HOUSE OF REPRESENTATIVES STANDING COMMITTEE ON ECONOMICS

REVIEW OF THE FOUR MAJOR BANKS AND OTHER FINANCIAL INSTITUTIONS

NAB

NAB67QW:

In July 2019, NAB contacted 13,000 customers about a data breach that had compromised their personal information. (NAB Media release - 'NAB Apologises to customers for data breach', 26 July 2019)
Regarding this data breach:

(a) Which two data companies received the unauthorised data transfer?

NAB elected not to publicly disclose the names of the website services companies after consulting with three cyber-intelligence consultants, the Australian Cyber Security Centre (ACSC) and the Office of the Australian Information Commissioner (OAIC). The names of the websites were provided on a confidential basis to the OAIC and to the ACSC.

We note that the organisations running these websites, offering simple data ordering tools and related services, did not solicit the data that was uploaded by one of NAB's technology personnel (in breach of their training and NAB's policies). The data was uploaded in order to make use of a simple data tool.

NAB's cyber team investigated whether the organisations or individuals connected with the publicly available simple data tool websites were involved or in any way connected with data harvesting or other nefarious activities. NAB also engaged three independent cyber-intelligence consultants specialising in cybercrime to investigate the background of the two websites and the individuals connected with them. No evidence connecting these websites to data harvesting, cyber-hacking or other nefarious activity was identified.

(b) Does NAB expect recipients of its customers' data to have their own protocols for ensuring any transfer has been authorised?

Authorised third parties are subject to a comprehensive information security risk assessment that reviews and assesses the service, information assets involved, method of transfer, controls in place to protect the NAB Group and its information including contractual, technical, assurance, business continuity, governance and fourth-party controls, of which is documented in a contractual agreement.

More specifically, formal processes for the management of information security incidents include prompt notification to NAB Group of any event with the potential to impact confidentiality, integrity, or availability of information/systems provided for or stored on behalf of the NAB Group.

As noted above, the two companies that received the data were not service providers procured by NAB. The (now former) NAB technology employee uploaded the data in breach of their training and NAB's policies in order to make use of simple data ordering tools available on the websites. NAB took the steps referred to in (a) above to assess the legitimacy of the companies and, following this process, NAB reached out to both companies to advise them of the uploads. Both companies were co-operative with NAB once advised of the incident and provided promptly confirmed and then later provided attestations that:

- the data was permanently and irreversibly deleted,

- had not be copied or accessed by any of their personnel, and
- was not forwarded, accessed by or otherwise made available to any other parties.

(c) Did NAB locate the failing, either within NAB itself or the data service companies, that allowed this unauthorised transfer to proceed?

The unauthorised upload was detected and triggered alerts in NAB systems, and an investigation into the event was immediately commenced.

(d) How did the unauthorised transfer proceed?

The unauthorised upload was the action of one of NAB's technology personnel. The action was in breach of their training and various NAB policies including those related to data security and the prohibition of transfers of NAB data to unauthorised third parties. The uploads were detected by NAB systems and raised an event. An investigation into the event was immediately commenced.

At the time of the event, there were insufficient technical controls in place to prevent transfers of this nature. NAB has uplifted these controls to prevent a similar event occurring in the future.

(e) NAB's media release on this matter noted the customers' information was uploaded without authorisation to the servers of the two data service companies. Please outline the normal authorisation path NAB follows for such transfers.

As noted above, this event was an unauthorised transfer of information to the unapproved third-party operators of data service websites and by unauthorised means.

NAB has robust processes, vetting and procedures that need to be completed before a third-party service provider can be appointed. NAB also has multiple approved and secure methods in place for authorised transfers of information to approved third parties as part of the Group Information Risk Policy including encryption, secure portals, email, and collaboration tools. The use of these tools would vary subject to the nature of the agreement with the third party, the type and frequency of information shared.

(f) Does NAB still use the data services of the two companies involved in the breach?

The two companies involved in the breach were not service providers at the time of the breach and are not currently third-party service providers.

(g) Are the NAB staff involved in the breach still employed by NAB?

An assessment of the employee's conduct in breach of their training and NAB policies was conducted. After conducting a procedurally fair process, the individual's employment contract was terminated.

(h) Have data sharing protocols been changed as a result of this incident?

Technical blocks have been implemented to prevent the unauthorised transfers of this nature to third parties.

In the days following detection of the event, several internal communications were released to raise awareness and to reiterate NAB's policies together with a mandatory, enterprise-wide online training module.

(i) How has NAB guaranteed this kind of unauthorised transfer cannot happen again?

NAB lawfully and appropriately monitors employee and contractor access and use of NAB's systems. NAB has uplifted technical controls to prevent similar transfers/uploads of NAB data to unauthorised recipients in the future. Additional controls have been implemented including blocking access to websites to prevent unauthorised uploads of this nature and blocking email externally in certain circumstances. NAB has also increased monitoring on these channels. Mandatory training and awareness regarding data security is ongoing.