FINANCIAL REVIEW

Computers
**Banks told to tighten data security**

Lucas Baird
599 words
27 August 2019
The Australian Financial Review
AFNR
First
20
English


New Payments Platform Australia, the real-time system owned by the big four banks and 11 other financial institutions, is under pressure to explain how almost 100,000 customers' personal details were accessed as part of its second data breach in three months.

Payments provider Cuscal confirmed on Sunday that hackers had accessed the PayID details of about 92,000 customers through its credit union client CUA.

Cuscal said this represented 3 per cent of the 3.5 million registered PayIDs, which are phone numbers, email addresses or ABNs connected to bank accounts.

The attack is the second breach of the PayID system since June and has experts asking why extra protections were not in place to prevent it from happening again.

Edith Cowan University associate dean (computer and security) Paul Haskell-Dowland said the most recent incident was identical to the previous hack of Westpac Banking Corporation.

In that event, scammers compromised 98,000 PayIDs with 600,000 PayID lookups over six weeks.

Dr Haskell-Dowland said that, although bad actors were not able to directly access bank accounts with the details obtained, it provided the seed of a broader scam incident.

"You've got the potential for what we call a phishing attack," he said. "They've now got means of contacting customers, their BSB and account numbers, and be able to quote individual information."

With this information, scammers could contact customers with enough authenticity to convince others that they are actually from the bank and trick them into handing over more sensitive information.

Dr Haskell-Dowland said even simple measures - such as a limit on the number of lookups an individual can make or an artificial intelligence algorithm that identifies searching patterns - should have been in place.

"Those protections should have been in place since the beginning or at least after the June breach," he said. "That prior incident should have caused a complete review of the system."

NPPA chief executive Adrian Lovney said the body had taken steps to increase its cyber security since June. "We recently commenced implementation of more targeted cyber security requirements upon participating institutions," he said.

The most recent breach came through CUA's systems, although several other institutions using the NPP, including the big four banks, were affected.

"CUA has worked closely with our NPP payment industry providers, NPPA and Cuscal to enable notification of affected individuals," a CUA spokeswoman said. "Information security is obviously of paramount importance. We are deeply disappointed this occurred and apologise to those affected."

The NPP is an industry-led initiative to standardise real-time payments between bank accounts, with the New Payments Platform Australia body governing its rollout.

Westpac, while also the centre of the first PayID breach, has been hit by the second breach, which occurred on August 16.

The bank has warned its customers to be wary of SMS phishing attempts, personalised messages that looks like a legitimate message from Westpac or another bank.

However, it said no customers from its subsidiaries Bank of Melbourne, St George, and BankSA were affected.

Westpac, along with the other big four banks, would not confirm how many of its customers had been affected by the breach.

The National Australia Bank, however, did say it has now put an extra layer of fraud detection and security controls in place to protect its customers.

"NAB has contacted impacted customers following the data breach event at another Australian financial institution, which exposed PayID details registered to customers from a number of banks, including some NAB customers," a spokesman said.

Document AFNR000020190826ef8r00022

 