Tips for Preventing Credit Card Fraud and Avoiding Chargebacks

TSYS®

Accepting credit cards is more than just a courtesy. It's practically a requirement. Consumers expect to be able to pay with plastic whenever and wherever they wish. By accepting credit cards, you meet the needs of customers and streamline your business.

Unfortunately, fraud is a fact of life for merchants and cardholders alike. According to the 2016 report *Global Consumer Card Fraud – Where Card Fraud Is Coming From*, nearly 30 percent of consumers worldwide have been victims of card fraud in the last five years. And of the 20 countries included in the study, the U.S. is in the top 3. Another survey about online fraud revealed that nearly 46 percent of North American merchants say fraud is becoming "cleaner" or harder to detect. In fact, it takes a merchant 45 days on average to know that an order is fraudulent. By then, a lot of expensive damage has already been done.

Security is something we take very seriously. We've compiled tips and precautions to assist you in preventing fraudulent/criminal activity. Taking precautions can help safeguard your business and avoid costly chargebacks.

Card Present Transactions

When you conduct business in person, you deal primarily in card present transactions. This type of transaction occurs when both the cardholder and the card are physically present. Face-to-face transactions make it easier to identify behavior associated with credit card fraud. Certain characteristics which, when observed separately, appear to be harmless. However, when several of them are present simultaneously, they may indicate that the transaction is not legitimate.

Be wary of customers who:

- Purchase several of the same type of merchandise or very expensive merchandise, especially if they do not ask any questions about the items
- Purchase a vast array of merchandise, seemingly without regard to size, color or price
- Make a purchase and then leave the store, only to return later to make additional purchases
- Try to distract or rush you during the transaction, especially if they're working in pairs or as a group
- Who make purchases right as the store is opening or closing for the day

In addition to being alert to suspect behavior, we recommend you adopt some rules for face-to-face transactions.

1. Never accept an expired credit card.
2. Never accept a card that appears to have been altered.
3. Make sure that the card is signed. If it is not, have the customer sign the card in your presence and then check the signature against a picture ID.
4. Inspect the card and keep it throughout the transaction. The embossing on the card should be clear and straight. The hologram should be smooth with the card and three dimensional. Make sure there has been no tampering with the signature panel.
5. Verify that the account number on the terminal matches the account number on the card—be it swiped, dipped or mobile pay. Compare the name printed on the electronic sales receipt to the name that appears on the card. Compare the signature on the sales draft with the signature on the back of the card too. If they do not match, discontinue the sale.

6. Visually compare the first four and last four digits of the card number to the four digits printed on the sales receipt to confirm that they are the same numbers in the same sequence. If they do not match, notify the authorization center and do not complete the transaction.
7. If the card will not register and you must manually key the card number into the terminal, get an imprint of the card using a flatbed imprinter. Then have the customer sign the carbon paper receipt.
8. When handwriting a sales draft, fill it out completely with the transaction date and items purchased.
9. Obtain an authorization for the full amount of the sale (hotels may authorize within 15 percent of the total).
10. If you receive a "call center" or "pick up card" message through your terminal, call the authorization center and follow their instructions.
11. If you receive a "do not honor" or "decline" message through your terminal, do not proceed with the transaction. Do not run the transaction again because even if you receive an approval code on a second attempt, there is no protection for a transaction after you have received a "decline" or "do not honor" message.
12. If a sale seems suspicious, call the authorization center. Ask for a Code 10 authorization which is a universal code that alerts the center that you have concerns about a transaction. The Code 10 operator will ask you a series of "yes" or "no" questions to help determine if it is a fraudulent transaction. Follow the operator's instructions.

One last word about authorization codes. Although the code is required on all transactions, it does not guarantee that the cardholder is legitimate or that the sale is valid. The authorization code only indicates only that the account is open and has the available credit at the time of the sale. A code does not guarantee payment.

Card-Not-Present (CNP) Transactions

Recognizing fraudulent behavior when taking orders online, by mail, telephone or fax (MOTO) can be trickier because neither the customer nor the credit card is physically present. Unfortunately, there are unscrupulous people who take advantage of CNP situations to obtain products and services through deceptive practices using lost or stolen credit cards, or account numbers generated by fraudsters. They order goods and have them shipped to an address to be picked up by themselves or a "runner" with whom they are collaborating.

When the true cardholder receives the statement with the fraudulent charge, they or their bank requests a chargeback. This is a reversal of the sales transaction and the amount of the sale is deducted from your merchant account. When fraudulent orders are made by MOTO or online, the resulting chargebacks are very difficult to fight because the merchant has no card imprint or customer signature to confirm the transaction.

To help avoid being on the receiving end of a fraudulent CNP transaction, watch out for orders that:

- Are larger than normal for your business, especially when you're not familiar with the customer
- Include several of the same item or very expensive items
- Include request "rush" or "overnight" shipment
- Ship to an international address that cannot be verified by an Address Verification Service (AVS). Consider this very risky unless the order is from an established customer you know well
- Ship to the same address and were purchased on different cards
- Are placed using email generated on a free email service (i.e. Yahoo, Gmail)
- Charge transactions to account numbers that are sequential
- Provide multiple card numbers from a single IP address
- Charge multiple transactions to one card over a very short period of time

Make it a practice to require the following for every MOTO or e-commerce sales draft:

1. Cardholder's credit card number, credit card validation code and expiration date
2. The name that appears on the front of the credit card
3. Cardholder's billing address and phone number
4. Description of merchandise and/or services rendered

Additionally, follow these steps for every CNP transaction to help decrease the chances of credit card fraud:

1. Use AVS. It's a service from your merchant account provider that compares the shipping address given to the merchant with the cardholder's billing address on file with the issuing bank. If the two do not match, do not ship the merchandise. AVS only verifies addresses within the U.S.
2. For an additional level of security, verify the card's authenticity by asking for the three-digit credit card validation code on the signature panel. It goes by various names, depending on the issuer. Such as CVV, CVC and CID. The code is often missing on fraudulent cards, or unavailable in the case of compromised card numbers or generated account numbers.
3. Ask the customer for additional information, such as a day and evening phone number. Then call them back later to confirm the sale. Alternatively, before sending the order to the customer, confirm the order via the billing address, not the "ship to" address.
4. Ask for the bank name on the front of the card, and the bank's customer service number from the back of the card.
5. Ship merchandise only to the cardholder's billing address. You may want to request a certified signature as proof that the merchandise was delivered.
6. Ask the card issuer to include your customer service telephone number in the billing name that appears on your customer's credit card statement. This gives your customer an easy way to contact you directly if they question a sale.
7. If you are uneasy about an unusual mail, phone or internet transaction and have a merchant account with TSYS, call us. We'll assist you in verifying the transaction with the issuing bank before you ship the merchandise.

We believe that a well-informed client is our best customer. We hope that you find these tips for preventing credit card fraud and avoiding chargebacks to be useful and informative. We highly recommend that you share these precautions with your employees who handle credit card transactions.

We're also very serious about our responsibility to our merchants and their customers. We're pro-active about taking the necessary security steps against the threat of data breach, credit card fraud and identity theft. If you have any questions on credit card fraud, processing and merchant accounts, please contact us.

To learn more:

contact 888.845.9457
or visit tsys.com.

twitter.com/tsys_tss
facebook.com/tsys1
linkedin.com/company/tsys

TSYS®