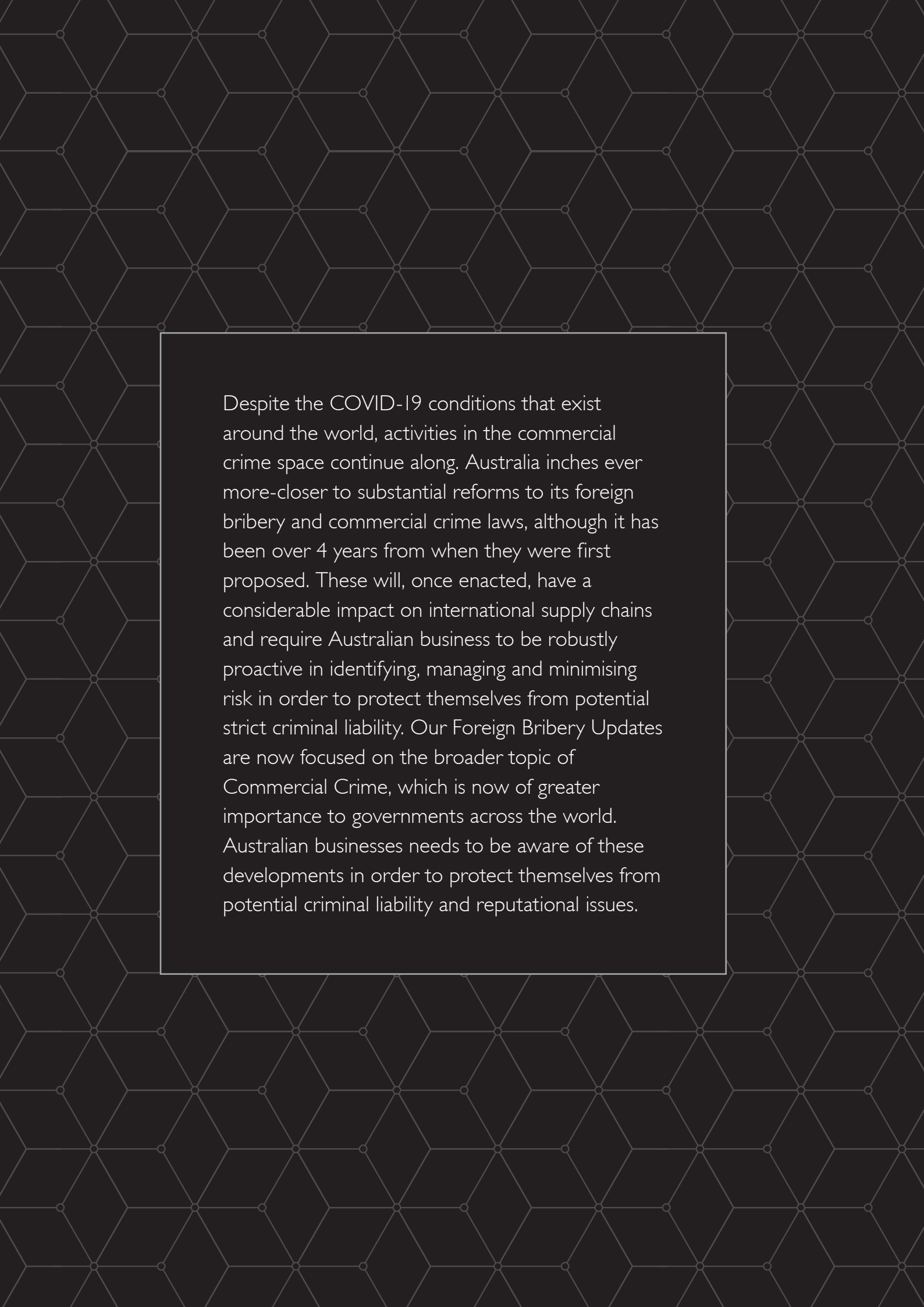

JOHNSON
WINTER &
SLATTERY

Corporate crime update

July 2020





Despite the COVID-19 conditions that exist around the world, activities in the commercial crime space continue along. Australia inches ever more-closer to substantial reforms to its foreign bribery and commercial crime laws, although it has been over 4 years from when they were first proposed. These will, once enacted, have a considerable impact on international supply chains and require Australian business to be robustly proactive in identifying, managing and minimising risk in order to protect themselves from potential strict criminal liability. Our Foreign Bribery Updates are now focused on the broader topic of Commercial Crime, which is now of greater importance to governments across the world. Australian businesses need to be aware of these developments in order to protect themselves from potential criminal liability and reputational issues.

AUSTRALIA	4
Long overdue reforms to Australia's foreign bribery laws	4
A "new" foreign bribery offence	4
A proposed Commonwealth DPA scheme	4
Foreign bribery test – dishonesty or improper influence	5
ASIC warrant powers	6
Private sector whistleblower protection regime	6
Australian Law Reform Commission review into Australia's Corporate Criminal Responsibility Regime	7
Cartel criminal prosecutions	8
Foreign surveillance requests	9
Foreign interference crimes	10
UNITED STATES	12
2019-20 A big year for Deferred Prosecution Agreements in the US	12
DOJ & SEC publishes FCPA Resources Guide 2nd Edition	12
DOJ refines FCPA Corporate Enforcement Policy	13
DOJ revises Guidance on Evaluation of Corporate Compliance Programs	13
SEC entitled to seek disgorgement of profits	14
ASIA	15
Hong Kong	15
Malaysia	15
South Korea	15
UNITED KINGDOM	17
Deferred prosecution agreements	17
Tesco Store Limited	17
Güralp Systems Limited	17
Sarclad Ltd	18
Serco	18
The future of DPAs – lessons for Australia	18
Unexplained Wealth Orders	19
Serious fraud updates	19
Foreign Conduct Authority	19
UK Parliament Treasury Committee – report on "Economic Crime: Consumer Views"	19
EUROPEAN UNION (EU)	21
Whistleblowing Directive	21
European Securities and Markets Authority	21
Money Laundering Directives	21
CONTACTS	23

Australia

LONG OVERDUE REFORMS TO AUSTRALIA'S FOREIGN BRIBERY LAWS

On 2 December 2019, the *Crimes Legislation Amendment (Combatting Corporate Crime) Bill 2019* (**Corporate Crime Bill**) was introduced to Parliament which seeks to address challenges associated with detecting and addressing serious corporate crime. The Corporate Crime Bill is available [here](#).

The Senate referred the Corporate Crime Bill to the Legal and Constitutional Affairs Legislation Committee (**Committee**). The Committee published its report in March 2020 and recommended that the Senate pass the Corporate Crime Bill. The report is available [here](#).

The Corporate Crime Bill seeks to enact the following four reforms:

- amendments to the existing offence of bribery of a foreign public official (**FPA**) in the Criminal Code;
- introduction of a new offence of failure of a body corporate to prevent foreign bribery by an associate;
- implementation of a Commonwealth Deferred Prosecution Agreement (**DPA**) scheme; and
- repeal and replacement of the existing definition of "dishonest" in the Criminal Code.

These reforms, if finally enacted, will mean Australian businesses with any operations overseas (through subsidiaries, joint ventures or other agents, consultants or third parties) will need to take a proactive approach to identifying and managing risk and, where possible, avoiding risk in transactions that might give rise to the possibility of foreign bribery.

A "NEW" FOREIGN BRIBERY OFFENCE

The Corporate Crime Bill seeks to amend the terms of section 70.2 of the Criminal Code which sets out the offence of bribing a FPA in a number of ways.

- It broadens the current definition of a FPA to include an individual standing or nominated as a candidate to be an FPA, in order to capture bribery of candidates with the intent of obtaining an advantage once they take office.
- It replaces the current requirement that the benefit or business advantage not be "legitimately due" with the

concept of "improperly influencing" an FPA to obtain or retain business or an advantage.

- It extends the existing offence of obtaining or retaining business or a business advantage to the obtaining or retaining of a personal advantage.
- It includes an offence-specific defence relating to whether a law in the relevant foreign jurisdiction would permit the provision of a relevant benefit to a FPA.

To address the perceived difficulty of attributing liability to an Australian parent company for the acts of an overseas subsidiary or other third party, the Corporate Crime Bill introduces a new offence of failure of a body corporate to prevent foreign bribery by an "associate".

An "associate" is defined broadly as a person undertaking services for or on behalf of another for profit. The offence has the same maximum penalty as the existing offence in section 70.2 of the Criminal Code and is intended to be a deterrent to companies being wilfully blind to corrupt practices within their business but separated from parent entities by offshore subsidiaries or other third party intermediaries. The offence is a strict liability offence.

However, it would be a defence if a company can demonstrate that it had adequate procedures in place designed to prevent the commission of the foreign bribery conduct by an associate. The Australian Attorney-General has published a Consultation Paper on the likely steps a company can take to ensure it has adequate procedures in place to prevent foreign bribery from occurring. The Consultation Paper is available [here](#). It is modelled on the Guidance published by the United Kingdom Ministry of Justice for the similar section 7 offence under the *Bribery Act 2010* (UK). The Consultation Paper proposes a high level set of principles for companies to adopt in proactively addressing foreign bribery risks to assist a prosecutor and a court in determining whether adequate procedures have, in fact, been implemented.

A PROPOSED COMMONWEALTH DPA SCHEME

To incentivise corporations to self-report, the Corporate Crime Bill seeks to enable the Commonwealth Director of Public Prosecutions (**CDPP**) to invite corporations who have

engaged in serious corporate crime to negotiate a DPA. The offer to negotiate a DPA can only be made to a company (similar to the UK position and narrower than in the US).

Any DPA must be assessed by the CDPP consistently with the existing Prosecution Policy of the Commonwealth of Australia (available [here](#)). In addition, the CDPP has published a Guidance on the factors that will be considered in circumstances where a company self-reports a potential offence and whether a DPA should be offered to it. The CDPP Guidance is available [here](#).

The Corporate Crime Bill largely maintains the features that were in an earlier version published in 2017, including:

- mandatory conditions as well as a non-exhaustive list of optional conditions;
- the extent of ongoing co-operation with investigations;
- the payment of financial penalties;
- the role of an independent monitor to assess compliance with a DPA;
- admission to agreed facts but not, importantly, any admission of liability;
- limitations on the admissibility in any subsequent civil or criminal proceedings of documents generated or provided to Commonwealth agencies during the course of negotiating or complying with a DPA; and
- the implementation of compliance programs.

The Australian court system is not involved in the DPA. There is no filing of any indictment or court attendance notice (as required under Australian State criminal procedure laws). This is because of the constitutional separation of powers and the ruling of the High Court of Australia that a prosecutor in a criminal case cannot make submissions on or agree to penalties; that is the exclusive preserve of the sentencing court. Accordingly, a DPA must be considered and approved by an “approving officer”, being a former judicial officer who is satisfied that its terms are in the interests of justice, and are otherwise fair, reasonable and proportionate.

The most significant failing in the model DPA scheme is that there is no clear obligation on the approving officer, or the CDPP, to publish reasons for a DPA. While the CDPP must publish the terms of a DPA (subject to any non-

disclosure requirements to protect ongoing investigations or prosecutions), the Corporate Crime Bill is silent on publishing reasons to support a DPA. This is a major drawback to the clear desirability for transparency, accountability and judicial reasoning by the approving officer.

The UK's DPAs have been subjected to clear judicial scrutiny and there are, at present, 7 leading judgments by senior UK Judges. The leading judgment still remains that of Lord Justice Leveson in the first DPA in *SFO v Standard Bank Plc* delivered in November 2015 (available [here](#)) where the Court clearly articulated with detail the balancing act that was required to assess the proposed DPA and the attitude of the courts towards assessing the company's conduct, both on liability and on mitigating factors.

Without such clearly published reasons, the Australian system runs the risk of being shrouded in secrecy and lacking transparency. This is counter-productive to the success of the proposed scheme and in generating community faith that it is indeed an open, transparent scheme, rather than a system designed to let companies buy their way out of criminal liability without proper public disclosure of what occurred.

FOREIGN BRIBERY TEST – DISHONESTY OR IMPROPER INFLUENCE

The current test for dishonesty requires proof of not only conduct that is objectively dishonest according to the standards of ordinary people, but proof that the defendant is aware that his or her knowledge, belief or intent is dishonest in the relevant sense. Under the new proposal, the subjective limb would be removed and the new definition for dishonesty would simply be “*dishonest according to the standards of ordinary people*”, to align the Criminal Code with the common law test endorsed by the High Court of Australia in *Peters v The Queen* (1998) 192 CLR 493.

The reforms seek to address the present difficulties in obtaining sufficient admissible evidence that a defendant is aware of or knows that his or her conduct is dishonest according to the standards of ordinary people. Several stakeholders have voiced significant concerns about the proposed reforms. For instance, the change in definition would affect at least 58 current Commonwealth offences without any specific attention as to whether the change and penalty is appropriate for each

particular offence. In addition to re-framing a number of offences in the Criminal Code, the reforms have the potential to unduly trespass on personal rights and liberties in a manner that may not be justified to merely make the prosecution of individuals easier for the Crown.

ASIC WARRANT POWERS

For a number of years, the investigative powers of Australia's corporate regulators has been criticised as being too weak or overly complex. As a result of the Hayne Royal Commission into the conduct of the financial and insurance sectors, the *Financial Sector Reform (Hayne Royal Commission Response – Stronger Regulators (2019 Measures)) Act 2019* (**Stronger Regulators Act**) implements certain recommendations arising from the Australian Securities and Investments Commission (**ASIC**) Enforcement Review Taskforce which was established in October 2016 and in response to the recommendations and implementation roadmap of the Hayne Royal Commission into a more robust regulatory framework for the corporate sector. The Stronger Regulators Act is available [here](#).

The reforms are aimed at eliminating the inconsistencies and deficiencies existing between ASIC's various search warrant powers which limited the usefulness of warrants and restricted ASIC's ability to use the material it seized. The changes can be summarised as follows.

- The *ASIC Act 2001* (Cth) (**ASIC Act**) and *National Consumer Credit Protection Act 2009* (Cth) (**Credit Act**) have been amended to apply by reference to the search warrant powers in the *Crimes Act 1914* (Cth) (**Crimes Act**) (contained in Pt IAA, Divs 1, 2, 4C and 5), modified as necessary. Those provisions are then applied to other ASIC-administered legislation, namely the Retirement Savings Accounts Act 1997 (Cth) and the Superannuation Industry (Supervision) Act 1993 (Cth), and the Corporations Act 2001 (Cth) (Corporations Act), with the practical effect that ASIC's search warrant powers are kept up to date as and when changes are made to the Crimes Act (the primary law for the use and enforcement of Commonwealth search warrants).
- ASIC now has available to it the ancillary powers included in the Crimes Act with minor modifications as necessary. For instance, ASIC can photograph and make video recordings of a search, operate electronic equipment on

the premises to access data, move devices to another place for processing to determine if they contain evidential material, and operate seized devices to access data.

- When seeking a warrant under relevant laws, ASIC must currently demonstrate to a Court that an issued Notice to Produce has not been complied with. The reforms seek to remove the requirement to issue a Notice to Produce. As such, ASIC is not required to forewarn a person under investigation that it may apply for a search warrant.
- Previously ASIC was required to specify particular documents thought to exist and any subsequent search and seizure was limited to those specified documents. Now ASIC is no longer required to specify the exact documents or evidential material that can be searched and seized. Instead, the Magistrate issuing the warrant must state the offence to which the warrant relates or another offence that is an indictable offence. ASIC can now seize other material *relevant to a particular offence* even if it is only uncovered in the process of executing the warrant, along with material relevant to a suspected indictable offence.
- Under existing provisions across ASIC-administered legislation, ASIC may only use books and records seized for the purposes of a criminal proceeding under Commonwealth, State or Territory law. Seized evidential material can now be used more broadly for the purpose of the performance of ASIC's functions or duties or the exercise of its powers. The material can be used in relation to the investigation of contraventions giving rise to civil proceedings or administrative action.

PRIVATE SECTOR WHISTLEBLOWER PROTECTION REGIME

In many commercial crime cases of recent years in Australia, information has only surfaced to investigators and regulators through whistleblowers and/or media reports. Whistleblowers had to fight against a culture of corporate and government silence, a dislike of transparency and accountability, and the personal pain of being victimised when they spoke out. While it may be fair to say such a culture may still exist, it is being addressed, albeit slowly, in reforms designed to protect and promote the value of speaking out and disclosing corporate misconduct.

In 2019, the *Treasury Laws Amendment (Enhancing Whistleblower Protections) Act 2019* (Cth) was passed which

expanded whistleblower protections in the corporate sector with effect from 1 July 2019. Where previously such protections were split across a range of legislation, they are now consolidated in Pt 9.4AAA of the Corporations Act and administered by ASIC, with corresponding amendments to the *Taxation Administration Act 1953* (Cth) administered by the Australian Taxation Office.

The whistleblower reforms extended protections to a broader class of persons (**eligible whistleblowers**) and a broader range of disclosures. The reforms also permit and encourage anonymous disclosures. Formerly only current employees, agents or contractors could be protected provided that they reported to the company that they sought to expose, and provided their name, proof of what they know, and their disclosure was made in good faith.

Under the new laws:

- eligible whistleblowers can make disclosures about a company, bank, provider of general insurance or life insurance, superannuation entity or superannuation trustee, incorporated association or other body corporate that is a trading or financial corporation;
- disclosures can be made either internally, externally or to an auditor or actuary of the company, an authorised whistleblower complaints service or hotline, ASIC or APRA;
- disclosures can be made by a current or former employee, officer, a supplier of goods or services, an individual who is an associate of a relevant entity, and a relative or a dependant of an individual or an individual's spouse;
- public interest or emergency disclosure may be made to a journalist or Members of Parliament subject to certain qualifications; and
- the individual making the disclosure must have reasonable grounds to suspect that the information disclosed involves the company or organisation, and concerns misconduct or an improper state of affairs or circumstances of the company.

The new regime also extends the protections afforded to whistleblowers. For instance, as a general rule the identity of a whistleblower or contents of a disclosure cannot be disclosed without that person's consent. Whistleblowers are protected against legal action, including criminal prosecution, civil litigation or administration/disciplinary action, as well

as from any direct or indirect detriment, which includes the threat of or actual dismissal, disadvantage or discrimination.

Public companies, large proprietary companies and corporate trustees of APRA-regulated superannuation entities must have in place a whistleblower policy consistent with these new laws from 1 January 2020. Failure to have and make available a policy is an offence of strict liability attracting a penalty of up to AUD\$126,000 for companies (and lesser penalties for individuals). The Corporations Act sets out, at a high level, the content requirements for any whistleblower policy including information about legal protections available to whistleblowers, an outline of how the company will investigate disclosures, and an explanation of how whistleblowers will be protected from detriment.

ASIC has released a number of useful guides in relation to private sector whistleblower protections:

- Information Sheet 238 – Whistleblower rights and protections (available [here](#));
- Information Sheet 239 – How ASIC handles whistleblower reports (available [here](#)); and
- Regulatory Guide 270 – *Whistleblower Policies* which assists entities in establishing a compliant policy (available [here](#)).

AUSTRALIAN LAW REFORM COMMISSION REVIEW INTO AUSTRALIA'S CORPORATE CRIMINAL RESPONSIBILITY REGIME

Over many years, there has been criticism of why Australia rarely commences criminal prosecutions against companies for financial crime. Prosecutors usually say that they like to focus on the conduct of individuals who drive corporate behaviour. In truth, they find it very difficult to establish criminal liability on a company where corporate conduct is diffused and spread out amongst the layers of management. The Australian law instead relied upon the traditional common law test of attribution by the directing will and mind of a company to establish corporate liability. It was considered very hard to establish given that those who direct a company, particularly large organisations, are rarely involved in hands-on misconduct. In 2001, Part 2.5, sections 12.1 to 12.6 of the Criminal Code established a statutory test for attributing criminal liability to a company, based upon the objective conduct of a Board of Directors and/or

the conduct of a “high managerial agent”. However, these reforms appeared illusory as corporate criminal prosecutions appeared to be no easier for prosecutors.

On 15 November 2019, the Australian Law Reform Commission (**ALRC**) was issued with broad Terms of Reference to review the existing law on corporate criminal responsibility and to consider what reforms if any, might be warranted.

On 29 April 2020, the ALRC published its report to the Australian Attorney General. Although it should be published within 15 parliamentary sitting days of the next Parliament, those sitting days have been truncated and focused on economic issues associated with COVID-19. Once the Report is published, it will be reviewed in a subsequent update.

CARTEL CRIMINAL PROSECUTIONS

For many years, since 2009, cartel conduct has been a criminal offence in Australia. The anti-competitive cartel provisions are investigated and enforced by the Australian Competition & Consumer Commission (**ACCC**). Where the ACCC suspects potential criminal conduct, it liaises with the CDPP to continue an investigation to determine if the conduct warrants a criminal investigation and prosecution (conducted by the CDPP) or civil penalty proceedings (conducted by the ACCC). The ACCC and the CDPP work together pursuant to a MOU between the two entities (available [here](#)).

There have been a few important cases that have made their way to the courts that shed light on the persistence of significant cartel conduct and the serious penalties that arise. The banking cartel case is the most significant case that is ongoing. The ACCC have made allegations of cartel conduct involving leading financial institutions who engaged in what many have regarded as commonplace conduct in the finance sector where share placements occur. The case will be closely watched. Some of the important cases in recent years are summarised below.

- In 2017, Nippon Yusen Kabushiki Kaisha (**NYK**) settled a criminal prosecution when NYK agreed, with other shippers, to plead guilty to a single charge of giving effect to a cartel provision, contrary to section 44XXRG(1) (now section 45AG(1)) of *Competition and Consumer Act 2018* (Cth) (**CCA**). While NYK pleaded guilty at a very early stage, the penalty could have been as high as

AUD\$100 million. In sentencing the company, the Court noted a number of mitigating factors. The Court then applied a 50% discount for the early guilty plea together with past and future assistance. Of that 50% discount, 10% specifically related to the future assistance. NYK was fined a total of AUD\$25 million with the possibility of AUD\$30 million if it did not comply with its undertaking on cooperation. The Court analysed the assessment of the penalty under the CCA in order to determine the appropriate fine. As this was a criminal prosecution, agreed penalties could not be made by submission; it was up to the discretion of the sentencing court. The judgment is *Commonwealth Director of Public Prosecutions v Nippon Yusen Kabushiki Kaisha* [2017] FCA 876 is available [here](#).

- In 2018, K-Line, part of the same cartel as NYK, agreed to plead guilty to a charge similar to NYK. The charge was that between about 24 July 2009 and 6 September 2012, in Japan and elsewhere, K-Line intentionally gave effect to cartel provisions in an arrangement or understanding with others in relation to the supply of ocean shipping services. Taking into account the severity of the offence, and the relevant mitigating factors, the court sentence was a fine of AUD\$34.5 million. The fine incorporated a global discount of just over 28% for K-Line's early plea of guilty and assistance and cooperation, together with the contrition inherent in or demonstrated by K-Line's early plea and cooperation. That means that, but for K-Line's early plea and cooperation, the fine would have been AUD\$48 million. The judgment is *Commonwealth Director of Public Prosecutions v Kawasaki Kisen Kaisha Ltd* [2019] FCA 1170 is available [here](#).
- In June 2018, the CDPP filed criminal cartel charges against three major investment banks for alleged criminal cartel conduct arising out of an institutional share placement. A media release published by the ACCC read as follows:

Citigroup Global Markets Australia Pty Limited (Citigroup), Deutsche Bank Aktiengesellschaft (Deutsche Bank) and Australia and New Zealand Banking Group Ltd (ANZ) have been charged with criminal cartel offences following an investigation by the ACCC. Criminal charges have also been laid against several senior executives: John McLean, Itay Tuchman and Stephen Roberts of Citigroup; Michael Ormaechea and Michael Richardson formerly of Deutsche Bank; and Rick Moscati of ANZ. The charges involve alleged cartel arrangements relating to trading in ANZ shares

held by Deutsche Bank and Citigroup. ANZ and each of the individuals are alleged to have been knowingly concerned in some or all of the alleged conduct.

According to media coverage of the case, in 2015 ANZ decided to undertake a capital raising in order to bolster its balance sheet in the wake of the Global Financial Crisis of 2007-2008. ANZ retained JPMorgan, Deutsche Bank and Citigroup as lead managers of the capital raising. A large block of the share placement did not sell and as a result, was held by the lead managers who had underwritten the placement. The ACCC allege that the three lead managers held a series of teleconferences together to discuss how they were going to unload what was nearly AUD\$800 million of ANZ shares without flooding the market and substantially driving down the share price. The ACCC allege that the conduct constituted an unlawful cartel, or arrangement or understanding

The case is being defended by the defendants and is continuing through the committal phase. No claim is made against the immunity applicant, JP Morgan, who disclosed the conduct to the ACCC.

Given the parties involved, including seventeen barristers and solicitors from nine law firms, it could not continue with any semblance of social distancing due to COVID-19 restrictions. Sensibly, the matter was deferred. Now with the easing of restrictions, the committal is due to recommence from late July 2020. Unless any of the cases are discontinued by the Crown, it is expected that all defendants will be committed to trial.

FOREIGN SURVEILLANCE REQUESTS

In March 2020, as Australia was slumbering under the “stay at home” COVID-19 orders, the Minister for Home Affairs introduced the *Telecommunications Legislation Amendment (International Production Orders) Bill 2020 (2020 Bill)*. The 2020 Bill is currently before the Parliamentary Joint Committee on Intelligence and Security for review. The 2020 Bill and supporting documents are available [here](#).

The 2020 Bill’s key features amend the *Telecommunications (Interception and Access) Act 1979 (Cth)* as follows (as the Parliamentary website states in plain language):

- provide a framework for Australian agencies to obtain independently-authorised international production

orders for interception, stored communications and telecommunications data directly to designated communications providers in foreign countries with which Australia has a designated international agreement;

- amend the regulatory framework to allow Australian communications providers to intercept and disclose electronic information in response to an incoming order or request from a foreign country with which Australia has an agreement; and
- remove the ability for nominated Administrative Appeals Tribunal (**AAT**) members to issue certain warrants.

The Bill is intended to provide a legislative framework for Australia to give effect to future bilateral and multilateral agreements for cross-border access to electronic information and communications data, such as that being negotiated with the United States for the purposes of the *US Clarifying Lawful Overseas Use of Data Act (CLOUD Act)*.

The *Explanatory Memorandum* published with the 2020 Bill gives, on its face, good reason to update the ability of intelligence and security agencies to more easily access electronic data:

Almost every crime type and national security concern has an online element—agencies require electronic information and communications data not only for cyber-investigations but also for investigations and prosecutions regarding violent crimes, human trafficking and people smuggling, drug trafficking, financial crimes, terrorism and child sexual abuse.

The exponential rise of global connectivity and reliance on cloud computing means that intelligence and evidence that was once stored within Australia and available under a domestic warrant or authorisation is now distributed over different services, providers, locations and jurisdictions, and is often only obtainable through international cooperation.

Criminals, including terrorists, typically access communications services that are supplied or operated by entities outside Australia. The overwhelming majority of data from these services is held by companies located overseas, including the United States. This places these service providers in a unique position to assist Australian law enforcement and national security efforts.

Quite what this means for individuals and any concept of their privacy rights remains to be seen. Under the 2020 Bill, an intelligence or security agency may seek an order to engage in surveillance over Australians on behalf of agencies of foreign governments who have an agreement with Australia. Initiating orders may be no more than a verbal approval by the Attorney-General. Traditionally, warrants for surveillance of Australians are signed off by judicial officers. Orders sought under the 2020 Bill can be signed off by a member of the security division of the Administrative Appeals Tribunal which is not the same as subjecting the requests to judicial scrutiny. In addition, it appears from media reports that the Commonwealth Ombudsman, which is to inspect and report on the operation of the 2020 Bill, does not yet know if it will have resources allocated to it to do so.

In short, it seems Australia is willing to permit foreign agencies to effectively spy on Australians by private agreement and request in circumstances where laws like the CLOUD Act:

- gives US agencies the power to demand US companies provide surveillance data no matter where in the world it is held;
- prevents other governments from directly requiring US firms to do the same; and
- prevents other governments from barring US firms from sharing data with the US government.

At one level, the grant of such powers to ministers or public officials might appear reasonable. Yet much will depend upon the independent scrutiny of the use of these powers and the willingness of the Australian Government to subject itself to transparent accountability, something that has so often been a challenge to it in the past.

FOREIGN INTERFERENCE CRIMES

In 2018, Australia enacted the *National Security Legislation Amendment (Espionage and Foreign Interference) Act 2018* (Cth) (**National Security Act**). The National Security Act had the effect of introducing a range of amendments to the Criminal Code and related legislation to create a range of criminal offences to cover foreign interference.

The National Security Act introduced a range of reforms to Australia's criminal law as follows:

- Strengthens existing espionage offences;
- Introduces new foreign interference offences targeting covert, deceptive or threatening actions by foreign actors who intend to influence Australia's democratic or government processes or to harm Australia;
- Reforms to secrecy offences, ensuring they appropriately criminalise leaks of harmful information while also protecting freedom of speech;
- Introducing new sabotage offences that effectively protect critical infrastructure in the modern environment;
- Reforms offences against government, including treason, to better protect Australia's defence and democracy;
- Introduces a new theft of trade secrets offence to protect Australia from economic espionage by foreign government principals;
- Introduces a new aggravated offence for providing false and misleading information in the context of security clearance processes; and
- Ensures law enforcement agencies have access to telecommunications interception powers to investigate these offences.

The primary offences are set out in section 92 of the Criminal Code. The offences are split between the offence of "intentional foreign interference" and of "reckless foreign interference". In summary, a person commits an offence if:

- the person engages in conduct; and any of the following exist:
 - the conduct is engaged in "on behalf of or in collaboration with a foreign principal or a person acting on behalf of a foreign principal";
 - the conduct is "directed, funded or supervised by the foreign principal or person acting on behalf of a foreign principal"; and
- the person intends that the conduct will:
 - influence a political or governmental process of the Commonwealth or a State or Territory;
 - influence the exercise (whether or not in Australia) of "an Australian democratic or political right or duty"; or

- support intelligence activities of a foreign principal; or
- prejudice Australia's national security ; and
- any part of the conduct;
 - is covert or involves deception; or
 - involves the person making a threat to cause serious harm whether to the person to whom the threat is made or any other person; or
 - involves the person making a demand with menaces.

The concepts of a "*foreign principal*" and "*foreign government principal*" are given a broad definition. The phrase "*national security*" defined in section 90.4 of the Criminal Code and means any of the defence of the country, the protection of the country (from espionage, sabotage, terrorism, political violence, foreign interference and activities that hinder or interfere with the country's defence force or any activity undertaken for the purposes of the country's defence or safety. The phrase "*an Australian democratic or political right or duty*" is not defined". It remains to be seen how the authorities and ultimately, courts, will interpret them in the context of alleged criminal conduct.

The offence of reckless foreign interference has the same elements as the intentional foreign interference offence, but the relevant person does not "intend" the conduct; rather, the person is reckless as to whether the conduct will in fact result in the same consequences. This is more of an objective test in contrast to intent that must be proved in the intentional foreign interference offence.

In June 2020, the AFP and the Australian Security Intelligence Organisation (**ASIO**) launched very public raids on properties and parliamentary offices of a NSW Labor politician, Shaquett Moselmane and one of his part time staffers, John Zhang. It was reported in the media that the raid concerned alleged foreign interference by an unnamed country (but presumed to be China due to public statements by Mr Moselmane in support of China and the background of Mr Zhang). The AFP and ASIO have not made any statements on the raids and no charges or allegations have been made or commenced against Messrs Moselmane or Zhang or anyone else.

United States

2019-20 A BIG YEAR FOR DEFERRED PROSECUTION AGREEMENTS IN THE US

2019 was a big year of Foreign Corrupt Practices Act (**FCPA**) enforcement in the United States including record breaking corporate resolutions. US monetary sanctions reached a high of US\$2.65 billion. Interestingly, FCPA enforcement fell disproportionately on foreign companies, with nine of the fourteen companies charged being based outside of the US. The most significant cases were the Ericsson US\$1.06 billion settlement and the Russian telecom company MTS US\$850 million resolution. There were five corporate FCPA resolutions each resulted in more than US\$200 million in penalties.

2020 started off with a bang. On 31 January 2020, Airbus SE (**Airbus**) announced a settlement was reached with the French, UK and US authorities to pay almost US\$4 billion in global penalties. Between 2008 and 2015, the authorities alleged that Airbus facilitated a bribery scheme in multiple countries in the form of all expenses paid events held on American soil. While the Department of Justice (**DOJ**) made it clear that it took a very dim view of Airbus's 'self-reporting' after the commencement of the UK SFO investigation, the resolution was approved by all regulators. The penalties were allocated as follows:

- in France, Airbus will disgorge EU€1,053,377,113 (or US\$1.2 billion) in profits and pay a further penalty of EU€1,029,760,342 (or US\$1.1 billion) for a total penalty of EU€2,083,137,455 (or US\$2.3 billion);
- in the UK, Airbus will disgorge GBP£585,939,740 (or US\$653 million) in profits and pay a fine of GBP£398,034,571 million (or US\$444 million), reflecting a 50 percent reduction and pay the SFO's costs of GBP£6.9 million (or US\$7.71 million); and
- in the US, Airbus will pay US\$294,488,085 (noting a credit of US\$1,797,490,796 owed to the French National Financial prosecutor, a criminal penalty of US\$237.7 million under the DPA and, as part of a civil forfeiture action, to forfeit a EU€50 million (US\$55 million) bond that was "traceable to the proceeds of contraventions of the International Traffic in Arms Regulations (**ITAR**)), and a US\$10 million settlement with the US State Department to resolve ITAR contraventions.

The Airbus DPA is significant not just because of its size but also because of the prevailing cross jurisdictional cooperation that led to such a coordinated outcome. The Airbus DPA highlights the importance and increasing prevalence of cooperation between countries in prosecuting large multinationals for breaches of foreign bribery laws.

DOJ & SEC PUBLISHES FCPA RESOURCES GUIDE 2ND EDITION

On 3 July 2020, the DOJ and the SEC published the 2nd edition of their *FCPA Resources Guide* (available [here](#)).

The Resources Guide was originally published in November 2012 and was a leading text on the views of the DOJ and the SEC on how they regarded FCPA matters, whether or not they were judicially "correct" or a US court might ultimately agree with their opinions. The Resources Guide picks up on numerous cases over the last 8 years and various other guidance published by the DOJ, particularly concerning corporate enforcement, compliance programs, the use of independent monitors and penalty issues. It still operates as an excellent summary of the issues non-US companies need to be aware of when they are potentially exposed to US jurisdiction.

A few highlights in the updated Resources Guide are as follows:

- while recognising the impact of the Second Circuit Appeals court in *United States v Hoskins* in barring the governments use of conspiracy and accessorial offences to expand the reach of the FCPA over foreign nationals, the Guide suggests such claims might still arise for the books and records and internal controls offences;
- the SEC is subject to a five year limitation period for penalty and disgorgement claims, applying *SEC v Kokesh* and the DOJ will now apply a six year limitation period for criminal charges of the FCPA accounting offences;
- the broad "non-exhaustive factors for a court to consider on whether an entity is an "instrumentality" is in line with *United States v Esquenazi*; and
- for successor liability, the Guide recognises that where an acquiring company discloses misconduct by the acquired entity, the successor may be eligible for a declination (no prosecution) even if aggravating factors existed in the acquired entity.

DOJ REFINES FCPA CORPORATE ENFORCEMENT POLICY

On 20 November 2019, the DOJ refined the cooperation requirements of the FCPA Corporate Enforcement Policy (**Enforcement Policy**) (available [here](#)).

The Enforcement Policy has always aimed to incentivise self-disclosure of potential breaches of the FCPA. The price of self-disclosure remains the disgorgement of profit, forfeiture and/or the payment or restitution of assets derived from the illegal conduct with penalties for the relevant misconduct with a 50% reduction at the low end of the US Sentencing Guidelines. The changes to the Enforcement Policy relate to companies' voluntary disclosure of potential FCPA violations to the DOJ, which can be summarised as follows.

- The first change relates to one of the three requirements a company must meet to receive credit for the voluntary self-disclosure of wrongdoing. The revision clarifies that a company must disclose the relevant facts known to it at the time of disclosure and changes the standard "violation of law" to "misconduct".
- The second change simplifies a prior requirement by stating that to receive full cooperation credit, a company that is aware of relevant evidence not in the company's possession must identify that evidence to the DOJ.
- The third change clarifies that the "presumption of declination" applies where a company discovers misconduct "by the merged or acquired entity", thereby encouraging companies to disclose conduct discovered after a merger and to assure that the acquirer will not face successor liability.

The Enforcement Policy acknowledges the practical realities of investigating and bringing enforcement actions against companies. The changes seek to promote greater consistency and flexibility related to the exercise of prosecutorial discretion by the DOJ whilst also providing substantial incentives for self-disclosure of suspected FCPA violations.

DOJ REVISES GUIDANCE ON EVALUATION OF CORPORATE COMPLIANCE PROGRAMS

On 1 June 2020, the DOJ published an updated Guidance on its Evaluation of Corporate Compliance Programs (**2020 Guidance**) (available [here](#) with an excellent summary and practical highlights by Washington DC law firm, Miller & Chevalier, available [here](#)). The 2020 Guidance is designed to assist US prosecutors to assess the extent to which a company's compliance program was effective at the time of offending conduct, at the time a prosecution is filed and at any resolution.

Some key themes that emerge from the 2020 Guidance include the following:

- Prosecutors will have a higher level of sensitivity to the circumstances and realities of a business under investigation (for example, if a complete due diligence was not performed prior to an acquisition, was it completed after and if not, why not);
- Prosecutors will examine the extent to which a company reviews and adapts its compliance program, learning from past issues or others in the region;
- Prosecutors are to test where a company asserts that foreign law dictates any aspect of the compliance program (with particular regard to GDPR issues on data privacy to be considered).

Companies need to consider the practical steps that the 2020 Guidance promotes, particularly any Australian business with operations in or subject to US jurisdiction, which include the following:

- the identification of risk factors by a company must be continuous and should result in updated policies, procedures and controls;
- access to compliance policies must be more than accessible, the DOJ will ask if the policies have "been published in a searchable format for easy reference" and for companies to track access to policies to assess those policies more relevant to employees (and if they are not tracked, to ask themselves, why not);
- ongoing training is critical, tailored to the audience size, sophistication and subject matter experience;

- reporting channels must not only exist but must be effective and the effectiveness must be demonstrated;
- third party relationships need to be managed throughout the term of a business relationship, not such during the engagement or on-boarding process; and
- on acquisitions, the DOJ will now consider not just due diligence on acquisition, but integration of the asset into existing internal compliance programs.

SEC ENTITLED TO SEEK DISGORGEMENT OF PROFITS

In an opinion published by the US Supreme Court on 22 June 2020, in *Liu et al v Securities and Exchange Commission* (available [here](#)), the Court upheld the authority of the SEC to obtain disgorgement as equitable relief under its statutory powers, but with some important limitations.

The Court reaffirmed two principles:

- equity grants authority to courts to strip wrongdoers of their ill-gotten gains; and
- as equitable relief is not a punitive sanction, the remedy is restricted to a wrongdoer's net profits to be awarded for victims.

The Court's opinion leaves open the question of whether the SEC can simply pay disgorged monies to the US Treasury, or whether it must take steps to identify victims. In addition, there will be a considerable factual debate between offenders, the SEC and their lawyers of what should be the "net profits" and what otherwise be characterised as legitimate business expenses. This disagreement is likely to add another layer of complexity in any SEC negotiations on what amounts should be subjected to a disgorgement order.

Asia

HONG KONG

In the recent decision of *Cheung Ka Ho Cyril v Securities and Futures Commission and another* [2020] HKCFI 270, the High Court of Hong Kong confirmed that the Securities and Futures Commission (**SFC**) has the power not only to seize digital devices in the course of executing a search warrant, but also to demand passwords to the seized devices and email accounts.

The applicant in this case sought judicial review of the validity of various search warrants obtained by the SFC to support its ongoing investigations into suspected breaches of the Securities and Futures Ordinance (**SFO**) relating to listing and bond placements. In construing the relevant provisions of the SFO, the Court held that the phrase “records or documents” in the context of search and seizure powers extended to digital devices which included in this case mobile phones, tablets, notebooks and computers. More significantly, the Court found that the SFC is empowered to require persons to provide means of access to email accounts and digital devices provided that they contain, or are likely to contain, information relevant to the SFC’s investigations. This development brings Hong Kong law closer to those now available to ASIC under its new warrant powers (see above).

MALAYSIA

Section 17 of the *Anti-Corruption Commission Act 2009* (Act 694, **MACCA**) prohibits the giving and receiving by an agent of “any gratification as an inducement or reward” for advantage in relation to the principal’s affairs or business.

In April 2018, the *Anti-Corruption Commission (Amendment) Bill* was passed to introduce a new section 17A which is scheduled to come into force in June 2020.

Section 17A introduces corporate liability for the giving and receiving of gratification, directly or indirectly, by “persons associated with” a commercial organisation, with intent to obtain or retain a business or other advantage for that organisation. The new provision applies to local companies and partnerships carrying on business in Malaysia or abroad, and foreign companies and partnerships carrying on business in Malaysia. “Associated person” is defined to include directors, partners and employees of commercial

organisations, as well as third parties performing services for or on behalf of such organisations.

Although section 17A is an offence of strict liability, it provides a defence where the commercial organisation can prove it had in place adequate procedures to prevent persons associated with the commercial organisation from undertaking the corrupt acts.

Significantly, directors, controllers, officers, partners or managers of commercial organisations will also be deemed liable for an offence committed by the commercial organisation unless it can be proven that:

- i. the offence was committed without their knowledge; and
- ii. they had exercised the requisite due diligence to prevent the commission of the offence.

The penalty for an offence under section 17A is a fine of not less than ten times the value of the gratification or RM 1 million (US\$247,300), whichever is higher, and/or imprisonment of up to 20 years. The existing financial penalty for an offence under section 17 is not less than five times the value of the gratification or RM 10,000 (US\$2,473), whichever is higher.

These amendments reflect the strict liability offence in section 7 of the UK Bribery Act and the pending reforms in Australia to the Criminal Code (see above). They reinforce the need for Australian businesses operating in Malaysia to proactively address potential foreign bribery risks. Absent adequate procedures which can be demonstrated, it will be very difficult to avoid strict criminal liability and potential personal liability on individuals.

SOUTH KOREA

On 15 July 2020, the *Establishment and Operation of the Corruption Investigation Office for High-Ranking Officials Act* is to come into effect. For many years, South Korea has had a patch work of agencies that might investigate corruption and more generic frauds. The lead agency has been the Office of the State Prosecutor. South Korea has experienced a range of high profile corruption cases over the last few years involving leaders of business conglomerates up to a former President of the Republic. The new Act has been introduced by the current South Korean Government against strong

opposition from the Government's political opponents. A constitutional challenge is pending against the Act, on the grounds that the office of the CIO is impermissible as it bypasses the prevailing criminal justice system

The new Corruption Investigation Office (**CIO**) will have exclusive authority to investigate and prosecute certain offences. The focus of the CIO's work will be the investigation and prosecution for certain alleged crimes involving high ranking officials, including the President, members of the National Assembly, public prosecutors, judges and their families. Private companies and individuals may be subjected to the CIO's scrutiny if they engage in potentially corrupt conduct with a high ranking official. The crimes within the CIO's jurisdiction include any offences by public officials under the Criminal Code, crimes associated with public documents, embezzlement and breach of trust, bribery, acceptance of illegal political funds, perjury and accessory crimes that might be engaged in by ordinary persons.

All Australian business that have dealings with potentially high ranking officials in South Korea will need to be alert to these developments and to ensure care is exercised, as it should be, in dealing with such officials.

United Kingdom

DEFERRED PROSECUTION AGREEMENTS

Deferred Prosecution Agreements (**DPA**) continue to be a hotly debated topic in the UK. DPAs allow a company to agree to certain conditions to resolve corporate offending for fraud, bribery and economic offences. The conditions can involve financial penalties, compensation to victims, disgorgement of profits, payment of prosecutions costs, co-operation with the prosecutors (on ongoing investigations) and measures to prevent future offending.

The UK's DPA system requires companies under investigation to conclude the process with the SFO in the early stages. The early conclusion means that the full extent of evidence likely to arise from an investigation is not available. An early conclusion is desirable for a corporate body who wants to prevent future indiscretions, to limit financial and reputational damage and to get back to business.

Whether a company should seek a DPA and the consequences that flow from that have given rise to some interesting statistics. The UK Law Society Gazette recently submitted a freedom of information request to the SFO to obtain its conviction rates (available [here](#)). The following was disclosed:

- five defendants were prosecuted in 2019 compared to the 17 in the year ending 31 March 2019 and 10 in year ending 31 March 2018;
- there was a decrease in the number of investigations with a 20% decrease from 75 in 2017/18 to around 60;
- seven investigations closed without charge between March 2015 and 2018;
- there were ten cases closed since January 2019; and
- of the six (now seven with the Airbus) DPAs that have been approved, there has been no convictions of any individuals.

So what does this tell us? At one level, the revenue generated from the fines secured from the 7 DPAs will be a pleasing result for the Government. Companies admit to wrong-doing, engage in a cooperative negotiation with authorities and pay large fines. What happens to the individuals? This is where things seem to go awry. There are some cases that suggest the strength of the alleged corruption underlying certain of the

recent DPAs may not be all that people thought and questions might be asked, such as, why did companies admit to such conduct so quickly, throwing individuals under the proverbial bus? Maybe it's a matter of shifting blame. Companies can be quick to take credit for entrepreneurial success and it seems, equally quick to run a mile from individuals when the wheels fall off the bus.

TESCO STORE LIMITED

The SFO entered a three-year term DPA with Tesco Store Limited (**Tesco**) on 10 April 2017 for false accounting practices. Between February and September 2014, Tesco encouraged illegal practices to meet accounting targets by improperly recognising income and pulling forward income from subsequent reporting periods. The DPA required Tesco to pay a GBP£129 million fine and GBP£3 million for SFO's investigation costs and to undertake and implement and ongoing compliance programme. On 10 April 2020, the three year term ended with SFO serving a Notice of Discontinuance confirming Tesco's compliance with the DPA.

At the end of the DPA, there have been no successful prosecution of the individuals responsible for the company's alleged offending conduct. Three individuals, Carl Rogberg, John Scouler and Christopher Bush held senior management roles in Tesco's UK business and were all charged with allegations of fraud and false accounting on 9 September 2016. John Scouler and Christopher Bush were acquitted of all charges after the High Court held that they had no case to answer at trial which was upheld on appeal (see *Regina v Bush & Scouler* [2019] EWCA Crim 29 available [here](#)). Carl Rogberg was later acquitted of all charges after the SFO presented no evidence against him. The Trial Judge found the case to fail on a no case submission, with insufficient evidence for a jury to convict the accused. The Court of Appeal upheld that finding.

GÜRALP SYSTEMS LIMITED

The SFO approved a DPA with Güralp Systems Limited (**GSL**) in October 2019 for conspiracy to make corrupt payments and failure to prevent an employee's bribery offences. Under the DPA, GSL agreed to disgorge £2,069,861 of profits, to continue to cooperate with the SFO, to continually review and report annually on its

enhanced anti-bribery and corruption procedures and to report evidence or allegations of fraud by itself, its officers, directors, employees or agents.

The three individuals involved were subsequently charged with conspiracy to make corrupt payments and they were acquitted in December 2019. The alleged offences involved employees making payments to a South Korean public official between 2002 and 2015. While the Court accepted that the proposed DPA was fair, reasonable and proportionate in light of GSL's precarious financial position, the detrimental effect of GSL's services being removed from the market, the individuals were no longer involved with the company and GSL's substantial cooperation, the prosecution against the individuals again failed due to lack of sufficient evidence for the Crown to prove its case beyond reasonable doubt..

SARCLAD LTD

The SFO commenced an investigation into the conduct of Sarclad Ltd, a steel industry product design and manufacturing company, concerning how a number of contracts had been secured. This resulted in a DPA with the company on 6 July 2016. Sarclad accepted the charges of corruption and failure to prevent bribery in relation to the systematic use of bribes to secure contracts for the company between June 2004 and June 2012. The contracts had a total value of over £17m.

As a result of the DPA, Sarclad agreed to pay GBP£6,553,085, comprised of a £6,201,085 disgorgement of gross profits and a GBP£352,000 financial penalty. An amount of GBP£1,953,085 was paid by Sarclad's US registered parent company as repayment of a significant proportion of the dividends that it received from the company over the indictment period. Sarclad agreed to cooperate with the SFO and to provide a report addressing all third party intermediary transactions, and the completion and effectiveness of its existing anti-bribery and corruption controls, every twelve months for the duration of the DPA. The DPA concluded on 16 July 2019.

The SFO also charged three individuals in 2016 with conspiring with various agents to agree bribes in relation to 27 overseas contracts. The company was anonymised at the time the DPA was announced in accordance with reporting restrictions, to protect the individuals' right to a fair trial. On

16 July 2019, Michael Sorby, Adrian Leek and David Justice were acquitted of the charges.

SERCO

The SFO entered into a DPA with Serco Group subsidiary Servo Geografix Ltd (**Serco**) approved on 4 July 2019. Serco agreed to take responsibility for three fraud and two false accounting offences resulting from a scheme to dishonestly mislead the UK Ministry of Justice as to the true extent of the profits made between 2010 and 2013 by its parent company, Serco Limited. As part of the DPA, Serco has agreed to pay a financial penalty of GBP£19.2 million and GBP£3.7 million for SFO's investigation costs. Serco also agreed along with Serco's parent company to fully cooperate with SFO and other law or regulatory authorities, to report evidence of fraud by itself or related companies and individuals and to enhance and report annually on the effectiveness of its ethics and compliance programme.

On 16 December 2019, the SFO charged two individuals, Nicholas Wood (former Finance Director of Serco Home Affairs) and Simon Marshall (former Operations Director of Serco Field Services), with fraud by false representation and false accounting in relation to representations made to the Ministry of Justice between 2011 and 2013. Mr Wood was additionally charged with false accounting in relation to Serco's 2011 statutory accounts. The investigation is ongoing and it is yet to be seen whether the DPA will have a detrimental effect on the SFO's prosecution of the responsible individuals.

THE FUTURE OF DPAS – LESSONS FOR AUSTRALIA

What is the future for DPAs in Australia? They are as yet untested. For companies, they might bring a relatively short and painless procedure into play to settle allegations of criminal conduct without the risk of long-term reputational damage and a criminal conviction. They can be characterised as a "get out of jail card" by voluntary disclosure, cooperation and the payment of fines. Yet that cooperation will inevitably require one key feature – turning over records that might incriminate individuals (often former employees and executives) who are likely to be "thrown under the bus" by a company in an attempt to secure its own freedom, but at what price?

For authorities, cases against individuals are fraught with risk. They have to consider complex criminal charges and prove them beyond reasonable doubt. The ability of defendants to resist prosecution, with the inevitable stress that entails, means prosecutors hope for an early guilty plea to avoid the time, effort and cost of proving complex cases.

UNEXPLAINED WEALTH ORDERS

Unexplained Wealth Orders (**UWO**) were introduced in 2018 by amendments to the Proceeds of Crime Act 2002. They allow the National Crime Authority (**NCA**) to require anyone with assets of over GBP£50,000 in value to provide information on how they obtained the property so the NCA can assess whether a person's lawful income is sufficient to justify obtaining and owning the assets. The NCA can also assess whether the person is involved in any serious crime or is a politically exposed person (PEP) or is connected to either.

In April 2020, in *National Crime Authority v Baker* [2020] EWHC 822 (available [here](#)), the Court of Appeal set aside earlier orders of the High Court, returning property assets to the claimant who had supplied appropriate documents to support her claim over marital assets, which the NCA had considered were acquired by the alleged unlawful conduct of her deceased husband, a former banker and Kazakh politician who had since died. The important points from the case are as follows:

- once a target has explained who owns a property and how it was acquired, whether the property should be forfeited as the proceeds of crime is to be resolved in civil recovery proceedings if the NCA chooses to bring them;
- a proactive approach to the NCA is much to be preferred, so that the draconian powers of the UWO can be neutralised; and
- the merely holding of assets in complex offshore structures or trusts is not enough for an UWO, there must be evidence that leads to an "irresistible inference" that a structure is being used for illegal purposes.

SERIOUS FRAUD UPDATES

The SFO has updated its Operational Handbook to include a chapter on how organisations can evaluate their compliance programme. The new chapter outlines the compliance

programmes at different stages of a SFO investigation and prosecution. The Operational Handbook does not constitute official SFO guidance and is designed to be instructive to third parties to demonstrate SFO's approach to matters. The new chapter does not prescribe a particular approach to investigating a compliance programme as individual cases will differ from each other. The SFO instead proposes how an organisation can assess their compliance programme by arranging the assessment around the six principles in the Ministry of Justice's Bribery Act 2020 Guidance.

FOREIGN CONDUCT AUTHORITY

The *Money Laundering and Terrorist Financing (Amendment) Regulations 2019* (UK) (**Regulations**) (available [here](#)) came into effect on 10 January 2020, amending the *Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017* (UK) (available [here](#)). The Regulations align the UK's regime with the international standard set by the Financial Action Task Force's Fifth Money Laundering Directive (**MLD5**).

The Regulations require firms to include new additional high-risk factors to assess whether an organisation needs enhanced due diligence, seek additional information or starts monitoring customer activity. The Regulations also amend the customer due diligence on records and e-money thresholds, duty to respond to requests for information by authorities, crypto-asset activities and reporting discrepancies in information held to the Companies House Register. However in May 2020, the European Commission has issued the UK among other member states with a letter of formal notice for only partially transposing the MLD5.

UK PARLIAMENT TREASURY COMMITTEE – REPORT ON “ECONOMIC CRIME: CONSUMER VIEWS”

On 22 October 2019, the House of Commons Treasury Committee released the 'Economic Crime: Consumer View' Report (**Report**). The Report focuses on how UK legislation directly and indirectly affects its customers who have experience financial crime with financial service firms.

The Report sets out a number of recommendations including:

- The Contingent Reimbursement Model Code should be compulsory for financial services firms. Upon adopting the Contingent Reimbursement Model Code, financial services firms should consider retrospectively reimbursing victims who have relied on the payee name especially where the customer falls into the Code's definition of vulnerability.
 - Implementing a 24-hour delay on all first-time payments.
 - Financial service firms missing the March 2020 Confirmation of Payee deadline should be sanctioned.
 - The Financial Conduct Authority should set tight deadlines for financial firms to block accounts that are receiving stolen funds once suspicious activity has been identified.
 - Banks should be more transparent around de-risking and only use artificial intelligence if they have a high degree of assurance that it will not be biased.
-

European Union (EU)

WHISTLEBLOWING DIRECTIVE

The EU enacted its *Whistleblowing Directive* (2019/1937) (**Directive**) to protect persons who report breaches of EU law (available [here](#)). The Directive obliges all Member States to guarantee whistleblowers adequate protection. However, the Directive is only applicable to certain breaches of EU law such as areas of public procurement, financial services and products, and EU competition and State aid law. The Directive does provide for the establishment of internal external reporting channels which prohibits retaliation and includes support measures. The implementation period is four years for companies with 50 to 249 workers and two years for larger companies.

EUROPEAN SECURITIES AND MARKETS AUTHORITY

The European Securities and Markets Authority (**ESMA**) published the 'Final Report: Peer Review on the collection and use of suspicious transaction and order reports under the Market Abuse Regulation as a source of information in market abuse investigations' on 12 December 2019 (**Final Report**).

The Final Report details how national competent authorities handle suspicious transactions and order reports under the Market Abuse Regulation (**MAR**). The MAR seeks to strengthen EU Member State market abuse frameworks by extending its scope to new markets, new platforms and new behaviours. It contains prohibitions of insider dealing, unlawful disclosure of inside information and market manipulation, and provisions to prevent and detect these practices.

Persons who professionally arrange or execute transactions, investment firms and trading venues are required to report suspicious transactions and order reports to their national competent authorities. Their national competent authority then analyses suspicious behaviours and investigates possible cases of insider dealing or market manipulation.

The Final Report assessed all the national competent authorities to evaluate the effectiveness of their suspicious transactions and order reports. The ESMA found a significant increase in suspicious transaction and order reporting and that national competent authorities can do more to ensure financial participants are contributing to combat market abuse. The Final Report found that the national competent

authorities' analysis of suspected market abuse would be aided by closer cooperation and sharing of practices.

The ESMA recommends national competent authorities can improve their procedures by:

- ensuring all financial players subject to the requirements, including wholesale market participants such as asset managers, are complying with the suspicious transactions and order report requirements; and
- enhancing their focus on suspected non-reporting and poor-reporting of suspicious transactions and order reports including, where appropriate, enforcing and sanctioning non-compliance.

MONEY LAUNDERING DIRECTIVES

MLD4

The Joint Committee of European Supervisory Authorities (**ESAs**) published guidelines on co-operation and information exchange between national competent authorities supervising credit and financial institutions under the Financial Action Task Force's Fourth Money Laundering Directive (**MLD4**). ESA's guidelines clarify the practical aspects of the supervisory co-operation and information exchange. The guidelines create a framework that national competent authorities can use to have oversight from an anti-money laundering and combating the financing of terrorism perspective.

MLD5

On 21 January 2020, senior EU officials expressed concern that many Member States have missed the MLD5 implementation deadline of 10 January 2020 and proposed initiating infringement proceedings.

On 12 February 2020, the European Commission issued formal notices to Cyprus, Hungary, the Netherlands, Portugal, Romania, Slovakia, Slovenia and Spain for not transposing the MLD5. In May, the European Commission also sent letter of formal notice to Belgium, the Czech Republic, Estonia, Ireland, Greece, Luxembourg, Austria, Poland and the UK for having only partially transposed the MLD5. The European Commission also announced that they have sent a letter of formal notice to Estonia because it has incorrectly transposed MLD4. As part of the press

releases, the European Commission stated that *'legislative gaps occurring in one Member State have an impact on the EU as a whole. That is why EU rules should be implemented and supervised efficiently in order to combat crime and protect our financial system.'* The European Commission has stated that if the Member States do not provide a satisfactory response within four months, the Commission may publish further opinions to encourage compliance with MLD4 and MLD5.

Contacts

SYDNEY

**ROBERT WYLD**

Editor and Consultant

+61 2 8274 9593

+61 419 337 557

robert.wyld@jws.com.au**ANDREAS PIESIEWICZ**

Partner

+61 2 8274 9518

+61 408 140 888

andreas.piesiewicz@jws.com.au**ROBERT JOHNSTON**

Partner

+61 2 8274 9581

+61 409 504 444

robert.johnston@jws.com.au**ANGUS HANNAM**

Associate

+61 2 8247 9678

+61 422 642 406

angus.hannam@jws.com.au

MELBOURNE

**CHRIS CONNOR**

Partner

+61 3 8611 1309

+61 411 360 131

chris.connor@jws.com.au

PERTH

**GEORGE CROFT**

Partner

+61 8 6216 7212

+61 418 339 800

george.croft@jws.com.au

BRISBANE

**JOHN POWELL**

Partner

+61 7 3002 2513

+61 418 736 204

john.powell@jws.com.au

ADELAIDE

**BEN RENFREY**

Partner

+61 8 8239 7158

+61 422 602 634

ben.renfrey@jws.com.au

JULY 2020

ADELAIDE

BRISBANE

MELBOURNE

PERTH

SYDNEY

www.jws.com.au