LexisNexis

Financial Services Newsletter

2021 . Vol 20 No 5

Contents

Information contained in this newsletter is current as at July 2021

LexisNexis Butterworths

General Editor's note

Karen Lee *LEGAL KNOW-HOW*

Financial services licensees and credit licensees will be familiar with the requirements relating to responsible managers. Responsible managers are the people a licensee relies on for its organisational competence. In the past year, ASIC has increasingly held responsible managers accountable for a licensee's failure to comply with its license conditions and compliance obligations. In their article "ASIC singling out irresponsible managers", editorial board members **Andrea Beatty**, **Chelsea Payne and Shannon Hatheier** (Piper Alderman) explore the role and purpose of responsible managers in ASIC's regulatory regime and consider why and how the increased enforcement action should prompt responsible managers to consider their duties.

People sometimes sell financial products they do not own with a view to repurchasing them later at a lower price. This is known as "short selling". "Activist short selling" involves a person taking a short position in a financial product, then publicly disseminating information directly or through an agent to negatively impact the price of the product. ASIC has now released long-awaited guidance on its regulatory stance on activist short-sellers. In his article "New guidance for activist short sellers and target boards", editorial board member **Fadi Khoury** (Corrs Chambers Westgarth) takes a look at what is considered better practice for activist short sellers, target entities, as well as market operators.

In May 2021, Fitch Ratings reported that "[r]ansomware attacks increased 485% in 2020 globally, according to Bitfdefender, accounting for nearly one-quarter of all cyber incidents, with total global costs estimated at $20 billion, per Cybersecurity Ventures".[1]

While ransomware attacks are certainly concerning for financial services lawyers and their clients, there are things we can do to mitigate the risks. In his article "Ransomware attacks: prevention and protection guide for financial services lawyers", **Frank Downes** (Juris IT Services) shares with us some practical tips, with actionable items set out in a handy checklist.

I hope you enjoy reading the articles in this issue of the *Financial Services Newsletter*.

Karen Lee
Principal
Legal Know-How
karen.lee@LegalKnowHow.com.au

Karen Lee is the General Editor of the Australian Banking & Finance Law Bulletin and the Financial Services Newsletter. She also partners with LexisNexis in other capacities, including as Specialist Editor for precedents in banking and finance, mortgages and options, and as contributing author of a number of other publications, including Australian Corporation Finance Law, Halsbury's Laws of Australia and Practical Guidance General Counsel. Karen established her legal consulting practice, Legal Know-How, in 2012. She provides expert advice to firms and businesses on risk management, legal and business process improvement, legal documentation, regulatory compliance and knowledge management. Prior to this, Karen worked extensively in-house, including as Head of Legal for a leading Australasian non-bank lender, as well as in top-tier private practice, including as Counsel at Allen & Overy and Clayton Utz.

Footnotes

1. Fitch Ratings, Ransomware Attacks a Growing Global Security and Financial Threat, 17 May 2021, www.fitchratings.com/research/insurance/ransomware-attacks-growing-global-security-financial-threat-17-05-2021.

ASIC singling out irresponsible managers

***Andrea Beatty**, **Chelsea Payne** and **Shannon Hatheier** PIPER ALDERMAN*

Over the past 12 months, the Australian Securities and Investments Commission (ASIC) had increasingly held Responsible Managers accountable for the licence holders' failure to comply with its license conditions and compliance obligations. This is in contrast to the fact that during the Royal Commission into Misconduct in the Banking, Superannuation and Financial Services Industry, the roles of Responsible Managers were largely overlooked.

This article seeks to explore the role and purpose of Responsible Managers in ASIC's regulatory regime and how the increased enforcement action should prompt Responsible Managers to consider their duties under their licence.

Responsible Managers

Responsible Managers are a construct created by ASIC for the purpose of licensees demonstrating their competence to provide financial services or credit under their Australian Financial Services Licence (AFSL) or Australian Credit Licence (ACL). Responsible Managers are not mentioned at all within the legislation; they are instead created by guidance in Regulatory Guide 105 AFS Licensing: Organisation competence[1] (RG 105) and Regulatory Guide 206: Credit licensing: Competence and training[2] (RG 206).

Prescribed by s 912A of the Corporations Act 2001 (Cth), AFSL holders are required to, amongst other obligations, "maintain the competence to provide . . . financial services."[3] Similarly, s 47 of the National Consumer Credit Protections Act 2009 (Cth) requires ACL holders to comply with a host of general licence obligations. Accordingly, RG 105 and RG 206 clarify that ASIC considers having people with appropriate knowledge and skills who manage the financial services or credit business as a means of demonstrating such competence.

Enforcement action

ASIC's increased scrutiny of Responsible Managers has led the regulatory body to engage its powers under statute to enforce banning orders and disqualify Responsible Managers from partaking in the provision of financial services or engaging in credit activities. In most instances, the offending conduct was a consequence of the Responsible Manager engaging in unlawful conduct in respect of an ancillary role within the company. As a result, enforcement action has primarily been taken against Responsible Managers in smaller firms within which the Responsible Manager is often a director or a member of senior management who is subject to complementary legal obligations and duties.

Examples

John Carlton Martin, director and former Responsible Manager of Union Standard Group Pty Ltd was banned from providing financial services for 10 years as of 1 June 2021. ASIC found that Mr Martin was involved in Union Standard's failure to do all things necessary to ensure that it provided financial services efficiently, honestly and fairly and take reasonable steps to ensure that its representative complied with financial services laws. Specifically, Mr Martin failed to address misconduct when alerted to instances of representatives providing personal advice to clients when not licensed to do so and making representations to clients that were likely to be misleading. The financial products issued by Union Standard were high-risk products, comprised of potentially difficult-to-understand features. Accordingly, Mr Martin owed a heightened duty to ensure compliance, especially when corporate authorised representatives were located overseas. ASIC concluded that Mr Martin's complete lack of understanding or regard for compliance was so serious that it justified the making of a significant banning order.

Anthony David Wynd, former Responsible Manager and sole director of Financial Circle Pty Ltd, was permanently banned by ASIC on 4 September 2020 and upheld by the Administrative Appeals Tribunal (AAT) from performing any function involved in the engaging of credit activities. The AAT found that Financial Circle's business activities constituted egregious breaches of minimum standards required under both the financial services and credit legislation. It was concluded that Mr Wynd's involvement and lack of oversight in respect of Financial Circle's flawed business model was so troubling as to justify a permanent banning order. The decision of the AAT followed an application by Mr Wynd in August 2019 for a review of ASIC's decision to cancel Financial Circle's Australian financial services licence and permanently ban Mr Wynd from engaging in credit

activities. In upholding ASIC's decision, the AAT nevertheless found that Mr Wynd was not the sole architect of Financial Circle's offending conduct and should therefore be allowed to be employed by an authorised deposit-taking institution and assist borrowers to obtain loans independent of financial services.

Maximum penalties

There are significant civil and criminal penalties for Responsible Managers who breach their statutory obligations. Generally, Responsible Managers can face a civil penalty of up to $1.05 million or alternatively three times the benefit derived or detriment avoided where this amount exceeds the maximum prescribed penalty units.[4] In addition, Responsible Managers can face up to 5 years imprisonment under criminal law as well as a financial penalty of anywhere up to $420,000.[5] In most instances, the offending individual will be banned from providing financial services[6] and disqualified from managing corporations.[7]

Protections

ASIC's recent enforcement actions speak to the importance of the role Responsible Managers play within financial firms. A Responsible Manager is not merely a procedural role but one that requires ongoing deference to ensure the licensee's obligations are being met. However, where a licensee fails to comply with its obligations and enforcement action ensues, Responsible Managers can protect themselves by way of an indemnity deed, similar to a director's deed of indemnity. It is considered usual practice for a licensee to agree to indemnify its Responsible Managers for liability arising from the performance of their roles. A good indemnity deed will also cover the Responsible Manager's legal costs in connection with defending proceedings.

However, it is important to be aware that s 12GBD of the Australian Securities and Investments Commission Act 2001 (Cth) prohibits a body corporate from indemnifying its officers against liability to pay a pecuniary penalty in relation to the consumer protection provisions under the Act. Likewise, s 199A of the Corporations Act prohibits a company from indemnifying its officers against liabilities under pecuniary penalty orders and compensation orders, and for legal costs in defending such proceedings.

Takeaways

ASIC explicitly states in RG 105 that Responsible Managers who also play a direct role in the day-to-day functioning of a financial services firm "must have enough time available to fulfil their responsibilities."[8] Accordingly, before nominating a Responsible Manager, it is important to consider their overall business commitments and capacity to adequately monitor the licensee's compliance obligations.

It is critical that Responsible Managers are aware of their role and the potential consequences of non-compliance. Responsible Managers should regularly review their licence authorisations and be familiar with conditions such as the obligation to act "efficiently, honestly and fairly"[9] under s 912A of the Corporations Act and the general conduct obligations under s 47 of the National Consumer Credit Protection Act 2009 (Cth). Being a Responsible Manager is not a figurehead role but, as mentioned above, one that carries with it substantial civil and criminal penalties and should accordingly be carried out with the utmost diligence.

Andrea Beatty
Partner
Piper Alderman
abeatty@piperalderman.com.au
www.piperalderman.com.au

Chelsea Payne
Associate
Piper Alderman
cpayne@piperalderman.com.au
www.piperalderman.com.au

Shannon Hatheier
Law Clerk
Piper Alderman
shatheier@piperalderman.com.au
www.piperalderman.com.au

Footnotes

1. Australian Securities and Investments Commission *AFS licensing: Organisational Competence* Regulatory Guide 105 (April 2020).
2. Australian Securities and Investments Commission *Credit licensing: Competence and training* Regulatory Guide 206 (December 2016).
3. Above n 1, at 4.
4. Corporations Act 2001 (Cth), s 1317G.
5. Above, s 1311.
6. Above n 4, s 902A.
7. Above n 4, s 206C.
8. Above n 1, at 6.
9. Above n 1, at 7.

New guidance for activist short sellers and target boards

Fadi Khoury *CORRS CHAMBERS WESTGARTH*

The Australian Securities and Investments Commission (ASIC) has released long-awaited guidance on its regulatory stance on activist short-sellers, including those operating offshore.[1] ASIC also provides better practice guidance to targets that are put under the spotlight of activists, as well as protocols for the Australian Securities Exchange (ASX).

Although common in other markets, increased activist short-selling campaigns attracted media and market interest as campaigns (called "short and distort")[2] were launched by local and offshore hedge funds against various high-profile Australian companies. Some campaigns delivered a massive impact on a company's trading price, and in some cases, threatened the viability of targets.

Better practice for activist short sellers

In the recently released guidance, ASIC sets out various recommendations for activist short sellers and authors of short reports. These include the following:

- *Short reports should be released outside of Australian trading hours and not immediately before the market opens*
  Target entities have complained that reports are often released during or immediately before trading hours. By the time the target has had a chance to respond, the market may have moved. By requiring activists to release the reports *outside* of trading hours, the aim is that targets have time to prepare a more complete response so that the market can be fully informed before any trading takes place.
  Although fair guidance, activist short sellers may ignore ASIC's invitation to forewarn its targets. Even if an activist did approach the target, the target has a challenging task in responding to what is more usually a complex and detailed thesis. A sensible response is unlikely to be written by the target overnight.
- *The activist should fact-check the short report with the target before release*
  The aim is that this will help ensure that patent errors are rectified and any misleading information is addressed before reaching the public.
  A difficulty with ASIC's guidance is that the insider trading and selective disclosure rules would generally preclude the target from engaging with the activist on an open-access basis. It may also be contradictory to ASIC's (sensible) guidance that short sellers should not share their investment thesis selectively.
- *Reports should be founded on verifiable facts*
  ASIC has rightly focused on the need to ensure that these reports are not misleading, incomplete, or unsubstantiated. Failure to do so raises the risk of a claim for breach of Corporations Act 2001 (Cth) laws relating to misleading conduct or market manipulation.
  Reports should contain clear and objective statements that are based on reliable information. Any recommendation or opinion should be formed on a reasonable basis. Authors should not be selective with the facts that they choose to include.
  This reflects existing market practice for the more sophisticated short sellers and is no different from the expectations that ASIC places on any issuer making a release to the market.
- *Reports should avoid using overly emotive language*
  Emotive, immoderate or vague language can distort facts and prompt panicked decision-making by investors. ASIC notes that only balanced, precise and unbiased statements should appear in the report.
- *Disclosure of conflicts*
  As is common practice already, the author of a report should disclose if it has a short position from which it expects to profit if the share price drops.
- *Australian financial services licensing considerations*
  ASIC reminds operators of the breadth of the Australian licensing regime. Short reports are, by their nature, intended to influence a person's decision in relation to a share and may therefore fall within the concept of financial product advice. An offshore provider of financial product advice

should seek counsel on whether this involves the carrying on of financial services business in Australia and therefore requires a licence. The jurisdictional nexus test for licensing purposes is broadly construed if retail persons are involved.

It remains to be seen whether ASIC's guidance will be effective in encouraging less scrupulous players to operate within the boundaries of best practice. It is expected that some operators based offshore will be content to operate at the margins of Australian laws, in the knowledge that they are probably outside of ASIC's reach, whether from a technical or practical enforcement perspective.

Better practice for target entities

ASIC sets out its expectations of targets. In particular, targets must prepare a detailed response to any short report released against them. Responses should address each assertion with "sufficient detail" and be "backed up with evidence"[3] wherever possible. ASIC provides that, even where the target considers the report to be whole without merit, "broad statements dismissing an entire report as being false are unlikely to address investor concerns."[4]

Where a target has received prior notice of a short report, the target is expected to prepare a response quickly enough so that it can be released at "around the same time"[5] as the report. Targets are advised to request a trading halt in instances where they have not had sufficient time to prepare an adequate response.

It is possible that ASIC's guidance imposes a heavy burden on a target in responding to an activist campaign. Companies should be free to make their own assessment of the credibility of the short report and to factor that assessment into their market response. Applying a blanket approach on how targets should respond could lead to a situation where companies find themselves in an endless round of trading halts while they respond to claims with which they disagree or which they consider are spurious or not worthy of comment. Under ASIC's guidance, it is effectively the target who bears the compliance risk.

Better practice for market operators

Building on the ASX's obligation to ensure the market is fair, orderly and transparent, ASIC points to better practices for the ASX (and other market operators).

Although the guidance is largely unsurprising, the publication of guidance by ASIC and effective mandating of protocols may assist in reducing the stigma of action taken by the ASX and the relevant listed entity during a short and distort campaign. In particular, ASIC expects that if ASX becomes aware that a listed entity targeted by a campaign has made a material price impact, ASX should immediately pause trading in the entity and require the entity to provide a comprehensive response. If follow on short reports are published, the entity may also need to respond to such reports if there are issues to address.

Fadi Khoury
Partner
Corrs Chambers Westgarth
fadi.khoury@corrs.com.au
www.corrs.com.au

Footnotes

1. Australian Securities and Investments Commission, Activist short selling campaigns in Australia Information Sheet 255, May 2021, https://asic.gov.au/regulatory-resources/markets/short-selling/activist-short-selling-campaigns-in-australia/.
2. Above.
3. Above n 1.
4. Above n 1.
5. Above n 1.

Ransomware attacks: prevention and protection guide for financial services lawyers

Frank Downes *JURIS IT SERVICES*

Ransomware is a type of malware that locks up your files until a ransom is paid, typically payable using an online digital currency or cryptocurrency such as Bitcoin. It can also steal a copy of your files to coerce you to pay the ransom by threatening to publicly leak or sell your data. The latter outcome is particularly concerning for lawyers working in the financial services industry. This information will normally be confidential, the leak of which will damage you and your clients.

Your presence (and susceptibility) in the digital world is larger than you think. On a personal level you use the internet for online shopping, banking, storing and sharing photos and documents. Professionally, your client's information is stored in the cloud; you access numerous work-related websites in the course of everyday. These services all connect back to you and your sensitive information — this is what cybercriminals want.

Take the steps outlined below to proactively prevent a ransomware attack on your practice. These steps could also be used by financial services lawyers to craft an advisory practice role where you can assist your clients in meeting their compliance and regulatory requirements in this area. The Financial Services Industry is classified as Critical Infrastructure and the provisions are complex, presenting you with an opportunity for providing additional helpful advice to your clients.

1. Update your device and turn on automatic updates

Having an up-to-date operating system (Windows, macOS or other) and security software reduces the chance of a cybercriminal using a known weakness to hack your computer. It also provides security upgrades and protections for your device against other threats.

2. Turn on two-factor authentication

Multi-factor authentication (MFA) typically requires a combination of something you know (PIN, password/passphrase) and something you have (mobile phone, smartcard, physical token) or something you are (fingerprint, iris scan).

MFA makes it harder for cybercriminals to gain initial access to your device, account and information by making them jump through more security hoops and additional authentication layers. This means that the cybercriminal will have to spend more time, effort, and resources to get into your device before any ransomware attacks can begin. Two-factor authentication is the most common type of MFA. It provides enhanced security to traditional usernames and passwords/passphrases and increases confidence that the user requesting access is actually who they claim to be.

3. Set up and perform regular backups

A backup is a digital copy of your most important information (eg photos, financial information or health records) that is saved to an external storage device or the cloud. Backing up is a precautionary measure, so that your information is accessible in case it is ever lost, stolen or damaged through a ransomware attack. The best recovery method for a ransomware attack is a regular offline backup made to an external storage device and additionally a backup in the cloud. Regularly backing up your files is recommended. What that looks like, whether it's daily, weekly, monthly or less often, is ultimately up to you. Backup frequency depends on the number of new files you load onto your device and the number of changes you make to files. We encourage you to test your backups so you are familiar with the process and ensure your backups are working appropriately.

Due to the increasing use of backups, ransomware actors have adapted their methodology to taking copies of the data and then threatening to publish it. In the context of a financial services lawyer this is particularly problematic as your client's confidential information could be published with serious consequences.

4. Implement access controls

Implementing access controls is an important step in managing who can access what on your devices. This is especially true in the context of legal practice within the financial services industry.

Access controls help minimise the risk of unauthorised access to important information, which then helps to minimise the consequences of ransomware running on devices by limiting the amount of information it can encrypt, steal and delete.

5. Principle of least privilege

The principle of least privilege is the safest approach for most. It gives people access only to the software applications and files they need to perform their job.

6. Turn on ransomware protection

Ransomware protection has the ability to prevent many types of ransomware attacks from happening. In the unfortunate event of an attack, ransomware protection can also interrupt the ransomware from encrypting all your data, which minimises the extent of the damage.

If you are using Windows 10, you can enable built-in ransomware protection to protect your files. If you are using another operating system, you will need to source and install ransomware protection for your devices. There are many types of ransomware protection available. Ask your professional information technology service provider what operating system you are running.

In addition to installing ransomware protection, the best course of action is to backup your information (see step 3). That way, even if an attack is successful, you will at least have your important information accessible elsewhere.

7. Run simulations and conduct training

Clicking on what appears to be a legitimate link in an email is the most common method for ransomware to gain entry into your system. Regular training through the use of simulated emails helps to keep staff awareness high and identifies who may be clicking on links inadvertently.

8. Prepare your cyber security emergency plan

Prior preparation is the key here. Get to know your critical information and devices. Know what you are willing to live without and what you are willing to go above and beyond to save.

Consider the following:

- what you can and cannot replace
- to what extent will you invest to recover the information or device
- protect your information and devices:
  - — what it is you are seeking to protect
  - — what the impact is if it is lost
  - — where it is located
- who are your emergency contacts
  - — stakeholders
  - — IT professionals
- what email accounts need to be protected
- who needs to be notified

9. Ransomware action checklist

- Update your device and turn on automatic updates.
- Turn on two-factor authentication.
- Set-up and perform regular backups.
- Implement access controls.
- Turn on ransomware protection.
- Run simulations and conduct training.
- Prepare your cyber emergency checklist.

Taking the actions on this checklist will also help prevent successful phishing attacks which is the other most common method cybercriminals use to gain unauthorised access to computer systems.

Take this checklist to your IT provider and ensure that each one of these steps has been provisioned and implemented correctly.

Frank Downes
CEO
Juris IT Services
frankd@jurisit.com.au
jurisit.com.au

About the author

Frank Downes is the CEO of JurisIT, an IT services company that assists law firms with technology, information security, information compliance and successfully implementing, securing and maintaining remote work environments.

For editorial enquiries and unsolicited article proposals please contact newsletters@lexisnexis.com.au.
Cite this issue as (2021) 20(5) *FSN*
SUBSCRIPTION INCLUDES: 10 issues per volume plus binder www.lexisnexis.com.au
SYDNEY OFFICE: Locked Bag 2222, Chatswood Delivery Centre NSW 2067
CUSTOMER RELATIONS: 1800 772 772
GENERAL ENQUIRIES: (02) 9422 2222
ISSN: 1035-2155 Print Post Approved PP 25500300764