CHASE Paymentech

Prevent Fraud in a Card-not-Present Environment

Reduce credit card fraud and protect your business from unnecessary risks [1]

Fraud is a real issue in business and there is a heightened risk for merchants who support card-not-present transactions. Because mail and phone order merchandising has exploded into a business that generates more than $100 billion per year, card-not-present merchants should be aware of some of the potential risks and tools available to them. At Chase Paymentech, we take fraud seriously. We hope that you will review the fraud prevention strategies that we have included in this article.

It is important to implement fraud prevention at an early stage and make it a major part of new employee training - because employees are in one of the best positions to have a significant effect on a company's fraud losses. Reinforcement of fraud training for employees (including seasonal and part-time employees) could help you - especially when holidays and peak seasons approach and fraud potential may be elevated.

Some helpful fraud prevention practices to follow in a card not present environment include, but are not limited to the following:

1) Training and Education
Train operators to pay particular attention to anything suspicious in the way the caller speaks or responds to questions. One simple tip-off is a long pause or a hesitant answer. Make it a policy to request the name of the credit card issuing bank for any sale over a pre-set amount. If the caller doesn't know the bank's name, this could signal that he or she may be using a stolen credit card number.

2) Cardholder's Billing and Contact Information
Always ask for the cardholder's billing address. Ask for the cardholder's day and evening telephone numbers "in case there's a question." Orders with a "ship to" address that is different from the cardholder's billing address may be a warning sign. If you are suspicious, attempt to contact the cardholder on a second phone to verify the order. If your system allows you, compare the "ship to" and "bill to" addresses with the catalogue's "mail to" address.

3) Keep a List of "Negative Transactions's
Develop and maintain a "negative file" of fraudulent names, addresses, postal codes, credit card numbers and companies you come across. Compile a postal code listing that spotlights areas in which you've experienced high fraud.

4) Take a Closer Look at P.O. Boxes
If the address is a P.O. Box in a large city, further checking is suggested, especially if the order is from a new customer. Mail delivery services require a street address and will not ship to P.O. boxes.

5) Don't Brush off Rush Orders
Carefully examine a "rush" order request – especially from a new customer. Be especially alert when the caller appears ready to order whatever merchandise is in stock, regardless of size or style.

Continued...

6)Closely Examine Unusual Orders
Carefully examine any order with an unusually high dollar amount, special requests, or any order which involves an out-of-the-ordinary situation. Other suspicious orders that merchants may come across that need closer examination can include:

- Customers attempting to use multiple cards
- Customers attempting to use multiple cards all issued from the same BIN (Bank Identification Number)
- Requests by merchants to apply a portion of funds (for any reason) by way of wire transfer

7) What to Ask For When Accepting Credit Cards
Here are some features for credit cards issued by some of the card payment brands. We recommend visiting their respective sites to make note of the card security features available.

- What to Ask for When Accepting **American Express** Cards:

For American Express® customers, ask for the 4-digit, non-embossed CID number printed on the front of the card (on the right border of all American Express Cards).

- What to Ask For When Accepting **MasterCard** Cards:

For MasterCard+, ask for a non-embossed 3-digit code on the back of the card following the card number. It should match the card validation code (CVC2). Also, ask for a description of the security character -- a stylized MC embossed on the line next to the valid dates on the face of the card.

- What to Ask For When Accepting **Visa** Cards:

For Visa* cards, ask for the non-embossed number which appears above the first 4 digits. It should match the first 4 digits of the credit card number. Ask the caller to describe the embossed symbol (CV on Visa Classic, BV on Visa Business and PV on Visa Gold cards) to the right of the expiration date. Also, ask about the repetitive pattern of the Visa wordmark throughout the signature panel.

For more information and examples of card-specific security features and characteristics, you can visit the respective card brand website:

American Express: **www.americanexpress.com/canada/en/merchants/2-4_fraud.sht**

MasterCard: **www.mastercard.com/ca/merchant/en/security/what_can_do/getting_started.html**

Visa: **www.visa.ca/en/merchant/fraud-prevention/visa-card-security-features/**

8) Verify the Caller
You may be able to use Automated Number Identification (ANI). Verify that the telephone number returned to you is the same as the one provided by the caller.

Continued...

Additional Tools and Resources: Address Verification Service and Card Security Codes

The tools provided by card associations can help verify a cardholder's identity in real time and provides business owners some added security measures. However, these still cannot eliminate all instances of fraud and chargebacks.

Credit Card Authentication

This authentication process verifies a cardholder's account ownership during an online purchase. Services such as Verified by Visa™ (VbV) and MasterCard Secure Code™ can help card-not-present merchants by adding another validation measure when assessing the legitimacy of a transaction.

When a cardholder shops at a participating VbV or SecureCode merchant site, the checkout process remains the same until the "buy" button is selected. If the bankcard is registered with a participating issuer, consumers will be asked for their VbV password or their SecureCode issuer-specific access credentials. Through this simple checkout process, the card issuer confirms a consumer's identity in real time.

Merchants must deploy a software module (referred to as a Merchant Plug-in) or develop their own software capabilities to support VBV and SecureCode. This allows merchants to pass cardholder credentials to cardholder registration servers, and receive responses. Merchants must capture and send authentication data to Chase Paymentech.

Address Verification Service (AVS)

AVS may help reduce the risk of accepting fraudulent transactions by verifying the cardholder's billing address on file with the card issuer. AVS compares the billing address given to you by a customer against the billing address on file with the credit card issuing bank. Visa, MasterCard and American Express offer similar AVS features.

- AVS is only a tool to help prevent fraud. As such, AVS is most effective when you use it together with other fraud detection practices.
- The instance of fraud is usually greater when there is no AVS match and when the order is for a high dollar amount; the caller requests overnight delivery to an address that is located in a high fraud area; or the "mail to" address differs from the "billing address."

Card Security Verification

This card-not-present tool compares the card security code – the non-embossed, three- or four-digit numeric code on the credit card, with what the issuer has on file. These codes are three digits printed in the signature panel on the back of Visa and MasterCard issued credit cards or four digits printed on the front of American Express cards.

Credit card verification programs are offered by the major card associations and are known as CVV2 (Visa), CVC2 (MasterCard) and CID (American Express). Many card-not-present processing solutions support validation of card security codes and will prompt for them during a transaction.

- If the customer cannot provide the card security code from the front or back of the actual card, it indicates that the card is not present and that the card number provided is possibly stolen.
- If the customer does provide the card security code, but it does not match what the issuer has on file, you will receive a response indicating that there was not a match. You may wish to ask the customer to confirm the code as it may have been given in error. If it still does not match, you should decline the transaction.

Continued...

Always be Observant

You may significantly reduce credit card fraud by taking direct steps and implementing protocols to counter potential fraudulent activity. Often, increased diligence and a proactive approach may help you protect your company against fraudulent activities.

Be Aware of Internal Fraud

Employee theft does exist and can affect your business. One type of fraud that is unique to direct marketers is the misdirection of refunds to a fraudster's credit card. Businesses should monitor mismatches between the credit cards used for ordering and any subsequent refunds. Also, watch for employees who may purchase goods and charge them to customers' credit cards. In addition, you may consider taking some additional steps to protect your business:

- Monitor your employees;
- Safeguard credit card numbers; and
- Balance your funds on a daily basis.

Your Takeaway

Business owners should be proactive in minimizing their fraud liability. The key message derived from these fraud prevention strategies is for business owners to educate themselves and their staff so that they can help protect their business and customers.

There are many fraud prevention strategies and tools available to businesses that provide valuable information to help update risk management and fraud prevention protocols.

For more information please visit our webiste at: **www.chasepaymentech.ca**