

August 23, 2007

Protect your business against card 'skimming'

VANCOUVER: Last week's debit card breach at Park Royal Shopping Centre gave a stark reminder to businesses to be proactive in protecting themselves and their customers from fraud. That is why the Better Business Bureau of Mainland BC and the BC Crime Prevention Association are combining their efforts to give companies practical tips on how to enhance their security and how to handle information breaches.

"We all want shopping to be a safe and convenient experience for everyone,"

says BBB president Lynda Pasacreta, "but, to maintain consumer trust, businesses have to make it their focus to train and educate staff and find unique solutions to prevent frauds."

A common debit scheme is called: 'card skimming.' This involves the unauthorized copying of electronic data from your debit card. Hidden equipment, such as pin-hole cameras and card reading devices, are installed to obtain your PIN and card data, and the stolen data is then encoded onto a counterfeit card, which is used to withdraw funds without your knowledge

(source: Interac website)

"It has always made good sense for business managers and supervisors to conduct a regular walkabout of their premises to ensure all equipment is in working order" adds Valerie MacLean, Executive Director, BC Crime Prevention Association "but with the growing reports of debit card PIN pad substitutions, stronger theft deterrence measures may be required."

Here are some tips for businesses to think about to enhance their workplace's security:

1. Strike a sensible balance between the desire to offer customer convenience through moveable debit card PIN pads (on accordion cables) and the requirement to prevent removal, exchange or interference with such pads by fraudsters
2. Consider securing PIN pad terminals to metal posts and brackets to the counter but ensure that shields are installed around the terminal to facilitate customer privacy during the PIN entering phase
3. Add business name stickers to the PIN pad in a prominent position so that substitutions will be more quickly discovered
4. Train staff to be on the alert for fraudsters using a shoplifting distraction technique when during an unguarded moment the legitimate terminal is unplugged and replaced by a trojan-style terminal
5. Train staff to report to management if they notice any physical changes in the architecture of PIN pad terminals. Staff should immediately shut down payment processing until the merchant payment processor is contacted
6. Ensure surveillance cameras are trained on the Point of Sale area to record suspicious activity

If a company has had an information breach they have a legal responsibility to make "reasonable security arrangements" to protect customer data under Personal Information Protection Act (PIPA) and Payment Card Industry Data Standard (PCIDS).

The BC Information and Privacy Commissioner has recently released guidelines for businesses to follow if there has been a security breach involving personal information. These guidelines outline some of the key steps in responding to the breach. Included in these voluntary guidelines is information on what should be included in a notification and a recommendation to contact the privacy commissioner in BC if there is a breach.

You can access a copy of these guidelines at privcom.gc.ca. To contact the privacy commissioner in BC, contact the Office of the Information & Privacy Commissioner at oipc.bc.ca

For more information on how to prevent debit fraud, contact your Better Business Bureau of Mainland BC (1-888-803-1222 or bbbvan.org) or BC Crime Prevention (bccpa.org or 1-888-405-2288).