12 Tips to Fight Credit Card Fraud

1) Educate Your Employees About Fraud - You need to be aware of fraud to avoid it, but so do your employees. You both make up the first line of defense. Train your employees well to know the signs of potential fraud and remind them periodically to always stay alert.

2) Compare Signatures and Ask for Identification - Very few retailers take the time to glance at the signatures anymore, but it's simple and quick. Check for misspellings and make sure the name on the card matches the signature. Address the customer using the name on the credit card. If he or she doesn't respond, ask for a photo ID and compare those signatures.

3) Ask to See the Card - Look for the card's security features, such as a clear hologram with a moving picture and the Bank Identification Number above or below the first four digits of the account number. Check the numbers themselves for signs of alteration and look for signs of tampering on the signature strip.

4) Be Wary of Customers Who Keep the Credit Card Separate From Their Wallet - Most legitimate customers will keep their credit cards in their wallet along with some form of ID. Fraudsters are more likely to keep the fraudulent credit card separate from their wallet, so they do not have any means of ID with them.

5) Watch Out for Customers Who Are Distracting - They may either be very talkative or very angry. Or they may wait until the last second before closing time to make a big purchase. Either way, they could be a potential fraudster trying to rush the clerk and keep their attention off the card authorization process.

6) Think Twice Before Manually Entering Damaged or Worn Cards - Fraudulent cards are often damaged on purpose so the magnetic strip cannot be swiped. Instead, the customer may insist the clerk manually key in the card number, which bypasses the antifraud features of the magnetic strip. Always swipe the card, no matter how damaged. If the card can't be read, ask for another form of payment.

7) Do Not Accept "Letters of Authorization" - Some fraudsters will present a letter from the cardholder that authorizes the use of their credit card. This should never be accepted as a form of verification. No one is allowed to "borrow" another person's card, regardless of relationship. Only the cardholder is authorized to use their credit card.

8) Take Note of What the Customer is Purchasing - Have they purchased more than one of the same expensive item? Did they make their selections quickly, without thought to size or color or price? Or maybe they want a costly rush delivery to a different address, or they want to carry their purchase out of the store when it's something normally delivered (such as large appliances or furniture). All these could be signs of a potential fraudster looking to leave your store quickly with their "hot" card and goods.

9) Use the Address Verification System (AVS) - Address Verification is most common with card-not-present situations (like online purchases), but it can also be used when the card is present at the POS. In addition to the usual checkout process, the terminal asks for the customer's billing ZIP code. The transaction will reject if the ZIP code entered doesn't match the one on file.

10) Know Your POS System and Equipment - Sophisticated criminals can access information on the magnetic strip of a credit card when it is swiped at checkout. This process is called "skimming," and it requires an actual attachment to the terminal that reads the card. To combat this, make sure you know what your payment processing equipment looks like and how it should work. If you see an extra device or notice malfunctioning software, you know to investigate further before continuing to accept credit cards from customers.

11) Keep Accurate Records of Credit Card Transactions - Some fraud situations result from legitimate cardholders who make authorized purchases, only to fraudulently dispute the charges later. You can fight this kind of fraud if you are armed with the right information. Your acquiring bank can assist you with the process, but at minimum you will need the customer signature and evidence that you swiped the card and received an authorized approval.

12) When in Doubt, Call - If you feel something is not quite right, do not hesitate to call the card issuer for authorization. Keep the card with you and move away from the customer to make the call. You may feel you're risking a sale by making the customer wait, but even if they are legitimate cardholders, it's for their protection as much as yours.

Best Practice Tips to Avoid Skimmers

- Have an Incident Response Plan for reporting tampered or substituted devices.
- At the beginning of each shift log the inspection of each device for tampering or placement of skimming devices.
- Train personnel to be aware of suspicious behavior of customers and to report tampering or substitution of devices immediately as outlined in the incident response plan.
- Periodically rotate the individuals performing the device-checking to ensure nothing gets missed and to eliminate collusion
- Surveillance cameras should be sited such that they record the area around the PIN entry device but allow no method of actually recording or viewing any PINs entered
- Locate cameras to cover primary site entrances. Facility cameras provide a level of deterrence and a record of activity that can be used to support investigations.
- Support PCI DSS guidelines for 90-day storage of surveillance images

Skimming Device Recovery Response

- If a skimming device is discovered on a POS terminal, document and take pictures of the skimming device as-is.
- Document before and after removal (date/time)
- Use protective gloves to remove the device (criminals may leave DNA on device)
- Review surveillance to determine the window of exposure
- Notify local law enforcement and the FBI or U.S. Secret Service office so they can recover the skimming device.
- Protect any video surveillance that may be used to identify any perpetrators and confirm timing of when the device was placed on the POS terminal.
- Notify your Acquirer with your Incident Response Form with information detailing the incident. *Please include the following information:*
- Date and time the skimmer was identified and removed
- Date and time skimmer was placed on the terminal (*This can be determined from surveillance camera or logs from monitoring)*
- Pictures of the skimmer
- Contact information for the Law Enforcement Agency handling the investigation
- Summary of any action taken