Financial Services Newsletter

2020 . Vol 19 No 3

Contents

Information contained in this newsletter is current as at June 2020

LexisNexis® Butterworths

General Editor's note

Karen Lee *LEGAL KNOW-HOW*

Welcome to the *Financial Services Newsletter*. We are living in unusual times, and I hope you are staying well.

Many of us would be familiar with the acronym "DDO" by now. The term "design and distribution obligations" is often abbreviated to DDOs. These obligations will come into force on 5 April 2021 and businesses need to start planning now to ensure that they can comply with them when they commence. In this issue, I am pleased to bring to you an article by editorial board member **Jon Ireland** and his co-author **Anjelica Balis** (Norton Rose Fulbright Australia). The title of the article is "Product design and distribution obligations — ASIC's consultation and implications for fund managers". Facing now the impending commencement of the new DDO regime, the authors explore the requirements, draft guidance and implications for fund managers.

"COVIDSafe" is a smartphone app introduced by the Australian Government to "trace" individuals who have tested positive for COVID-19 and notify those users who have been in close contact with the infected individual. In their article "Is 'COVIDSafe' privacy safe? Is Big Brother concerned for your health?", editorial board member **Andrea Beatty** and her co-authors **Chelsea Payne** and **Chloe Kim** (Piper Alderman) discuss the concerns raised and the broader implications on privacy law, how the government has responded to these concerns in releasing the app, and importantly, its impact on financial firms.

Have you ever considered COVID-19's impact on financial firms and financial institutions? In his article "The insider threat to a financial services firm's information security", **Frank Downes** (Juris IT Services) sheds some light on this topical subject, and provides practical guidance on how to help a client reduce the insider threat to their information security during and after a pandemic or crisis.

Please enjoy this compilation of articles on the latest legal developments and timely practice guidance for financial services lawyers!

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 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 Corporate Finance Law, Halsbury's Laws of Australia and Practice Guidance for 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.

Product design and distribution obligations — ASIC's consultation and implications for fund managers

Jon Ireland *and* ***Anjelica Balis*** *NORTON ROSE FULBRIGHT AUSTRALIA*

Overview

The Financial System Inquiry first recommended in November 2014 the introduction of a design and distribution regime, after concerns that the current regulatory framework was insufficient in protecting consumers and too reliant on general advice and disclosure. As a consequence of this recommendation, the Treasury Laws Amendment (Design and Distribution Obligations and Product Intervention Powers) Act 2019 (Cth) was passed on 5 April 2019 introducing the Australian Securities and Investments Commission's (ASIC) product intervention powers as well as design and distribution obligations (DDOs) under Ch 7 of the Corporations Act 2001 (Cth).

The design and distribution obligations were scheduled to commence on 5 April 2021, however due to the impacts of COVID-19, ASIC has announced a deferral of the commencement date by 6 months until 5 October 2021.

ASIC has issued *Consultation Paper 325: Product Design and Distribution Obligations*[1] accompanied by its draft regulatory guidance on the DDO regime. In this article, we explore the requirements, draft guidance and implications for fund managers.

What products does the DDO regime apply to?

The DDOs apply to the following types of financial products:[2]

- products that require disclosure in the form of a Product Disclosure Statement (PDS) in accordance with Pt 7.9 of the Corporations Act
- securities for which a disclosure document must be prepared under Pt 6D.2 of the Corporations Act (however this excludes ordinary shares) and
- financial products under Div 2 of Pt 2 of the Australian Securities and Investments Commission Act 2001 (Cth), however do not include products regulated under Pt 6D.2 or Pt 7.9 of the Corporations Act — these include, for example, consumer leases and credit contracts

There are some financial products which are excluded from the DDO regime. These include (but are not limited to) default superannuation (MySuper products), margin lending facilities and fully paid ordinary shares in a company.[3]

To whom does the regime apply?

The DDO regime applies to both issuers and distributors of financial products. Issuers include persons who must prepare a disclosure document under the Corporations Act, for example as the responsible entity of a managed investment scheme or a superannuation trustee, or issuers and sellers of financial products that require a prospectus or PDS.

Distributors are "regulated persons", which include Australian financial services (AFS) licensees and authorised representatives.[4] The act of distribution means "retail product distribution conduct" in relation to a consumer, which includes dealing in a financial product, giving a disclosure document in relation to a financial product and providing financial product advice.[5]

What are the DDOs for issuers and distributors?

Issuers

The issuer of a financial product which is subject to the DDO regime must make an appropriate "target market determination" (TMD).[6] A TMD must:

- be in writing and be made publicly available
- describe the class of consumers that comprises the target market for the product
- specify any distribution conditions and restrictions on distribution
- specify any event that reasonably suggests that the TMD is no longer appropriate, known as "review triggers"
- specify when the first review and subsequent reviews of the TMD must occur
- specify when the distributor should provide information about the numbers of complaints to the issuer and

- specify the information the distributor(s) must report to the issuer and how frequently, in order to enable the issuer to identify whether the TMD may no longer be appropriate

Issuers are also required to:

- take reasonable steps to ensure that distribution is consistent with the most recent TMD[7]
- notify ASIC if it becomes aware of a significant dealing in the product that is not consistent with the TMD as soon as practicable but within 10 business days[8]
- review the TMD within 10 business days if it knows, or ought reasonably to know, that a review trigger (ie, an event which suggests that the TMD is inappropriate) has occurred, and must periodically review the TMD to ensure it remains appropriate[9] and
- keep complete and accurate records of decisions made in relation to TMDs, reviews and reasons for those decisions, as well as distribution information[10]

The TMD requires identification of a *class* of consumers based on their common objectives, financial situation, and needs, which may also include describing the "negative target market" (ie, for whom the financial product is clearly unsuitable).[11]

With respect to managed funds and the review of TMDs, in its draft regulatory guidance ASIC has suggested that the issuer of interests in a managed investment scheme may consider the following factors when identifying "review triggers" that may indicate the target market is inappropriate or that the product should be redesigned:[12]

- the performance of the product compared to its original targets (if any) and appropriate benchmarks
- any losses suffered and whether the product is likely to achieve the issuer's original goals
- whether the product remains liquid and is capable of offering regular withdrawals
- the taxation implications of the product compared to other similar products
- the fees of the product compared to other similarly performing products
- whether there has been a significant increase in fund outflows
- whether the product remains on approved product lists for key distributors and
- the number, nature and outcomes of complaints

Distributors

Distributors generally interact with the end consumer and must take reasonable steps that will, or are reasonably likely to, result in its retail product distribution conduct being consistent with the TMD.[13] Fund managers will generally fall into this category where they are also acting as distributors (eg, dealing directly with the end consumer). Distributors must comply with the following obligations:

- They must not engage in retail product distribution conduct in relation to a product unless the distributor reasonably believes (after making all such reasonable enquiries) that a TMD has been made, or that a TMD is not required.[14]
- A distributor must take reasonable steps that will, or are reasonably likely to, result in a distribution being consistent with the most recent TMD.[15]
- The distributor must notify the issuer if they become aware of a significant dealing in the product that is not consistent with the TMD as soon as practicable, but within 10 business days.
- They must keep complete and accurate records of distribution information, including the number of complaints received about a product as well as information specified by the issuer in the TMD.[16]

ASIC has provided draft guidance on what it determines will be relevant in considering whether a distributor has met its obligation to take "reasonable steps":[17]

- the types of distribution methods used (eg, online, inbound/outbound telephone sales and face-to-face) and whether they are appropriate for the particular financial product
- compliance with distribution conditions specified by the issuer in the TMD
- the content and medium of delivery to consumers of marketing and promotional materials
- the effectiveness of the distributor's product governance framework
- the steps the distributor has taken to appropriately manage or eliminate the risk that incentives may inappropriately influence behaviours which could result in consumer harm or distribution inconsistent with the TMD
- reliance on existing information about the consumer
- whether the distributor has given staff involved in distribution operations sufficient training and assessed their skills in order to perform their obligations and
- how the distributor forms a reasonable view that a consumer is reasonably likely to be in the target market for certain products

Next steps

In light of the impending release of ASIC's final guidance on the new DDO regime, we recommend fund managers to start planning from now and review their current products and put in place their product governance framework to ensure they can comply with the DDO regime once it commences. We also recommend to continue monitoring closely any impact that the current COVID-19 crisis may have on the timing of the guidance and this new regime.

Key takeaways:

- *Key obligations on issuers* — Issuers must make TMDs for each relevant financial product, identify review triggers, review the TMD to ensure it remains appropriate, notify ASIC about significant dealings which are not consistent with the TMD and keep adequate records.
- *Key obligations on distributors* — Distributors must not distribute financial products caught within the regime unless a current TMD is in place. Distributors must also take reasonable steps to ensure that the distribution is consistent with the TMD and notify the issuer of any significant dealings which are not consistent with the TMD.
- *Product governance framework* — Both issuers and distributors should implement a product governance framework whereby their systems, processes, procedures and arrangements help ensure that they comply with the DDO regime.
- ASIC has engaged in a consultation process regarding its draft regulatory guide and has proposed to issue its finalised regulatory guidance by the end of 2020, however no specific date has been given at this stage.

Jon Ireland
Partner
Norton Rose Fulbright Australia
jon.ireland@nortonrosefulbright.com
www.nortonrosefulbright.com

Anjelica Balis
Associate
Norton Rose Fulbright Australia
anjelica.balis@nortonrosefulbright.com
www.nortonrosefulbright.com

Footnotes

1. Australian Securities and Investments Commission (ASIC) *Consultation Paper 325: Product Design and Distribution Obligations* (December 2019) https://download.asic.gov.au/media/5423121/cp325-published-19-december-2019.pdf.
2. Corporations Act 2001 (Cth), ss 994AA and 994B(1).
3. Above, s 994B(3).
4. Above n 2, s 1011B.
5. Above n 2, s 994A(1).
6. Above n 2, s 994B(1) and (5).
7. Above n 2, s 994E(1).
8. Above n 2, s 994G. "Significant dealing" has not been defined under the Corporations Act as whether or not a dealing will be regarded as significant or should be determined on a case-by-case basis.
9. Above n 2, s 994C.
10. Above n 2, s 994F(1) and (3).
11. Above n 2, s 994B(5)(b). The law does not require the issuer to state the negative target market in the TMD, however ASIC is of the view that this will likely assist the issuer in defining the target market at a sufficiently granular level.
12. ASIC *Regulatory Guide 000: Product Design and Distribution Obligations* (December 2019) RG 000.130 https://download.asic.gov.au/media/5423109/attachment-to-cp-325-published-19-december-2019.pdf.
13. Above n 2, s 994E(3).
14. Above n 2, s 994D.
15. Above n 2, s 994E(3).
16. Above n 2, s 994F(3).
17. Above n 12, RG 000.163.

"COVIDSafe" privacy safe? Is Big Brother concerned for your health?

***Andrea Beatty**, **Chelsea Payne** and **Chloe Kim** PIPER ALDERMAN*

The Australian Government is encouraging its citizens to download an app, COVIDSafe. Media reports suggest COVID-19 restrictions being relaxed are conditioned on the take-up of the app.

The COVID-19 global pandemic has demonstrated the power of technology, fuelling businesses and individuals' ability to stay connected while in isolation. As technology becomes more ingrained into the operation of businesses and individuals' lives, the concerns over privacy has become a significant point of consideration. The Australian Government has introduced a smartphone app, "COVIDSafe" which will permit individuals who have tested positive for COVID-19 to upload an automated list of contacts which have been collected by the app and enable the Department of Health to then notify those users who have been in close contact with the infected individual. This article will discuss the concerns raised and the broader implications on privacy law, and how the government has responded to these concerns in releasing the app.

Background

The COVIDSafe app became available for download on 26 April 2020 and is intended to combat the spread of the pandemic and "flatten the curve" by allowing the government to identify people who have had close contact with positive cases and notify them of their proximity. As the Australian Government moves to lift lockdown bans and social integration begins again, being aware of which individuals have tested positive has become an important consideration to prevent community transmissions.

App operation

The Government introduced COVIDSafe based on Singapore's already functioning app, "TraceTogether" that would operate utilising Bluetooth technology which would "ping" and conduct a "digital handshake" if the device comes into close proximity with each other. This connection would be encrypted and logged.

If the individual with the COVIDSafe app tests positive for COVID-19, they are asked to upload the log to a central server so that their local health authority could access and decrypt the data. The applicable state or territory health department will then contact anyone who has been in contact with the positive COVID-19 individual and alert them to that fact. The health officials will also provide advice on symptoms, the testing process and how to protect friends and family from exposure.

The government says there needs to be a minimum of 40% of the population that downloaded the app for it to be effective. At the time of writing, almost five million Australians have downloaded the app.

Government's response to privacy concerns

As revealed in an Essential Research survey commissioned by *The Guardian*, approximately 57% of Australian voters were concerned about the app due to the security and privacy issues regarding the collection of their personal information.[1] However, Government Services Minister Stuart Robert announced the only information required when people download the app is their name (or pseudonym), age range, postcode and phone number. Furthermore, the government has released the Office of the Australian Information Commissioner's (OAIC) privacy impact assessment commissioned by the Department of Health, conducted with the Australian Cybersecurity Centre's assistance, with the source code which has been reverse engineered off the apps themselves soon becoming available so the public can view it. This will ensure that researchers and analysts can verify how the app operates and assist in finding and addressing any possible issues with it.

The Biosecurity (Human Biosecurity Emergency) (Human Coronavirus with Pandemic Potential) (Emergency Requirements — Public Health Contact Information) Determination 2020 (Cth) (Determination) has also been implemented which outlines the relevant requirements for the: collection, use or disclosure; treatment; decrypting; and coercion for the use of the COVIDSafe data.

The Determination was made in accordance with s 477(1) of the Biosecurity Act 2015 (Cth) which allows the Minister for Health to determine any emergency requirements necessary to prevent or control a human disease such as COVID-19.

As noted in the Determination's Explanatory Memorandum, the Determination will override any inconsistent requirements that would apply under Australian legislation including the Archives Act 1983 (Cth) or even the Privacy Act 1988 (Cth) unless it is information concerning an individual. However, this does raise issues of inconsistency among the legislation applicable and should be clarified when the operation of the Privacy Act and relevant Australian Privacy Principles (APPs) concerning the management of personal information are overridden.

On 4 May 2020 the Attorney-General released the draft Privacy Amendment (Public Health Contact Information) Bill 2020 (Cth) (Bill) enforcing greater legislative protections for app users. The Bill which greatly mirrors the existing Determination will be introduced into Parliament soon and will override the Determination once in force.

Building upon the existing Determination, the Bill will make a contravention of the requirements outlined in it a criminal offence, a breach of the Privacy Act or both. The Bill makes clear that if any criminal offences under the Bill occur, the Australian Federal Police will be able to commence an investigation. Furthermore, the Bill allows individual users of the app to commence enforcement action by having their complaints heard by the Office of the Australian Information Commissioner (Commissioner) or the relevant privacy regulator in each state or territory.

The Bill outlines that the:

- collection, use or disclosure of data retained from COVIDSafe which is not for the purposes of contract tracing
- coercing of an individual to use the app
- storing or transfer of data to a country other than Australia
- decryption of the data from the app,

will be considered a criminal offence which can be penalised by 5 years' imprisonment or 300 penalty units ($63,000).

Similar to the implementation of "My Health Record", the COVIDSafe app raises several privacy concerns regarding the opt-out options, metadata access and penalties for mishandling of information. In addition, the "My Health Record" system crash is a significant concern for the operation of COVIDSafe, where the app's system crash could lead to users coming into contact with positive COVID-19 individuals without the app properly recording the data.

Specific privacy issues addressed by the Government

Prior to its launch, commentators raised a number of privacy issues in relation to the COVIDSafe app. We list these issues raised below, and how the Government has since addressed these concerns through its guidelines. Users would need to provide informed consent.

There are very serious privacy implications for obtaining an individual's personal information without consent. Prime Minister Scott Morrison has emphasised that consent would be integral to the operation of the app. Therefore, the app is required to seek and obtain the informed consent of users before the government can collect, use, handle and disseminate their personal information.

However, some individuals may lack the legal capacity to provide personal consent. This includes minors. Accordingly, arrangements should be made to ensure their informed consent is being provided. The OAIC has identified that if an individual lacks capacity, then the government could consider if another individual can act on the individual's behalf including a:

- guardian
- power of attorney
- person recognised by other relevant laws — for instance, in NSW, a "responsible person" under the Guardianship Act 1987 (NSW) may be a spouse, partner, carer, family member or close friend and
- person the individual nominated in writing when they were capable of giving consent[2]

The "COVIDSafe" app should also require new consent from users before it introduces any updates that vary information collected. Implied consent should not be sufficient in these circumstances.

Deletion or de-identification of personal information

The Government has announced that contact information stored on COVIDSafe on a user's device (that is not uploaded) will be deleted on a 21-day rolling cycle, taking into consideration the COVID-19 incubation and testing period.[3] This has been verified by code review of reverse engineered source code.

Furthermore, Minister Robert has identified that once the pandemic is over, the Government will delete the app ensuring that all the data held on the server will be deleted or de-identified. However, if an individual is to delete the app prior to the pandemic ending, the information stored will only be destroyed at the end of the pandemic. Any requests for prior deletion would have to be specifically requested utilising the data deletion form.

In order to address the concerns around the retention of personal information, the app should expressly identify the requirements of how the data will be deleted or destroyed after it has been uploaded. This should be

done in accordance with the APPs, especially APP 11 which identifies the necessary guidelines for destroying or de-identifying personal information. Furthermore, there should be a determined fixed period for data to remain on the state and territory health authorities before it is no longer required and consequently can be removed from the databases.

Collection of users' personal information

States and territories

As the app provides data access to state and territory health bodies, particular concern has been raised that state and territory agencies are generally not regulated by the Privacy Act, and some states and territories do not have any privacy statutes.

Minister Robert identified that the data will only be made available to state and territory health authorities so that not even the Commonwealth will have access to it. However, to ensure that the information that has been consented to only stays within state and territory boundaries, there should be specific consent for cross-border information transmission. This may arise in circumstances where individuals travel across states. This would also prevent authorities from data matching and instead, require them to obtain express consent. However, in accordance with the Bill, if a complaint has been made regarding a breach of the Bill, the Commissioner may be able to refer or share information or documents with other state or territory privacy authorities.

Under s 6(2)(a)(i) of the Determination, "a person employed by, or in the service of, a State or Territory health authority" is not prevented from collecting, using or disclosing COVIDSafe data. The loose association of "in the service of" could cause potential issues on which categories of health services could have access to the data. As addressed in the Explanatory Memorandum individuals "who are not technically employees or officers of a State or Territory health authority" could have access which raises concerns about the spread of data especially if they have not been contracted to keep the information confidential.[4] However, the parameters outlined in the Bill limit collection, use or disclosure strictly to contract tracing.

Secondary disclosure

In contrast to secondary use purposes permitted under the APPs, secondary disclosure of information should be prohibited in relation to COVIDSafe data. Public trust in, and up take of, the app will only occur when there is full separation between COVIDSafe data and all other government functions and their department and agencies, including law enforcement agencies, security agencies, courts and other statutory bodies.

Impact on financial firms

The introduction of COVIDSafe reflects developments in the banking and financial sector as the Consumer Data Right becomes ingrained into how customers and banks share, access and provide information. Therefore, the guidelines produced for the COVID-19 tracking app should influence how the Consumer Data Right rules are developed. As the Determination, Bill and following legislation regarding COVIDSafe will regulate how individuals' information will be handled and retained, it is likely to have an influence on how accredited persons, accredited data recipients, data holders and designated gateways should also uphold necessary safeguards in relation to financial data.

Conclusion

Although COVIDSafe has been created in the hopes of "flattening the curve" and ensuring a safe transition into social interaction there are several privacy issues that must be considered. The Government should place particular emphasis and provide greater clarity on the competing legislation which will be applicable, the process of obtaining individuals' consent, deleting or de-identifying information and collection and tightening the access and disclosure of health data.

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

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

Chloe Kim
Law Graduate
Piper Alderman
ckim@piperalderman.com.au
www.piperalderman.com.au

Footnotes

1. M Farr "Guardian Essential poll: suspicions about tracing app offset by approval of Covid-19 response" *The Guardian* 28 April 2020, www.theguardian.com/australia-news/2020/apr/28/guardian-essential-poll-suspicions-about-tracing-app-offset-by-approval-of-covid-19-response.

2. Privacy Act 1988 (Cth), s 6AA(1).
3. Biosecurity (Human Biosecurity Emergency) (Human Coronavirus with Pandemic Potential) (Emergency Requirements — Public Health Contact Information) Determination 2020 (Cth), s 7.
4. Determination Explanatory Memorandum, p 6.

The insider threat to a financial services firm's information security

Frank Downes *JURIS IT SERVICES*

Over the last 6 months, we have seen a series of events that have increased the need for individuals to work away from the standard office environment. This includes financial services lawyers and their clients. The bushfires and floods at the end of 2019 meant a good proportion of people around the country could not make it to their workplace during these times of natural disasters. The fires and floods were a precursor to an economy-wide requirement to work from home with advent of COVID-19 and the ensuing lockdowns and restrictions on movement.

Whether a client is in the business of providing financial product advice or traditional trustee company services, working from home or working remotely is now a permanent feature of the workplace and this is not likely to change even when the restrictions on movement are lifted completely.

In March, the initial focus was on getting people out of the office and into a safe health environment. This meant many common information security requirements were ignored for the expediency of enabling the appropriate health outcomes.

Whilst the news and media tend to focus on hackers, the main threat a financial services firm or financial institution will face to its information security is from the inside — malicious or inadvertent. This new business environment has the potential to increase the motivation and capabilities of employees to engage in harmful activity that will impact their employer.

Malicious activity

Employees and staff can develop a motivation to engage in malicious activities aimed at the organisation they work for. This intent normally develops over time and can be caused by the following:

- Disillusion with the response of the organisation to the COVID-19 pandemic or management of their particular circumstances. This is gradual and can be managed with regular feedback and monitoring of changing employee attitudes.
- Isolation leading to a disconnectedness with the company relating to the perception and impact of the COVID-19 pandemic. Again, this is something that develops over time and can be monitored. If the social distancing restrictions remain in place for any length of time, this sense of disconnectedness will grow.
- Financial hardship or uncertainty concerning employment stability. Whilst a financial services firm or financial institution may ensure that these situations do not occur, employees will be exposed to this uncertainty vicariously through other family members and friends.
- Impaired judgment and decision-making due to adverse social and mental health impacts; this is simply that over time the grinding nature of the uncertainty we are now faced with wears people down. Some employees will lack the resilience or support networks to cope with this. This can be exacerbated by:
  - — prolonged anxiety and stress
  - — prolonged periods of isolation, including impacts on physical health and relationships
  - — travel restrictions impacting business and personal contact
  - — increased substance abuse
  - — social and workplace disconnect
  - — uncertainty as to the future in a post-COVID world

Capability

With the move to remote working environments, there is an increase in the capability to conduct such activity. In the rush to get people out of the office, many of the standard security protocols applicable for remote work have not been adhered to as forcefully as is normally the case. The current altered working arrangements across organisations and government departments are impacting on information communications technology, physical access and personnel security arrangements. Including:

- individuals accessing areas, systems and information at altered or extended hours, including early morning, late evening and weekends — combined with reduced security personnel coverage across these times

- reduced presence of co-workers/supervisors in workspaces
- increased remote access to computer systems and information to facilitate "work from home" arrangements — including:
  - — granting of access to systems and information that may not normally be routinely available remotely
  - — increased use of lower classification systems that may be more security-vulnerable and
  - — increased use of external devices (eg, laptops, USBs and external hard drives) and remote access tokens
- increased access (including granting "global access") within computer systems to enable alternate working arrangements
- reduced frequency of information system and technology auditing and monitoring capabilities due to reductions in workforces and
- reduced awareness and reporting of security-related behaviour due to reduced direct workplace contact between employees

Non-malicious activity

Historically, this is actually the most common method of data breach; simple human error or lack of attention has been the cause of some of the most catastrophic (in terms of impact on the organisation) breaches that have occurred.

The COVID-19 environment increases the potential for non-malicious insider activity, whereby poor or lax security processes result in inadvertent access and/or disclosure of high-harm confidential material. The threat from inadvertent disclosure or compromise may exist into the future in cases where material leaves a lasting electronic footprint on the internet.

How to reduce the insider threat to information security

A financial services firm or financial institution should consider the following mitigation measures to reduce the potential for increased malicious and non-malicious insider activity:

- Where possible and within government guidelines relating to essential workers, staff safety and social distancing — employers should maintain physical security and information security policies, structures and resourcing.
- Where possible, maintain centralised records on increased computer system accesses, permissions and justifications, access to premises and removal of information and assets. At minimum, sufficient data should be collected to enable meaningful analysis of access to information, facilities and assets, should an insider investigation be required.
- Staff working from home, or on less secure systems, or under different working arrangements, should be reminded of their ongoing requirement to maintain the security of information, and the importance of separating corporate and personal systems (including social media) where possible.
- Staff (including those working from home) should be reminded of ongoing contact reporting requirements and made aware of the potential for approaches online.
- Employers should ensure staff are made aware of in-house and/or external options for mental health support, including options (if any) for financial support in that regard.
- Employers should maintain robust arrangements for regular check-ups on staff on long-term leave, those with significant caring responsibilities, those who are self-isolating and those who identify as at heightened risk of serious impacts from COVID-19.
- Staff should be encouraged to remain aware of and report any real or potential breaches of security observed by other staff members to their supervisor.

It is time for financial services firms and financial institutions to check that their current work from home set-ups meet the information security requirements required by the various regulators that they are subject too. The Australian Securities and Investments Commission (ASIC) has not suspended their regulatory requirements, and whilst there may be some leniency, financial services firms and financial institutions cannot rely on that. Now is the time to ensure all information security is up to scratch.

In particular, legal practitioners should note that clients may be subject to *Regulatory Guide 259: Risk management systems of responsible entities*[1] and *Report 429 Cyber resilience: Health check*.[2] The Australian Prudential Regulation Authority (APRA) *Prudential Standard CPS 234: Information Security* will be relevant for many readers also.[3]

The first step in ensuring a financial services firm's or financial institution's information security is maintained is to assess where the organisation is now. Some time has passed since introducing "work from home" and it is now time to consider the following questions:

- What processes have been affected?
- How can these processes be modified for the new environment?

- What hardware needs to be upgraded for remote working to be secure?
- Who else will have access to the information in a home environment?
- Should any new technology be introduced?
- How are staff managed with regards to working from home?

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

About the author
Frank Downes is the CEO of JurisIT, an IT services company that assists organisation with information security and successfully implementing, securing and maintaining remote work environments.

Footnotes

1. Australian Securities and Investments Commission *Regulatory Guide RG 259: Risk management systems of responsible entities* (27 March 2017).
2. Australian Securities and Investments Commission *Cyber resilience: Health check* Report 429 (March 2015).
3. Australian Prudential Regulation Authority *Prudential Standard CPS 234: Information Security* (July 2019).

For editorial enquiries and unsolicited article proposals please contact Shomal Prasad at shomal.prasad@lexisnexis.com.au.
Cite this issue as (2020) 19(3) *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