# Financial Crime Trend Bulletin:

# Card-Not-Present (CNP)

## 2017-12-15

**FRAUD: Recognize, Reject, Report**

**Purpose**

This bulletin was prepared to provide awareness on Card-Not-Present (CNP) Fraud, which continues to target Canadian businesses. It depicts the trends and patterns associated to the fraud, as well as warning signs to prevent victimization.

**Overview**

CNP Fraud is defined as the unauthorized and/or fraudulent gathering, trade and use of payment data (card numbers, expiry dates and passwords). For CNP to occur, this data must be used in instances where the card and cardholder are not present (via phone, email, fax, or website). Most commonly, CNP transactions are performed by email, as it is one of the most unsecure methods to conduct card orders.

A scammer places an order for a product or service via a merchant's Card-Not-Present channel (phone, email, fax, or website) intending to make the payment using a stolen payment card. The merchant, believing this to be a legitimate purchase, processes the payment on the stolen payment card(s) and provides/ delivers the product(s) or service(s). Eventually the real cardholder identifies and disputes the unauthorized charge. As a result, the merchant receives a chargeback and subsequently loses any product or service rendered. Furthermore, it is the responsibility of the merchant to pay back the amount charged on the stolen card. Any merchant who accepts CNP orders can become a victim if they are not aware of fraud protection protocols or not abiding by the regulations.

It is also common to witness an overpayment request when dealing with CNP fraud transactions. Scammers may demand the merchant charge extra on the card and forward funds to a third party – often a *moving company* to facilitate the shipment. By doing so, scammers are essentially turning stolen credit cards into cash.

Another version of CNP fraud seen within the airline industry is for scammers to purchase airline tickets using stolen credit cards and sell the tickets for a cheaper price online on classified ad sites. In situations like this, the merchant is not the only victim, so is the person purchasing the tickets being resold. In most cases, the purchaser will not be able to use the tickets as the merchant cancels them once fraud is confirmed.

Based on complaints received at the CAFC from 2016-2017 the industries most targeted by CNP fraud are: retail, airline and food/ hospitality.

**Warning Signs - "Common Red Flags":**

*Product / Order Flags*

- Larger than normal orders
- Multiple orders for the same product; especially "big ticket" items
- Orders from repeat customers that differ from their regular spending patterns

*Delivery Flags*

- Customer requests "rush" or "overnight" delivery
- Single card used with multiple shipping addresses
- Billing address different than shipping address
- Request that extra funds be sent to a 3rd party shipping company

*Customer Flags*

- Orders made using different names, addresses, and card numbers but are from a single IP address
- Internet addresses at a free email service

- Multiple cards used for one order (cards keep getting declined)
- Purchaser name and cardholder name are different

**How to Protect Yourself:**

- Know the Red Flags and compare to the transaction(s) received.
- Prior to shipping merchandise, call the phone number the customer provided and verify the transaction information.
- Be sensitive to priority shipments for fraud-prone merchandise, which may indicate a fraudulent transaction.
- Be aware of orders that occur with a request for urgent shipment, especially if the shipping address does not match the billing address on the credit card provided.
- Be aware of orders from repeat customers that differ from regular spending patterns.
- Use available verification services (address and card validation code 2 (CVC 2), etc.) of the credit card network companies – Mastercard and Visa.
- Contact your processers and ensure security measures are established to prevent victimization and reduce unwanted charge backs.

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 report online at http://www.antifraudcentre.ca