VISA CHECKOUT MERCHANT HOLIDAY BEST PRACTICES

The holiday season is upon us. As merchants prepare for the expected bump in ecommerce traffic during this extended shopping season, fraudsters are preparing to exploit system weaknesses for fraudulent transactions.

Recognizing this, Visa recommends three best practices to help merchants mitigate fraud attacks during this holiday season:

1. Establish transaction controls and velocity limits.

Use internal transaction controls to identify high-risk transactions. These controls help determine when an individual cardholder or transaction should be flagged for special review.	☑ Set review limits based on the number and dollar amount of transactions approved within a specified period of time. Adjust these limits to fit average customer purchasing patterns. ☑ Set review limits based on single transaction amounts. ☑ Ensure that velocity limits are checked across multiple characteristics including shipping address, telephone number, and e-mail address. ☑ Adjust velocity limits as customers build history with your business. The limits should be constricted for new customers and loosened for existing customers with a solid purchasing and payment track record. ☑ Contact customers who exceed these limits to determine whether the activity is legitimate and should be approved, provided that the issuer also approves the transaction during the authorization process.

2. Require shipping address to match billing address for higher risk transactions.

When the shipping and billing addresses of the transaction are different, merchants should pay incremental attention to the shipping address. While it is common for a consumer to have goods shipped to a work and home location, this becomes a lot more challenging during the holidays with the shipment of holiday gifts to multiple addresses. Hence it is critical during this time to conduct special screening for high-risk shipping addresses such as:

- ☑ Maildrops or P.O. Boxes
- ☑ Hotels where the customer is listed as a guest
- ☑ Third Party Shipping Agents
- ☑ Hospitals
- ☑ Prisons
- ☑ Addresses with known fraudulent activity

There are online tools available over the Internet to determine if the shipping address is potentially a home, commercial facility, or other location.

3. Stay alert for the following fraud indicators – Any one of these factors could indicate a higher degree of fraud risk:

- ☑ *Larger-than-normal orders.* Because stolen cards or account numbers have a limited life span, criminals need to maximize the size of their purchase.
- ☑ *Orders consisting of several of the same item. Having multiples of the same product increases profits.*
- ☑ *"Rush" or "overnight" shipping*. Criminals want their fraudulently obtained items as soon as possible for the quickest possible resale, so they aren't concerned about extra delivery charges.
- ☑ *Shipping outside of the merchant's country*. There are times when fraudulent transactions are shipped to fraudulent criminals outside of the home country.
- ☑ *Inconsistencies in Information in the order details, such as billing and shipping address mismatch, telephone area codes falling outside of billing zip codes, e-mail addresses that do not look legitimate, and irregular time of day when the order was placed.*
- ☑ *Multiple transactions on one card over a very short period of time.* This could be an attempt to "run a card" until the account is closed.
- ☑ *Shipping to a single address, but transactions placed on multiple cards.* This could involve an account number generated using special software, or even a batch of stolen cards.
- ☑ *Multiple transactions on one card or a similar card with a single billing address, but multiple shipping addresses.* This could represent organized activity, rather than one individual at work.
- ☑ *Multiple cards used or attempted to be used from a single IP (Internet Protocol) address.* More than one or two cards could indicate a fraud scheme.
- ☑ *Transactions originating from a VPN / proxy or VOIP service provider IP address.* The fraudsters may be trying to hide their location and to make it harder to trace or track the fraud back to their device.
- ☑ *Orders from Internet addresses that make use of free e-mail services*. These e-mail services involve no billing relationships, and often neither an audit trail nor verification that a legitimate cardholder has opened the account.

  Special attention should be given to the structure of the email addresses used in the enrollment process. Merchants should focus on the username in the email address, as it is common to use free email services such as Gmail, Outlook, or Yahoo. Common fraudulent email address formats include, but are not limited to:

  - Email names with a numeric value (# indicates a numeric value):
    - firstname##lastname###@email-domain
    - firstnamelastname###@email-domain
    - firstinitiallastname###@email-domain
  - Generic email names with a username unrelated to the cardholder's first and last name or initials.

In addition to these 3 recommendations, merchants can find more resources and best practices at https://usa.visa.com/support/merchant/library.html