Information Bulletin

Point of Sale Terminal Fraud

Since early April 2013, the “E” Division RCMP Federal Serious and Organized Crime Section - Integrated Counterfeit Enforcement Team have noted an increase in an emerging trend involving fraudulent point of sale terminal (pin pad) refunds occurring at various retail businesses throughout the Lower Mainland and on Vancouver Island in British Columbia. We have seen both hardwired and wireless Point of Sale (POS) units being targeted. The refunds far exceed the normal transactions that would be processed at that particular business and it appears all the fraudulent refunds are being put through via debit card.

How the fraud is committed:

The suspect(s) enters a business and selects something to buy at the business and when they are handed the retailer POS terminal, they insert their card (as if using for payment) but instead they use the standard merchant security password to override the system and refund cash into their account. The amounts vary from $500 to $999. Suspects then immediately go to a financial institution and withdraw the funds from their accounts to which the money was refunded.

This issue can be prevented by having the business merchant change their standard security password on their POS machine and by making it a regular practice to change the standard password often.

PreventionTips:

- Always change the refund code of the POS when one is received.
- Never keep the refund code out in the open where everyone can see it.
- Only authorized staff should know the refund code.
- The refund code should be changed regularly, especially when key staff leaves the business.
- To reduce losses if fraud occurs, the merchant can ask his acquirer to limit the refund parameters of the POS.
- Do not leave the wireless POS terminal unattended (suspects are swapping the business wireless POS terminal with a dummy POS terminal and then conducting refunds using the stolen wireless POS terminal)