ADDISONS

Direct Selling Legal Update 2022

December 2022

Addisons delivers commercially-minded legal solutions that help drive the ongoing business success of our Australian and international clients.

addisons.com

Welcome to the December 2022 edition of the Addisons Direct Selling Legal Update.

2023 is almost here! In this edition of our Direct Selling Legal Update, we look at some of the legal issues which have been relevant to those operating in the direct selling sector in Australia in 2022. Issues which regularly come across our desks include **how best to manage a product recall, privacy and data protection requirements, as well as what claims may be made when conducting marketing campaigns.**

If you have any questions or would like to discuss or provide feedback, please reach out to any of Addisons' Direct Selling team.

Jamie Nettleton
Partner
+61 2 8915 1030
jamie.nettleton@addisons.com

Cate Sendall
Special Counsel
+61 2 8915 1028
cate.sendall@addisons.com

Arthur Davis
Partner
+61 2 8915 1045
arthur.david@addisons.com

ADDISONS

Table of Contents

ADDISONS

The Addisons Difference

Delivering bespoke legal solutions drives us every single day – and has done for over 140 years. Passionate and committed to ensuring your success, we excel in helping clients to achieve business outcomes with solutions underpinned by commercially-sound legal advice.

Building and nurturing relationships is in our DNA. Our immersion approach facilitates a detailed understanding of your business, culture and operations so we can support your commercial opportunities and help you navigate market challenges.

We're proud to be a diverse group of experts who work together to ensure all your needs are seamlessly managed. Our partners actively lead every engagement proudly supported by our lawyers to ensure you experience the ultimate levels of accountability and service.

Our commitment to sustainable and organic growth ensures we attract and retain like-minded individuals committed to the long-term needs of our clients.

Direct Selling Expertise

The Addisons team has been extensively involved in assisting the direct selling sector for many years. We have an intimate understanding of the business issues faced by the sector.

The Addisons team advises on the structure of global and Australian multi-level marketing and direct selling organisations in relation to their Australian operations, taking into account all applicable laws and their relationship with distributors and customers. We also assist on all aspects of marketing and advertising law in relation to product development, branding, packaging and promotion.

Our key areas of focus:

- Independent consultant agreements
- Compensation Plans and Policies and Procedures
- Pyramid selling issues
- Branding and trade mark strategies
- Pre-vetting creative concepts
- Website development and e-commerce issues
- Marketing and promotional materials
- Packaging and labelling
- Sponsorship, trade promotions and events
- Consumer protection issues
- Structuring and business establishment in Australia
- Data protection and privacy compliance
- Regulatory and compliance issues

Labor delivers on its promise of penalties for unfair contract terms

Authors: Renee Shipp and Lisa Csomore

It's time to dust off your standard form contracts because penalties for unfair terms in small business contracts have arrived and due to an expansion of the definition of "small business contract" the unfair contracts laws will apply to a much broader range of contracts than ever before.

Delivering on its election promise, Labor's proposed legislation to make unfair contract terms illegal was passed by Parliament in October this year and the Treasury Laws Amendment (More Competition, Better Prices) Act 2022 (Cth) (**Act**) was given royal assent on 9 November 2022.

What's new for unfair contracts?

Under existing laws, the worst-case scenario for an unfair term is that it is declared void. Following a strong push by the ACCC, the Act introduces civil penalties for unfair contract terms for the first time, which raises the stakes significantly for those with unfair terms in their standard form small business contracts.

Take a deep breath because each unfair term is a separate breach and could result in a penalty for companies equal to the greater of:

- $50 million;
- 3 x the value of the benefit of the unfair term; and
- 30% of the adjusted turnover in the breach turnover period (which is the period that is the longer of the 12 months leading up to the end of the breach and the period between the start and end of the breach).

In addition to these hefty new penalties, the Act significantly broadens the threshold for a "small business contract" with the effect that these laws will now apply to standard form contracts with businesses which have:

- less than 100 employees (as opposed to less than 20 employees currently); and/or
- an annual turnover of less than $10 million (as opposed to an upfront price less than $300,000 or, for contracts with a duration of more than 12 months, $1 million).

Courts will also have broader powers to make other orders to redress or prevent loss or damage caused by the unfair term on the application of a party to the contract or the ACCC.

When do these changes come into effect?

The good news is that businesses have an opportunity to get their house in order over the coming 12 months as the changes to the unfair contract laws will come into effect on 10 November 2023.

What other changes have been made?

As reported in our paper '50 million shades of pain – the new competition and consumer law penalties and the ACCC's updated priority areas', the Act also increases the maximum civil penalties for breaches of certain provisions of the Competition and Consumer Act 2010 (Cth) (**CCA**). It is important to note that, unlike the changes to the unfair contracts laws, the increased penalties for other CCA offences are already in effect.

What does this mean for businesses?

The ACCC has proven to be very active in pursuing businesses with unfair terms in their standard form contracts across an array of industries and has listed unfair contracts as one of its enforcement priorities. This has been the case even without the ACCC having the benefit of financial penalties in its armoury.

The grace period over the next 12 months provides businesses with a valuable opportunity to review their standard form contracts before the consequences of this regime increase in severity and scope.

Addisons' top ten tips for managing a product recall

Authors: Laura Hartley and Sarah Best

Manufacturers and suppliers of consumer goods need to have a clear understanding about how to best manage a product recall if a product safety issue comes to light.

Issues surrounding product safety have never been more important for manufacturers and suppliers, in an era where the ACCC is serious about protecting Australian consumers from unsafe products and class actions are on the rise. In a recent speech by the new ACCC Chair at the National Consumer Congress1, the ACCC launched its seven new product safety priorities for 2022-23. The priorities include a focus on safety issues relating to lithium-ion batteries as well as high risk issues affecting young children and strengthening product safety online[2].

Recalls are stressful, expensive, eat up precious management time and can have enormous effects on reputation. Invest in developing a recall action plan now so you are ready in a crisis.

Addisons' top ten recall tips

1. **Have a recall plan in place now**

The plan should be tailored to your business. It should set out the steps you need to take if a product safety issue arises and identify the team from across your business and trusted external advisors who will help you manage the issue.

Create a plan today to help save you time, stress and money at the time of a recall.

2. **Take out recall insurance**

A recall is expensive and can take some time to resolve, so make sure you are protected. Do this now!

3. **Notify your insurer**

If a product safety issue arises, notify your insurer immediately.

4. **If death, illness or injury has occurred, notify the ACCC**

If the consumer good which you've supplied has resulted in death, illness or serious injury, notify the ACCC within 2 days of becoming aware of the situation. Failure to provide the notice is an offence and a pecuniary penalty may apply.

5. **Always conduct a speedy but comprehensive risk assessment so you can make an informed decision about the need for a recall**

You may need to undertake technical tests to determine the root cause of the fault. You should check customer call logs and determine whether there are any reports of injuries, issues or complaints with this or any product you sell that is similar to it. Under the *Australian Consumer Law* (**ACL**), where a "*consumer*

good" has been identified as posing a safety risk to consumers, the supplier of that product **must** initiate a recall of that product. A product will be considered likely to pose a safety risk to consumers include instances where:

- the product will or may cause injury to a person; and/or
- a reasonably foreseeable use (including a misuse) of the product will or may cause injury to a person.

6. **Develop a comprehensive corrective and preventative action plan (CAPA)**

Develop a CAPA once you have determined that there is an issue with the consumer good you sell so the issue does not occur again. This will be a very important document to determine the effectiveness of your recall.

7. **Quarantine the recalled goods and communicate to customers and consumers**

Once you make the decision that you need to commence a recall, you will need to do the following asap:

- Stop your product going to market by quarantining the product in your distribution centres.
- Advise your trade customers/resellers about the recall and get them to quarantine any product on hand.
- Get a PR agent on board to help you navigate the reputational aspects of a recall.
- Prepare a consumer communications strategy to effectively publicise the recall to those consumers who are likely to have purchased your product and are affected by the recall. Traditional print ads in State and Territory newspapers are still generally required by the ACCC, although publicity by way of website banner ads, pages or microsites and your socials are also very common these days.
- Think about any specific disposal or destruction requirements that may apply to your product to ensure environmental and other laws are complied with.
- Set up a process for verifying claims for refunds and the processing of refunds to consumers within a reasonable period of time.

If the consumer good you sell is a type of good governed by specific legislation (e.g. food, therapeutic goods, electrical goods), you will need to take account the special requirements of those laws too.

8. **Notify the ACCC of the recall**

Within two days of commencing the recall, notify the ACCC by submitting an online recall form. There is a penalty for failing to do so.

If a product is a specific type of good governed by specific laws, and not just a general merchandise or a "***consumer good***", your regulator may not be the ACCC – i.e. the Therapeutic Goods Administration

governs therapeutic goods and Food Standards Australia New Zealand governs food. Check the appropriate regulator before starting any recall as their requirements and processes may differ.

9. **Notify your export customers about the recall**

If you have exported your product outside Australia, provide a copy of this notice to the Commonwealth Minister/ACCC within ten days.

10. **Keep good records of your recall**

Such as how many trade customers and consumers have responded, what has happened to the products you have onsite, in storage, with any reseller etc, the root cause of the safety issue, your proposed CAPA etc. This information will be needed for the regular progress reports that you must give the ACCC to allow them to monitor the effectiveness of your recall.

The ACCC will generally only close-out a recall if it's satisfied your recall has been effective – usually when the numbers of people returning your product stabilises and the ACCC considers those numbers reflect a good response/return rate given the risks involved. You'll then be told that you no longer need to file reports.

Cheat Sheet for Businesses: How to Manage Online Reviews in Compliance with the Australian Consumer Law

Authors: Laura Hartley and Rachel White

Customer reviews can be a great way to establish your brand credibility. But do you know how to manage the legal risks associated with soliciting and publishing those reviews online?

In October 2022, the ACCC commenced a "sweep" of online reviews and testimonials across a range of business websites, Facebook pages, and third-party review platforms. At least 100 businesses will be covered in the sweep, which will target popular sectors such as household appliances, electronics, fashion, beauty products, food and restaurants, travel services, sport, home improvement, kitchenware, health products, as well as furniture and bedding.

According to then ACCC Deputy Chair, Delia Rickard, the regulator is "***looking to identify businesses, review platforms or sectors where there is a pattern of misleading online reviews and testimonials that have the potential to cause significant consumer or small business harm***".

This will form part of a series of internet sweeps by the ACCC focusing on misleading practices in the digital economy. Also in October 2022, the ACCC commenced a sweep of "greenwashing" claims across at least 200 company websites. Once these sweeps are concluded, next in the firing line will be social media influencers who fail to clearly disclose advertising or sponsorship arrangements.

The ACCC has warned that the sweeps will be followed up with compliance, education, and potential enforcement activities.

What does this mean for you?

The obligations under the *Australian Consumer Law* in respect of misleading and deceptive conduct apply to online advertising the same way they do to other types of advertising. That means you can't make any false or misleading claims and all claims in your online reviews need to be capable of substantiation.

Below are some quick tips to help you and your team navigate the different stages of preparing a customer review marketing strategy.

Stage 1: How to solicit reviews

- **No fake reviews**: A number of businesses have landed themselves in hot water in the past by posing as "genuine customers" and posting reviews about their own products or services or, in some cases, even a competitor's products or services. Reviews should only ever be posted by genuine consumers who have used the product or service. The reviews must also accurately reflect the consumers' independently held opinions. In July 2020, an online tasking platform, Service Seeking, was fined $600,000 in relation to its "Fast Feedback" feature. This feature allowed businesses which advertised their services on the platform to rate and review themselves after completing each job, thereby creating a false impression about the number of favourable reviews and star ratings which those businesses had received from actual consumers.

- **No strings attached**: If you are planning on providing incentives to reviewers in return for their reviews, then you need to make clear upfront that all reviewers will be entitled to receive an incentive regardless of whether they provide you with a positive or negative review. You then also need to follow through with that promise by delivering those incentives to all of your reviewers.

- **Everybody gets a say**: You cannot selectively solicit reviews by only offering the opportunity to review your product or service to individuals whom you believe will provide you with positive reviews. The Federal Court issued a $3 million fine to serviced apartments accommodation provider Meriton in July 2018 for "masking" email addresses of unhappy guests. This prevented guests whom Meriton suspected would provide negative reviews from receiving a follow-up prompt email from TripAdvisor to provide feedback on their experience.

- **Prepare and maintain a substantiation dossier**: When it comes to making any kind of marketing claims, substantiation is always key. Wherever possible, we recommend getting a written acknowledgment from each of your reviewers confirming that they have in fact used your product or service and that the review which they have provided reflects their genuine and independently held views about the product or service.

Stage 2: How to publish and monitor reviews

- **Think twice before republishing**: In certain circumstances, you can be held liable for claims made in customer testimonials which are false or misleading – even if they are genuine customer testimonials. This applies to all testimonials which are "republished" by your business either on your website or Facebook page or any other online forum over which your business has reasonable control (e.g. a sponsored article). This means that if a customer believes and states that your product or service provided them or their family member with a particular benefit for which you have no substantiation (e.g. "*This air purifier stopped my family from getting sick this winter*"), then you should not republish that review – no matter how flattering it may be. If the customer has already published the review (e.g. by leaving a comment on your Facebook page), then you need to take steps to remove that review or respond publicly in order to correct the review (e.g. by posting a reply to the comment on your Facebook page). The golden rule to apply is: *If you cannot make a particular claim about your product or service because you know that it is false or misleading or cannot be substantiated, then you cannot simply sit back and allow someone else to say it in a customer review.*

- **Be transparent about incentives**: If you have provided your reviewers with an incentive in return for their review (e.g. freebies or a gift voucher), then you need to clearly disclose that upfront in connection with the customer's review.

- **No cherry picking**: You cannot selectively remove or edit any negative (but genuine) customer reviews which have been published on your website or Facebook page or a third party review website in order to try to create a better impression of how your product or service is viewed by the public.

[1] ACCC product safety priorities announced at National Consumer Congress | ACCC

[2] See 2022-23 Product Safety Priorities (accc.gov.au)

Privacy Act amended to increase penalties significantly for data breaches

Authors: Donna Short, Cate Sendall, Michiel Brodie

On 12 December 2022, legislation substantially increasing the penalties in the Privacy Act 1988 received Royal Assent. The amendments significantly increase penalties for interferences with a person's privacy and expand the powers of the Australian Information Commissioner (**Commissioner**).

Higher Penalties

The previous maximum penalty in the Privacy Act 1988 (Cth) (**Privacy Act**) for a breach of, for example, section 13G (serious interference with privacy) was 2000 penalty units[1] for individuals or 10,000 penalty units for a corporation which means the maximum fine available per offence committed by a corporation could have been as much as $2.2 million.

The amendments to the Privacy Act have increased penalties substantially and incorporate the contemporary approach to setting penalties for corporations that takes account of the commercial benefit which may have been obtained from a breach of law. Now penalties will be the greater of:

- $50 million;
- three times the value of any benefit obtained through the misuse of information; and
- 30 per cent of a company's adjusted turnover in the relevant period.

These penalties are similar to the structure of civil penalties that exist in the Corporations Act.

In respect of the 30 per cent of adjusted turnover provision, the Court making a penalty judgement, may determine the adjusted turnover based on the full period of the contravention or the earlier of 12 months up to when the conduct ceased or proceedings in relation to the contravention were instituted.

Enhanced powers for the Information Commissioner

The Commissioner's enforcement powers have been enhanced, including by:

- expanding the types of declarations that the Commissioner can make in a determination at the conclusion of an investigation
- amending the extraterritorial jurisdiction of the Privacy Act to ensure foreign organisations that carry on a business in Australia must meet the obligations under the Privacy Act, even if they do not collect or hold Australians' information directly from a source in Australia
- providing the Commissioner with new powers to conduct privacy assessments
- providing the Commissioner with new infringement notice powers to penalise entities for failing to provide information without the need to engage in protracted litigation, and

- strengthening the Notifiable Data Breaches scheme to ensure the Commissioner has comprehensive knowledge of the information compromised in an eligible data breach to independently assess the particular risk of harm to individuals.

Improved Information Sharing

The Commissioner's ability to share information has been enhanced by:

- clarifying that the Commissioner is able to share information gathered through the Commissioner's various functions
- providing the Commissioner with the power to disclose information or documents to an enforcement body, an alternative complaint body, and a State, Territory or foreign privacy regulator for the purpose of the Commissioner or the receiving body exercising their powers, functions or duties
- providing the Commissioner with greater power to publish determinations and other materials acquired during the course of an investigation or assessment, if the Commissioner determines that such a release is in the public interest.

The Australian Communications and Media Authority Act 2005 (Cth) has also been amended to expand ACMA's ability to share information to any non-corporate Commonwealth entity where the information will enable or assist the entity to perform or exercise any of its functions or powers.

Implications

The new penalty provisions significantly expand the financial penalties associated with a serious interference with privacy, but have not changed the tests associated with whether an offence under section 13 or section 13G of the Privacy Act, has occurred.

The increased penalties and the recent cyber incidents experienced by Optus and Medibank, highlight the importance of cyber security teams and privacy teams working together to reduce the risk of unauthorised access but also to assess and reduce the volume of data at risk if systems are compromised.

Privacy teams, at this time, should be looking very hard at their data governance approach especially their policy settings related to data retention and destruction. The cyber incidents, in particular, bring into sharp focus the trade offs between deep customer data pools and the costs of losing control of that data.

[1] A penalty unit is determined by the Crimes Act 1914 (Cth) and was increased in May 20202 to $222.

ACMA issues record $2.5 million penalty to an Australian business for Spam Act breaches and requires business to issue refunds of approximately $1.2 million

Authors: Jamie Nettleton and Cate Sendall

Earlier this year, the Australian Communications and Media Authority (**ACMA**) issued a record penalty of $2.5 million to Sportsbet for breaches of Australia's *Spam Act 2003*.

This amount is the largest infringement notice penalty issued by ACMA. Further, Sportsbet is required to issue customer refunds which will total approximately $1.2 million for money lost on bets associated with the spam messages.

This enforcement action is a timely reminder to all direct selling companies to ensure that their electronic direct marketing processes and the messages themselves comply fully with the *Spam Act*.

Background

Between January 2020 and March 2021, Sportsbet sent marketing texts and emails to consumers which included:

- incentives to place bets; and
- upcoming race alerts.

In an investigation conducted by ACMA, Sportsbet was found to have sent more than 150,000 text and email marketing messages to more than 37,000 consumers. Some of these customers had tried to unsubscribe from marketing campaigns but were not removed from marketing lists. Further, more than 3,000 marketing messages were sent without an unsubscribe function.

In addition to the payment of the $2.5 million penalty, Sportsbet has provided a three-year court-enforceable undertaking which requires it to:

- implement a compensation program to refund those customers who lost bets made in connection with the spam messages. The amount of refunds is estimated to be about $1.2 million; and
- review its policies, systems and training, with the review to be conducted by an independent consultant.

Does your business keep records of marketing consents?

The Spam Act requires that any electronic marketing messages are sent only with the recipient's consent. Consent may be:

- express consent e.g. where a recipient ticks a box to subscribe to a newsletter or fills in a form; or

- implied consent e.g. where a person has an ongoing relationship with the business (which can be verified) and the marketing messages relate directly to the relationship (such as where the recipient has subscribed to a service and the relevant marketing message relates to the service).

It is important to keep a record of how and when a person provides their consent. Should your business be the subject of an ACMA investigation, details of records of consent may be requested by ACMA. Would your business be in a position to provide records of this nature?

Do your marketing messages comply with the unsubscribe requirements?

Electronic marketing messages must contain an unsubscribe option which is functional for at least 30 days after the message is sent. Unsubscribe instructions must be presented clearly. Exercising the unsubscribe option must not require the payment of a fee and cost no more than the usual cost of exercising the option (for example a standard text charge if texting STOP to op-out). Any unsubscribe requests must be actioned within 5 working days. Do your marketing messages comply with these requirements?

An expensive cautionary tale

Sending marketing materials without a recipient's consent, or to someone who has unsubscribed, breaches the Spam Act. All direct selling business are strongly recommended to review their marketing programs and systems to ensure that they comply fully with their obligations under the Spam Act and, if they are a member of Direct Selling Australia (DSA), their obligations under DSA's Code of Practice which apply to their marketing activities.

Electronic marketing messages must not be sent to recipients who have not provided consent or who have unsubscribed.

Getting it wrong can be very costly!

Industry Jury puts BabyLove in a Corner With its "Chance to Win $1 Million" Promotion

Authors: Laura Hartley and Lisa Csomore

The Ad Standards Industry Jury (**Industry Jury**) has determined its first case in relation to the promotion of a game of chance, finding the advertisements complained about were misleading and deceptive in breach of the *Australian Consumer Law* and the advertising industry's self-regulatory code.

On 8 August 2022, the Industry Jury upheld a complaint filed with it by Kimberly-Clark Australia Pty Ltd against Unicharm Australasia Pty Ltd. It held that Unicharm had made a number of misleading or deceptive representations in its "BabyLove Chance to Win $1 Million Dollars" promotion (**Promotion**) in breach of the Australian Association of National Advertisers' (**AANA**) Code of Ethics and the *Australian Consumer Law*.

This decision highlights that significant limitations to the "chance to win" mechanic in trade promotions must be clearly and prominently disclosed in all advertising for these promotions to avoid being misleading and deceptive.

AANA Code of Ethics and role of the Industry Jury

As mentioned in our previous paper 'Brand owners and advertisers beware! New influencer marketing guidelines in the spotlight', the Code of Ethics (**Code**) adopted by the AANA, the advertising industry's self-regulatory body, provides a mechanism for competitor vs competitor complaints to be heard in relation to advertising and marketing which breaches laws, including the *Australian Consumer Law*.

The Industry Jury's decision

On 19 April 2022, Kimberly-Clark lodged its complaint against Unicharm. The complaint centered around the headline claim (**Representation**):

"Buy BabyLove for your chance to Win $1 Million*

The Representation was made on Unicharm's BabyLove Nappies' website, in retail stores and on social media (**Promotional Materials**).

Towards the bottom, or at the bottom, of each item of Promotional Material there was a reference in smaller font as follows:

Ts and Cs apply"

In all cases, the copy surrounding the headline claim provided a link to the full terms and conditions of the Promotion.

The complainant alleged Unicharm had made two representations in the Promotional Material which were misleading or deceptive:

- the "**Eligibility Representation**" which conveyed that all a prospective entrant was required to do was to register their purchase of an eligible BabyLove product and provide proof of purchase to be in with a "chance" of being selected from all the other eligible entrants to win the $1 million prize, when in fact once the entrant had been selected by chance from all other eligible entrants, they had to randomly select from 100 envelopes, the one envelope that contained the $1 million prize; and

- the "**Prize Winning Representation**" which created the impression that one of the eligible entrants who entered the draw would in fact win the $1 million prize, when in fact there was a 99% chance that no eligible entrant would win the $1 million prize.

The Industry Jury agreed with the complainant by determining that both the Eligibility Representation and Prize Winning Representation were misleading or deceptive, or likely to mislead or deceive, in breach of section 18 of the Australian Consumer Law and sections 1.1 and 1.2 of the Code.

Providing full T&Cs aren't enough: the importance of prominent and clear qualifying statements

The Industry Jury rejected as an insufficient Unicharm's submission that the full details of the entry instructions, prizes and the additional step of having to select the winning envelope out of a possible 100 envelopes were clearly set out in the full terms and conditions for the Promotion and that these full terms were referred to in the Promotional Material and readily available to entrants. The Industry Jury stated that the Promotional Materials did not, and should have, made clear that the chance to win the $1 million prize was effectively a chance to win a further chance to win the $1 million prize.

Unicharm submitted that the ordinary or reasonable prospective entrant would have read the full terms and conditions of the Promotion. The Industry Jury rejected this submission too as despite the requirement that the entrant check the "I agree to the Terms and Conditions" box on the entry form for the Promotion, the Industry Jury held that the "ordinary" prospective entrant would not necessarily be "savvy" to various promotional activities and the importance of reading the full terms and conditions of trade promotions. Although some members of the target audience would know the importance of reading the full terms and conditions, some would not.

Conduct of other competitors is not an excuse

Unicharm also attempted to justify that the Promotional Materials were not misleading on the basis that "a chance to win a million" promotion is a common type of promotion and provided examples of other similar promotions. The Industry Jury rejected this, noting that problematic claims run by other advertisers would not absolve the Promotional Materials from being misleading or deceiving.

The Industry Jury's decision is a reminder to businesses and advertisers that, just because everyone is doing it, doesn't mean it's right.

Key takeaways

Advertisers and businesses should keep the following in mind when putting together their next trade promotion that:

- When advertising a trade promotion, be clear and upfront about the rules of the promotion, including all entry requirements and how winners are selected.
- Don’t think you can rely on consumers to read the full terms and conditions.
- If there are any material qualifications to chances to win the promotion, call them out in all promotional materials.
- Don’t rely on what your competitors may be doing to guide how you run your marketing.

The price of poor password protection: ASIC makes an example out of first cybersecurity lawsuit

Authors: Robert Kerr, Donna Short, Cate Sendall and Donna Kwon

On 5 May 2022, the Federal Court handed down its judgment in *Australian Securities and Investments Commission v RI Advice Group Pty Ltd [2022] FCA 496.*

We previously reported on ASIC's commencement of its proceedings against RI Advice Group Pty Ltd (RI), an Australian Financial Services Licence (AFSL) holder, in our paper titled '"Getting away with it" not enough as ASIC's first cybersecurity lawsuit focuses on systems, not outcomes.'. This is the first time ASIC has ever exercised its enforcement powers for failure to have adequate cybersecurity and cyber resilience systems.

Settlement

This matter was settled between ASIC and RI prior to the commencement of the final Federal Court hearing. Justice Rofe received proposed declarations and orders to be made by consent and an agreed statement of facts, in which RI admits to having breached sections 912A(1)(a) and (h) of the Corporations Act.

Judgement

Pursuant to the settlement, Justice Rofe made the following declarations and orders:

1. **Declaration of contravention**: that as a result of its failures to have documentation and controls in place to adequately manage cyber risk across its authorised representative (AR) network, RI breached sections 912A(1)(a) (failure to do all things necessary to ensure the financial services covered by its licence were provided efficiently and fairly[1]) and 912A(1)(h) (failure to have adequate risk management systems) of the Corporations Act.

2. **Order (cybersecurity expert)**: that RI must engage a cybersecurity expert to identify and implement any further measures necessary to adequately manage cybersecurity risks across RI's AR network.

3. **Order (costs)**: that RI pay $750,000 towards ASIC's costs.

Interestingly, although ASIC had initially sought that RI pay a pecuniary penalty, neither the settlement nor the judgment imposes one against RI.

Takeaways

- The general obligations of an AFSL-holder under section 912A of the Corporations Act apply to management of cyber risks.

"As a public regulator, it is in the interests of ASIC to seek the declarations concerning the application of s 912A(1), particularly in circumstances such as the present case, where the declarations may clarify to licensees that the relevant provisions of the Act also apply to the area of the management of risks in respect of cybersecurity."

- A failure to adequately manage cyber risks constitutes a breach of AFSL obligations. Justice Rofe emphasised the importance of cybersecurity for AFSL holders:

"Cybersecurity risk forms a significant risk connected with the conduct of the business and provision of financial services. It is not possible to reduce cybersecurity risk to zero, but it is possible to materially reduce cybersecurity risk through adequate cybersecurity documentation and controls to an acceptable level."[2]

- Whether there are "adequate" risk management systems in place in the context of cyber risk management is ultimately a question for the court, considering the risks faced by a business in respect of its operations and IT environment and informed by technical expert evidence.

Final thoughts

- Assuming ASIC considers this a "win", will this outcome encourage ASIC to undertake a program of similar litigation? Time will tell, but it seems quite likely. Given ASIC 'strongly encourages all entities to follow the advice of the Australian Cyber Security Centre and adopt an enhanced cybersecurity position to improve cyber resilience'[3], it also seems likely that ASIC's focus will expand to non-AFSL holders.

- We're still left wondering whether ASIC will also focus on enforcement action against individual directors for breaching their directors' duties in relation to cyber risks. We think this is likely, particularly with ASIC's Chair Joe Longo recently confirming that "Boards play a key role in recognising and managing risk, including cyber risk. They should consider where they have an obligation to report breaches to ASIC, and where it may be appropriate to make disclosure to the market as either continuous disclosure or in financial reports."[4]

What should you do?

Regardless of whether you are an AFSL holder or not, you should ensure your organisation:

- has policies, procedures, frameworks, systems, resources and controls in place which are reasonably appropriate to adequately manage risk in respect of cybersecurity and cyber resilience;

- regularly undertakes cybersecurity and cyber resilience risk assessments given 'risks relating to cybersecurity and the controls that can be deployed to address such risks evolve over time'[5]; and

- if a cybersecurity incident occurs, is able to quickly, appropriately and adequately respond to the incident.

[1] Although the statutory general obligations under section 912A(1)(a) cover providing financial services "efficiently, honestly and fairly", it was never contested, and ASIC never alleged that RI failed to act "honestly" with respect to cyber risk and security and resilience measures for its AR practices.

[2] Australian Securities and Investments Commission v RI Advice Group Pty Ltd [2022] FCA 496, [58]

[3] https://asic.gov.au/about-asic/news-centre/find-a-media-release/2022-releases/22-104mr-court-finds-ri-advice-failed-to-adequately-manage-cybersecurity-risks/

[4] https://asic.gov.au/about-asic/news-centre/speeches/asic-s-corporate-governance-priorities-and-the-year-ahead/

[5] Australian Securities and Investments Commission v RI Advice Group Pty Ltd [2022] FCA 496, [58]

Level 12, 60 Carrington Street
Sydney NSW 2000 Australia

ABN 55 365 334 124
Telephone +61 2 8915 1000

mail@addisons.com
www.addisons.com