Crime Prevention Week
November 1st to 7th, 2019
Crime Prevention is Everyone's Responsibility

Preventing Credit Card Fraud

~ Protecting Businesses from Costly ChargeBacks

Fraud affects almost every merchant at some point and can represent a considerable cost. Point-of-sale (POS) fraud is a relatively new crime trend involving suspects manipulating a POS terminal in order to complete a fraudulent transaction that results in chargebacks to merchants.

Forced Authorization Fraud

"Force Authorization/Sale' fraud occurs when a customer's (the fraudster's) card is declined and he/she has the merchant perform a "force authorization" to complete the transaction. In a forced authorization, any combination of digits forming the "code" will override the denial.

The fraudster then tells the merchant "this happens all the time" and instruct them to enter a combination of alpha numeric characters or makes a call for an authorization code him/herself.

If the merchant enters the fake authorization code instead of calling the cardholder's issuing bank to obtain a valid code, the transaction will go through. However, the merchant assumes all the risk. If the authorization code is fraudulent and performed by the merchant, they are not be able to file a dispute.

Alternately, the fraudster asks to manually enter their card information into the POS themselves, or distracts the merchant so access to the POS system can be gained manually to alter the transaction where an overpayment is processed. Immediately after the transaction has completed the fraudster will complain about the error and attempt to obtain a cash refund.

Credit Card Skimming

Credit card skimming is a type of credit card fraud where criminals use a small device to steal credit card information in an otherwise legitimate credit or debit card transaction.

When a credit or debit card is swiped through a skimmer, the device captures and stores all the details stored in the card's magnetic stripe. The stripe contains the credit card number, expiration date and the card holder's full name. Thieves can use the stolen data to make fraudulent charges either online or with a counterfeit credit card.

There are several ways a fraudster can manipulate a POS terminal. Merchants can provide general deterrence by taking preventative measures and by being attentive during transactions. Merchants are encouraged to visit their payment provider's website for information about protecting their POS along with proper card acceptance tips.

- Do not leave PIN pads or point of sale terminals unattended and remain present while transactions are being completed.
- Be aware of distractions while transactions are being completed.
- Be suspicious if the customer appears to be entering many 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, forced post or offline transactions.
- Store your Admin Cards in a safe place and control access to them. Report the theft of an Admin Card.
- 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.
- Merchants need to be responsible for protecting their POS devices. Treat these devices like cash. Devices can be protected by tethers (steel cable) or secure stands. Security seals and daily inspections of devices and serial numbers can identify whether devices have been tampered with.

Card Not Present Fraud

A card-not-present transaction occurs when neither the cardholder or the credit card is physically present at the time of the transaction. This fraud is committed by fraudsters online, by phone, mail, or card on file payments using credit card information obtained fraudulently.

Because both the card and cardholder aren't physically present (and fraudsters often steal complementary information like the CVV and billing address), it can be difficult for merchants to verify the purchaser's identity.

According tto a US Payments Forum report, CNP fraud accounted for 76% of all fraud in Canada between 2010-2015. When CNP fraud occurs, the merchant typically bears the loss.

Potential Indicators of Card-Not-Present Fraud

- FFirst-time shopper
- Larger than normal orders: Because stolen cards or account numbers have limited life spans, criminals maximize the size of their purchase buying as much as they can at one time.
- Orders contain multiples of the same item(s).
- Order is made up of 'big-ticket' items.
- Rush or overnight shipping request, as criminals are not concerned about the extra delivery charges
- Shipping to a single address, but purchase transactions placed on multiple cards.
- Multiple transactions to one card over a short periodtime.

Preventing Fraud from Within

Along with external fraud threats to businesses, internal fraud committed by employees can have a significantly impact of a business.

- Know your employees. Be alert to changes in behaviours, attitudes and lifestyles.
- Communicate to employees their expectedpractices and roles.
- Review bank statements regularly for anomalies. Separate cash responsibilities from financial administrative responsibilities.
- Maintain current and accurate accounting records.
- Minimize the number of authorized cheque signers. Never sign blank cheques.
- Physically secure business premises and assets.
- Review computer security.
- Provide a means for employees to report attempted or suspected fraud.

Preventing Card-Not-Present Fraud

- Authenticate Authenticate the transaction using the card verification numbers (CVN), the three or four digits on the back of the credit card.
- Implement a second authentication method such as an address verification system (AVS) to verify the address of the person claiming to be the credit card holder. The payment processing system will verify the billing address of the credit card provided by the customer with the address on file at the credit card company.
- If an order from a repeat customer deviates from their established pattern, contact the customer and validate the transaction.
- Create an internal 'blacklist' file containing data from fraudulent transactions. When a new order is received containing information that matches the data on file, your payment system can be set-up to automatically identify the mismatch and trigger the need for further examination.
- Several credit card companies offer authentication services (i.e. Verified by Visa or MasterCard Secure Code) which enables the cardholder to authenticate themselves before the transaction is completed.