



Litigation Forecast 2022

Certainty in uncertain times
E wāwāhi ngaru ana te waka

MinterEllisonRuddWatts.

Contents

02	Introduction	16	Increasing risks on the horizon
03	The regulators: More stick less carrot?	17	Coping with compliance risk in a rapidly changing world
04	The FMA's approach to enforcement	18	The climate-related financial disclosure regime
06	Commerce Commission: ready to rumble in 2022	20	Cyber threats
08	Reserve Bank's new enforcement vision for 2022 onwards	24	Cartel criminalisation
12	Health and safety regulators to increase focus on 'upstream' duty holders	27	It's getting lonely at the top: directors' risks
13	Privacy stock take	28	Ever increasing risks for directors and managers
		30	Insurance risks for directors and officers
		32	Risk checklist for directors and executives
		33	How will 2022 shape up for employers and employees?
		34	Working with Covid

Introduction

Navigating uncertainty and adapting business planning will be a key factor for businesses in 2022. This is not only due to COVID-19, but also due to increasing regulatory intervention, climate change, class actions and swift legislative change for some sectors. Our litigation forecast sets out our predictions for 2022 and recommendations for businesses to approach these changes. Given the increasing focus on leadership from the top, we have also included a planning checklist to help directors and senior managers to step back at the beginning of 2022 and reflect on how their business is set up to avoid or mitigate inherent risks (see page 18).

Jane Standage

We are experts in risk and our full service Band 1 litigation team is ready to assist your team with litigation, mediation, arbitration as well as risk management at the executive and board level.



Jane Standage
Partner

+64 9 353 9754
+64 21 411 728

jane.standage@minterellison.co.nz



Briony Davies
Partner

+64 4 498 5134
+64 27 444 9736

briony.davies@minterellison.co.nz



Sean Gollin
Partner

+64 9 353 9814
+64 21 610 867

sean.gollin@minterellison.co.nz



Andrew Horne
Partner

+64 9 353 9903
+64 21 2451 545

andrew.horne@minterellison.co.nz



Megan Richards
Partner

+64 4 498 5023
+64 21 676 430

megan.richards@minterellison.co.nz



Stacey Shortall
Partner

+64 4 498 5118
+64 21 246 3116

stacey.shortall@minterellison.co.nz



Richard Gordon
Partner

+64 4 498 5006
+64 27 705 5113

richard.gordon@minterellison.co.nz



Nick Frith
Partner

+64 9 353 9718
+64 21 920292

nick.frith@minterellison.co.nz



June Hardacre
Partner

+64 9 353 9723
+64 21 105 9616

june.hardacre@minterellison.co.nz



Aaron Lloyd
Partner

+64 9 353 9971
+64 21 532 000

aaron.lloyd@minterellison.co.nz



Gillian Service
Partner

+64 9 353 9817
+64 21 366 760

gillian.service@minterellison.co.nz



Oliver Skilton
Partner

+64 9 353 9731
+64 27 513 7594

oliver.skilton@minterellison.co.nz



The regulators:
More stick less carrot?

The FMA's approach to enforcement

Recent cases and guidance from the Financial Markets Authority (FMA) suggest that regulated entities can no longer expect a light touch response to unintentional regulatory breaches – even where those breaches are self-reported and corrected.



Previously, an entity which inadvertently breached its obligations might expect to work with the FMA on an appropriate resolution out of court. However, recent cases and guidance make it clear that regulated entities should be prepared for more court action. It is therefore more important than ever for regulated entities to ensure that they have invested in their systems and processes for managing compliance risks, and to take care when engaging with the FMA.

A shift in approach?

A few years ago, when problems arose, regulated entities were able to liaise with regulators to focus on compensation and rectification rather than prosecution. For example, in 2016, the FMA entered into a settlement with Westpac (and the Commerce Commission) to resolve an issue involving some \$4 million in fees which had inadvertently been overcharged to New Zealand customers using ATM machines in Australia. Westpac prudently self-reported this issue when it became aware of it and agreed with the regulators to pay compensation to affected customers.

Similarly, in 2017, the Commerce Commission, with the FMA's involvement, entered into a settlement agreement with Tower Insurance to resolve an overcharging issue. Tower informed the regulators of the issue and the matter was resolved by Tower compensating affected customers and making a charitable donation to reflect its inability to reimburse some customers. No proceedings were issued, and no penalty was paid.

Fast forward a couple of years, however, and we saw the first proceedings issued under the fair dealing provisions in the Financial Markets Conduct Act 2013 (FMCA) for similar – or even less serious – breaches. For example, in 2019, ANZ Bank informed the FMA that it had identified issues with some of its credit card repayment insurance policies. It had issued multiple policies to a small number of customers and issued policies to an even smaller number of customers who were ineligible to claim under their policies because of their age. These errors were inadvertent, and their monetary value was relatively low – particularly compared with earlier cases. ANZ reimbursed the affected customers in full, with interest. Unlike the previous cases, however, the FMA issued proceedings against the bank, which were ultimately resolved with the bank admitting the claim and agreeing to pay an agreed penalty of \$280,000. While the proposed penalty was agreed in a settlement agreement, as proceedings had been issued, it took the form of a fine imposed by the Court.

The FMA has taken a similar approach to certain issues raised by AIA Insurance, issuing proceedings in 2021. AIA had identified and self-reported three issues in 2018 as part of the FMA's review of life insurers at that time: a purported enhancement of policy benefits, charging premiums after the termination of a policy and treating policies as terminated when they should have remained in force, and incorrect inflation adjustments. AIA has admitted the claims in the proceedings and the FMA has indicated that the parties have agreed on a joint penalty recommendation of \$700,000, which remains subject to a penalty hearing in court which has been set down for 3 February 2022.

The FMA also announced in early December 2021 that it has filed proceedings against Kiwibank for false and misleading representations in breach of the fair dealing provisions in the FMCA. Kiwibank self-reported to the FMA that its general terms and conditions provided that customers

The FMA's approach to enforcement

would not pay transaction fees on their accounts if they also had their home loan with Kiwibank. Inadvertently Kiwibank charged fees to its customers. Self-reporting was prompt and remediation will refund overcharged customers and include use of money interest. Nevertheless, the [FMA decided to issue proceedings](#) to seek a declaration of contravention and a penalty, stating the "nature of the underlying conduct will always be the driving factor".

This shows that the FMA is keen to get penalties confirmed by the courts and is less likely than before to reach an out of court settlement.

The FMA's comments on enforcement

The [FMA's enforcement approach](#) was recently commented on by Ms Karen Chang, Head of Enforcement and Acting General Counsel of the FMA, in a speech setting out the FMA's views on self-reporting, remediation and inadvertent breaches and how these inform the actions the FMA may take to regulate breaches.

In this speech, Ms Chang commented that "none of what I'm saying should be novel" but observed that regulated entities have expressed surprise when enforcement action is commenced for inadvertent

breaches that have been self-reported. Ms Chang stated that the FMA considered that enforcement action is often justified in these circumstances as the breaches may be indicative of a wider problem, such as an inappropriate deferral to a marketing team or under-investment in systems or processes. Insufficient investment in compliance processes may be evidence of an intent to prioritise profits over compliance – particularly as, in the FMA's view, manual exceptions processes are destined to fail. Enforcement action may, therefore, be used to incentivise the allocation of sufficient resources to systems and processes to comply with obligations to customers.

Further, while self-reporting would colour the FMA's view of an entity's conduct, the FMA regards self-reporting as a minimum requirement. It is "a sign that entities take their legal and licensing obligations seriously – and by informing us, they will endeavour to fix the issues quickly". However, for an entity to receive any credit for self-reporting an issue, the self-reporting should be proactive (rather than made in response to a request for information) and prompt; entities should not "wait until they have fully unravelled" any problems engaging with the FMA.

While proactive and early self-reporting will be taken into account when the FMA considers its enforcement response, it does not insulate an entity from litigation. Enforcement action is more likely to be taken where there is customer harm or serious misconduct – particularly as the FMA considers that regulated entities have had enough time to understand and meet their obligations. While the FMA may have been willing to take an educative approach to early regulatory breaches, entities that have been regulated since December 2016 can expect to be met with less patience.

Finally, Ms Chang confirmed that customer remediation is regarded as a "bare minimum". Relevant to the FMA's view of how the entity has conducted itself includes whether remediation "was timely, well organised and communicated or whether there were delays and mistakes".

Key message

The key message from Ms Chang's speech and the FMA's recent enforcement actions is the importance of devoting appropriate resources to managing and monitoring compliance risks.

What to consider?

Consider whether your systems are operating correctly and whether you have an effective process for escalating issues. Keep records of your efforts and ensure that when issues do arise, they are self-reported promptly and that they are remediated quickly and effectively. Care must also be taken when engaging with the FMA to ensure that correct and complete information is provided.

Commerce Commission: ready to rumble in 2022

With increased yearly funding on the horizon that will almost double between 2021 and 2024, we expect to see a higher level of enforcement action by the Commission. But where will it focus its attention? While the Commission is yet to release its specific priorities for 2022/2023, we make our predictions on the hot topics for next year:



Credit-related enforcement

Credit-related enforcement particularly for the [new regime](#) which came into force on 1 December 2021, include the requirement that directors and senior managers exercise due diligence, the new suitability and affordability regulations and the duty to provide disclosure about debt collection. These are complex requirements which require lenders to pay detailed attention to their operations to ensure they are not caught out.

The amendments were initially set to come into force on 1 October 2021, however, the amendments were delayed due to the disruption caused by the recent lockdowns across New Zealand. Instead they came into force on 1 December 2021 (except for chapter 12, which comes into force on 1 February 2022). The Government considered the delay necessary due to the impact on lenders'

implementation of the amendments, that had the effect of disrupting training and other preparations and forced a reprioritisation of lenders' resources to support existing customers. Although time was extremely tight even for the December deadline (especially given the last minute guidance issued by the Commission in September), we expect the additional time lenders had to finalise their systems following this delay will mean the Commission will take a proactive approach to monitoring compliance with the amended provisions, in particular the new duty for directors and senior managers of consumer lenders to exercise due diligence to ensure compliance with CCCFA. We expect that the Commission will be on the lookout for suitable cases to prosecute, to deter, and also to obtain useful guidance from the courts.



Unfair contract terms

The unfair contract terms regime has been extended to include certain business to business contracts worth less than \$250,000 per year. This change will come into effect in August 2022 via the Fair Trading Amendment Bill. A term in a low value business-to-business contract will be unfair if the term:

- (a) would cause a significant imbalance in the parties' rights and obligations arising under the contract;
- (b) is not reasonably necessary in order to protect the legitimate interests of the party who would be advantaged by the term; and
- (c) would cause detriment (whether financial or otherwise) to a party if it were applied, enforced, or relied on.

Given the one-year delay from Royal Assent to the date these provisions come into force, it is likely this will be a matter of focus

for the Commission, who we anticipate will take a firm stance on compliance. Only the Commerce Commission can seek a declaration that a term is unfair (rather than a contractual counterparty). Before these amendments come into force, those who rely on standard form contracts will need to review and update their contracts to ensure they are not caught out by this extension.

There is also a new prohibition on unconscionable conduct which is designed to cover serious misconduct which goes far beyond what is commercially necessary or appropriate. A breach of this provision carries a maximum fine of \$600,000 for businesses and \$200,000 for individuals. This is obviously a high threshold and so we do not expect this will make much difference to businesses who have good procedures and policies in place and clear expectations of employees including marketing teams.



Substantiation of claims

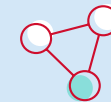
Since the prohibition on making unsubstantiated representations came into force on 17 June 2014, there have been only 18 investigations by the Commission under this provision. There are currently no open cases on the Commission's books regarding unsubstantiated representations. With little judicial guidance, the Commission will be looking closely for some example cases to pursue. A representation is unsubstantiated if the person making the representation does not, when the representation is made, have reasonable grounds for the representation, irrespective of whether the representation is false or misleading. It does not matter if substantiation is later found to corroborate the

statement, what matters is whether that information was held by the person making the representation at the time the representation was made.

A higher degree of substantiation is required for claims around health benefits, claims that are difficult for consumers to evaluate or that purport to be backed up by scientific research. We expect this will be an area closely monitored by the Commission particularly in the context of the global pandemic.

The Commission has previously commented that it would be pragmatic in its approach to its enforcement during COVID-19 lockdowns, but we expect to

see a renewed focus from the Commerce Commission on substantiation of claims once the COVID-19 crisis has abated. For 2022, as a practical risk management action, we recommend documenting the steps taken in the due diligence process to substantiate any representations, the date the information was obtained, the source of information relied on, who in your organisation reviewed the information, and (for scientific claims) the qualification of personnel interpreting results. For larger companies, it is also prudent to facilitate critical information flow between marketing, legal and product development teams and ensure a standardised process is in place for due diligence and audit to ensure all claims are substantiated.



Cartels

Cartels are always a priority focus for the Commission, but with the criminalisation of cartel conduct in April 2021, the Commission will be looking to bring its first prosecution for cartel conduct as soon as there is an appropriate case.



Reserve Bank's new enforcement vision for 2022 onwards

How will it be put to work?

In March 2021, the Reserve Bank of New Zealand established a new Enforcement Department following a lengthy consultation process to settle upon some [Enforcement Principles and Criteria](#) to inform its approach.

The Department's work is expected to begin in earnest in early 2022. This will result in closer scrutiny of entities that are regulated by the Reserve Bank and an increased number of regulatory prosecutions and other actions.

What has changed?

The creation of a new Enforcement Department indicates that the Reserve Bank intends to focus more upon its enforcement powers than it has done previously, and determine how it will use them in a more structured way. This began with work to develop an enforcement framework to guide the Enforcement Department's activities. In October 2021, the Reserve Bank released a paper outlining proposed Enforcement Principles and Criteria and sought submissions from stakeholders. The Enforcement Principles and Criteria are expected to be released in early 2022.

The Reserve Bank exercises enforcement powers under various statutes which govern the financial sector, such as the Anti-Money Laundering and Countering Financing of Terrorism Act 2009, Reserve Bank of New Zealand Act 1989, Insurance (Prudential Supervision) Act 2010, Non-bank Deposit Takers Act 2013 and Financial Markets Infrastructures Act 2021. Soon, there will be two more: the Reserve Bank of New Zealand Act 2021, replacing the 1989 Act of the same name, and a new Deposit Takers Bill – an exposure draft that is currently being consulted on with the expectation it will come into force in 2023.

Until 2021, the Reserve Bank managed its enforcement work as part of its general operations, without a dedicated enforcement arm. Perhaps as a result of this, it has generally been less active in using its enforcement powers than the primary financial sector regulators, the Financial Markets Authority (FMA) and the Commerce Commission.

The Reserve Bank gets an enforcement department

What will the Enforcement Department do?

The Enforcement Department will investigate breaches of regulatory requirements, provide input to supervisors on compliance matters, and recommend enforcement actions where appropriate. Though it is operationally separate from the Reserve Bank's Supervision Department, it is expected that the two will cooperate in these functions in light of their shared membership in the broader Financial Stability Group.

The Enforcement Department's activities will be guided by the enforcement framework. The Reserve Bank says this framework will be tied to three goals:

- incentivise and monitor prudent behaviour;
- promote confidence in compliance; and
- enforce compliance by holding institutions to account for non-compliance.

In addition, the Reserve Bank has formulated three high-level Enforcement Principles and four Enforcement Criteria that are intended to apply across all the areas that the Reserve Bank regulates. The three enforcement principles are high-level ideals that guide its enforcement strategy: risk-based, proportionate and transparent. The four criteria are specific considerations for use when deciding on the appropriate enforcement response in each case: seriousness of conduct, responsiveness, public trust and confidence, and efficacy.

Principles in practice

The Reserve Bank offers the following examples of how these high-level ideas are intended to guide the way it approaches enforcement in particular cases:



Risk-based principle

The Reserve Bank will focus its efforts and its enforcement resources to address conduct around issues that could have the potential to damage the financial system or the New Zealand economy significantly. Perhaps surprisingly, however, the example given is AML/CFT regulation, which is not obviously an issue that poses the greatest threat to the financial system or the economy (compared, for instance, to the need to ensure that deposit takers and insurers are undertaking only prudent exposures and have sufficient financial reserves).



Proportionality

The Reserve Bank will determine its enforcement response in a case after considering aggravating and mitigating factors, the broader compliance context

and internal and external (i.e. cases with other regulators) precedent. It will seek to apply the regulatory tool that is appropriate for the nature and magnitude of the non-compliance, the particular entity and its general attitude to compliance, the risk posed by the non-compliant activity and the public interest.



Transparency

The Reserve Bank will publish key guidance and enforcement outcomes unless there are exceptional circumstances that make it inappropriate to do so. Transparency also means engaging openly and honestly with regulated entities during investigations and not publishing allegations during the investigation phase unless it is appropriate to do so.

The Reserve Bank gets an enforcement department

What do the Enforcement Criteria tell us?

The Reserve Bank has broken each of its four criteria down into factors that it will consider when making enforcement decisions.

Seriousness of conduct

- prevalence of non-compliance (i.e. whether the entity has a history of breaches);
- magnitude and impact (including whether a breach is technical or not and whether it presents systemic risk or shows up failings in a compliance programme – again AML/CFT is given as an example, which appears to signal a particular focus on that aspect of regulated entities' conduct; and
- executive or operational knowledge (including whether the relevant conduct was known at a senior level, how long it persisted, and whether there was negligence or recklessness).

Responsiveness

- cooperation with the Reserve Bank in addressing the breach, including whether it was promptly admitted and fully and willingly disclosed;
- the entity's compliance history (which seems to duplicate the same point under the seriousness factor and could in our view be omitted from this one); and
- the entity's conduct in resolving the breach, including any proactive and voluntary remedial action.

Public trust and confidence

- Public confidence – whether enforcement action will promote public confidence in the financial system. Interestingly, the Reserve Bank seems to be willing to acknowledge that some enforcement action may risk financial instability, such as a 'run on the bank' – a very welcome indication of necessary pragmatism.
- Deterrence value – whether enforcement action is likely to modify the behaviour of the entity and others.
- Consistency and fairness – whether the enforcement response is consistent with previous action by the Reserve Bank and other regulators.
- Promoting maintenance of the law – whether enforcement will promote regulatory objectives and policy objectives, as well as whether there is a need to clarify the law.

Efficacy

- Strength of evidence – the Reserve Bank will be pragmatic about its prospects of success on the evidence. In some cases there may be a tension as a regulated entity may cooperate in the hope of resolving an issue, but in doing so provide the Reserve Bank with the evidence it requires.
- Available legal defences – a fundamental and necessary consideration, because if a credible defence is available, no wrong has been committed, in which case the Reserve Bank has no business bringing enforcement proceedings.
- Supporting other regulators and working with them when regulatory areas overlap.
- Potential outcomes – the effect upon overall financial system stability (also a consideration under the public trust and confidence factor) and whether the proceeding is likely to result in a conviction, compensation or penalty – and also whether a warning or another lesser response is appropriate.

The Reserve Bank gets an enforcement department

What effect will the consultation process have on the enforcement framework?

Generally, we view the draft Enforcement Principles and Criteria as appropriately pragmatic. Indeed, they closely resemble the equivalent frameworks adopted by the other New Zealand financial market regulators.

However, other regulators are more specific about their priorities. While the Reserve Bank says that its principles are intended to be high-level, it offers only one indication of a priority area: AML/CFT regulation.

The FMA, by comparison, is much more specific and recently issued a revised set of priorities in response to the effects of the COVID-19 pandemic, including supporting investors to make good decisions, responding to scams, monitoring treatment of customers in vulnerable circumstances and responding swiftly to market disruptions and significant events.

We expect stakeholders, especially those potentially subject to enforcement action by the Reserve Bank, to have communicated to the Reserve Bank that greater specificity would enable regulated entities to respond more effectively. If such submissions are received and taken on board by the Reserve Bank, this would hopefully result in greater detail as to the Enforcement Department's areas of focus for 2022.

What should we expect from the Enforcement Department in 2022?

We expect to see more enforcement activity from the Reserve Bank in 2022, as a natural consequence of resources being invested to develop a dedicated enforcement arm. Based on the approach that the FMA took when it was set up, activity may be restrained at first, as the Enforcement Department develops its internal processes and identifies strategies for targeting priority areas.

Over time, we expect to observe a significant increase in enforcement action, as we have seen with the FMA. As the only issue specifically identified in the draft Enforcement Principles and Criteria, AML/CFT is likely to be a real focus (as it has been for the FMA), at least initially.

One issue to monitor is how the Reserve Bank manages the risk that enforcement action may have on trust and confidence in the financial system generally – an issue it acknowledged in the draft Enforcement Principles and Criteria. The Reserve Bank will be cautious of taking action that may trigger a collapse in public confidence in a systemically important financial institution or in the financial markets generally, possibly resulting in a calamitous outcome. This is not a factor that the FMA or the Commerce Commission are normally expected to take into account when regulating conduct.

The inherent conflict between enforcing conduct rules and preserving confidence in the financial system is one of the key reasons for the separation of conduct and prudential regulation under the "Twin Peaks" model as originally developed in Australia in the Wallis Report, and partially applied in New Zealand. This is reflected in the potential conflict between the Reserve Bank's proposed principle of transparency (expressed in its intention to publish the outcomes of its investigations) and its criteria of public trust and confidence (which may be damaged by the same publication).

While we view the emphasis on public trust and confidence as important and consistent with the financial stability goals of the Reserve Bank, it highlights the inherent conflict referred to above and potential conflicts between the Reserve Bank's response in particular cases and the responses of other financial services regulators. In our view, this issue should be considered and addressed by all of New Zealand's financial services regulators, particularly if a rise in class actions (notwithstanding the completion of regulatory action) is on the horizon.



We expect to see more enforcement activity from the Reserve Bank in 2022, as a natural consequence of resources being invested to develop a dedicated enforcement arm."

Health and safety regulators to increase focus on 'upstream' duty holders

What is your level of influence and control over the way in which work is carried out at a workplace?

This question is set to take centre stage in 2022 – with our prediction that WorkSafe and the other health and safety regulators will increase their focus on 'upstream' duty-holders, including directors and officers. If you're not paying attention to how your decisions influence the work carried out by others, there is a good chance that WorkSafe will instead.

As we are all getting to grips with managing COVID-19, it is important not to lose sight of broader health and safety obligations. WorkSafe appears to be facing resourcing pressures, but the range of those who owe duties under the Health and Safety at Work Act that it is focusing on is growing wider.

So, what are we likely to see in 2022?

- A willingness by health and safety regulators to continue to investigate and prosecute directors and officers, where they consider there to have been clear and/or repeated failures in meeting their due diligence duties. With the trial of the directors of the entities associated with the ownership of Whakaari White Island set to take place in 2023 and the high-profile prosecution of a former CEO of a significant company working its way through the courts, the regulators have signalled a clear intention to prosecute those directors and officers who they consider to have breached their obligations.
- A widening of the regulators' focus on PCBUs with 'upstream' duties whose work or decisions may impact on those more proximate to the work being carried out. These PCBUs include businesses that design, manufacture, import, supply or install plant, substances or structures. In short, we expect the regulators to look closely at the work of upstream PCBUs, what they provide to others and their level of influence and control over the work being carried out. This anticipated targeting of upstream duty-holders reflects that they often have the ability to influence the way in which work is carried out by others, even if they are a step removed from the actual carrying out of the work.
- The Health and Safety at Work Act has been in force for almost six years now. We are now well out of any grace period and the expectation of compliance and the risks of non-compliance are becoming increasing clear, particularly for officers and upstream PCBUs. Criminal liability cannot be avoided simply because you're too senior, too far up the supply chain, or otherwise too far removed from the place where the actual work is carried out. Taking steps to consider how to keep all workers safe where you have a level of influence and control over a workplace is where the regulators want to see the dial shifted in New Zealand and that's where we expect to see a significant focus from the health and safety regulators in 2022.



Privacy stock take

Stronger enforcement planned

One year into the application of the Privacy Act 2020, the strengthened privacy protection regime has had plenty of opportunity to shine through the COVID-19 pandemic response.



Werner Sevenster / Unsplash

¹Liz MacPherson has been appointed as a Deputy Privacy Commissioner for up to 12 months while recruitment for the Privacy Commissioner role is underway.

It would be easy to predict 2022 as the year that the Office of the Privacy Commissioner (OPC) switches gear from education to enforcement under the enhanced privacy regulatory framework.

But while there are signs that the OPC is indeed feeling emboldened, we have not yet seen any of the large-scale investigations or enforcement litigation that are underway in Australia or the United Kingdom. Instead the OPC appears to be treading carefully, making examples of the worst cases only, and focusing on widescale education and compliance rather than enforcement.

This means that organisations still have an opportunity to get their house in order. But now is the time to make use of this extra breathing space. Longstanding Privacy Commissioner John Edwards finished up in the role in December 2021. The new Commissioner will have big shoes to fill. Commissioner Edwards was widely regarded as having been a force for good in terms of balancing privacy protections with the need for efficient and effective government and security forces. Before too

long, the new Commissioner will want to make their mark.¹ A stronger enforcement approach and proactive assertion of privacy rights and protections would be a one way to do that – and would certainly align the office with the ‘less carrot, more stick’ approach being taken by other regulators around New Zealand.

The OPC report also contains a none-too-subtle warning about timely data breach notifications:

“In June this year, we clearly set out our expectation around the timeliness of privacy breach notification. A notifiable breach should be reported to us no later than 72 hours after an agency has become aware of it. Currently, less than half of all serious breach notifications are being made within the expected timeframe. You should not wait until you have all the details of the privacy breach, our tool allows you to update the notification at a later stage, as more information becomes available. The sooner we know about a breach, the sooner we can support you to reduce potential harm to affected individuals.”



Mandatory breach reporting – the early lessons

The new Commissioner's focus will no doubt be informed by lessons learned so far. We now have the first 12 months of data on mandatory data breach reporting in New Zealand. The OPC marked the occasion with a new report analysing the types of privacy breaches being reported under the mandatory reporting regime.

Key findings include:

- There was almost a four-fold increase in the number of privacy breach notifications in the first 10 months of the new regime as compared to the 10 months prior – a total of 697 privacy breach notifications.
- 33% of all reported breaches met the Act's threshold for "serious harm".
- Between 1 December 2020 and 31 October 2021, 35% of serious breaches reported to the OPC involved emotional harm. Only 14% involved reputational harm, 13% involved identify theft and 11% involved financial harm.
- The majority of serious breaches reported are the result of human error. The second main cause is malicious attack.
- The top five industries reporting serious privacy breaches in 2021 were (in order) health care and social assistance (at 79 serious breach notifications); public administration (at 51 serious breach notifications); education (at 24 serious breach notifications); 'services' (a broad sector, but likely to include services across the professional services, IT and entertainment sectors, at 19 serious breach notifications); and finance and insurance (at 14 serious breach notifications).

The OPC report also highlights the ongoing need for high-quality and regular staff training around protection of privacy as a first line of defence against the risk of serious breach, and possible enforcement action going forward. Investing properly in digital security is also fast becoming a baseline requirement for any organisation handling more than minor amounts of sensitive personal information.

2022 edging towards increased compliance and enforcement measures

There are some signs that the OPC is already edging towards more proactive regulatory enforcement. One indicator is its recent launch of a new compliance monitoring programme targeting property managers and agencies, and landlords, with the Commissioner observing that the sector is now "on notice" that there are no excuses for over-collection and unauthorised use of personal information and that there will be consequences for non-compliance.

In many ways, the property sector is an intriguing choice for early focus, given the industries where the OPC now knows serious privacy breach reporting is taking place. It suggests that the OPC is seeking

to function as a fence at the top of the cliff rather than just the ambulance at the bottom once a serious privacy breach has occurred.

The programme seeks to prevent breaches through, among other steps, an annual survey to audit application forms, contract forms, and privacy policies of letting agencies, property managers, and third-party service providers, to give tenants and prospective tenants more confidence in the way their personal information has been collected, used, stored, and disclosed by their landlord or property manager. Aside from naming and shaming, a rarely used option in the past, there are now a range of tools at the OPC's disposal now for any non-compliance with Privacy Act requirements that come out of this compliance programme, including warning letters, access directions and compliance notices (which attracts a fine of up to \$10,000 if not complied with).

Another sign that the OPC is moving towards more proactive enforcement is the Commissioner's issue in September 2021 of the first Compliance Notice under the new Act after a cyber-attack exposed that the Reserve Bank of New Zealand was not, in the OPC's opinion, meeting its obligations around the safe storage and security of personal information. The Compliance Notice – still the only one made public at the time of print followed what the Commissioner described as “a significant breach of one of the Bank's security systems”. The breach was described as one which involved multiple areas of non-compliance, and one which “raised the possibility of systemic weakness in the Bank's systems and processes for protecting personal information.” The Compliance Notice essentially provided a template for the Bank to report on to the OPC, confirming the improvements to their policies and procedures required by the Commissioner to make their systems more secure.

These sorts of actions suggest that the OPC's expectations are slowly but surely rising. That provides organisations with the window many still need to ensure proactive privacy risk management is a C-suite issue, regularly reported on and built into new initiatives.

Evidence based assessments – the new norm

COVID-19 has no doubt been a significant factor in the lack of urgency around stepping up enforcement action to date, both because of the need for the OPC to balance COVID-19 issues with BAU projects, and to balance the need to protect individual privacy against collective public health outcomes in a global pandemic.

One indicator of the Commissioner's approach to balancing these requirements can be found in his submissions as intervenor in *Te Pou Matakana v Attorney-General* – the recent judicial review of the Ministry of Health's initial decisions to withhold data on the vaccination status of certain groups of Māori from a local Māori health provider. The health provider was seeking this information to better target its vaccination programme for local Maori in the lead up to the application of the now live COVID-19 traffic light framework.

As an intervenor in the Court action, the Privacy Commissioner has made clear his view that:

- in relation to rights to privacy and to health, the actions and decisions of public bodies must be proportionate and evidence-based – both in relation

to whether it is necessary to disclose and use the individuals' information, and whether that disclosure and use presents a realistic prospect of preventing or lessening the health risk; and

- privacy and human rights principles can be, and are, reconciled as necessary to protect the lives and wellbeing of individuals and the wider public, but individuals and the wider public can also be reassured that their rights are still being upheld and protected within the bounds of the Privacy Act.

The Court agreed that the framework of privacy and health rights, and the need to act consistently with both, requires an evidence-based approach to decision making. It found that that the Ministry of Health “did not conduct the necessary objective, evidence-based assessment” of the relevant issues in that case and directed the Ministry to remake its decision accordingly. Several decisions and additional Court applications and decisions later, the Ministry did eventually agree to release the information following an assessment of what was necessary to lessen the threat posed by COVID-19 – but only with clear privacy protections in place for the data as it was to be used by Te Pou Matakana/Whānau Ora Commissioning Agency.

As requirements for sharing personal information around vaccination status and movements increase, it will be important for all organisations undertaking privacy risk assessments to take extra care to seek out an evidence base for decision making, and to be prepared to rely on that evidence base to defend its decisions whichever side of the disclosure equation it lands on.

Picking the future battle grounds

Commissioner Edward's parting advice to the new Commissioner suggests further caution ahead. In a recent seminar (December 2021), he suggested that the new Commissioner should pick their battles wisely for the greatest impact, as the OPC has a limited amount of influence even with its new enforcement powers. The new Commissioner will need to build up their influence by calling out good behaviour as well as bad, and by helping organisations to achieve their objectives in ways that respect privacy. But when the new Commissioner does see something that will seriously affect individuals, they are likely to feel a need to make people sit up and take notice. So the window for organisations to get their house in order seems likely to rapidly narrow in the next 12 months.



Increasing risks
on the horizon

Coping with compliance risk in a rapidly changing world

A guide for directors and executives

The significant increase in business regulatory activity that began with the Global Financial Crisis and Pike River mine incident, and expanded further with large-scale inquiries into the conduct and culture of banks, insurers and other financial institutions, shows no signs of slowing down.



Recently, regulators such as the Financial Markets Authority and the Reserve Bank have significantly increased their resourcing and set up new enforcement teams. New legislation governing financial advice and privacy, and proposed new laws around climate disclosure have introduced (or will introduce) new penalties, including possible criminal liability for directors. Long-awaited changes to introduce a class action regime appear likely to come to fruition soon, further exposing directors to additional risks.

Most significantly, financial services regulators in many jurisdictions have become increasingly concerned with conduct and culture, leading to the establishment of the Royal Commission into Misconduct in the Banking, Superannuation and Financial Services Industry in Australia in 2017, and to the Reserve Bank of New Zealand and the Financial Markets Authority launching a series of inquiries into the conduct of financial institutions in New Zealand and bringing court proceedings against those who have made mistakes. As we discussed on pages 4 and 5, financial institutions are now expected to ensure that they invest appropriately in their systems to ensure good customer outcomes, monitor those systems proactively for compliance and demonstrate leadership from the board to ensure that the institution's culture

encourages good customer outcomes. While issues are often self-reported, action is increasingly taken against entities even where errors were unintentional and self-reported, especially if self-reporting is delayed and the errors could be blamed on insufficient investment in compliance processes or systems. The need to get things right is stronger than ever, and the onus is on boards and senior executives to drive a strong culture of compliance from the top. We are increasingly seeing this view applied by other regulators outside the financial sector.

Boards and executives must also consider a broader range of risks than in days gone by. The Financial Sector (Climate-related Disclosures and Other Matters) Amendment Act 2021 will shortly require certain entities to identify and report on the impact of climate change on their organisations and disclose their greenhouse gas emissions, with the threat of criminal liability for directors if misleading statements are made. Furthermore, there are heightened business integrity risks such as the criminalisation of cartel conduct and the COVID-19 pandemic has intensified cyber risks.

We discuss each of these risks in the following articles.

The climate-related financial disclosure regime

New enforcement risks

In our 2021 litigation forecast, we considered the possible avenues for climate change litigation to be brought in New Zealand in light of the landmark climate change proceeding, *Smith v Fonterra*, where we represented two of the defendant parties. Following the decision of the Court of Appeal striking out the claims, permission has now been sought to appeal to the Supreme Court. We also reported that a new climate-related financial disclosure regime announced by the Government in September 2020 might soon provide a further avenue for enforcement of climate change related commitments for entities falling within the regime's scope. A year on from that announcement, the climate-related financial disclosure regime has quickly taken shape. On 27 October 2021, the Financial Sector (Climate-related Disclosures and Other Matters) Amendment Bill (CRD Bill) received Royal assent, only six months after its introduction to Parliament in April 2021.

What does the CRD Bill do?

The CRD Bill amends a number of statutes to introduce mandatory climate-related disclosures for businesses subject to the Financial Markets Conduct Act 2013. Once in force, the CRD Bill will require certain entities, known as Climate Reporting Entities (CREs), to produce annual climate statements that identify and report on the impact of climate change on their organisation and disclose greenhouse gas emissions.

Premised on the acknowledgment that climate change is an economic risk that should impact an organisation's long-term and short-term decision-making, the CRD Bill is the next step in the increasing adoption of legal solutions to climate-related risks. The Bill aims to ensure that

the effects of climate change are routinely considered in business, investment, lending and insurance underwriting decisions.

The CRD Bill will apply to approximately 200 CREs, comprised of:

- listed issuers of quoted equity securities or quoted debt securities (i.e. entities with a market capitalisation exceeding \$60 million);
- large registered banks, licensed insurers, credit unions and building societies (with total assets exceeding \$1 billion, or, in the case of licensed insurers, where premium income exceeds \$250 million); and
- large managers of registered managed investment schemes (with total assets exceeding \$1 billion).



The new regime will impose additional disclosure obligations on CREs in each financial year. CREs will be required to:

- prepare climate statements that disclose information about the effects of climate change on their organisation and are in accordance with climate standards issued by the independent External Reporting Board (XRB);
- keep proper records that will enable the CRE to ensure that its climate statements comply with the climate-related disclosure framework. The entity must retain these records for at least seven years;
- to the extent that the statements are required to disclose greenhouse gas emissions, obtain an assurance engagement in relation to those statements; and

- lodge copies of its climate disclosure statements with the Registrar of Financial Service Providers within four months after the balance date of the CRE and include a copy of the climate statements prepared by the CRE in its annual report.

Climate disclosure statements will be made in accordance with climate standards issued by the XRB. The XRB has modelled the approach of the Task Force on Climate-Related Financial Disclosures and structured CRE's disclosure obligations into four thematic pillars: Governance, Strategy, Risk Management and Metrics and Targets.

In November 2021, the XRB completed its consultation on the Governance and Risk Management sections of the proposed regime.

The climate-related financial disclosure regime

Governance disclosures will focus on the level of oversight that boards and management have in overseeing, assessing and managing climate-related issues. Risk management disclosures will focus on how CRE's climate-related risks are identified, assessed and managed and how those processes are integrated into existing risk management processes. The XRB anticipates that the Strategy and Metrics and Targets pillars of the disclosure framework will be released for consultation in March 2022.

Enforcement and Risk

Importantly, the CRD Bill has teeth. Failure to comply with the reporting obligations will expose CREs to enforcement action by the Financial Markets Authority (FMA). The regime will introduce a range of penalties including:

- Infringement offences: Failure to keep CRD records in the prescribed manner, make CRD records available for inspection, lodge the climate statements or include the climate statement in an

annual report are infringement offences and a CRE is liable on conviction to a fine not exceeding \$50,000.

- Civil liability: Where a CRE fails to keep proper CRD records or prepare or lodge climate disclosure statements, this may give rise to civil liability of a penalty not exceeding \$1 million in the case of an individual or \$5 million in any other case. Failure to keep CRD records for seven years may give rise to a penalty not exceeding \$200,000 for an individual or \$600,000 in any other case.
- Criminal liability: It is a criminal offence for a CRE and its directors to knowingly fail to comply with the climate standards in any of the climate statements prepared by the CRE. A director is liable for a fine not exceeding \$500,000 or a term of imprisonment of up to five years (or both), and in any other case, a fine not exceeding \$2.5 million.

The FMA has indicated that, at least initially, it will be "focused on supporting climate reporting entities and other relevant stakeholders as they prepare for the new regime...in the early stages of the new regime, enforcement action is likely to be focused only on serious misconduct, such as failure to produce climate statements or where climate statements are false or misleading".

In addition to potential enforcement action by the FMA, the emerging CRE regime and increasing transparency of climate-related risks could give rise to multiple avenues for climate change litigation. CREs should be aware that their climate disclosure statements, if they contain "greenwashing" or are otherwise misleading, could lead to liability under the Fair Trading Act 1986 and the fair dealing provisions of the FMCA for misleading or deceptive conduct or false, misleading or unsubstantiated representations:

- CREs' climate disclosure statements and annual reports could become the subject of a claim of misleading or deceptive conduct by way of greenwashing, meaning that a CRE's disclosure statement includes disclosures that are false or misleading, that a CRE has been unable to fulfil, or that identify climate issues or risks that are not adequately addressed.
- A claim may be brought against a CRE on the basis that inadequate disclosure (or non-disclosure) of a material climate risk constitutes misleading or deceptive conduct. While we are yet to see such a claim in New Zealand, similar litigation has occurred in Australia (*Abrahams v Commonwealth Bank of Australia*).

- With the disclosure of CRE's climate-related risks and management strategies, there is also a risk of claims being brought against CRE's by shareholders or investors for alleged failures to appropriately consider or adapt to the risks posed by climate change, where that failure impacts on private interests.

Where to from here?

The CRD Act is coming. The XRB is scheduled to issue a climate standard by December 2022, meaning that CREs will be required to make disclosures in accordance with that standard for accounting periods beginning on or after 1 January 2023. It is therefore important that CREs begin to work on their compliance arrangements now.

Other non-CRE businesses should also monitor developments as it is likely that the CREs they deal with may require similar compliance and disclosure as a condition of business. Moreover, over time, the CRD regime may expand to cover other large organisations.

Cyber threats

An increasing risk requiring a multi-faceted legal response

Cyber-attacks on businesses and other organisations are on the rise as is the damage they cause. Cyber-crime is now thought to have surpassed all other types of crime combined. It is no longer unusual to read of a major cyber-attack that has caused significant disruption, often to a 'household name' firm or organisation.

In the past year alone, the Reserve Bank of New Zealand, the Waikato District Health Board, users of Microsoft Exchange, Air New Zealand via its passenger processing system provider SITA, NZ Post, Inland Revenue, MetService, Kiwibank and ANZ have all been the targets of cyber-attacks, resulting in varying degrees of disruption and damage.

Perhaps the most significant of these was the attack in May 2021 upon the Waikato DHB, which threw the public health system in the Waikato region into disarray. This left the DHB unable to manage and carry out routine medical procedures, resulting in cancellations of many patient procedures. The DHB eventually resorted to manual record-keeping and workarounds, including transferring a number of patients to other regions along with their clinicians. A month later, while some services and systems had been restored, many had not and there was still a long way to go.

The most significant development has been the increasing prevalence of 'ransomware' - software that infects a system and encrypts files which cannot be accessed until a ransom is paid for a decryption key. In most cases, ransomware gains access to systems through 'phishing' emails in which staff click on a link to a fraudulent website. Cyber criminals increasingly take time to review data after gaining access, to identify the most valuable or sensitive data and the most critical systems, before making a targeted attack. When this approach is taken, ransom and extortion claims are typically much higher.

Typically, businesses are unable to operate properly for between 7 and 10 days following a cyber breach, although as the DHB has shown, the effects may last much longer.

These incidents illustrate the risks that New Zealand organisations face from cyber criminals and the disruption and damage their actions may cause.

For the year ahead we see



Increasing numbers of cyber-attacks and resulting losses



Regulatory claims against targets of cyber attacks, including privacy penalties



Increasing difficulty in obtaining cyber insurance and onerous demands by insurers



Increasing numbers of legal claims arising from cyber-attacks, including in areas such as professional negligence claims and other liability claims by owners of data against the targets of the attacks, claims against service providers for failing to prevent attacks



Insurance claims and disputes

Cyber threats

The nature of cyber-attacks mean that national borders are meaningless. New Zealand organisations are as likely to be targeted as those in larger countries.

A technical perspective

Cyber-crime is low-risk for offenders because they operate remotely and remain anonymous. Cyber criminals usually either steal users' or their customers' data or deny users access to data or systems. In either case, they usually demand ransoms and threaten to release or delete confidential data if they are not paid. Information about the amounts paid to cyber criminals is difficult to find because most organisations do not publicise their ransom payments, and their insurers are also reluctant to share information – but the crimes would not be committed if they were not profitable.

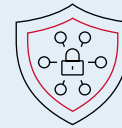
Some technical experts warn that New Zealand is a soft target for cyber criminals, because we have become accustomed to thinking of ourselves as outside the main areas of commerce and criminal activity because of our geographical isolation. This means nothing in a cyber-connected world, in which New Zealand is as exposed as anywhere else to cyber criminals. Our naivety makes us an easier target than

countries that are more accustomed to defending their organisations from fraud and crime.

Organisations are now more exposed than ever because of the changing ways in which we work. Remote working is increasingly common, which means systems are more frequently accessed remotely through personal connections that are more difficult to monitor and secure. Organisations increasingly allow customers into their business processes through shared portals, online logins and other means which create further points of entry.

Experts advise that getting the technical basis right is important. Up to date software patches, identity verification, email security, multi-factor authentication and device security are all important. [CERT NZ's top 11 suggestions](#) for cyber security are a good place to start.

Staff are weak links and must be trained and tested often so that they do not fall victim to 'phishing' or 'trojan' attacks. A managed EDR (Endpoint Detection and Response) solution to protect devices is also critical, as this is a key risk of unauthorised access to a network.



Organisations can take steps to protect themselves from legal risks during and immediately following a cyber-attack. These include:

- Take prompt steps with appropriate IT assistance to mitigate any loss.
- Make no admissions about the adequacy or otherwise of cyber security arrangements or any other matter. Expressions of regret that an incident has occurred may be appropriate but take legal advice first.
- Consider taking PR advice. Your insurer may pay for this as well.
- Before an attack, make sure that you have sufficient visibility of your technical environment and have tools such as EDR already deployed so that you are ready to respond.
- Involve insurers at the outset. They will often have a pre-approved panel of IT specialists and lawyers who can help. Take their advice early. You can make things worse by trying to deal with the issue yourself.

Cyber threats

The legal impact of cyber-attacks

A cyber-attack or cyber security breach will inevitably require a legal response as well as an IT response. The following legal claims and issues often arise:

- The target organisation suffers its own losses – money is stolen through payment diversion schemes or data is stolen or locked up so that it cannot be accessed, and normal operations are affected. This causes financial loss to the target.
- The target organisation incurs liability to customers or other third parties such as those whose personal information is released. Customers' money may be lost, or their data locked up or released to the public.
- Regulatory action by the Privacy Commissioner, the Financial Markets Authority or other regulators may result in defence costs, fines and penalties. The new Privacy Act allows for class actions to be brought against a company in the event of a privacy breach. As discussed on page 15, the Privacy Commissioner issued a privacy compliance notice to RBNZ as a result of its recent cyber-attack.
- These losses could potentially lead to actions by shareholders against directors if they have not put effective cyber security in place.

The role of insurance

Cyber-attacks usually result in insurance claims. These can be complex, because they touch upon multiple aspects of insurance cover. Insurable losses may include the following:

- Extortion and the cost of paying ransoms.
- Event management costs – IT forensics and legal counsel are required to respond to technical and legal issues.
- Potential customer claims.
- Network interruption losses – business interruption loss of profit.
- Security and privacy – regulatory actions, defence costs and fines.

These losses may result in claims under the following types of insurance policy:

- Professional indemnity policies. These may provide cover for claims by customers and others who suffer loss as a result of negligence that fails to prevent a cyber-crime. Increasingly, however, professional indemnity policies exclude cyber losses.
- Cyber policies. These primarily provide cover for losses to the insured's own business and costs incurred in responding to the event, but they also usually provide some third party liability cover.

- Statutory liability policies. These may provide cover for fines, penalties and defence costs.
- Crime policies. These may provide cover for losses caused by cyber-crime.
- D&O insurance is potentially relevant if there is a possibility of claims against directors for failing to take the necessary protective steps.
- Business interruption policies do not normally provide useful cover, because the necessary element of physical damage is not present.

Cyber-attacks are increasingly expensive for the insurance industry, so insurers are asking detailed questions of insureds and they will not generally offer cyber risk insurance to organisations that do not have adequate cyber security systems. Even if insurers are prepared to offer cover, the price will depend on the security environment.

Insurers are looking particularly carefully at the following factors:

- Types of businesses and exposure to cyber-crime – whether they are likely to be a target. At-risk organisations hold customer data, have access to other parties' systems or data as part of the service they provide or are information conduits for service providers.



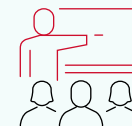
Organisations are now more exposed than ever because of the changing ways in which we work."

- Similarities in deficiencies and controls of prospective insureds' businesses to those of victims, to gauge when prospective insureds may be vulnerable.
- Capacity to insure in certain areas.

One advantage of cyber insurance is that it helps organisations to identify weaknesses in their systems and it encourages them to increase investment in security to reduce premiums. From a business perspective, the fact that an organisation has obtained cyber insurance may become a mark of quality of its existing security measures which may be a selling point for customers.

What should organisations' boards and managers do?

We recommend that boards and managers consider the following to guard against increased cyber risk:



- Be aware of their organisation's key information assets and the risks to those assets. A cyber risk dashboard should identify key risks to the organisation and what is done to mitigate them.
- Identify acceptable and unacceptable risks and plan resourcing accordingly.
- Demonstrate leadership, provide support and ensure that sufficient resources are made available to maintain and develop the necessary IT protections and provide sufficient ongoing training and testing to create a culture of cyber security.
- Ensure that reporting is non-technical and understandable, with necessary context such as trends, progress, a risk matrix and financial metrics
- Consider a progress dashboard, which may include criteria such as patching and vulnerability scanning, phishing simulation click failures by staff and cyber security training compliance. Consider asking questions about key risk mitigation strategies, which include patching (in particular how long it takes for patches to be applied), multi-factor authentication, backup strategy including protection of backups from ransomware and ease of access, and scanning for vulnerabilities.
- Ensure that a robust plan is in place to deal with incidents if they arise. Test the plan regularly.
- Consider all risks and ensure that adequate insurance is in place.

Directors and executives should also be alive to the prospect of representative (or "class") action proceedings. The risks discussed in this article commonly arise in businesses with large customer bases, many of whom could suffer loss as a result of a breach of duty or compliance failure. With the courts rapidly developing their own means of dealing with group litigation, and the Law Commission due to present recommendations about their management this year, we can only see the risk of these types of actions increasing in New Zealand. One standout feature is that any statutory regime ought to facilitate easier access to the court system by a greater number of prospective plaintiffs. This, in turn, ought to feed into directors' and executives' quantification and weighting when allocating resources to risk mitigation and elimination. In the past, risks like those discussed in this article might have been perceived as unlikely to result in material claims. With increased regulator oversight, and the likelihood of a more accessible route to combined claims, these risks deserve a greater focus.



Cartel criminalisation

Nine months ago, cartel misconduct became a criminal offence under New Zealand law. Whilst the first criminal cartel prosecution is yet to be taken, it is only a matter of time before the Commerce Commission elects criminal charges over civil ones for blatant cartel misconduct.

The adoption of cartel criminalisation was a 'game changer', and criminal law, and the processes and consequences it brings, means that:

- it is even more important to ensure that you have plans in place to prevent cartel misconduct occurring in your business;
- you should have criminal misconduct experts on hand, to assist you should allegations of misconduct be raised regarding your business; and
- this is an excellent opportunity to consider your broader organisational integrity risks, and what plans are in place to manage them.

A recap on the new law

For cartel conduct occurring after 8 April 2021, the Commerce Commission can elect to file civil or criminal proceedings against any organisation or individual alleged to have entered into, or given effect to, a cartel arrangement. The Commission has indicated that criminal cartel prosecutions are likely to be reserved for the most egregious breaches of the law, but significantly, that philosophy is enshrined in the Commission's enforcement policy rather than the law itself, and any intentional entry into an arrangement which contains a cartel prohibition is open to prosecution by the Commission as a criminal offence – it is not necessary for the actor to have known they were undertaking a criminal act.

Cartel criminalisation

Section 82B of the Commerce Act 1986 provides for imprisonment of up to seven years, or fines of up to \$500,000, or both, for individuals who engage in cartel misconduct. For organisations, the potential fine is up to \$10 million, three times the commercial gain from the illegal activity, or up to 10% of the turnover of the organisation involved, whichever is the greater.

Organisations or individuals engage in cartel misconduct if they enter into a contract or arrangement, or arrive at an understanding, that contains a cartel provision, or act to give effect to a cartel provision. A cartel provision is one which facilitates:

- price fixing;
- the restricting of output; or
- market allocation.

Because it is a criminal law prohibition, Parliament has adopted a requirement that the offender intend to engage in price fixing, restricting output, or market allocating, or intends to give effect to one of these things. However, it is important to note that this intention requirement does not require the offender to know that the effect of their actions is illegal, or that they undertake their actions with dishonest or fraudulent intent.

In addition to the usual criminal law defences, there are statutory defences available if the defendant held an honest and reasonable belief that their actions were reasonably necessary for:

- the purpose of a permitted collaborative activity;
- vertical supply contracts; or
- joint buying and promotion agreements.

However, these exemptions are not open-ended, and require certain conditions to be met.

Prevention is better than cure

It is essential not only to try and avoid misconduct occurring at the outset, but also as part of a forward-looking defence should misconduct occur. It is an important plank in being able to show that the organisation itself, and senior leaders (including directors), did not encourage, acquiesce, or aid misconduct committed by potential rogue employees. This is a critical part of a broader defence strategy should the business get caught up in cartel misconduct in any way.

Policies and procedures should be simple to understand, pragmatic and effective. They also need to involve training, and re-training, to ensure complacency doesn't creep in. Keeping records of the training undertaken is also an important part of an effective policy.

Since criminalisation was seriously mooted, we have seen New Zealand businesses take a more cautious approach in interactions with competitors. This includes using protocols for situations where an organisation's employees or officers are meeting with their counterparts in competitive organisations. Business or industry forums, commercial meetings (e.g. contracting, or merger or acquisition discussions), and the recognition that in a small market like New Zealand, general catch-ups and interactions will inevitably occur, driving the need for clear protocols alongside training and policies.

There is significant value added by using external counsel in the implementation of your policies (particularly training) in addition to drafting and advising. This approach allows subject matter expertise and sends a strong message regarding the seriousness with which this topic is being treated, particularly at more senior levels of your organisation.

A criminal prosecution is inevitable

The Commission's recent court action against Hutt and City Tax Limited highlights the risks for directors and senior managers in their personal capacity, as well as the risk to business, of engaging in cartel misconduct.



Avoiding misconduct is always better than tidying up the mess after it occurs. Accordingly, ensuring you have good and effective policies and training addressing the risk of cartel misconduct in place, and clearly setting out your organisation's expectations of how your team operate, is critical."

Although that case was taken in the Commission's civil jurisdiction (given the misconduct occurred in 2020), there is little doubt that the Commission would have considered criminal prosecution had this conduct qualified. Obtaining a penalty of \$150,000 against the business, the Commission's press release confirmed the deliberate nature of the breaches, and that directors were aware of the misconduct and approved it – a clear nod to party liability in the criminal context.

Cartel criminalisation

In the case of Hutt and City Taxis, the directors were issued formal warnings by the Commission. The Commission's referencing of the new criminal regime when announcing the outcome of the case sends a clear message that similar conduct is likely to be pursued criminally in the future.

In our view, it is only a matter of time before the Commission instigates criminal proceedings against a New Zealand corporate, and potentially also individuals, involved in cartel misconduct. The strong messaging around the Hutt and City Taxis directors also suggests the Commission will consider prosecutions of people in senior leadership or governance positions if they are aware of, and encourage or acquiesce to, the misconduct.

Criminal expertise is critical

With the increase in criminal regulatory restrictions affecting business, it is important that your team, and those advising you, have criminal law expertise alongside corporate legal knowledge. Criminal prosecutions proceed in a different manner than civil court proceedings, with different investigative powers applying, different court procedures (including the

possibility of a jury trial), and a higher burden of proof. These all impact on strategy.

The increased white-collar criminal and regulatory response to business misconduct provides an important platform for directors and senior leaders to pro-actively manage organisational integrity risk. We know that government investigations and prosecutions of organisational misconduct will increase. If you ensure your business is identifying, managing, and preparing to respond to this you are getting ahead of a curve that we know is coming.

For organisations already proactively managing regulatory and white-collar criminal risks, a cartel risk programme can form part of that broader risk management setup. For organisations yet to begin, it might provide an excellent place to start.



Have a response plan in place should any allegations arise

In addition to policies, training, and protocols, it is important to have in place a ready-to-go response plan if allegations of cartel misconduct arise in the business.

This should include:

- a 'dawn raid' response plan, setting out how your business will respond to the Commission or any government regulator executing a search warrant (including who will take responsibility for what tasks, and how you will contact and involve external counsel);
- a plan for how any allegations of misconduct made internally or received from an external (non-governmental) source will be investigated; and

- plans for how the business will respond to any inquiries by the regulator, including identifying who is responsible for liaising with the regulator, how external counsel will be notified and brought into the process, and what public statements will be made (if any).

Again, the use of external counsel as part of your response team is invaluable. Not only does this bring crucial objectivity and subject matter expertise, but work done advising you on your legal position and the appropriate strategy is likely to be protected by legal professional privilege, meaning you can safely explore issues without the risk of compromising your position with the regulator.



It's getting lonely at
the top: directors' risks

Ever increasing risks for directors and managers

Parliament is increasingly interested in imposing personal responsibility on directors and senior managers for ensuring that their entities comply with their legal obligations.



This trend started with the Health and Safety At Work Act 2015 under which directors are required to exercise due diligence to ensure that certain H&S requirements are met and that trend will continue this year with a raft of new changes to credit laws, climate-related disclosures and proposed changes to the obligations of directors of deposit takers. This increase in director obligations may stray beyond the health and safety and financial sector in coming years as personal liability becomes a common theme for Parliament to consider in proposing new legislation.

Proposed criminal sanctions for climate-related disclosure breaches by directors

As discussed on page 19, the Financial Sector (Climate-related Disclosures and Other Matters) Amendment Bill 2021 will, if passed, introduce a new requirement that would criminalise directors' conduct where an entity knowingly fails to comply with a climate reporting requirement. Under this proposed provision, a director of a climate reporting entity commits an offence if any of the following statements fail to comply with an applicable climate standard, and the

director knows they fail to comply when those are lodged:

- the climate statements of the entity prepared under section 461W;
- group climate statements in relation to a group comprising the entity and its subsidiaries prepared under section 461X;
- the climate statements or group climate statements prepared by the entity under section 461Y; or
- in the case of a manager of a registered scheme, the climate statements for any separate fund or for the scheme prepared under section 461Z.

A director who commits an offence under this proposed provision would be liable on conviction, in the case of an individual, to imprisonment for a term not exceeding five years, a fine not exceeding \$500,000, or both; and in any other case, to a fine not exceeding \$2.5 million.

Proposed new duties for directors of deposit takers

The Reserve Bank of New Zealand has been conducting a review of the Reserve Bank Act (2017 Review) which considered whether executive accountability should be increased. A new Deposit Takers Act has

been proposed, which will amongst other things impose a new duty on directors to ensure there are adequate systems, processes and policies in place so that the deposit taker complies with its prudential requirements and obligations. Whether the new Act should impose duties on senior managers was considered, however, it was ultimately decided that this would create an unduly intrusive supervisory model.

Unlike the current attestation regime which relies on an individual reporting where they believe the bank systems are non-compliant, the new Act will impose a positive duty on directors to ensure there are adequate systems, processes and policies in place so that the deposit taker complies with its prudential requirements and obligations. These duties would be applied through a 'positive accountability framework' where directors are required to take certain actions separate from the regulated entity, such as 'reasonable steps' to ensure the entity is run in a prudent manner.

A defence for a breach of this duty is available where a director can show they took reasonable steps to meet their obligations. However, directors would be permitted to take out personal insurance against penalties for such breaches.

Ever increasing risks for directors and managers

The new due diligence duty under the Credit Contracts and Consumer Finance Act (CCCFA)

The CCLAA introduces a new duty for directors and senior managers regarding compliance with the CCCFA. The aim of this change is to oblige and incentivise individual corporate officers to drive a culture of compliance with the CCCFA from the top down.

From 1 December 2021, every director and senior manager of a lender under a consumer credit contract (CCC) must exercise due diligence to ensure that the lender complies with its duties and obligations under the CCCFA. This duty will apply to obligations owed under contracts entered into on, or after, 1 December 2021 and may apply to contracts entered before 1 December 2021 where there are ongoing obligations under those contracts such as ongoing disclosure obligations.

This is an entirely new legal obligation and represents a substantial change to the law. It is also a personal obligation, meaning directors and senior managers will face personal liability for breaches.

What does the due diligence duty entail?

The exact parameters of the duty will vary from case to case. The test is an objective one. Broadly speaking, directors and senior managers must ensure the lender:

- has systems and procedures in place to ensure compliance with the CCCFA;
- requires its employees and agents to follow those procedures or ensures that the business has automated procedures in place that are designed to do that;
- undertakes reasonable checks on whether the procedures do what they are meant to and whether they are being used correctly;
- has methods in place to systematically identify problems with the effectiveness of its procedures; and
- promptly fixes any problems it discovers.

Importantly, directors and senior managers will not necessarily be found to have breached their due diligence duty just because the lender breaches the CCCFA. Directors and senior managers are likely to satisfy the duty by requiring management to undertake key tasks (to fulfil legislative and regulatory obligations), setting the approach to resource allocation and prioritisation, and driving a culture of compliance.

The duty also requires directors and senior managers to take prompt action where the lender has identified failures within systems and procedures. This may include setting clear requirements for reporting and timeframes for addressing and remediating non-compliance; ensuring the lender has a procedure in place to ensure that reporting is prompt and accurate; and ensuring the lender has appropriate systems to promptly remedy the deficiency and remediate affected customers.

If there is a breach of the due diligence duty, the court can order payment of pecuniary penalties of up to \$200,000. If, in addition to the breach of duty, the lender has breached the CCCFA, the relevant director or senior manager may face joint or several liability for statutory damages and compensation with the lender.

Directors and senior managers may not obtain indemnification from a body corporate or use insurance to indemnify themselves against penalties under the CCCFA or costs involved with defending civil proceedings in which penalties are imposed. Insurance can, however, be used to cover payment of statutory damages.

What does this mean?

Given the trend here, we anticipate that whenever new legislation is proposed that drafters will consider whether any personal liability should fall on directors, officers and senior managers. If this trend continues it could put undue pressure on finding qualified directors who are willing to take on the risks. As such, a balance should be struck with defences available for directors where reasonable steps to comply have been demonstrated.



The key question directors and senior managers should be asking themselves is:

Have I exercised the care, diligence and skill that a reasonable director or senior manager of a lender of the type and size of my business and with my role and responsibilities would have exercised?

Insurance risks for directors and officers

Developments in company director liability in New Zealand and Australia in the past three years have affected insurers' perceptions of the risks faced by directors and officers. This has resulted in difficulties in obtaining and renewing Directors and Officers or 'D&O' insurance cover.

What have D&O insurers been doing?

Many insurers have demanded substantially higher premiums, in some cases multiples of prior years' costs, even for reputable companies with good claims histories. At the same time, policy limits have reduced, exclusions from cover have been added and deductibles have increased.

Insurers are increasingly demanding more detailed information from insureds and have taken longer to provide quotes for cover and negotiate terms.

Insurers have also returned to what the industry refers to as "technical underwriting", in which premiums and other terms are set by reference to technical actuarial assessments of risk rather than influenced by an insurer's understanding of a client's business and its specific risks and confidence in its management.

Exclusions from cover have continued to increase in scope. Most recently, insurers have been introducing exclusions for cover for certain types of cyber incident. This is particularly the case for Lloyd's underwriters who have been obliged to report on their cyber risk coverage since the beginning of 2021. This has coincided to an extent with the growth of dedicated cyber insurance, although insurers, faced with increasing cyber claims, are also increasingly wary of writing cyber insurance as well. Insurers are also introducing insolvency exclusions for companies that appear less robust or that operate in challenging sectors, including those affected by the COVID-19 pandemic.

Listed companies and those about to list for the first time have seen the most significant challenges. Dual listed companies that appear on both the ASX and NZX have been particularly affected. Some, albeit for a range of reasons, have elected to de-list on one



of the exchanges. This reflects insurers' apprehension of the increased risk of claims against listed companies, which is driven primarily by the Australian experience of significant increases in the number and size of those claims in recent years. The New Zealand claims experience has been different but insurers – particularly foreign insurers – do not generally distinguish between the two markets.

Many companies have found their renewals in 2021 to have been less challenging than they were in the two previous years. This seems to reflect insurers' comfort with premium levels following the dramatic increases of the past two years, combined with a relatively normal claims experience of late. However, premiums continue to increase and restrictions upon policy coverage continue to expand.



Listed companies and those about to list for the first time have seen the most significant challenges with dual listed companies that appear on both the ASX and NZX having been particularly affected."

Insurance risks for directors and officers

Why has this been happening?

High value D&O cover is provided on a global scale, with primary cover often written in New Zealand but upper layers of cover written by Lloyd's of London or in other overseas markets. This means that New Zealand is viewed as one part of a global market and international developments, or regional factors such as increasing claims in Australia, influence the availability and terms of cover for New Zealand.

The risk environment for directors in New Zealand also continues to change. Increased numbers of representative actions or 'class actions' by investors globally and an increasingly aggressive regulatory environment locally mean that New Zealand is no longer viewed as a relatively benign environment for director risk.

In addition to the large concerns referred to above, insurers are also increasingly concerned about other types of claims, such as:

- cyber crime and cyber incidents;
- COVID-19 related losses and insolvencies;
- AML/CFT regulatory prosecutions;
- claims arising from large scale or systemic sexual or other personal abuse which an organisation failed to prevent;

- environment, Sustainability and Governance (ESG) obligations, including new reporting requirements; and
- insolvency claims.

Which companies are most affected?

Public listed companies have seen the most significant increases in premiums and reductions in cover, reflecting insurers' perceptions of their increased risk. However, the type of company and listing is important:

- companies that are listed only on the NZX have the widest appeal of any listed companies to insurers;
- insurers are more likely to consider companies that are listed on the NZX with foreign exempt status on the ASX, as for the most part they are entitled to comply only with relevant New Zealand rules;
- companies that are fully dual listed on the NZX and the ASX are seeing no or very limited capacity from insurers.

In all cases insurers are reducing the limits of cover they are offering, to reduce their exposure.



What can companies do to improve their renewals?

- Select and instruct an appropriate broker carefully.
- Engage early with insurers. The process is taking longer and more time may be required.
- Expect insurers to misunderstand your risk at first and that you will need to provide more information.
- Expect to be more open with insurers about what the company is doing.
- Provide information about company-specific risks and the risks facing the wider sector, including any mitigating factors. Insurers' willingness to write cover has become more considered and the perceived quality of the risk for the company and its sector plays an increasingly significant role.
- Expect lengthy and detailed questioning and demands to see procedures to reduce risk.
- Consider bringing senior executives in to speak directly to insurers so they may see the people who are responsible for corporate governance in action. Brief them well.
- Expect to explain why your risk is not the same as others and otherwise resolve insurer concerns. Consider using hard data and analytics. Legal help may be of value in explaining risk to insurers.
- Consider priorities for cover and where cover limits may be appropriately reduced or combined for risks that are unlikely to occur together.
- Expect to pay more and receive less. Do not expect to play insurers off against each other – it may work against you.



Risk checklist for directors and executives

Identify and assess risks

- Have we identified and assessed all material risks relevant to our organisation?
- Are we challenging each other and the executive team to consider new and developing risks?
- How do we keep abreast of regulatory changes, and developments in risk governance and management practices? Are there any gaps in our training, knowledge and understanding?
- Are we prioritising the most critical risks faced by our organisation? How often do we re-assess our prioritisation of risks?
- Are critical risks fully understood, and managed and monitored appropriately?
- How do our risks (e.g. conduct and culture, cyber, climate/environmental, regulatory, insurance, etc) intersect or interact? How does this inform our approach and strategy to risk management?
- Are risks currently within the tolerances and expectations set by the leadership team and the Board? Are there any organisational "blind spots" warranting attention?

Ensure you have a robust risk management infrastructure

- Do we have a robust risk management infrastructure (people, processes, and technology/systems) in place to identify, measure, evaluate and control risks?
- Do we have clearly defined roles, responsibilities and accountabilities for risk management activities?
- Do our performance and KPI frameworks reflect and appropriately incentivise risk management behaviour?
- Have we developed a consistent approach to risk management across our business?
- Have we decided what different levels of risk mean to our organisation (with reference to our risk appetite and risk tolerance) and what reporting and actions are required at each risk level?
- How does information on risk get escalated to the leadership team and board?
- Have we ensured that adequate insurance is in place?

Define and communicate your organisation's approach to risk management, and ensure risks are understood and properly resourced

- Have we defined and communicated our commitment and expectations regarding risk management (including our risk appetite and risk tolerances) to our organisation?
- Have we created an appropriate culture of risk awareness throughout the organisation? Is our risk culture encouraging the right behaviours?
- Is further training or guidance required for management and staff to carry out their individual roles and responsibilities for identifying, managing and escalating risks?
- Do risk committees and senior management have access to the people and resources they need to carry out their risk responsibilities?
- Have we invested properly in compliance systems and checks to ensure they are operating as they should?


Monitor risk outcomes and ensure adequate governance and oversight

- Do we continually monitor and assess risk management activities? Is there effective remediation of any areas of non-compliance on an on-going, enterprise-wide, and individual-entity basis?

- Is there adequate oversight of risks to ensure that the Board is aware of how risk management activities are being implemented across the organisation? Is the Board asking senior management the right questions to accurately monitor and assess the organisation's risk management activities?
- Do risk reporting processes provide management and the Board with the information they need about key risks and how they are managed?
- Does the Board have an enterprise-wide view of risk across the organisation to locate gaps in risk management or points of overlap between key risk functions?
- Has the Board incorporated key risk considerations in its overall business decision-making? Is risk appetite for key risks embedded in the organisation's business model, strategy and execution?
- Have we benchmarked our risk practices against other organisations who may be willing to share insights into their practices?

Continually reflect on and improve risk management activities

- Do we reflect on and review the effectiveness of our risk management strategy and activities? How often do we do so?
- Are we improving our risk management capabilities continuously to ensure we are managing our risks effectively in a changing business environment?



How will 2022 shape
up for employers and
employees?



Working with Covid

After living relatively COVID-19 free in the first half of 2021, the arrival of Delta prompted a swift return to stringent lockdowns for many parts of the country, as well as the reactivation of the Government's wage subsidy and business support payments. Although lockdowns have lifted, the recent arrival of the more infectious Omicron variant has prompted a return to the restrictive "Red" traffic light setting, at least for the near future.

Although Public Health Orders were introduced mandating vaccination among high-risk sectors such as border workers, healthcare, and education, the majority of employers were left to grapple with the health and safety, operational, business continuity, and litigation risks associated with COVID-19 and navigate a raft of new regulations addressing vaccination.

As the "elimination strategy" has eased, we have seen the introduction of vaccination certificates and a new COVID-19 Protection Framework. Organisations are now working through a matrix of further regulations and legislation, intended to simplify the health and safety risk assessment and assist employers in determining whether certain work needs to be performed by a vaccinated person.

Workforce planning and worker retention

Until our national border reopens without restriction, employers will continue to face fundamental challenges sourcing, recruiting and retaining talented workers. Faced with limited supply, strategies for the retention of skilled workers will be at the forefront of workforce planning for many organisations. Based on what we have seen in other countries, the arrival of Omicron variant is expected to cause significant disruption to business continuity, most notably a reduction in manning levels as workers recovering from Covid-19 or isolating as a close contact remain away from the workplace. Where viable, employers would do well to prepare by having additional staff on hand, or up-skilling existing workers in areas outside their usual tasks, in preparation for covering absent workers.

It is yet to be seen whether New Zealand will experience the “great resignation” seen in other geographies. Many young workers will have delayed OEs (Overseas Experiences), and with the eventual reopening of borders it is possible that some of these skilled workers will head offshore (although borders are, at this stage, unlikely to be open by March or April, which is the time that workers traditionally head to the northern hemisphere on their OE).

The challenges faced by employees working remotely during lockdown has reinforced the need for organisations to ensure their ways of working are sustainable and support wellbeing. In a climate of uncertainty, employers will remain competitive by enabling flexibility, protecting workers’ health and safety,



The challenges faced by employees working remotely during lockdowns has reinforced the need for organisations to ensure their ways of working are sustainable and support wellbeing.”

demonstrating adaptive leadership, rewarding good performance, and fostering a supportive workplace culture.

When our borders re-open we expect the existing ‘critical worker’ visa framework to be pared back significantly (if not wound up altogether) giving employers renewed access to migrant labour. A new ‘Accredited Employer Work Visa’ will also be introduced in July 2022, giving accredited employers greater access to skilled migrant labour.

COVID-19 related employment litigation

We predict a continued flow of COVID-19 and vaccination-related litigation. Some employees have successfully challenged unilateral reductions of wages during periods of partial or full closure due to COVID-19. However, to date proceedings brought by dismissed border workers challenging decisions made under Public Health Orders mandating vaccination have been unsuccessful. Employers who are proactively introducing vaccination policies on health and safety grounds (as opposed to the Health Orders) may well see these policies, and other decisions made by them, tested in the courts.

Once Omicron cases eventually subside and more employees return to shared workspaces, we may see more vaccinated employees expressing hesitancy to work proximate to unvaccinated colleagues or in locations where vaccination rates are not high. While not all workplace disputes will escalate to litigation, conflict and tension in the workplace can still cause significant disruption. We’ve already seen societal division regarding the vaccination roll-out and so we expect to see these differing views being expressed in the workplace.

The Ministry of Social Development has initiated legal action against employers who received (and have not repaid) wage subsidies but did not meet the requirements for accessing such payments. This scheme was “high trust” and relied on self-declared compliance with the subsidy’s criteria. Criminal charges have been laid against two individuals and we expect to see more employers come under scrutiny.

As it becomes increasingly common for employers to collect information about employees’ vaccination and health status, we expect to see an increase in privacy-related legal challenges. Employers are required to ensure personal information is protected from misuse and the Privacy Commissioner has a range of tools available

to enforce the legislative framework. We expect to see these powers being used in 2022 where employers have failed to meet their obligations.

Other areas of potential litigation

As the COVID-19 related restrictions reduce, we expect to see discussions about the Government’s proposed new system of Fair Pay Agreements recommence. The Government initially advised that draft legislation would be introduced in late 2021 and passed in 2022. It is likely those timelines will have been pushed out due to the interruptions caused by COVID-19.

Internationally we are seeing employment regulations (and indeed the definition of “employment” itself) being tested by platform workers engaged to provide transport and food delivery services. Typically, these workers are engaged as independent contractors, but many are challenging that classification on a class action basis to claim the protections of employment law. In New Zealand, challenges regarding worker status are currently assessed on a case by case basis, limiting the ability for groups of workers to bring a class action. We may see a push for legislative change to allow this issue to be litigated at a group or class action level.

Our litigation and dispute resolution team

Our national dispute resolution team has an outstanding track record for resolving the most challenging disputes, and providing clients with practical advice on the law and litigation strategies that enhance their prospects of success.

A large full-service team, we act on the most complex large-scale commercial and regulatory disputes in New Zealand. Our team leads the way in providing legal advice on a wide range of disputes in the commercial, insurance, insolvency, financial, consumer, regulatory, energy and environmental, public law and IT spaces, as well as in health and safety matters, litigation funding and class actions, and cross-border disputes.

Ranked Band 1 by The Legal 500 Asia Pacific, we have some of the country's most experienced and proactive litigators

Our aim is to help our clients avoid disputes wherever possible, which is why our team offers commercially astute advice to resolve matters at an early stage and guide you through mediation and arbitration if that is the right option. We are also right at home at all levels of the

court system including the High Court, Court of Appeal and Supreme Court.

Legal advice across borders and quick access to courts is no problem either, thanks to our international network through the MinterEllison Legal Group.



The team has a very good reputation for complex dispute resolution and litigation, with their litigators being outstanding; their responsiveness, analysis and effectiveness were all peerless"

Chambers Asia-Pacific 2021

