FLETCHER INTERNATIONAL EXPORTS PTY LTD

ABN 64 003 213 652 ACN 003 213 652
Lot 11 Yarrandale Road, Dubbo, NSW 2830
Locked Bag 10 DUBBO NSW 2830 AUSTRALIA
Telephone: +61 2 6801 3100
Main Office Fax: +61 2 6884 2965
Export Office Fax: +61 2 6884 6566
Email: mailbox@fletchint.com.au

17 May 2023

Fletcher International Exports (**FIE**) recently experienced a cyber security incident where an unidentified third-party gained unauthorised access to an area of its I.T. environment.

Upon discovery of the incident, FIE immediately engaged external cyber security and IT forensics experts to secure its digital infrastructure and to conduct an investigation into what occurred, including determining if any personal information was involved.

The investigation is now complete, and it has identified that a small set of data was downloaded by the unknown third-party during the incident.

FIE has no evidence to suggest any of this information has been or will be misused. However, we are notifying our clients and current and former employees so they may take some proactive steps detailed below to protect their information as a precautionary measure.

FIE has identified that there some individuals who it is unable to contact directly, either due to invalid contact details or the absence of contact details. For this reason, it is publishing this statement for any individuals who may be concerned that their information was involved.

FIE takes cyber security and the protection of information very seriously. In response to the incident, we have rebuilt a number of key systems and implemented heightened security measures to mitigate the risk of recurrence.

We have also reported the incident to the relevant authorities including the Australian Cyber Security Centre and the Office of the Australian Information Commissioner.

If you have any concerns about the incident, there are steps that you can take to protect yourself and your information, and advice regarding these protection measures is detailed below.

FIE sincerely apologises that this has happened and is committed to supporting individuals who may be affected by this incident. If you have any queries, please contact our dedicated inbound support team on assistance@fletchint.com.au.

Steps you can take to protect yourself from potential data misuse

Questions and Answers

Q: What information was affected?

A: The following personal information was contained within the affected dataset:

- Contact information (name, email address, phone number)
- Driver licence number/card number (number only, not card copy)
- Tax File Number (**TFN**)

Q: Why did FIE have this personal information?

A: Regulations in Australia require us to retain certain employee data for a specific period of time depending on the employment type. Beyond that required period of time, we take the utmost care in deleting any data that we are no longer required to hold.

Q: What precautionary steps do you recommend?

A: Based on the types of information that may have been accessed, we recommend that you take the following proactive steps (depending on the types of information you have previously provided to FIE):

Contact information

Where a third party may have accessed your information, it is important to:

- Be aware of email, telephone and text-based scams. Do not share your personal information with anyone unless you are confident about who you are sharing it with.
- When on a webpage asking for your login credentials, take note of the web address or URL ('Uniform Resource Locator'). The URL is located in the address bar of your web browser and typically starts with https://.
- If you are suspicious of the URL, do not provide your login details. Contact the entity through the usual channels to ensure you are logging into the correct web page. Please note that FIE will never contact you to ask for your username or password.
- Enable multi-factor authentication for your online accounts where possible, including your email, banking, and social media accounts.
- Ensure you have up-to-date anti-virus software installed on any device you use to access your online accounts.
- Read the Australian Competition and Consumer Commission's Scamwatch guidance for protecting yourself from scams here: https://www.scamwatch.gov.au/get-help/protect-yourself-from-scams/.
- For more information, read the OAIC's tips for further guidance about protecting your identity: https://www.oaic.gov.au/privacy/your-privacy-rights/tips-to-protect-your-privacy/.

Driver licence number

The affected dataset included some employee driver licence numbers (only the number, not a photocopy).

Any unauthorised access to a driver licence number does not affect its validity, and it can still be used for its intended purpose, including as a valid form of proof of identity.

As a precautionary measure, we recommend anyone whose driver licence may have been accessed by an unauthorised third-party review and continue monitor their consumer credit report for any discrepancies or unusual activity. Information about obtaining a credit report or credit ban is provided towards the end of this notification statement.

Affected individuals may wish to consider the impact of replacing a driver licence, as this may prevent it from being used as a form of ID or for obtaining credit for legitimate purposes. Please consider this advice and your own circumstances before deciding to replace your ID.

Tax File Number

Some employee TFNs were included in the affected dataset.

We have informed the Australian Taxation Office (**ATO**) of all the affected TFNs. The ATO has set up monitoring and applied protective measures for these TFNs to prevent them from being misused. As a result, we consider the risk associated with this information to be low.

There is nothing further you need to do, however, affected individuals may wish to contact the ATO directly via telephone on **1800 467 033** (available 8am to 6pm AEDT, Monday to Friday).

For more information, visit the ATO website.[1]

Q: I think I need a credit report or ban, where can I go to get one?

A: You can apply for an annual free credit report from one of the consumer Credit Reporting Agencies below.

You can also consider contacting the below credit reporting bodies to place a temporary ban on your credit report. This means that they will not be able to share your credit report with credit providers without your consent for 21 days (unless extended).

Name	Website
Equifax	https://www.equifax.com.au/personal/products/credit-and-identity-products
Illion	https://www.creditcheck.illion.com.au/
Experian	http://www.experian.com.au/consumer-reports

1 Please see: https://www.ato.gov.au/general/online-services/identity-security-and-scams/Help-for-identity-theft/Data-breach-guidance-for-individuals.

Q: How do I determine whether I am impacted by this incident?

A: Please contact the FIE support team on assistance@fletchint.com.au. The support team will be able to confirm whether you are impacted by the incident, and if so, what steps you can take to protect yourself against any harm.

Q: Who can I contact for more information about cyber security and protecting my online identity?

A: Additional general resources on identity protection and cyber security can be found here:

- https://www.oaic.gov.au/privacy/data-breaches/data-breach-support-and-resources/
- https://www.idcare.org/

If you have any other questions after reviewing this notification, please contact the FIE support team on assistance@fletchint.com.au.