



Payment Card Crimes

Canadian Financial Institutions reported losses nearly reaching 1 billion dollars in the last 2 years. While Canadian consumers do not suffer direct financial loss, ultimately losses are recouped through increased fees administered by the financial institutions. Additionally, consumers can suffer adverse consequences such as having their account frozen resulting in late payment of bills and subsequently loss of trust in the banking system.

The criminal use of payment cards is divided into the following categories by the Canadian Banking Association (CBA):

- Counterfeit card use: This represents the largest category of credit card fraud, organized criminals have acquired the technology that allows them to "skim" the data contained on magnetic stripes, manufacture phony cards, and overcome such protective features as holograms.
- Cards lost by or stolen from the cardholder: Typically the cards are stolen from the workplace, vehicles, health clubs, golf clubs, etc.
- Fraud committed without the actual use of a card: No-Card Fraud or Card not Present Fraud (CNP)
- Fraud committed on cards not received by the legitimate cardholder (non-receipt fraud): Non-Receipt Fraud where cards are intercepted prior to delivery to the cardholder.
- Cards fraudulently obtained by criminals who have made false applications: Fraudulent Applications involve the criminal impersonation of creditworthy persons in order to acquire credit cards.

Card-Not-Present Fraud

CNP fraud has been identified as one of the fastest growing payment card crime concerns in many parts of the world. In 2011, the CBA identified that CNP fraud accounted for \$259,498,535.00 in losses up 47.35 from 2010.

Card- fraud is defined as the unauthorized and/or fraudulent gathering, trade and use of payment card data, in instances where the card and cardholder are not present.

Email is one of the most unsecure methods to conducting payment card orders. The primary method that the Canadian merchants are being solicited with Card-Not-Present fraud is by email, followed by, ecommerce websites, telephone, facsimile, in person and mail. This means that many Canadian merchants are either not aware of fraud protection protocols or not following them.

The overpayment variant usually involve suspects using compromised credit cards to purchase a product for more than the listing price. Target selection usually occurs online through an auction site or online classified ad. The vendor is then asked to send the extra amount back (e.g. send it to the shipping agent). Consumers and Merchants are often responsible to pay back any funds and may lose the sold merchandise if it has been shipped. (U)

Another variant involves fraudsters purchasing products such as airline tickets using stolen credit card data and then reselling the product by listing it at a discount price, usually through a website or classified ad. Not only do merchants loose the product sold they are often required to pay back the funds to the financial institution.

How to protect yourself

You can minimize the occurrence of fraudulent transactions for your business, so your customers remain confident about conducting online, mail order, and telephone transactions, through safeguards such as the following:

- Prior to shipping merchandise, call the phone number the customer provided and verify the transaction information. Often, fraudsters are unable to verify the information they originally provided, since they order at random and do not keep a record of what they requested.
- Be sensitive to priority shipments for fraud-prone merchandise, which may indicate a fraudulent transaction.
- Be wary of orders from past customers that differ from their usual purchasing patterns.
- Use address verification services and Card Validation Code 2 (CVC 2) services of the credit card network companies (MasterCard and Visa)
- Protect online transactions with MasterCard SecureCode® and Verified by Visa security protocol
- Visa provides a variety of prevention protocols merchants may utilize to prevent card not present fraud at the following links:

<http://usa.visa.com/download/merchants/global-visa-card-not-present-merchant-guide-to-greater-fraud-control.pdf>

http://usa.visa.com/merchants/risk_management/card_not_present.html

If you think you or someone you know has been a victim of fraud, please contact the Canadian Anti-Fraud Centre at 1-888-495-8501 or www.antifraudcentre.ca. FRAUD: Recognize It, Report It, Stop It.