WEBSITE NOTICE

NOTIFICATION OF SUSPECTED DATA BREACH

Smith Channon & Co (**Smith Channon**), was recently the subject of a cyber attack which resulted in a data breach of electronically stored information.

At Smith Channon we take privacy and security seriously. We set out below details of the breach and what we have done and what we are doing to safeguard any information we hold.

As part of the preliminary investigation into the suspected data breach, we have identified that some of your information held on the Smith Channon data base may have been accessed by an unauthorised party.

What information do we hold?

As part of our business we hold customer's shipping documents and other information in respect of the importation of goods into Australia. Any information sent via email including customer email addresses and other contact details are also held within our system.

What we have discovered and done to date

As soon as Smith Channon became aware of the nature of the suspected data breach, it took immediate steps to mitigate the breach, commenced an investigation to determine the information which may have been accessed and how the data breach occurred, and is notifying individuals and companies who may be at risk of harm from the data breach.

Our investigations to date have shown that email addresses of customers sorted on our systems have been used in phishing attempts.

On 19 November 2020, the email account of an employee in the Smith Channon business was breached causing a phishing email to be sent on behalf of the employee to email addresses internal and external to the wider business. Steps were taken to contain the suspected data breach on that date.

In the belief that the suspected data breach had been contained, the employee's email account was reactivated on 1 December 2020. However, the employee and other employee's email accounts were subsequently used to send further phishing emails to email addresses internal and external to wider business. The suspected data breach was identified on 1 December 2020 and a further investigation was commenced on behalf of Smith Channon, in collaboration with the business' support teams including the IT and legal teams.

Smith Channon is continuing its investigation to determine how the suspected data breach occurred with the aim to prevent reoccurrence and understand whether any data has been compromised.

Recommended steps to reduce the risk of harm

Smith Channon recommends that individuals who received the phishing email takes the following steps to reduce the likelihood of serious harm occurring:

1. reset access passwords, and where possible, activate Multi-Factor Authentication; some websites which may assist include:

   https://www.cyber.gov.au/acsc/view-all-content/advice/multi-factor-authentication
   https://www.cyber.gov.au/acsc/individuals-and-families
   https://www.cyber.gov.au/acsc/small-and-medium-businesses
   https://www.cyber.gov.au/acsc/large-organisations-and-infrastructure

2. monitor inbound and outbound emails of work and personal email addresses for unusual activity;
3. monitor bank accounts for suspicious transactions; and
4. be vigilant for any unusual contact from unknown individuals or entities requesting information.

WHAT YOU SHOULD NOT DO

DO NOT reply to suspicious mails from Smith Channon, including emails that ask you to click on a link or provide information.

DO NOT open attachments to any of our emails.

While we work on our investigation, please call Smith Channon if you receive an email asking you to provide banking or other details, or to open any suspicious attachment on our privacy hotline:

Martin Bourn – contact number (08) 8447 1011

You may also call your usual Smith Channon contact to verify any email, but DO NOT use the contact details within the suspicious email. Only use a means of contact that you can independently verify.

It is unlikely that we will change our banking or contact details. If you receive an email providing details of new bank or contact details, DO NOT action it but call us immediately on the number above.

Next steps

Our investigations are ongoing, and we are yet to determine whether this information is an eligible data breach under the *Privacy Act* 1988 (Cth).

Further contacts

Please feel free to contact us with any questions via our dedicated privacy contact:

Claire Robertson – General Counsel and Company Secretary

companysecretary@linxcc.com.au

Smith Channon is part of the LINX Cargo Care Group whose Privacy Policy can be found at https://linxcc.com.au/privacy-policy/

Additional information can be found on the website of the Office of the Australian Information Commissioner (OAIC) at www.oaic.gov.au

Additional information in respect of cyber security breaches can be found at - Australian CyberSecurity Centre at https://www.cyber.gov.au