

FRAUDULENT DEBIT CARD TERMINALS HURT BUSINESSES AND CUSTOMERS

Burnaby, April 12 2007:

BC Crime Prevention Association offers tips for debit card users and businesses to prevent debit card fraud and to alert their financial institutions when unauthorized transactions have occurred.

The recent debit card fraud at North Delta's Scottsdale Centre highlights the inevitable consequence of the increased popularity of debit card usage in Canada - the risk that fraudsters will find new ways to exploit this method of payment. In the Delta incident a Point of Sale (POS) keypad at a Mall merchant was tampered with and modified to record customer account information from the magnetic stripe as well as the PIN.

"Customers are helpless in these situations" comments BC Crime Prevention Association Executive Director, Valerie MacLean "because the PIN pad looks normal from the outside so they have no reason to suspect that anything is wrong. Even protecting their PIN will make no difference!" She adds: "unauthorized transactions can have unexpected consequences for consumers including bounced cheques and pre-authorized payments that cannot be processed."

The Association offers the following advice for debit card users:

1. Do not use the terminal if there are obvious signs of tampering (reassembled with screws instead of factory rivets or wires showing through ventilation grilles/slots)
2. Keep track of all purchases by saving transaction receipts as this information will be valuable to bank follow-up investigations
3. Reduce the size of losses by establishing a limit on the amount that can be withdrawn at an ATM (consult your bank to set this up)
4. Check your account balance frequently using any of the following options:
 - telephone or online access to your bank account
 - note the balance after making an ATM deposit or withdrawal and retain the receipt
 - consider commercial software that will immediately alert you via e-mail or cellphone/PDA text message about all new transactions (authorized and unauthorized)
5. Notify your financial institution immediately if you discover unauthorized transactions. In most cases of debit card fraud, consumers will be reimbursed by the financial institution for any money lost.
6. Regardless of whether or not the PIN pad has been tampered with, ALWAYS shield your PIN

The burden of responsibility shifts towards retail merchants in cases where POS terminals have been switched or tampered with. Jeff Burton, Crime Shield Co-Coordinator for BC Crime prevention Association, points out that the Association has always encouraged consumers to be alert for alterations made to ATM architecture such as overlays, skimming devices and pinhole cameras. "It is equally important", says Burton, "that businesses be proactive in noting changes to fixtures and electronic devices. As part of their daily inspections of premises staff should be checking not only for substituted or tampered POS PIN pads but also for keystroke logging devices and any other covert devices that would compromise customer information." Although it would not prevent removal, substitution of PIN pads could be thwarted by securing them to a counter with the right hardware.

The BC Crime Prevention Association points out that retail merchants who provide the customer convenience of paying by debit card are obligated under British Columbia's Personal *Information Protection Act* (2004) to protect data collected from these cards and take reasonable precautions to prevent unauthorized access to such stored information.

Consumers wishing to learn more about their responsibilities with respect to debit card use can refer to the *Canadian Code of Practice for Consumer Debit Card Services*

(http://www.fcac-acfc.gc.ca/eng/industry/RefDocs/DebitCardCode/DebitCardCode_e.asp)

- 30 -

Media Contacts:

Valerie MacLean

Executive Director

BC Crime Prevention Association

604-291-9959 Ext. 226

v.maclea@bccpa.org

Jeff Burton

Crime Shield Co-Coordinator

BC Crime Prevention Association

604-291-9959

j.burton@bccpa.org