Staff factsheet: cyber incident

This factsheet [provides information that is current as at 25 November 2022.

When did the data breach occur?

- The cyber incident occurred on Thursday 3 November 2022.
- We quickly moved our files to the new, secure SharePoint cloud-based service and not connected to the old networks and systems.
- We know that data which was compromised was stored on a Legal Aid computer or network drive on or before Thursday 3 November 2022.

What kind of information do we keep?

- Name, date of birth, gender, address
- Contact details
- Pay, tax, salary sacrificing (especially for 2021-22 financial year)
- Superannuation membership information
- Bank BSB and Account Number
- Tax File Number
- Photos of passport and/or other ID (licence/birth certificate)
- Legal Aid credit card numbers.

What kind of information do staff sometimes keep?

- Sometimes staff keep personal information on their work computer or network.
- We encourage you to think about the personal information you might have stored including:
  - bank statements, invoices or tax returns
  - medical information such as medical reports or details of your medical team
  - password lists for work or home
  - email addresses of family and friends
  - personal correspondence such as letters to your child's school
  - photos taken at private or social events such as birthday celebrations

Warnings and recommended precautionary steps

Passwords

- If you have used a password at work that is also used on personal accounts, such as your banking or myGov, you should change them as soon as possible.
- If you use a password that includes things such as your date of birth or name, you should change it.
- Set up two-factor authentication (2FA) and review account settings to confirm that no unauthorised changes to login details have been made.
- Review these accounts to confirm that your contact details are correct and have not been changed.

Tax File Number (TFN)

- **Complete this step as soon as possible if your TFN has been stolen.**
- Your TFN, in combination with other forms of ID that have been accessed, can be used to set up financial services in your name, including buy-now-pay-later credit services.
- If you think your TFN was stolen, you should inform the Australian Taxation Office (ATO) by calling the client identity support line on 1800 467 033.
- This process generally takes about half an hour.
- You will be connected to a service representative who can confirm whether there have been recent attempts to use your TFN, assist in setting up additional security measures, and place a flag on your account against any future suspicious activity.
- When you call, wait for the automated messages to finish
- You will be prompted to enter your TFN and date of birth.
- Following this, you will be prompted to set up a voice verification service.
- Once this has been completed, listen to the options and press 3.
- Then, press 3 again in the next menu.

Bank details

- It is unlikely that your bank account can be accessed or compromised with the information that was part of the hack unless you had stored your password on a work computer.
- There is a slight risk that a direct debit could be set up by the cyber criminals.
- Monitor card and account statements to note any unauthorised transactions.
- Notify your bank of the breach as they will flag your account and suggest safety precautions.

Driver's licence

- If you believe you had stored a copy of your driver's licence on a work computer/in work files, you can seek to get it replaced.
- Access Canberra will replace a driver's licence for $42.60; this will not change your licence number but will change the card number.
- To pass a Document Verification Service (DVS) check, a scammer would need both the licence and card numbers.
- More information about replacing an ACT driver licence is available here.

Credit/Identity fraud

- Your credit reports provide a means to assess whether someone has attempted to obtain credit in your name.
- It is important to obtain your credit report from all three agencies (Equifax, illion and Experian) as some may gather credit information others have missed.
- In Australia, you can obtain a free credit report every three months, or more often if you have been refused credit within the last 90 days, or your credit-related personal information has been corrected.
- To apply for your credit reports, please see IDCARE's Fact Sheet on Credit Reports Australia.
- Where you think someone has attempted to access credit in your name, you can apply for a credit ban to 'freeze' access to your credit file without your written consent.

Phishing

- You may see an increase in targeted phishing attempts via email, text messaging or telephone calls, where the scammer uses details specific to you that might have been lost in the cyber incident (such as your full name, date of birth, phone number, or pay/tax amounts).
- Never click on links in unsolicited or unexpected emails or text messages, no matter how legitimate they appear.
- Do not be pressured to respond, whether it is by email, text message or telephone.
- Instead, contact the organisation sending the message directly using contact details you know to be correct.
- These phishing attempts may 'spoof' or falsify their caller ID/sender email in order to appear more legitimate.
- Unless you were expecting a call, you should independently verify who you are speaking to with details other than the ones listed above.
- Some scammers will spoof your phone number in order to call other people – this does not charge your account (they only steal the 'appearance' of your number) but may lead to return calls or messages from other people accusing you of scamming or spamming them.
- Unfortunately, if your number is being used to call others, IDCARE advises there is little that can be done – advise your telco and they may have assistance, otherwise generally the use of the number will decrease within one to two weeks.

Basic ongoing precautions

- Do not open suspicious emails or text messages – when in outlook flag using the 'Report Phishing' or 'Junk Email' buttons and delete them.
- Install and update anti-virus software on personal devices.
- Use secure, unique, passwords which are hard to guess for each service you log in to.
- Review your existing accounts, particularly for financial institutions and myGov, to check for unauthorised changes or logins.
- Be cautious on social media and limit the amount of personal information you make publicly available online.

Where to go for more advice

- If you think that one of your personal accounts has been compromised or wish to seek more advice regarding how to mitigate risks of identity theft and fraud, there are some services available to help.

IDCARE

- LAACT has partnered with IDCARE, Australia's national identity and cyber support community service.
- They have expert case managers who can work with you in addressing concerns in relation to personal information risks and any instances where you think your information has been misused.
- This is a free service for our staff - IDCARE's services are at no cost to you.
- If you wish to speak with one of their expert Case Managers please complete an online 'Get Help' form at www.idcare.org or call 1800 595160.
- IDCARE specialist case managers are available from 8am-6pm AEDT Monday to Friday excluding public holidays.
- When engaging IDCARE, **please use the referral code LAC22** to get prioritised help.
- IDCARE also provides a range of factsheets online which are accessible at-will, and provide some information about topics including credit reporting, identity fraud, scam prevention, social media, and device security.

ATO identity theft support

- The ATO can provide a range of actions where you believe your tax information, ATO online services, myGov, and myGovID has been misused or inappropriately accessed.
- Their website provides further information about different services that should be called depending on what you think has occurred.

Employee support

- Employees are able to access psychological support via our Employee Assistance Provider, Benestar (1300 360 364).
- Alternatively groups may seek to speak with Elise Wald from the Cairnmiller Institute (debriefing services).
- Information for both of these services is available on our Health & Safety Boards around the Commission.
- Where employees are experiencing unreasonable financial impacts as a result of this please speak with the HR team.