduct. There is a notable shift towards focussing on emerging technologies to ensure they remain regulated and subject to enforcement action.
- AUSTRAC released its regulatory priorities for 2026-2027, which centres around monitoring the effects of the new obligations under the AML/CTF Act, which took effect in 2026, including focusing regulatory interventions on both newly regulated reporting entities and reporting entities that were previously regulated who do not manage their ML/TF risks effectively. They have also committed to helping reporting entities improve the quality of their suspicious matter reports and contribute to money laundering and counterterrorism financing risk management within the broader Pacific region.
- The ACCC continues to spotlight the supermarket, retail and digital market sectors, focusing on misleading pricing and manipulative practices. The ACCC has committed to tackling consumer issues within the aviation sector and misleading claims of essential service providers. One of the main priorities across all sectors is fostering competitive markets and fair trading behaviour. The regulator has also committed to prioritising consumer concerns for greenwashing and false or misleading environmental claims.

Chambers | Practice Guides

Chambers Global Practice Guides bring you up-to-date, expert legal commentary on the main practice areas from around the globe. Focusing on the practical legal issues affecting businesses, the guides enable readers to compare legislation and procedure and read trend forecasts from legal experts from across key jurisdictions.

To find out more information about how we select contributors, email Luke.Wilson@Chambers.com