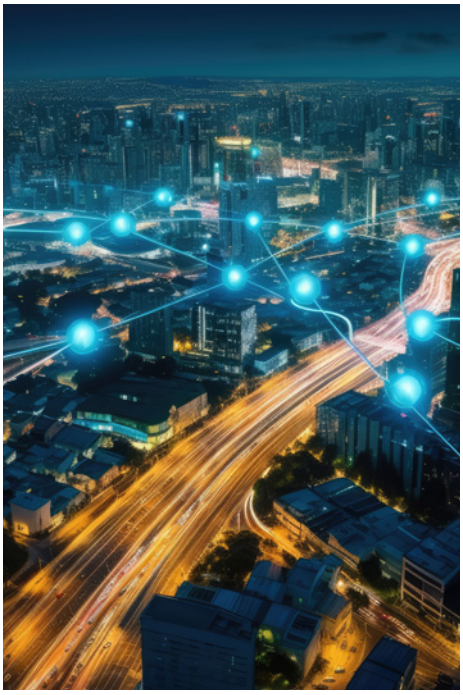
HERBERT SMITH FREEHILLS

CORPORATE CRIME & INVESTIGATIONS OUTLOOK 2024

In this issue



Corporate crime and investigations outlook 2024: Trends in Australia and beyond

Welcome to the HSF Corporate Crime and Investigations Outlook 2024: Trends in Australia and Beyond.

There are five key trends to watch in 2024:

1. **Social and governance expectations on business are ever-increasing, propelled by the wider ESG agenda.** The hardening corporate crime landscape is an important reminder for corporates that these expectations involve strict conduct and compliance expectations, not just reporting or transparency requirements. Our articles on foreign bribery reforms and the new way of prosecuting companies for a 'failure to prevent' offence, as well as whistleblowing developments over the last year, explore those increasingly strict expectations on business.
2. **Failing to adequately appreciate corporate crime expectations within the risk environment continues to expose companies to regulatory and enforcement scrutiny,** and in some instances, legal challenge. Our article on recent AML enforcement highlights the criticality of robust risk assessment and meaningful Board/senior management oversight in compliance programs. We also profile a recent court decision that illustrates some of the complexities that can arise for entities when seeking to adhere to regulatory expectations and managing their risk in an AML/CTF context.
3. **Within this environment, there are live calls for yet more adjustments to regulatory settings.** 2024 will be the year of further Government consultation and reviews, with whistleblowing and public interest disclosure regimes either currently under review, or expected to be under review in 2024, as we discuss in our article. The Government will also report back on its review of the autonomous sanctions regime, and the review of the *Modern Slavery Act*. In the oversight area, Government has already moved to establish a new Anti-Slavery Commissioner, and is actively monitoring whether additional oversight bodies are warranted, such as a Whistleblower Protection Authority or Commissioner. Another area of live debate concerns whether Australia needs a deferred prosecution agreement (**DPA**) regime, with that aspect still contested in the context of foreign bribery reforms currently before the Federal Parliament.
4. **Scrutiny over integrity concerns more generally persist.** In the coming year, the newly equipped National Anti-Corruption Commission (NACC) will start to flex its very significant powers, as we review in our article. We also expect a continuation of the clear trend within corporates to utilise internal investigations, which we reviewed in our survey of internal investigations. You can read the highlights of that survey here.
5. **Amidst ongoing global volatility, business needs to be alert to further legal change as well as evolving areas of risk.** The Australian sanctions environment, which we survey in our article, provides a good case study on the need to stay current with evolving legal requirements. In the international arena, overseas law-makers are demonstrating an appetite to further broaden corporate crime laws. The UK's *Economic Crime and Corporate Transparency Act* will be a game-changer for how companies are held criminally liable for fraud and malpractice, as our HSF London colleagues consider in these briefings and podcasts. We expect Australian authorities to closely monitor and consider following such overseas trends, as we have already seen in the foreign bribery space and the long-awaited introduction of a 'failure to prevent' offence.

You can rest assured that your HSF Australian corporate crime and investigations team will continue to keep a close eye on these trends and any related developments in 2024. Our Australian CC&I team will be sharing tips about how to make sure your business is prepared and ready to respond - watch this space.

Foreign bribery law reform: third time lucky?

From top
Jacqui Wootton
Madeleine Ryan

In July 2023, the Australian Government re-enlivened some, but not all, previously lapsed reforms to strengthen Australia's anti-bribery and corruption laws and bring them into line with laws in the UK. At the commencement of the 2024 Parliamentary year, a "failure to prevent" foreign bribery offence for corporates is back before the Senate, for the third time, and the possibility of a future deferred prosecution agreement (DPA) scheme alongside the new offence is up for debate.

After the Crimes Legislation Amendment (Combatting Corporate Crime) Bill 2019 (Cth) lapsed in 2022, the future of these reforms was uncertain. However, the new Federal Government quickly established that integrity was high on its agenda with the establishment of the National Anti-Corruption Commission (NACC). The introduction of the Crimes Legislation Amendment (Combatting Foreign Bribery) Bill 2023 soon followed. When introducing the new Bill, Attorney-General Mark Dreyfus announced the Labor Government "is cracking down on foreign bribery by Australian companies by removing barriers to investigations and prosecutions". Based on the latest developments, it looks like 2024 will be the year when these reforms finally make their way into law.

A new way of prosecuting companies: 'failure to prevent' offences

Like previous iterations of this reform package, introduced by the two previous Federal Governments, this Bill contains amendments to the foreign bribery provisions in the Commonwealth *Criminal Code*, most notably to:

1. **broaden the offence of bribing a foreign public official**, including by expanding the definition of "foreign public official" to include candidates and to include bribery for the purpose of obtaining or retaining a personal (not just a business) advantage.

2. **introduce a new offence of failing to prevent foreign bribery** with an "adequate procedures" defence.

   A company will be liable if they fail to prevent bribery of a foreign public official by "associates" acting for the company's profit or gain, unless the company can establish that, at the time, it had in place "adequate procedures" designed to prevent bribery of foreign public officials by its associates. "Associate" is defined very broadly, and includes any person who performs services for or on behalf of a company (encompassing third party agents, consultants and suppliers). The offence will be strict, and it will not be necessary to prove that the company approved, or even was aware of, its associate's conduct.

   The Attorney-General will be required to publish guidance on what "adequate procedures" might look like, but there will be no checklist or one-size-fits-all approach. Adequate procedures will need to be tailored and proportionate to the size and risk-profile of each business. The fact that foreign bribery has occurred will not be taken, of itself, be taken to mean that the company did not have adequate procedures.

3. **assign substantial penalties to the new "failure to prevent" offence**, of not more than the greatest of:

   (a) 100,000 penalty units ($31,300,000 as at 1 July 2023); or

   (b) three times the value of the benefit obtained from the offence; or

   (c) where the value of the benefit cannot be determined, 10% of the company's annual turnover at the relevant time.

In a decision released in August 2023, the High Court confirmed that, in a similarly drafted penalty provision, the "value of the benefit" is the gross benefit from the relevant contract, rather than net benefit from the contravening conduct (overturning the New South Wales Court of Criminal Appeal's interpretation handed down in 2022). This maximises the value of the second limb and reinforces the intended deterrent effect.

You can read more about the features of the current Bill compared to its predecessors here.

What about deferred prosecution agreements?

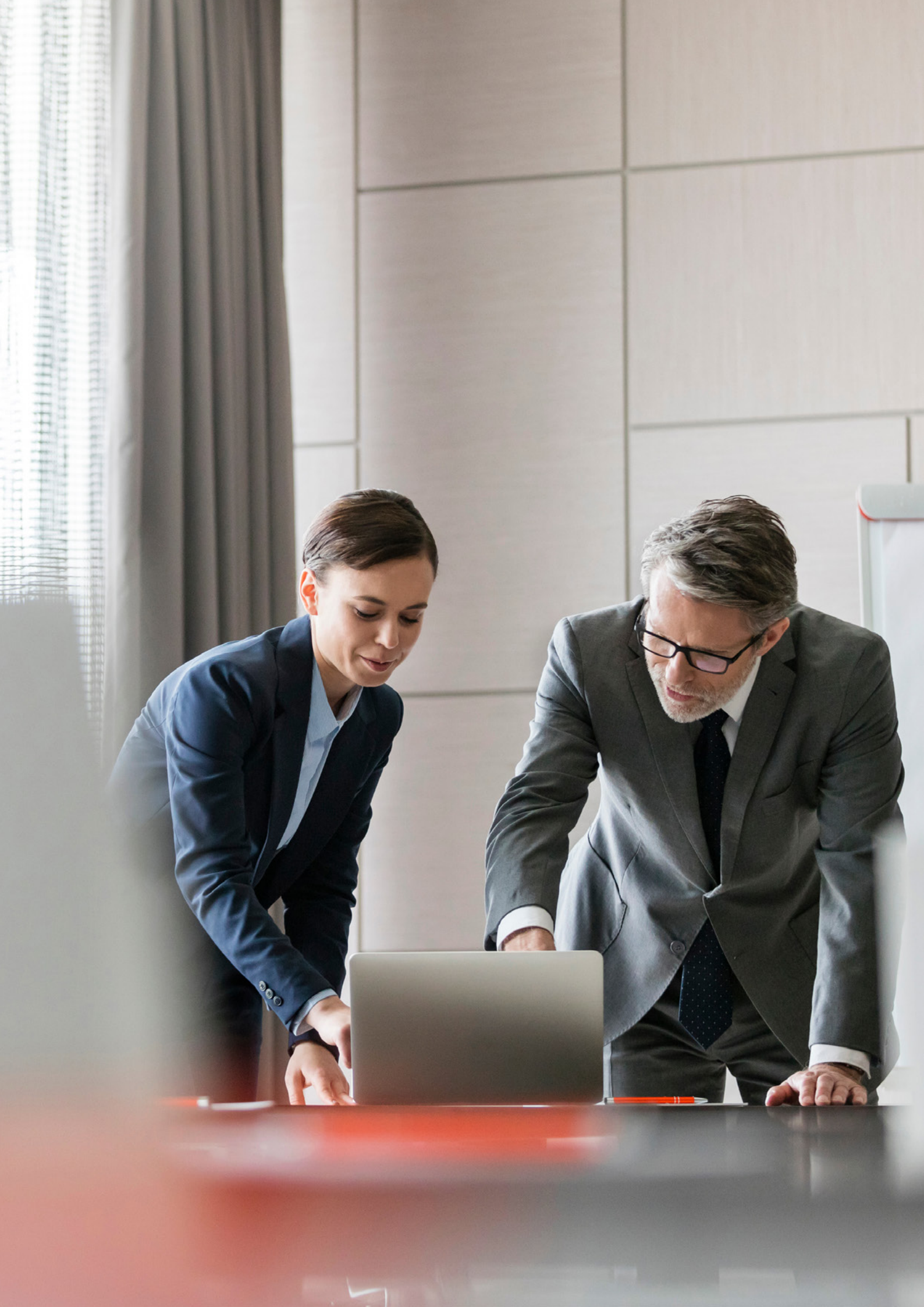
Unlike the previous iterations, this Bill does not include a DPA scheme, which would allow a company and the Commonwealth Director of Public Prosecutions (CDPP) to agree that the CDPP will not prosecute the company if it complies with specified conditions. In other words, for corporates, it is all stick and no carrot. This is out of step with other jurisdictions. The new "failure to prevent" offence is consistent with the UK's approach to economic crime (including the new failure to prevent fraud offence passed in 2023), but the Government's omission of the DPA regime is a departure from the UK model. DPAs are also available in several other foreign jurisdictions, including the US, Canada, France and Singapore.

The Opposition has tabled amendments to put a DPA scheme back in the Bill but it appears unlikely that these amendments will be adopted before the Bill is passed. Labor have previously been vocal opponents of DPAs, and while both the Greens and independent Senator Pocock expressed support for a DPA scheme in theory, they do not support the Opposition's amendments in their current form.

Given the remainder of the Bill, especially the main foreign bribery amendments, has bipartisan support, we do not expect the debate over DPAs to be a significant roadblock to the Bill's progress. The Labor Government is clearly motivated to tackle corruption issues, evidenced by the establishment of the NACC, recent Public Interest Disclosure reforms and expressions of Australia's commitment to the OECD Anti-Bribery Convention. Even though the Opposition reiterated that the Bill is an incomplete solution without DPAs, which have proven effective in enhancing the efficiency of foreign bribery prosecutions in other jurisdictions, they have indicated their support for the Bill regardless as part of their commitment to opposing foreign bribery. All of these developments suggest this Bill will move faster than its predecessors, even with a speed bump.

Once passed the Combatting Foreign Bribery Bill will be the most significant shake up of Australia's anti-corruption landscape for companies since the foreign bribery offence was introduced in 1999. The nature of these reforms will be familiar to businesses with a global footprint, and should not be surprising in light of increasingly loud calls for business integrity and good corporate citizenship. Australian businesses should review, and if necessary introduce or uplift, their anti-bribery and corruption compliance processes to ensure they are up to task when the Bill becomes law.

You can rest assured that your HSF Australian corporate crime and investigations team will continue to keep a close eye on the progress of this Bill and any related developments in 2024. Our Australian CC&I team will be sharing tips about how to make sure your business is prepared - watch this space.



More than words: whistleblower protections begin to bite

From top
Liz Macknay
Chris Hicks
Stephen Waddington

2023 saw some major developments relating to Australia's corporate whistleblower laws, and the agenda for 2024 is already full.

In March 2023, ASIC published its report entitled 'Good practices for handling whistleblower disclosures'. The report summarises the findings of ASIC's targeted review of the whistleblower programs of seven entities. The targeted review was part of ASIC's ongoing review into the implementation of the enhanced whistleblower laws.

In the report, ASIC identifies the following seven good practices for handling whistleblower disclosures:

- establishing a strong foundation for the whistleblower program (for example, through procedures and systems to embed the program's requirements);
- fostering a culture and practices to support whistleblowers;
- informing and training those involved in receiving or handling disclosures about protecting whistleblowers and treating material confidentially;
- monitoring, reviewing and improving the program (including seeking feedback from whistleblowers);
- using information from disclosures to address underlying harms and improve company performance;
- embedding senior executive accountability for the program; and
- creating frameworks to entrench effective director oversight.

The report builds on ASIC's existing guidance, including Regulatory Guide 270 regarding the whistleblower policy requirement. Consistent with that guidance, the report confirms ASIC's expectation that whistleblower policies should be detailed and specific, and backed by clear procedures for handling and investigating disclosures and protecting whistleblowers. ASIC also expects that entities' whistleblower programs will be living frameworks that improve over time in response to experience and feedback.

Also in March, ASIC brought its first case alleging civil contraventions of the revamped whistleblower protections in Part 9.4AAA of the *Corporations Act*. In proceedings in the Federal Court, ASIC alleges that ASX-listed coal miner TerraCom Limited, and certain of its directors and former directors, caused detriment to a former employee who raised concerns about falsified coal analysis certificates. ASIC alleges that the defendants caused the whistleblower emotional, reputational and economic harm by making false, misleading and 'otherwise hurtful' announcements that named the whistleblower and described his allegations as 'false' and 'unfounded'. The case is likely to go to trial in 2024 and will be test the scope of the whistleblower protections. It signals that ASIC has moved into a more proactive phase of enforcement.

There have been some notable developments in relation to public sector whistleblowing. The Commonwealth Attorney General intervened to discontinue the long-running and controversial prosecution of ACT lawyer Bernard Collaery, who was accused of conspiring with a client to share official government secrets. However, a separate case against whistleblower and former army lawyer David McBride went ahead and, in November, McBride pleaded guilty to disclosing military secrets. He will be sentenced in 2024.

Also in November 2023, the Commonwealth released a consultation paper as part of its ongoing reform of public sector whistleblowing laws. The process was commenced following the 2016 review of the *Public Interest Disclosure Act* (PID) by Philip Moss AM. The Government is seeking public input on issues such as:

- who can make and receive protected disclosures, including a 'no wrong doors' referral approach;
- pathways to make a disclosure outside of government, including requirements for external disclosures, access to professional assistance, and the treatment of intelligence information;
- protections and remedies available under the PID Act, including requirements to access protections and extending immunities to cover preparatory acts;
- a potential dedicated Whistleblower Protection Authority or Commissioner.

The results of the consultation are expected in 2024. We can also expect continued scrutiny on whistleblower legislation in the second half of 2024, with the 5-year review of the refreshed *Corporations Act* whistleblower provisions expected to commence.

AUSTRAC v Crown judgment: Key points of interest for reporting entities in Australia's Anti-Money Laundering/Counter-Terrorism Financing regime

From top
Bryony Adams
Danielle Briers
Maritsa Samios

The Federal Court of Australia has approved a settlement between AUSTRAC and both Crown Melbourne and Crown Perth (**Crown**), resulting in a $450 million penalty for breaches of the *Anti-Money Laundering and Counter-Terrorism Financing Act* (**the Act**). This case contains many points of interest for reporting entities and highlights the criticality of robust risk assessment and meaningful Board/senior management oversight in AML/CTF programs.

Key Points

On 11 July 2023, the Federal Court of Australia handed down its judgment in *CEO of AUSTRAC v Crown Melbourne Limited & Anor* [2023] FCA 782.

Lee J of the Federal Court approved the settlement reached between Crown and AUSTRAC, including a penalty figure that the parties had calculated at $450 million, based on breaches of ss 36 and 81 of the Act, although seemingly not without some considerable hesitation.

We set out below some key points of interest for reporting entities when considering the impact of the parties' negotiated statement of agreed facts (**SAFA**) and the Court's judgment.

The critical importance of risk assessment

Consistent with the position that AUSTRAC has adopted in its various other civil penalty proceedings to date, it is plain from the Crown case that AUSTRAC sees a robust assessment of the risk of financial crime activity (ML/TF risk) as foundational to any reporting entity's ability to comply with its obligations under the Act.

In the Crown case, AUSTRAC's position was that 'Part A' of an AML/CTF Program (for which the primary purpose must be to identify, mitigate and manage the ML/TF risks that the reporting entity may reasonably face) will not be *capable* of holding that purpose unless it at least:

- refers to or incorporates a **written ML/TF risk assessment methodology** that is capable of appropriately identifying and assessing the ML/TF risks of all designated services provided by the reporting entity;
- is **aligned to the ML/TF risks reasonably faced** by the reporting entity with respect to designated services, as **periodically assessed** in accordance with an appropriate ML/TF risk assessment methodology;
- includes **appropriate risk-based systems and controls** that are capable (as a matter of design) of identifying, mitigating and managing ML/TF risks reasonably faced by the reporting entity, consistent with risk appetite; and
- includes or establishes an appropriate framework for **approval and oversight by Board and senior management**.

Lee J accepted that Crown's AML/CTF Program failed to meet these criteria for a period and that it was therefore deficient throughout that period.

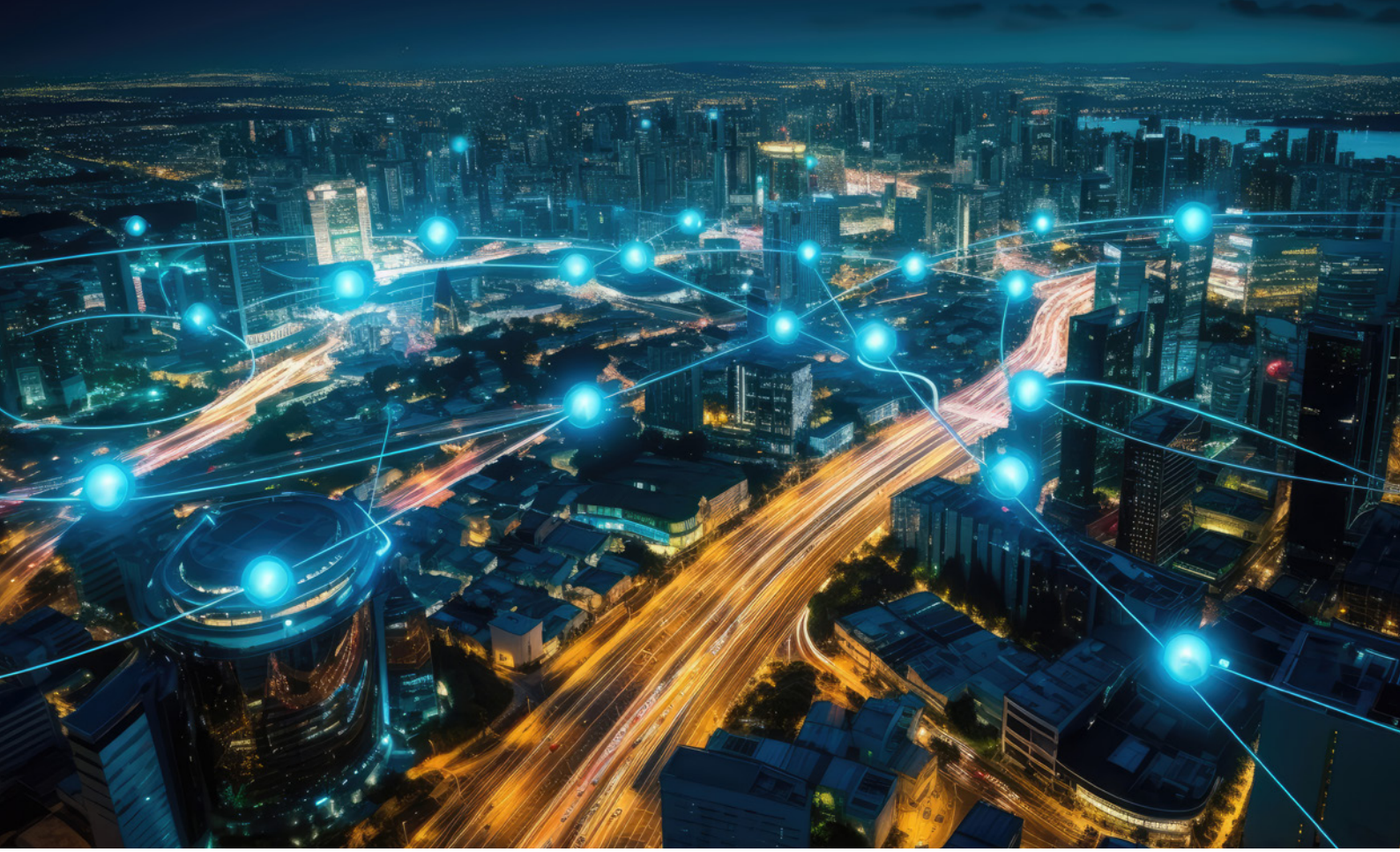
This serves as a useful illustration to reporting entities that (contrary to misconception) they cannot hope to mitigate their risk of non-compliance with the Act by adopting a high level and non-prescriptive program framework – rather, a failure to both undertake and document a detailed assessment of risk and then to reflect that risk in well designed and specific processes, systems and controls will simply increase the prospect of their program being found to be deficient.

'Appropriate risk-based procedures, systems and controls'

AUSTRAC's position acknowledged that the Act 'does not require ML/TF risks to be eliminated' and that it does not (presently) prescribe exactly how a reporting entity is to manage its ML/TF risks. Rather, mirroring the language of Justice Perram in *CEO of AUSTRAC v TAB Limited (No 3)* [2017] FCA 1296, it 'reposes trust' in reporting entities to design and implement risk management procedures, systems and controls to detect and deter ML/TF, which are appropriate for its business and which it will adopt and maintain through its AML/CTF program.

Lee J's judgment confirms that an AML/CTF program will not include 'appropriate risk-based procedures, systems and controls' if the reporting entity has designed them without taking into account:

- the nature, size and complexity of its business; and
- the ML/TF risks it reasonably faces, having regard to:
  - the types of designated services it provides;
  - the types of customers it provides designated services to;
  - the channels through which it delivers designated services; and
  - the foreign jurisdictions with which it deals.



Further, the judgment confirms that an AML/CTF program will only meet this standard of 'appropriate' risk based procedures, systems and controls if those procedures, systems and controls are 'aligned and proportionate to the risks reasonably faced', having regard to those matters.

In the Crown case, his Honour considered there to be particular deficiencies in Crown's risk management of its junkets channel, which involved complex transactional chains and higher attendant ML/TF risk but was not said to warrant sufficient separate risk scrutiny and management in its AML/CTF program. This serves as a further reminder (consistent with past AUSTRAC enforcement actions) of the need to ensure that separate and careful focus is given to (and recorded in respect of) any aspects of a reporting entity's business (impacting customers, channels, services, jurisdictions, new technologies, etc) that may carry a higher inherent risk of financial crime activity.

The requirements of board and senior management oversight

Crown acknowledged that Part A of its AML/CTF program had not been approved by the governing board and senior management and that:

- reporting to the Crown boards and senior management on AML/CTF compliance and ML/TF risks was ad hoc and incomplete;
- the Crown boards did not determine ML/TF risk appetite for the purpose of the Program;
- the Crown boards did not have documented process in place to asure in-depth discussion of ML/TF risk as against measurable criteria at regular intervals as part of a rolling agenda; and
- there was a lack of clarity and understanding within Crown as to reporting lines from senior management and their roles and accountabilities.

These deficiencies, along with concerns about the appropriateness of the governance framework reflected in Crown's Part A, contributed to the findings that Crown did not have a compliant Part A program for a significant period of time.

This is the first time that AUSTRAC has so clearly positioned the adequacy of board governance and oversight as itself contributing to an assessment of program compliance and will be of particular interest to boards of reporting entities in seeking to discharge their approval and oversight responsibilities.

Of course, while there are some governance requirements that are peculiar to the AML/CTF context, AUSTRAC's heightened focus on governance and oversight in a non-financial risk management context is consistent with a broader regulatory trend over recent years, including in other high focus areas such as ESG.

Transaction monitoring requirements

Lee J held that Crown's transaction monitoring as reflected in its Part A did not fully comply with the requirements of the AML/CTF Rules, including because it:

- was not aligned with an appropriate ML/TF risk assessment, given such an assessment had not occurred (as noted above);
- was not capable of detecting various well known ML/TF typologies and vulnerabilities faced by casinos;
- was instead reliant on manual and observational processes, which were inadequate given the nature, size and complexity of Crown's business and the types of ML/TF risks it faced.

Further information on these deficiencies were reflected in the SAFA, which noted that Crown's transaction monitoring processes were focused on individual transaction sets, and not capable of consistently detecting suspicious or unusual patterns of transactions or behaviours across complex transaction chains involving multiple designated services.

In addition, the parties agreed that:

- the transaction monitoring program did not provide adequate review criteria for the system-generated transaction activity reports that were central to the manual processes and nor did it provide adequate guidance on how to identify unusually large transactions;

- staff reviewing the system-generated transaction activity reports did not receive adequate ML/TF risk awareness training;
- the resourcing of Crown's AML / financial crime function 'did not support the consistent generation, review and actioning of systems-generated or exceptions- based reports';
- the data underlying the system-generated transaction activity reports were unreliable in various ways, including due to manual data entry susceptible to human error, incomplete data collecting processes for certain customers / transactions, and unreliable linking of transactions to customers; and
- there were no appropriate assurance processes to ensure that the systems and controls in the transaction monitoring program were being applied correctly, were operating as intended, and remained appropriate.

The above is not an exhaustive list but serves as a useful reminder to reporting entities of the complexity and issues that can arise in establishing a compliant and effective transaction monitoring regime.

Customer identification, due diligence and reporting requirements

Lee J also held that there were deficiencies in Crown's Part A program in relation to its approach to customer due diligence and reporting.

Of particular concern in this context was Crown's approach to enhanced customer due diligence (**ECDD**) in circumstances where many of its customers were higher risk, such as junket operators, international VIP customers and politically exposed persons.

A related issue in this context was Crown's approach to customer identification and verification (**IDV**) under Part B of its AML/CTF program. Crown conceded in the SAFA that:

- customers were automatically rated as low risk for IDV purposes without appropriate consideration given to the ML/TF risk posed by the customer type; and
- its review of customer risk ratings was too infrequent to appropriately identify high risk customers and this process did not involve a referral of the customer for full ECDD.

These design concerns then tied in with specific customer due diligence contraventions in the case of 546 admitted instances.

Calculation of penalty

Notable aspects of the penalty imposed in this matter included:

The deferred payment plan sought by Crown/AUSTRAC

After some deliberation, the Court approved a payment plan whereby Crown must pay $125 million within 28 days; a further $125 million within one year; and the remaining $200 million within two years. The need for a payment plan was linked to Crown's financial position, including the significant impact of COVID-19 restrictions on its business, continuing challenging trading conditions and the need to maintain sufficient liquidity to continue as a going concern and withstand future unanticipated costs.

Justice Lee tested AUSTRAC and Crown on this point, wanting to be satisfied that the sum was in the appropriate range (including in circumstances where the payment plan

and a lack of provision for interest meant its net present value was $405 million).

His Honour expressed the view that aspects of the evidence of Crown's financial position were 'scant, unsupported by business records, or not addressed'; and commented that in hindsight it may have been prudent to appoint an amicus curiae (friend of the court) to test the evidence and form a view on whether cross-examination was warranted (in circumstances where AUSTRAC 'had become... a friend of the deal' and would not be seeking cross-examination).

Ultimately, though, his Honour was content to impose the payment plan (albeit with a mechanism for Crown's financial position to be revisited at the end of FY23 and FY24 so that AUSTRAC can apply for payment sooner if its financial position has improved).

Size of penalty relative to number and severity of contraventions / other cases

Justice Lee was satisfied the $450 million penalty was within the permissible range of appropriate penalties, but said this 'on balance and not without some hesitation'.

His Honour noted that the facts pointed to the 'necessity for a very substantial penalty'. The factors his Honour viewed as particularly important in approving the figure were:

- In light of Crown's size and financial position, the proposed penalty cannot be regarded as a mere 'acceptable cost of doing business' and is adequate to ensure that Crown is deterred from engaging in future non-compliance;
- Crown's non-compliance 'arose from a breach of the trust reposed in it by Parliament' - the contraventions were 'appalling', resulting in innumerable breaches of s 81(1) and a significant number of breaches of s 36(1) of the Act;
- The contravening conduct had real consequences for the Australian community and financial system. In the absence of appropriate risk-management programs, Crown failed to manage the risk of ML/TF posed by junkets and high-risk customers until November 2020. This resulted in a failure to monitor billions of dollars in suspicious transactions, which inhibited the investigation and prosecution of serious crimes by law enforcement agencies;
- The contraventions persisted over a considerable period of time, namely six years from March 2016 to March 2022. They were not isolated events: they arose out of a fundamental failure to maintain an appropriate program for managing the risk of ML/TF; and
- Crown obtained significant revenue streams during the period in which its AML/CTF programs were non-compliant, including revenue from high-risk channels (such as junkets) which bore the typologies of money laundering activity.

Whilst the figures in past AML/CTF cases run by AUSTRAC are higher, the judgment in this case illustrates how the appropriate penalty to achieve the primary (if not sole) objective of deterrence can only be determined by taking all circumstances into account, including the entity's size and financial situation. As a result, an approach of looking at past AML/CTF cases can one take one so far in conducting the 'instinctive synthesis' required to arrive at an appropriate penalty figure.

Human Appeal v Beyond Bank: tipping off, debanking and managing money laundering risk

From top
Bryony Adams
Stephanie Crosbie
Brenda Li

A recent decision by the New South Wales Supreme Court illustrates some of the complexities that can arise for reporting entities when seeking to adhere to regulatory expectations and managing their risk in an AML/CTF context.

In *Human Appeal International Australia v Beyond Bank Australia Ltd (No 2)* [2023] NSWSC 1161, a banking customer had its account facilities closed unilaterally without being provided with reasons for the bank's decision. The customer took action against the bank, claiming that it could only be debanked on reasonable grounds and that those grounds had not been established. The Court essentially agreed with the customer.

There was some suggestion in the judgment that the bank may have felt unable to explain its decision due to the 'tipping off' provisions in the *Anti-Money Laundering and Counter-Terrorism Financing Act 2006* (Cth) (the **AML/CTF Act**): see ss 123 and 124 of the AML/CTF Act. Those provisions essentially constrain reporting entities from communicating information to third parties from which it is either clear, or could reasonably be inferred, that the reporting entity has been required to file a 'suspicious matter report' with AUSTRAC. The case therefore provides food for thought to other entities seeking to navigate challenges associated with off-boarding customers without risk of offending the tipping off provisions.

Background

Human Appeal International Australia (**Human Appeal**), a charitable organisation, established banking facilities with Beyond Bank Australia Limited (the **Bank**) in March 2021. In mid-August 2021, the Bank notified Human Appeal that it was closing its facilities but declined to give any reasons for its decision other than to say that a review had been conducted and the business was not suitable.

The Bank's terms and conditions specified that it 'may, at any time, close any of your Accounts by giving you 20 days written notice. The notice does not have to specify the reasons for the closure'.

Notwithstanding this, Human Appeal brought proceedings against the Bank, claiming that:

1. the Bank's termination of its facilities was invalid. It argued that the Bank's right to terminate was subject was to an obligation of good faith and reasonableness, and because the Bank did not admit any evidence demonstrating it had a valid reason to terminate, it should be inferred that no reasonable grounds existed; and
2. if the Bank's terms and conditions did permit termination without cause, this would be inconsistent with the Customer Owned Banking Code of Practice (the Code), being the industry code of the Customer Owned Banking Association to which the Bank had voluntarily subscribed and expressly incorporated into its terms. Human Appeal contended that compliance with the Code could be enforced against the Bank and that orders should be made compelling the Bank to vary its terms and conditions so as to require the existence of reasonable grounds in accordance with the Code.

Interaction of tipping off obligations and notices to produce

In dealing with the evidence, Parker J made a number of observations regarding the interaction of the AML 'tipping off' obligations and notices to produce.

Human Appeal sought production by the Bank of documents relating to its decision to terminate Human Appeal's facilities. In response, the Bank provided bank statements of Human Appeal's accounts, template letters for the notification of an account closure, and correspondence between the Bank and Human Appeal relating to the termination. However, the Bank did not produce any records of the review or the decision, and there was nothing said to suggest that the Bank had withheld any documents from production.

As such, it was not clear why the Bank withheld the relevant documents, or if there were any documents withheld in the first place. The Bank's formal position was that there were no other documents to be produced. However, when asked whether there were other documents caught by the notice, senior counsel for the Bank gave a more qualified response, indicating that the notice had been complied with in accordance with the Bank's statutory obligations and that the AML/CTF Act prevented it from disclosing whether or not any additional documents were caught.

Justice Parker did not attempt to resolve this point given the adequacy of the Bank's response to the notice was not formally raised as an issue. However, his Honour did observe that the Bank would not be justified in withholding documents without also disclosing the fact that it had done so.

His Honour also considered the interaction between the tipping off provisions and an entity's disclosure obligations under a notice to produce. His Honour observed that:

- s 123(1) and (2) of the AML/CTF Act prevent disclosure of the information to another person, such as a party to court proceedings. However, they do not prevent disclosure to a court itself because a court is not relevantly a 'person';
- s 123(10) of the AML/CTF Act, which addresses disclosure to courts, is not therefore an exception to the primary tipping off restrictions but instead operates as a stand-alone provision; and

- in the case of a notice to produce to court (or a subpoena), subsection (10) may be applicable. However, in the case of an inter partes notice to produce, it is arguable that s 123(10) does not apply at all and that considerations of tipping off are focussed purely on subsections (1) and (2).

In either event, his Honour observed that the tipping off provisions should not be read as preventing disclosure, in general terms, of the administrative burden that the AML/CTF Act, together with other reporting obligations, imposed on a reporting entity. Instead, tipping off restrictions ought to be considered and interpreted strictly on their terms and by reference to their purpose of managing risk that persons under investigation are relevantly 'tipped off'.

While this conclusion is superficially unsurprising, in practice there can of course be significant challenges in navigating the extent to which information can be shared with third parties without falling foul of the tipping off provisions. Those provisions are notoriously difficult to interpret. They are not limited in their operation to communications made to persons under investigation and are not assessed by reference to the reporting entity's intent (but instead by reference to an objective assessment of whether it *could* reasonably be inferred from the information that a suspicious matter reporting obligation had arisen). They expose the entity to a criminal offence. It is therefore equally unsurprising that reporting entities often choose to be cautious in their approach to tipping off in the context of document productions.

Validity of termination

Duty of good faith and reasonableness

The Bank in this case conceded that it was only entitled to terminate Human Appeal's banking facilities if it had a valid commercial reason to do so. Accordingly, Parker J left open the question of whether a bank's right to terminate is *always* subject to an implied obligation of good faith or reasonableness. Instead, his Honour proceeded on the basis that the concession was likely informed by the fact-specific consideration that the Bank's terms and conditions may arguably be said to contain an *express* obligation of good faith and reasonableness.

A key consideration was that the Bank had incorporated Part C of the Code in its terms and conditions. The Code listed '10 Key Promises' made to customers which relevantly included that the Bank would be 'fair and ethical in [its] dealings' and would treat its customers 'fairly and reasonably in all [its] dealings'.

Issues with the Bank's terms and conditions

Through its incorporation of the Code, the Bank's terms and conditions were seen as requiring it to 'strike a fair balance between your legitimate needs and interests as our customer, and our interests and obligations, including our prudential obligations.' This was understood by Parker J as imposing an obligation on the Bank to adopt revised terms and conditions if the existing terms did not reflect a 'fair balance' of the parties' interests. Justice Parker ultimately found that the clause enabling the Bank to terminate without reasons did not strike a 'fair balance' between the parties and that the Bank would need to adopt fresh terms and conditions. This was because:

- the Bank's concession that it was not entitled to exercise its termination right without a valid commercial reason had little practical value given the customer would still be left with no means of finding out the reason for the decision; and
- relatedly, there would be no way for a customer to know that the Bank now accepted that termination without a valid commercial reason would be ineffective.

Failure to discharge evidentiary burden

Justice Parker ultimately found the Bank's termination to be invalid on the basis that it did not put forward evidence of its reasons and therefore could not satisfy the Court that it had a legitimate commercial basis for deciding to off-board its customer.

His Honour observed that if it were the case that compliance with the AML/CTF Act had resulted in disproportionate time being spent by members of the Bank's Financial Crimes team on monitoring Human Appeal's accounts, and the Bank no longer wished to bear that 'administrative burden', there was no reason why the Bank could not have disclosed this rationale in clear terms (without going into detail about any specific transactions/reports).

His Honour did not accept that the rationale for off-boarding was inherently incapable of being disclosed due to the tipping off provisions. The Bank submitted that if its decision was based on suspected financial crime activity, it would have been prevented from giving evidence about it. To this, the Bank sought to rely on the decision in *Marundrury v Commonwealth Bank of Australia (No 2)* [2022] FCA 916 in which a claim was dismissed as an abuse of process on the basis that sections 123 and 124 of the AML/CTF Act prevented a reporting entity from defending itself against the plaintiffs' claims. However, Parker J distinguished the Marundrury decision on the basis that the claims pleaded by the plaintiffs in that case directly involved an allegation that the defendant had breached its suspicious matter reporting obligations, whereas any issue in the present case arose more incidentally.

It is, of course, entirely possible that the reasons for termination in this case did not engage the tipping off provisions and could therefore have been freely given. Extrapolating from his Honour's observations, even if the reasons for termination include the identification of suspicious activity, it may be possible for reporting entities faced with similar decisions in future to point to administrative burdens, risk appetite or other matters that do not require them to specifically raise the existence of suspicious activity as a reason for account closures. However, his Honour's reasons expose an ongoing challenge for reporting entities who wish to 'de-bank' customers where those reasons are in fact inherently tied to concerns that they are precluded by law from sharing.

A proposed change on the horizon

Some of the challenges that may arise for reporting entities when seeking to off-board customers without infringing tipping off obligations may be able to be addressed differently in the future, depending on the outcome of the public consultation on Australia's anti-money laundering and counter-terrorism financing regime announced on 20 April 2023 (the **Consultation**).

Among other things, the Consultation proposes that eligible agencies be authorised to issue a 'keep open' notice directly to a reporting entity that is concerned that the closure of an account will run too significant a risk of tipping off the account holder of the identification of suspicious activity.

Australian sanctions: A look back at 2023 and prospects for 2024

From top
Leon Chung
Natasha Reurts
Kayla Laird

Australia's evolving sanctions landscape in 2023 and into 2024 demonstrates the importance for companies to remain alert to legal change, and have robust compliance frameworks that equip their business to respond.

Throughout 2023, Australia has continued to impose sanctions against Russia in response to the ongoing political situation in Ukraine, as well as against Iran to curb its nuclear ambitions and prevent breaches of international arms regulations.

Expansions to the sanctions regimes in respect of Russia and Ukraine, and Iran have been instituted by a series of amendments to the *Autonomous Sanctions Regulations 2011* (Cth). These amendments have focused on key Russian individuals and entities influential in strategic and economic areas, as well as on those involved with supporting Iran's nuclear or missile initiatives, in defiance of UN Security Council resolutions or actions that compromise the sovereignty of other nations.

Key updates in 2023 include:

- The imposition of further targeted financial sanctions and travel bans in relation to Russian individuals and entities now totalling over 1,200 individuals and entities;
- An export prohibition on hand tools, nuclear reactors and electrical machinery and equipment (and parts thereof) declaring these goods as 'export sanctioned goods' for Russia and Ukraine;
- The reinstatement of sanctions and travel bans on 19 Iranian individuals and 57 entities linked to Iran's nuclear and missile programs, aligning with international partners and UN Security Council Resolution 2231, while adding new restrictions on three individuals and 11 entities associated with sanctioned parties. The Australian Government is determined to pressure Iran into compliance with its nuclear commitments and has signalled its dedication to nuclear non-proliferation by updating its autonomous sanctions framework to address threats to regional stability posed by Iran's actions; and
- Ahead of the sunsetting of the Australian autonomous sanctions regime, the Australian Sanctions Office conducted a review of Australia's legal framework for autonomous sanctions, evaluating Australia's current sanctions framework and suggesting potential improvements to support the Australian Government's foreign policy objectives.

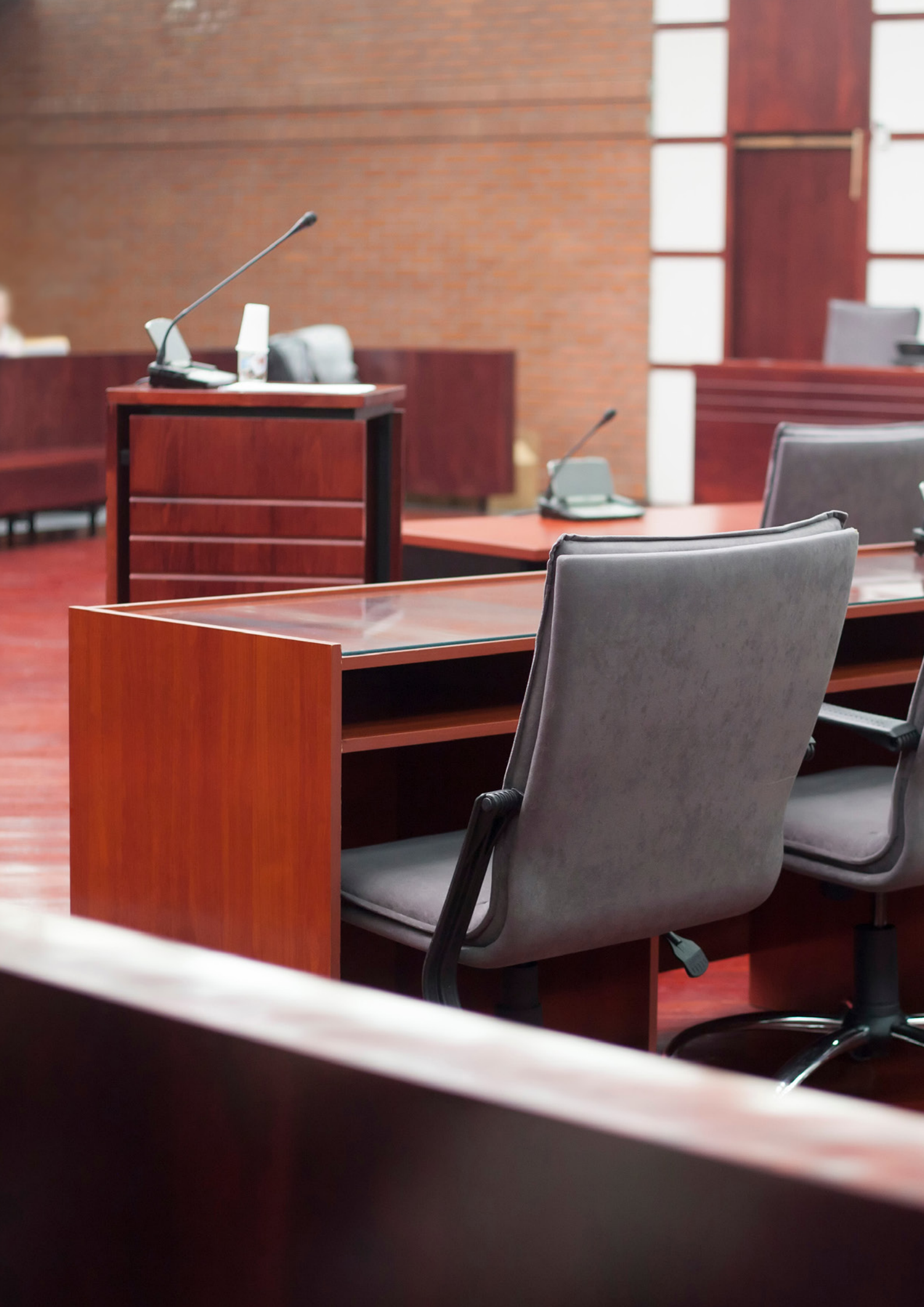
Developments in 2024

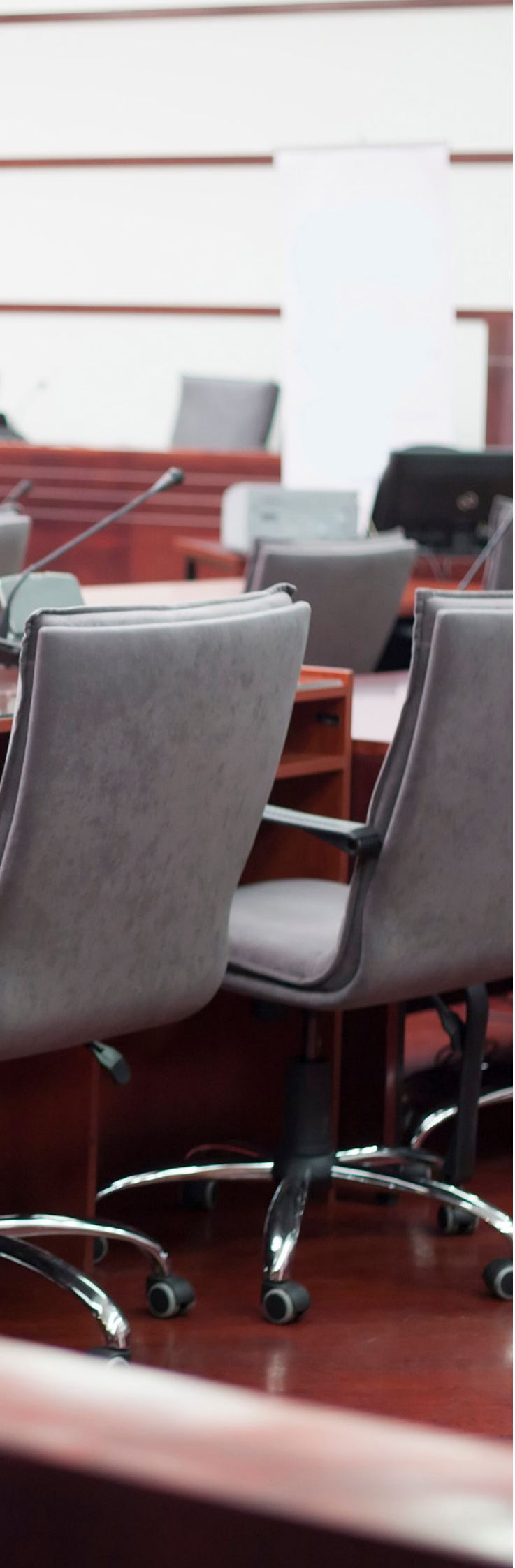
In late January 2024, following terrorist attacks perpetrated by Hamas, the Australian Government imposed further counter-terrorism financing sanctions on 12 persons and three entities linked to Hamas, Hizballah and Palestinian Islamic Jihad. These new sanctions mirror sanctions imposed on Hamas-linked individuals and entities by the United States, United Kingdom and the European Union.

In a first, on 23 January 2024, Australia imposed cyber sanctions on a Russian national for his role in the 2022 ransomware attack and compromise of Medibank Private. This is the first sanction targeting malicious cyber activity to be imposed following the introduction of new thematic regimes in December 2021 and, consistent with the *2023-2030 Australian Cyber Security Strategy*, highlights the Australian Government's intention to deter and respond to significant cyber incidents with sanctions.

As we move into 2024, we expect further developments in response to the situations in Ukraine and Iran. In particular, we expect the Australian Government will continue to align its sanctions measures with policy decisions of key jurisdictions such as the United States, United Kingdom and European Union, particularly if there are further developments in the political situation in Ukraine. Notably, in mid-2023 the EU and the UK introduced restrictions on the import of Russian origin iron and steel products, similar measures may be considered by the Australian government.

The Autonomous Sanctions Regulations are set to expire on 1 April 2024. It is therefore expected that legislative updates will be forthcoming, taking into account the feedback from the submissions received from Government and the private sector.





'Fearless but fair, independent and impartial': The NACC - Australia's new integrity body

Australia's new National Anti-Corruption Commission (**NACC**) was launched in July 2023, aiming to create a 'fearless but fair, independent and impartial' integrity body. Since then, the NACC has already received over 2,000 referrals, covering its broad remit in respect of the Commonwealth government, agencies and their contractors.

In 2024 we can expect to see the NACC start to flex its broad investigatory powers as it pursues its mandate to investigate 'serious or systemic' 'corrupt conduct'.

Corrupt conduct is broadly defined, and goes beyond criminally recognised corruption offences. It can be a breach of public trust, abuse of office or misuse of information by a Commonwealth public official. It can also include conduct of any person that (could) adversely affect(s) the honest or impartial exercise of a Commonwealth public official's powers or duties.

As we continue to monitor the NACC's enforcement activity, some key points for consideration are:

- **Businesses contracted to provide a good or service to the Commonwealth are deemed to be 'public officials':** If a company contracts with the Commonwealth or a Commonwealth agency for the provision of goods or services, then its officers, employees, and subcontractors who are responsible for the provision of such goods or services will be deemed to be 'public officials' under the NACC Act. The conduct of any person (whether or not a public official) that seeks to influence the honest or impartial exercise of the company's duties in respect to the Commonwealth contract may constitute corrupt conduct that may be investigated by the NACC. Investigation can include searches of company premises and persons, tapping of phones, and compelling employees to give evidence and provide documents.
- **The NACC Act adds another layer to the integrity framework:** The NACC Act creates a new avenue for reporting and investigating corrupt conduct involving public officials at the Commonwealth level. Though the NACC is an important source of best practice guidance for integrity frameworks, not only for Commonwealth agencies, but also for Australian businesses more broadly, it stands alongside the existing integrity legislation and whistleblowing frameworks in the *Public Interest Disclosure Act 2013* (Cth), *Corporations Act 2001* (Cth) and *Taxation Administration Act 1953* (Cth) as well as state anti-corruption commissions.

- **Anti-corruption experts have been appointed to the NACC:** The NACC is comprised of highly regarded senior public officials with a wealth of experience and expertise which will play an influential role in shaping how the NACC exercises its mandate in its early years. The first appointed Commissioner is The Hon Justice Paul Brereton AM RFD, who previously led the investigation into criminal misconduct by Australian Special Forces in Afghanistan. Commissioner Brereton indicated in his inaugural address that only a small proportion of matters referred to the NACC are expected to reach the stage of full investigation. Instead, the NACC will focus on whether and to what extent a corruption investigation by the NACC is likely to 'add value in the public interest'.
- **Any person who has relevant information regarding potential corrupt conduct can report to the NACC and receive protections:** Any person can voluntarily, and anonymously, contact the NACC to provide information or evidence about a corruption issue. Similar to other whistleblowing regimes, a person who makes a disclosure to the NACC will be entitled to certain protections under the NACC Act including immunity from civil, criminal, and administrative liability. They are also entitled to protection from reprisals such as dismissal, injury, alteration of an employee's position to their detriment, or discrimination.
- **The NACC has very broad and intrusive investigative powers, similar to state-level corruption commissions:** Some significant powers to be aware of include:
  - A person may receive a notice to produce (information or documents) that contains a 'non-disclosure notation', restricting the recipient from sharing the content or existence of the notice to produce with anyone, even their employer.
  - A person is not permitted to withhold information or documents subject to a notice to produce on the basis of legal professional privilege or privilege against self-incrimination. However, the production of such material to the NACC will not amount to a waiver of privilege and cannot be used against the individual in criminal proceedings. Legal professional privilege may still be claimed over legal advice provided in relation to appearing before or producing material to the NACC.
  - The NACC can hold private hearings and may only conduct public hearings in exceptional circumstances.
  - Premises occupied by Commonwealth agencies can be searched by the NACC without a warrant and any documents can be inspected, copied, or seized. The NACC may also apply for and execute search warrants for places, vehicles, and people.
- **Findings of corrupt conduct can be published in a public report:** At the conclusion of a corruption investigation, the NACC must produce a report of its findings for the Attorney-General and may publish the report in whole or in part if the NACC determines it is in the public interest to do so. A NACC investigation and report can therefore have significant reputational implications for any individual or company involved. However, critical findings or opinions are not published without the affected person having the opportunity to be heard and make submissions in advance. Commissioner Brereton has stated that nearly 90% of the NACC's reports have not been reported in the media.

Organisations can and should be taking steps to ensure compliance with the NACC and areas that may fall within NACC scrutiny. Examples of these steps include:

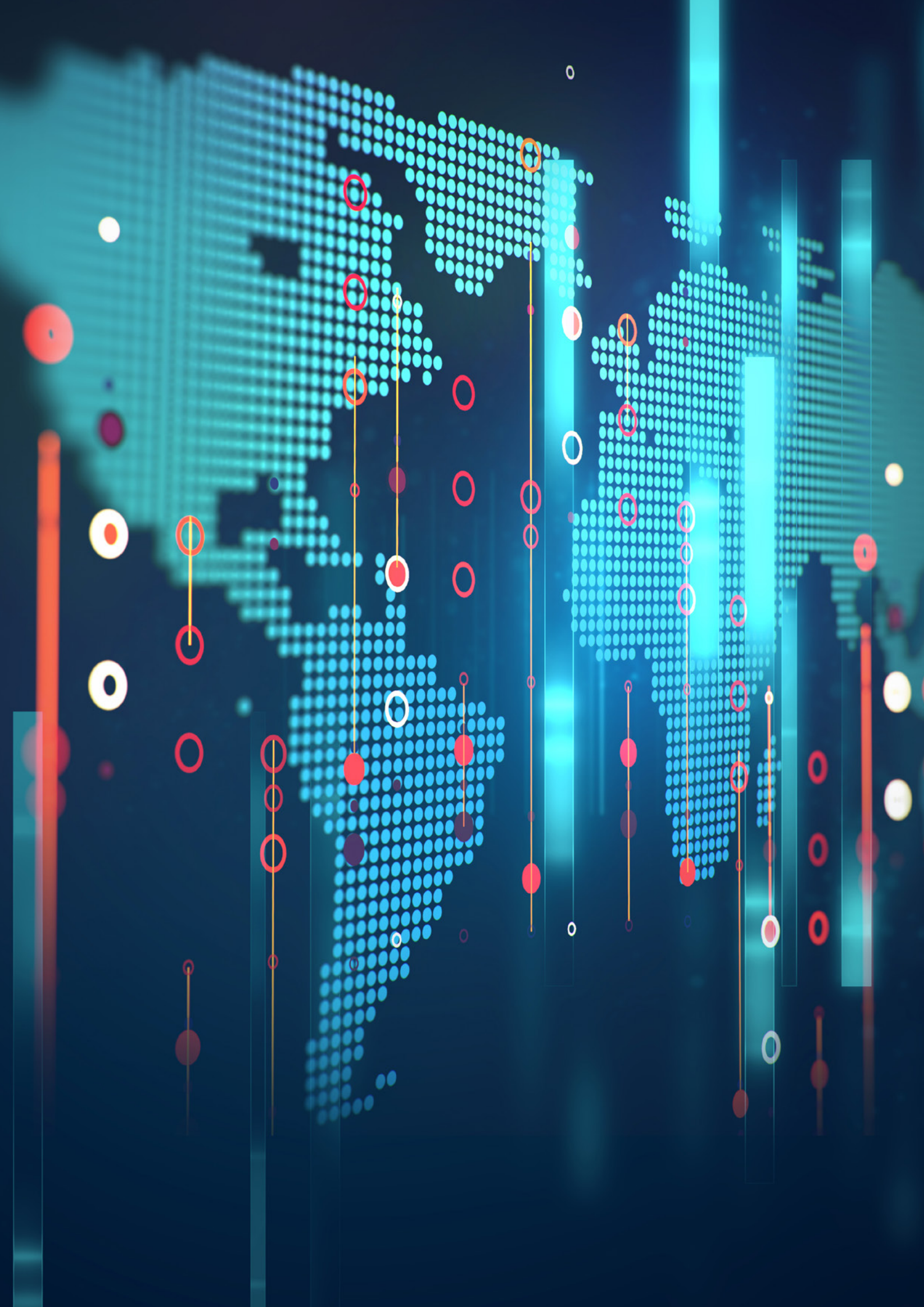
- Continuing to review policies and procedures relating to integrity and whistleblowing within your organisation to ensure that they are up to date and consider potential touch points with the NACC. Entities that are subject to both private sector whistleblower provisions in the Corporations Act (and Taxation is 'Administration Act or Public Interest Disclosure Act'), as well as potential NACC jurisdiction, should be reviewing their policies and procedures to ensure that they are clear on how to appropriately identify, handle, and escalate potential corruption concerns;
- Ensuring your organisation fosters a culture where employees feel comfortable reporting suspected corrupt conduct internally, and also considering what you need to communicate to your employees as well as suppliers in terms of integrity and probity expectations within your organisation; and
- Reviewing the guidance being published by the Attorney-General's Department on the NACC's operation.

From top

Jacqui Wootton

Madeleine Ryan

Caitlin Philp



Contacts – who can help?

Corporate Crime & Investigations team

Australia

Jacqueline Wootton
Partner and Co-head of Australian corporate crime & investigations team
T +61 7 3258 6569
jacqueline.wootton@hsf.com

Leon Chung
Partner and Co-head of Australian corporate crime & investigations team
T +61 2 9225 5716
leon.chung@hsf.com

Bryony Adams
Partner
T +61 2 9225 5288
bryony.adams@hsf.com

Kate S Cahill
Partner
T +61 2 9322 4413
kate.s.cahill@hsf.com

Andrew Eastwood
Partner
T +61 2 9225 5442
andrew.eastwood@hsf.com

Tania Gray
Partner
T +61 2 9322 4733
tania.gray@hsf.com

Elizabeth Macknay
Partner
T +61 8 9211 7806
elizabeth.macknay@hsf.com

Merryn Quayle
Partner
T +61 3 9288 1499
merryn.quayle@hsf.com

Mark Smyth
Partner
T +61 2 9225 5440
mark.smyth@hsf.com

Anna Sutherland
Partner
T +61 2 9225 5280
anna.sutherland@hsf.com

Christine Wong
Partner
T +61 2 9225 5475
christine.wong@hsf.com

For a full list of our global offices visit **HERBERTSMITHFREEHILLS.COM**