New Crime Trend: Point of Sale Credit Card Fraud

Thursday, September-27-18
Prepared by: Watson, Scott

Key Points:

- Several frauds have occurred in Grande Prairie where offenders use admin cards for the debit/credit terminals to alter transactions at the point of sale.
- Offenders can make fraudulent purchases worth thousands of dollars at retail businesses.
- Some businesses do not know they have been victimized until months after the crime occurred.
- Credit cards do not need to be physically presented so card owners may not know their card numbers have been used for fraudulent purchases.

Background:

A new trend in credit card fraud has recently emerged in Grande Prairie. However, similar occurrences have been reported in Edmonton, Kelowna, Morniville, Winnipeg, St. Albert, and Calgary. The MO for this crime is that the offenders will use a point of sale "admin" card from Moneris Debit and Credit Processing (Moneris is a company that maintains debit/credit machines and facilitates transactions from businesses to credit card companies) to alter the transaction at the debit/credit terminal. Admin cards are usually all white (*see photo below)* and issued to businesses to access their debit/credit machine. The cards are useable on other Moneris machines as well, not just the businesses they are associated with. Admin cards allow businesses to process credit card payments without a credit card present (similar to an over the phone transaction), change purchase amounts, or issue refunds.

The offender will present a card for the transaction and will likely say that the card's chip is not working and they must swipe the card. The swiped card will be an Moneris admin card. By swiping an admin card in the machine, the offender can alter the transaction from a point of sale purchase to an over the phone purchase. Then they can then enter a stolen credit card number and the security number from the back of the card instead of using a stolen credit card and pin number to complete the purchase. This transaction would appear as it was a transaction conducted over the phone but would be approved and appear normal on first glance to the employee. This crime can be conducted by 1 offender or by 2-3 offenders working as a group. The other offenders may distract the store employee to draw the employee's attention away so they don't notice that the purchaser is entering 16 digits into the machine instead of only 4 that are required for a pin number.

Another offence may occur where the offender will use the admin card to alter the amount of the purchase to a larger amount and then complete the transaction using a stolen credit card number. The offender would then point out the 'mistake' and have the business refund the over-charged amount to a different card the offender would switch out without the employee noticing. Therefore, the stolen

credit card is billed for the full amount and then the refund is issued onto the offender's personal card. This crime is most often found at locations where the offender leaves a tip such as restaurants, bars, etc.

These transactions may not be flagged as fraud right away and businesses may not know they have been victimized until months later. Another issue is that the offenders only need to steal credit card numbers, not the physical card. Therefore, the card may not be reported stolen as victims may not know someone has stolen their card numbers. Offenders have attempted this crime type but been blocked by the business, or failed to enter the number properly and the transaction doesn't go through. These occurrences are underreported and may be brushed off as unfounded, unsubstantiated, or as suspicious persons call. However, they could be attempted frauds and should be treated as such.

Recommendations:

[redacted]

- Provide the following recommendations to affected businesses:
    - Do not leave PIN pads or point of sale terminals unattended and remain present while transactions are being completed.
    - Insert or swipe the card yourself, don't let the customer do so.
    - Be aware of distractions while transactions are being completed.
    - Be suspicious if the customer appears to be entering a large number of digits during the transaction or is taking an unusually long time to complete the transaction.
    - Examine point of sale transaction receipts and verify how the transaction was processed. Watch for manual entry transactions, refunds, force post or offline transactions.
    - Store your Admin Cards in a safe place and restrict access to them. Report the theft of an Admin Card.
    - Where an admin PIN is used, do not select commonly used or easily guessed PINs like 0000 or 1234.
    - Take notice of the type of card that the customer is attempting to pay with. For instance, a white card may be an Admin Card. *See attached photo below.*

[redacted]

For More Information:

- https://edmonton.ctvnews.ca/jewelry-store-owner-issues-warning-over-alleged-fraud-attempt-1.3523997
- https://globalnews.ca/news/3969385/payment-scam-using-administration-cards-costing-calgary-businesses-thousands/
- http://morinvillenews.com/2017/08/27/rcmp-warn-of-credit-card-fraud-at-local-business/
- https://ca.news.yahoo.com/thieves-creative-defraud-artists-emporium-063000373.html
- http://bc.rcmp-grc.gc.ca/ViewPage.action?siteNodeId=2087&languageId=1&contentId=53319

Photo of Moneris Admin Card: