Guarding Against Online or Card Not Present Fraud

While there is no silver bullet, best practices in detecting fraud may help your business minimize the risk of fraud for online or card-not-present orders. Although we all want to maximize legitimate sales, a little prudence can help prevent fraud losses and associated fees.

Remember that a credit card authorization only indicates that the amount of funds authorized is available on the card. It does not mean that it is a valid charge, that the card number has not been stolen, that your business won't receive a chargeback from the card issuer, or even that your business will be paid in the end.

Below are some practices that can help detect online or card not present fraud.

Best Practices for Detecting Online Fraud

- ✓ **It's a first-time customer:** Pay special attention to first-time orders that are larger than your average ticket. In conjunction with other flags such as a mismatch on Address Verification Service, use of multiple cards for a single order, or a request for expedited shipping. Individually or collectively, these can all be signs of fraud.

- ✓ **Unusual orders:** Use caution when a consumer appears to be "buying" rather than "shopping." When consumers are shopping, they usually have specific preferences such as for color, size, etc. When a customer orders several different variations of the same product with no regards to preferences, it may indicate that the items will be re-sold and this can be a sign of fraud.

- ✓ **Orders shipped to an international address:** Orders from foreign countries are sometimes fraudulent. The Address Verification Service (AVS) cannot validate non-U.S. addresses. If your business does not typically service foreign customers, use caution when shipping to addresses outside the U.S., particularly if you are dealing with a new customer or a very large order. Sometimes social media or public data searches can be useful in helping to authenticate these types of orders.

- ✓ **Card Verification Value (CVV2) does not match:** If there is a mismatch on the CVV2/CVC2 security code, this could indicate a fraudulent transaction. Customers will sometimes enter this number incorrectly, but it may be a follow up item to help ensure the transaction is legitimate.

- ✓ **The shipping address is different from the billing address:** Although there are sometimes legitimate reasons for mismatching addresses such as during the holiday season or for commercial cards, in conjunction with other potential fraud warning flags, this should be considered.

- ✓ **Express shipping:** Expedited shipping is very frequently used on fraudulent orders as criminals want to receive the merchandise before you realize it's fraud and stop the fulfillment.

- ✓ **Orders made on multiple cards:** Criminals often don't know the limit or existing balance on stolen credit card numbers. As a result, they try to spread smaller authorization amounts across several stolen card numbers in order to avoid a limit decline which may raise concerns.

- ✓ **Multiple cards from a single IP address:** A customer's Internet Protocol (IP) address identifies the computer from which an order has been made. Be cautious of multiple orders from the same IP address using different customer identifiers and credit card numbers as this could indicate use of stolen data.

- ✓ **Orders via email:** Criminals will sometimes try to avoid online shopping carts and, instead, attempt to order items via email instead. Beware of this as well as requests to overpay your business for an order while sending the "difference" back to the customer. In many cases the original payment will later be returned as fraud while you take a loss on the "difference" that you sent to them.

What Else Can I Do?

Depending on the amount of time you or your employees are willing to spend on it, there are a few things that you can do to decrease the chance of fraud:

- Use open-source information such as social media or public listings to verify the identity and address of the customer.

- Use Google or other search engines to query the name, shipping address, email, etc, and input other key search terms such as "fraud, scam" or other pertinent words to see if there is any searchable information input by other online merchants.

- Use Google maps street view to attempt to verify the type of structure at the shipping street address to verify if it matches the type of customer with whom you think you are doing business. For instance, if the customer inputs an address like it's an apartment building (ex. Apt. #4), but street view shows a commercial mail receiving center (from which mail may be forwarded), it may be an indicator of fraud.

Real-Time Fraud Analytics

Lastly, Wind River has partnered with a real-time fraud analytics provider that uses state-of-the-art analytics to help identify fraudulent orders. A plugin or API from your e-commerce website sends transaction data to the provider and their system returns an answer to you in real-time as to whether the order should be fulfilled. Different plans are available including fraud chargeback reimbursement.

The business case for the cost of this solution may make sense from the standpoint of the amount of time employees are spending reviewing transactions for legitimacy. Deploying a fraud analytics solution may allow your business to re-task employees. Some studies have indicated that solutions like these can decrease false positives by up to 6% and allow your business to ship internationally with confidence.