Australians Hold Fall Conference in Sydney

NZ Targeted in Credit Card Scam

ACREDIT CARD SCAM WAS uncovered in November when authorities realized that a group of people reporting unauthorized charges on their credit cards had one point of purchase in common – a parking lot in Auckland, New Zealand. The 1970-space Downtown parking lot is owned and operated by the Auckland City Council.

Authorities suspect that the fraud was perpetrated by hacking into the Auckland parking lot's automated parking payment machines, exposing the credit card data to the thieves who then replicated the cards. The investigation is ongoing, and specific details have not been released to the public yet.

Craig Dowling, Media Relations Manager, Westpac New Zealand, says that his bank took the lead role in investigating how the card compromise may have occurred, since they are the acquiring bank for Auckland City Council. However, Dowling clarifies that actual cards impacted were spread across all credit card issuers.

"On our part, we have been taking instruction from the bank as to how to eliminate the risk of further fraud," says Dale Clements, Group Manager Parking, Transport, Auckland City Council. "To this end, as soon as were asked, we removed the credit card facility from our automatic payment machines at the Downtown car park, and as a precaution at our other three CBD car parks."

"Customers can still pay by credit card at the staffed kiosks using secure EFTPOS terminals," adds Clements. "The council is also now looking at options for updating the card acceptance systems across all car parks."

The total cost of the incident has not been disclosed. Affected banks expect that more than 100,000 credit cards will have to be replaced due to the scam.

"Ultimate accountability has yet to be determined," Dowling says. "Most importantly, no cardholders will face losses as they are protected from such scams by their general terms and conditions of card use and also by reference to the New Zealand Bankers' Association Code of Banking Practice."

"I can point out, from Westpac New Zealand's perspective, that many attempts at actually committing fraud on specific cardholder accounts were thwarted by bank security and fraud detection systems – the same systems that identified the common point of use of the initial fraud attempts," he adds. "The greater cost has probably been borne through the reissuing by card issuers of a large number of cards to stop the attempted use of the misappropriated details."

The Role of PCI DSS

The PCI DSS standards are in place to help merchants protect cardholder data, however, it is still unclear whether the Downtown parking lot's credit card payment system was PCI DSS compliant.

PCI DSS is a set of standards for payment account data security implemented by the PCI Security Standards Council, which includes American Express, Discover, JCB International, MasterCard and Visa. The purpose of PCI DSS is to minimize external and internal data breaches or hacker access. The standards apply to all merchants who store credit card data in any format, or have access to credit card details, or have systems which enable internet access to their company by the public.

"Originally this standard for credit card security was restricted to the USA but has become a worldwide issue during the past few years," says Gerhard Daxer, Product Manager for Car Access, Skidata.

Requirements of PCI DSS include building and maintaining a secure network by deploying a firewall to protect stored cardholder data; avoidance of vendor-supplied defaults for system passwords and other security parameters; encryption of transmissions of cardholder data across open, public networks; use of updated anti-virus software; restricting access to cardholder data by business need-to-know; and minimizing physical access to cardholder data.

Dowling of Westpac would not comment on whether the Auckland Downtown car park was compliant with PCI DSS, citing that this issue could not be discussed while still under investigation. The Council has made no comment on PCI DSS compliancy either.

Counting on Vendor Security

The security of the actual parking management system or automated parking payment system may be the key to avoiding incidents like the credit card scam at the Auckland car park.

"From my point of view, the highest fraud risk comes from parking systems that are not up-to-date from a technological point of view," explains Daxer.

"We have the absolute duty to offer our customers secure and technologically up-to-date parking systems," he continues. "This is indispensable nowadays – and it is also a matter of investment protection for our customers. But of course our customers, the parking operators, have to make their contributions for security as well."

In terms of PCI DSS, Daxer says that SKIDATA has validated its parking system software since the very beginning of the CISP/PCI standard, which was founded in 2000. According to Daxer, SKIDATA's next software release will be compliant to the latest and strongest regulations for payment applications, which is Payment Application Data Security Standard (PA-DSS) V1.2.

"I do not want to praise PCI to be a kind of universal remedy, but it makes life more secure for credit card users, that's for sure," says Daxer.

"A few words to the worldwide PCI rollout these days: the major card issuers – VISA , Mastercard, Amex, etc. – and the acquiring banks are currently adding 'PCI compliancy' to their merchant contracts," Daxer points out. "With these contract extensions, a shift of liability to the parking operators will take place. This means that the parking operators will be liable to have PCI compliant systems and a whole PCI compliant environment."

"So it is not just a matter of having a secure parking system, the parking operator also has to adapt his operational processes and policies concerning security," he continues. "In my opinion this an important fact that has to be accepted by every party concerned."

"And everyone has to be aware that the bad guys in this world have become very technology oriented, intelligent and fast," Daxer concludes, "so it is very important and vital for system suppliers and parking operators to be one step ahead."

PW