

5 Key Tips to Protect Against Credit Card Fraud

#1 VERIFY ADDRESS AND CVV CODE

Sounds simple, but this is a step that is often ignored. A CVV Code or CARD VERIFICATION VALUE code is a three or four digit code located on the credit card itself and is a security feature to help verify that the card is on hand for "card not present" transactions. Verifying the address and CVV code provides the confidence that the credit card is in the possession of the cardholder your dealing with and a positive address match should mean that your are shipping the product to an address recognized by the issuing bank.



#2 BE WARY OF SUSPICIOUS INTERNATIONAL SALES

I'm not saying that all International sales are fraudulent; however, it is important to realize the risks. Address verification cannot be performed and it is difficult for your merchant processor to verify the sale in question. Ask yourself does the sale make sense and why does this individual have to buy the product from you and not someone closer geographically?

#3 STAY ABREAST OF FRAUD TRENDS/SCENARIOS

More and more, we see merchants being approached for "humanitarian" causes with large purchases needed for orphanages, churches, etc. These are uncommon for the business and are usually sent via e-mail. Merchants are provided with multiple credit cards and are asked to split the sales to get them through. These sales are often invalid. Take the extra step if approached on a Teletypewriter (TTY) line. Unfortunately, another popular method for taking advantage of a merchant is using this device to shield one's identity. Look for the warning signs and take the proper steps to verify the sale.

#4 NEVER, EVER SEND MONEY TO THE CARDHOLDER

A self-explanatory red flag, there should never be a reason why you would need to refund money via bank or other wire service. If the cardholder even broaches this subject, WALK AWAY!

#5 NEVER HESITATE TO CONTACT US AND REQUEST A CODE 10

A Code 10 authorization request is to be utilized if a merchant is attempting to process a credit card and suspects fraud or suspicious activity. This request is forwarded to the card issuing bank from the merchant processor so information can be verified before the sale is processed. Remember, we're here to help. Your risk is our risk and we only want you to process valid sales.

Ultimately, the last bit of advice I can provide is this: **FOLLOW YOUR INSTINCTS.** Unfortunately, I have received emails and calls from hundreds of merchants who have been victimized stating that they "knew it didn't sound right" OR "it was too good to be true" yet completed the transaction against their better judgment.

ABOUT THE AUTHOR:

Rich Placa has 10 years experience supporting revenue growth by minimizing losses and approving new business in creative ways weighing the risk versus reward factors. He provides leadership within his department creating and implementing re-engineered risk management policies while creating procedures to work with merchants to maximize their processing while protecting Federated Payments. Prior to joining Federated Payments, Rich served as a Manager of Risk Management for First Data Corporation. Email Rich with any questions at rplaca@fpsemail.com