Your Knowledge

Newsletter – November 2022

p: (07) 4948 4444 www.apws.com.au
Suite 1, Cumberland House, 2 Island Drive, Cannonvale

Can you prevent a hack?

In the wake of the Optus data leak, legislation before Parliament will lift the maximum fine for serious or repeated breaches of the Privacy Act from $2.2m to up to $50m. But there are no guarantees that even the strongest safety measures will prevent an attack. So, what does that mean for business and their customers?

Legislation before Parliament will lift penalties for serious or repeated privacy breaches, provide new powers to the Australian Information Commissioner, require entities to provide detailed data to the Information Commissioner to assess public risk, and give the regulator greater information sharing powers.
In a statement, Attorney General Mark Dreyfus said, "When Australians are asked to hand over their personal data they have a right to expect it will be protected." But the question is, can any business claim that customer data will be protected from hackers?
If a customer needs to disclose their personal information to your business to work with you, at the point the data is collected, your business is the custodian of that data. A duty of care exists from the moment the data is collected to the point the information is no longer required and destroyed.

The Privacy Act requires organisations to take "reasonable steps" to protect the data collected. 'Reasonable' steps "requires the existence of facts which are sufficient to [persuade] a reasonable person." That is, in the event of a data breach, the business will need to prove the steps they have taken to protect client data.

Lessons from RI Advice

Australian Competition and Consumer Commission v RI Advice Group Pty Ltd was a landmark case. While specific to the obligations of an Australian Financial Services License (AFSL), it demonstrates that ASIC are willing to pursue not just companies that breach their duty of care but the directors and officers involved.
RI advice is a financial services company that, through its AFSL, authorised representatives to provide financial services. As you would expect, as part of providing financial services, the authorised representatives received, stored and accessed confidential and sensitive personal information. Between June 2014 and May 2020, nine cybersecurity incidents occurred at practices of RI Advice's Authorised Representatives. Enquiries following the incidents revealed:

- Computer systems which did not have up-to-date antivirus software installed and operating
- No filtering or quarantining of emails
- No backup systems or back-ups being performed; and
- Poor password practices including sharing of passwords between employees, use of default passwords, passwords and other security details being held in easily accessible places or being known by third parties.

RI Advice took steps to manage their cybersecurity introducing a cyber resilience program, controls and risk management measures for its representatives including training, incident reporting, and contractual professional standard terms, but by its own admission, it took too long to implement.
RI Advice was ordered to pay $750,000 towards ASIC's costs. Handing down the decision Justice Rofe said, "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."

Scams and how to avoid them

I got a text the other day "Hi Mum, I have broken my phone and I am using this number." The "Hi Mum" scam has exploded with more than 1,150 Australians falling victim to the ploy in the first seven months of 2022, with total reported losses of $2.6 million. Once the scammer establishes contact, they start requesting money for an urgent bill or a replacement phone etc.
For those with children or dependant family members, it is not that hard to believe. According to the Australian Consumer and Competition Commission (ACCC), two-thirds of family impersonation scams were reported by women over 55 years of age.
Another common scam is the lost or unable to deliver package texts and voicemail. With Christmas just around the corner, we can expect to see another escalation of this scam where tracking links purportedly from Australia Post, Toll, or Amazon etc., are used to instal malware. Once accessed, the malware will access your contacts and spread the malware and potentially access your personal information and bank details.
In July, the Australian Taxation Office (ATO) reported a new wave of 'Tax refund SMSF scams'. The texts purported to be from the ATO stating that the individual had a tax refund and to click on the link and complete the form. Another scam purporting to be from the ATO advised that the recipient was suspected

Accountancy Plus apw Whitsunday

p: (07) 4948 4444 www.apws.com.au
Suite 1, Cumberland House, 2 Island Drive, Cannonvale

of being involved in cryptocurrency tax evasion and requested that they connect their wallet. At which point the wallet was accessed and any assets stolen.
The ACCC's Targeting Scams report states that in 2021, nearly $1.8bn in losses were reported but the real figure is likely to be well over $2bn.
The largest combined losses in 2021 were:

- $701 million lost to investment scams with 2021 figures significantly increased by cryptocurrency scams - more scammers are seeking payment with cryptocurrency and losses to this payment method increased 216% to $84 million.
- $227 million lost to payment redirection scams.
- $142 million lost to romance scams.

Protecting yourself from scams

- Help educate older relatives. The over 55s are the most likely to fall victim to a scam.
- Always use the primary website or app of your suppliers not a link from a text or email.
- Don't click on links from emails or text messages unless you are (absolutely) certain of the source. For email, if the sending email domain is not clear or hidden, hover over the name of the sending account to check if the email is from the company domain.
- For Government services, use your MyGov account. Any messages to you from the ATO or other Government services need will be published to your MyGov account. Never click on links purporting to be from a bank, ATO or Government department.

Protecting your business from scams

Payment redirection scams, where the email of the business is compromised, caused the highest reported level of loss for business in 2021 at a combined $227 million.
Payment redirection scams involve scammers impersonating a business or its employees via email and requesting an upcoming payment be redirected to a fraudulent account. In some cases, scammers hack into a legitimate email account and pose as the business, intercepting legitimate invoices and amending the bank details before releasing emails to the unsuspecting business. Other times, scammers impersonate people using a registered email address that is very similar to one from a legitimate business.

- Educate your team about threats and what to look out for, the importance of passwords and password security, and how to manage customer information. Phishing attacks, if successful, provide direct access into your systems.
- Ensure staff only have access to the business systems and information they need. Assess what is required and close out access to anything not required. Also assess how customer personal information is accessed and communicated. Personal information should not be emailed. Email is not secure and it is too easy for staff to inadvertently send data to the wrong person.
- No shared login details or passwords.
- Complete a risk assessment of your systems and add cybersecurity to your risk management framework.
- Develop and implement cyber security policies and protocols. Have policies and procedures in place for who is responsible for cybersecurity, the expectations of staff, and what to do in the event of a breach. Your policies should prevent shadow IT systems, where employees download unauthorised software.
- Understand your organisation's legal obligations. For example, beyond the Privacy Act some businesses considered critical infrastructure such as some freight and food supply operations are subject to the *Security of Critical Infrastructure Act 2018*. This might involve small businesses in the supply chain.
- Use multifactor authentication on your systems and third-party systems.
- Update software and devices regularly for patches
- Back-up data and have backup protocols in place. If hackers use ransomware to lock your systems, you can revert to your backup.
- If customer data is being shared with related or third parties domiciled overseas, ensure your customer is aware of where their data is domiciled and your business has taken all reasonable steps to enforce the Australian Privacy Principles. Your business is responsible for how the overseas recipient utilises your customer's data.

Accountancy Plus apw Whitsunday

p: (07) 4948 4444 www.apws.com.au
Suite 1, Cumberland House, 2 Island Drive, Cannonvale

- Only collect the customer data you need to provide the goods and services you offer.
- Ensure protocols are in place for accounts payable.
- Don't forget the hardware – laptops, computers, phones.

Taxing fame: The ATO's U-turn

Sportspeople, media personalities, celebrities and 'insta' influencers beware. The ATO has taken a U-turn on how fame and image should be taxed.

If you're famous and make an income from your fame and image, the way the ATO believes you should be taxed on the income you make may change under a new draft determination set to take effect on 1 July 2023.

It is not uncommon for celebrities to attempt to transfer the rights to the use of their name, image, likeness, identity, reputation etc., to a related entity such as a company or trust. This related entity then manages these rights, generating income from exploiting their fame and image. For example, where a media personality's image is used on product packaging. One of the aims of arrangements like this is to enable the income to taxed in the entity at a lower rate of tax or to be distributed to related parties who might be subject to lower tax rates.

What will change?

The new draft determination (TD 2022/D3) deals specifically with the *rights* to use a celebrity's fame and image. The ATO's argument is that the individual doesn't have a proprietary right in their fame, which means that attempting to transfer the right relating to their fame to another entity would not be legally effective. That is, you cannot separate the fame from the individual, it vests with the individual regardless of any agreements put in place. As a result, any income relating to an individual's fame or image that is received by a related entity is treated as if it was simply being collected on behalf of the individual and should be taxed in the hands of that individual.

If the related entity isn't deriving income in its own right then it would be much more difficult for the entity to claim a deduction for expenses that it incurs.

The ATO's updated approach doesn't apply to situations where the individual is engaged by a related party to provide services. For example, if a celebrity is booked by a related entity to attend a product launch or promotional event the fees paid by the third party can potentially be treated as income of the related entity for tax purposes. However, in situations like this it is important to consider the potential application of the personal services income rules and the general anti-avoidance rules in Part IVA. The ATO's general position is that income relating to the personal services of an individual should ultimately be taxed in the hands of that individual.

While the ATO's new position will apply retrospectively and to income derived in future, the ATO indicates that a transitional approach will apply if the taxpayer entered into arrangements before 5 October 2022 that were consistent with the safe harbour approach that was set out in PCG 2017/D11. In these cases the ATO's new approach will apply to income derived from 1 July 2023. **-End-**

How high will interest rates go

Low interest rates have been a mainstay since the global financial crisis of 2008. When the pandemic hit, Governments pushed stimulus measures through the economy and central banks reduced interest rates even further. Coming out of COVID, housing market demand was strong and prices boomed but at the same time, supply chains remained restricted and the problems amplified by geo-political tensions increasing input costs. Supply could not keep up with demand to support the recovery, pushing inflation higher and broader than expected for a longer period of time. To control inflation, central banks have responded by tightening monetary policy and lifting interest rates. But the good news is that inflation is likely to ease.

Inflation in the US has started to decrease from a high of over 9% in June 2022 to 7.7% in October, suggesting that interest rates may not rise as high and as aggressively as expected.

Similarly in Australia, the Reserve Bank of Australia (RBA) Board raised the cash rate by 0.25% to 2.60% at its October 2022 meeting, a lower increase than many expected. The lower than expected rise suggests that inflation pressures, particularly wages growth, will be more subdued in Australia than overseas.

Comparatively, Australian households are more sensitive to interest rates with more than 60% of mortgages variable rate loans. This is unlike the US where most borrowers are on 30-year fixed loans.

The increase in interest rates is starting to take effect helping to restore price stability. However, in its

Accountancy Plus apw Whitsunday

p: (07) 4948 4444 www.apws.com.au
Suite 1, Cumberland House, 2 Island Drive, Cannonvale

statement, the RBA said that it will be a challenge to return inflation to 2-3% while at the same time "keeping the economy on an even keel". It concluded the path to achieving this balance is "a narrow one and it is clouded in uncertainty".
In housing, the correction in house prices deepened and broadened across Australia, with capital city prices falling by 1.4% in September 2022, rounding out a 4.3% decline over the third quarter. Housing finance approvals also continued to mirror the broader correction to date, with further declines across investor and owner-occupier loans.
So, where does all of this leave us? Inflation will stay higher for longer than originally anticipated. As a result, interest rates are expected to continue to increase, albeit at a slower rate, with the RBA resetting their view along the journey. Economists are predicting that the cash rate will increase to somewhere between 3.10% and 3.85% in the first half of 2023 and then remain stable until early 2024 before RBA policy pivots and interest rates lower in early 2024.
Canstar analysis suggests that a 3.85% cash rate translates to an average variable rate of 6.73%. The difference between a 5.73% variable rate mortgage and 6.73% is $650 per month on a $1 million, 30 year mortgage. **-End-**

30 November director ID deadline

The deadline for existing directors of Australian companies to obtain a Director Identification Number is 30 November 2022.
All directors of a company, registered Australian body, registered foreign company or Aboriginal and Torres Strait Islander corporation (ATSI) will need a director ID. **This includes directors of a corporate trustee of a self-managed super fund (SMSF).**
A director ID is a 15 digit identification number that, once issued, will remain with that director for life regardless of whether they stop being a director, change companies, change their name, or move overseas.
For those who have been a director since 31 October 2021, the deadline for obtaining a director ID is 30 November 2022 unless you are a director of an Aboriginal and Torres Strait Islander corporation, then the deadline is 30 November 2023.

For overseas directors, the process to obtain a director ID can be onerous as applications cannot be made online. In addition to the paper application form, you will need copies of one primary and one secondary identity document (or primary identity documents) certified by notaries public or at an Australian embassy. For those who have been invited to become a director but are not a director as yet, if you do not have a director ID, you will need to obtain one prior to being appointed.

You do not need a director ID if you are running a business as a sole trader or partnership, or you are a director in your job title but have not been appointed as a director under the Corporations Act or Corporations (Aboriginal and Torres Strait Islander) Act (CATSI).

Need an extension?

If you need an extension, as soon as possible contact the Australian Business Registry service on 13 62 50 (+61 2 6216 3440 outside of Australia). Your identity will need to be established so have your documentation ready. You can also apply for an extension using the paper form (https://www.abrs.gov.au/sites/default/files/2021-10/Application_for_an_extension_of_time_to_apply_for_a_director_ID.pdf)

What happens if I don't obtain an ID?

If you are required to obtain a director ID but don't, a criminal penalty of up to $13,200 might apply or a civil penalty of up to $1,100,000. Where an individual has deliberately applied for multiple IDs or misrepresented the director ID, the criminal penalty escalates to $26,640 and up to one year in prison.

Quote of the month

"The greatest glory in living lies not in never falling, but in rising every time we fall"
Nelson Mandela