

Helping to Protect Your Business

Your Guide to Fraud Awareness

Global Payments – Helping To Protect Your Business

For over 30 years merchants have relied on Global Payments to process credit and debit transactions through its payment processing system and to also deposit the proceeds from card sales into their business bank accounts. Today, almost one million merchant locations across North America continue to trust and rely on Global Payments to provide them with the point-of-sale solutions and services they need to run their businesses efficiently and effectively.

At Global Payments, we take your business seriously. That's why we've developed this brochure – "Your Guide to Fraud Awareness". It's designed to help you and your employees learn more about various fraud scenarios so that fraud can be stopped before it even starts. While it is not always possible to prevent fraud from happening, education and awareness are the best defenses against it. As your merchant advocate, Global Payments utilizes a highly sophisticated fraud detection system that monitors all submitted card transactions. This fraud detection system is one way Global Payments protects your business. Reading this guide, then sharing and practicing the information in it with your employees are steps you can take to protect your business.

Let us share with you what we know in order to help you become more aware of the many ways that fraudulent activity occurs, what to watch for, and the things that you and your employees can do to protect your business.

Take Charge of Chargebacks

Chargebacks are one of the most common – and costly – ways that fraudsters take advantage of merchants. For example, some fraudsters, appearing to be legitimate customers, will take both the "merchant copy" and "customer copy" of the sales slip after they have signed it. When they receive their credit card statement, they dispute the charge. And, since your company has no record of the transaction, the full amount is credited back to the consumer, and your business loses the merchandise.

There are steps that you can take to prevent chargebacks and fraud from occurring. Here are some examples based on the card processing method used:

1 - Processing Transactions Manually with an Imprinter

- When you process transactions manually, be sure to take an imprint of the card every time a purchase is made with a credit card
- Hold onto the credit card throughout the sale
- Be sure to call in for authorization for every credit card transaction
- Make sure you neatly print and fill out the sales draft so that it is complete, clear, and easy to read
- Have the customer sign the receipt while you watch and verify that this signature and the signature on the back of the card match
- Don't divide one purchase onto more than one sales draft
- Do not change or alter the sales draft after the customer has signed it – if there's a dispute, the customer's copy is treated as correct
- If a transaction has been cancelled by the customer, take the required steps to stop the billing or reverse it immediately
- Be sure to display your return policy at the point-of-sale – remember it is your responsibility to inform your customers of this policy
- Maintain a well-trained staff and ensure that they follow card acceptance check-out procedures correctly
- Save all copies of your sales draft in case of future disputes

2 - Processing Transactions Through an Electronic Point-of-Sale Terminal

- Consider using the fraud control programming that is available in most point of sale devices.
- Be sure to always swipe the card through an electronic point-of-sale device
- After swiping, compare the embossed card number to the card number that is displayed on the point of sale device to ensure they match.
- If you must key in a transaction, be sure to take an imprint of the card to reduce your exposure to potential chargebacks
- Hold onto the credit card throughout the sale
- Have the customer sign the receipt while you watch and verify that this signature and the signature on the back of the card match
- Be certain your return policy is stated clearly on all of your materials or receipts
- Keep your point-of-sale equipment clean and operating efficiently (be sure to change printer ribbons often to maintain clear sales slips)

3 - Mail and Telephone Orders

- If possible, establish the customer's identity by writing their name, address, credit card number, and expiry date on the sales slip (also include name of issuing institution)
- Be sure to call in for an authorization for every credit card transaction
- If you are taking an order over the phone, fax or Internet, only ship items to permanent addresses – steer clear of post office boxes or hotel lobbies
- Consider utilizing a shipping vendor that requires a customer signature for delivery of merchandise. Moreover, use a shipping vendor that can provide easy access to 'proof of delivery' information as this may assist in the chargeback process.
- Where applicable, utilize a billing system that provides address verification or CVV processes
- Always send a copy of the sales draft to the customer either when the product is ordered or when it is shipped

4 - Protecting Your e-Business

- Internet merchants should be just as aware of the risks of fraud as traditional merchants, and should consider ways to prevent fraud
- If you are either creating or operating an online store, be sure to learn about security risks by assessing your e-business procedures, securing your online transactions, and letting your customers know that your site transactions are safe

In addition, here are some key ways you can prevent Internet fraud:

- Post your purchase and return policies on your Web site where your customers can see them clearly
- Start by taking a few extra steps to confirm each order and reject orders that leave out important information
- Be careful when dealing with orders that have different "ship to" and "bill to" addresses
- Avoid shipping to any address where special instructions may be to leave parcel "at the door"
- Avoid shipping to untraceable addresses, post office boxes, hotel lobbies or other addresses that are not permanent, as these addresses can be harder to trace later
- Consider utilizing a shipping vendor that requires a customer signature for delivery of merchandise. Moreover, use a shipping vendor that can provide easy access to 'proof of delivery' information as this may assist in the chargeback process.
- Pay extra attention to orders that are larger or more expensive than your usual orders, as well as multiple orders and international orders, especially if express shipping is requested
- Note the customer's e-mail address and make sure it is valid and matches the cardholder's name
- Be sure that each transaction is authorized correctly and that proper procedures are followed
- Where applicable, utilize a billing system that provides address verification or CVV processes
- Do not accept other merchants' requests to deposit their receipts through your account – if any items are charged back, you will be responsible for them
- If you are skeptical of an order, call the customer to confirm

Types & Methods of Fraud

Factoring

Factoring scams occur when another merchant's sales are processed through your merchant account. Criminals often accomplish this act by asking for a favor from a business owner or bribing someone they know. Some merchants and employees, however, are not aware that processing another person's credit card transactions through your merchant account is in breach of your merchant agreement. For example, if an individual operates two separate businesses, they cannot process one store's sales through the other store's merchant account. Since you are ultimately responsible for all transactions that run through your merchant account, if any items are charged back, you are held responsible and your account will be debited for these transactions.

The reality is that if fraudulent transactions are processed through your merchant account through factoring, you are in violation of your merchant agreement and as a result, you could be fined and prosecuted.

Card-Not-Present Scams

The risk of fraud increases greatly if your customer and their credit card are not present at the time a purchase is made because you don't have the opportunity to inspect the card. "Card-not-present" transactions typically occur over the phone or fax, or are Internet sales or catalogue purchases. Without the card in hand, you are unable to inspect the card, check for suspicious markings or verify the customer's signature.

As a merchant, you put yourself and your company at greater risk by accepting these types of transactions. If you are processing card transactions by telephone, fax or Internet, make sure that you have signed the specific merchant agreement required to perform Mail Order/Telephone Order transactions where the card is not present. Even after you have the proper agreement in place, it is crucial that you take the precautionary steps to prevent potential chargebacks.

Skimming

In many instances, thieves are reaping the benefits of our rapidly growing world of technology. One example of skimming is where the fraudster uses a device to read and copy the data on the magnetic strip of a credit card – a process known as "skimming." Other times the information is received by tapping into phone lines. Regardless of the method used, skimming is responsible for millions of dollars of losses. Typically, fraudsters 'skim' the magnetic stripe in order to later use it to create a counterfeit credit card, ultimately with the purpose of defrauding a merchant like you.

Be on the lookout for devices used to swipe credit cards. They are usually box-shaped cordless devices that look like pagers and fit in the palm of your hand. Laptop computers have also been used to accomplish the same thing.

Don't Be Bullied

Here the customer attempts to intimidate the cashier by causing a fuss at the register so that the purchase is rushed, which may lead to improper check out. They may tell you that the card won't read and not to bother running it through – that you'll have to key it in manually. In such instances, customers have also been known to complain about the service or length of the line. They may even demand to see a manager – anything to keep the cashier's attention off of the authorization of the credit card. By creating a tense atmosphere, the cashier is often prone to rush the person through the process just to get the customer out of the store. This is when the criminal activity takes place. The result is usually a costly chargeback for the merchant.

Don't be intimidated by these bullies; always take your time and make sure the correct procedure is followed when authorizing the card. You may not be losing a sale by making the impatient customer wait – you may be saving your company the cost of a chargeback later.

Deceptive Deliveries

An easy way to spot a situation that may be fraudulent is to look at the delivery address. Often thieves will have a package delivered to an address that is not permanent or requires the package to be left at a front desk. Look carefully at orders that require deliveries to office complexes, hotel lobbies or post office boxes, as they are almost impossible to trace if the transaction is questioned. In this situation, it is best to call the customer and ask for a permanent address.

The Manual Key-In

Often fraud occurs when the thief damages the card on purpose so that you are forced to manually enter the number in the electronic point-of-sale terminal. Fraudulent cards are often damaged in order to bypass the antifraud features that are placed on them – the magnetic strip cannot be swiped and transmitted to the verification center for authorization in the case of a manual key-in.

If you have an electronic point-of-sales terminal, swipe every card that you come across – no matter how damaged or worn. And be wary of customers who let you know right away that their card won't read. If the card doesn't work and you end up keying in the number, make sure you take an imprint of the card. If the card is severely damaged, simply ask for another form of payment.

Borrowed Cards

Beware of people waving letters of authorization for use of a credit card. Under no circumstances are these letters an acceptable form of verification or authorization. Don't fall for children borrowing their parent's card either. Friends, coworkers, and spouses are not permitted to borrow each other's cards. The only person who should be presenting the card to you is the person whose name is on the front of the card and signature on the back of the card. Most often, the rightful owner gets the statement and a chargeback inevitably occurs.

One Person's Trash Is Another's Gold Mine

The garbage is probably the last place you would think to protect. Thieves look in your trash for credit card slips, banking information, warranty information, credit applications or returned slips – anything that has personal information such as a name, address or phone number.

Your "trash" could be a thief's treasure, with all of the information a criminal needs to make a false card, as well as information about your company that could hurt you later if it fell into the wrong hands.

Recognize materials that may contain private information and dispose of them properly. Destroy any documents that have any personal information on them with a paper shredder before declaring them trash. Protecting your customers and your business is worth a few extra seconds.

The Terminal Repair Scam

This is the oldest scam in the book, but also one of the most popular and most effective ways for thieves to lift confidential information. We're all familiar with the "bait and switch" technique. They come into your business and tell you that your POS terminal needs to be repaired – offsite. But don't worry, they'll replace your broken one with a loaner. Once the loaner is in place, all of the information you scan through is recorded, and now the information is theirs. You may not even see it coming, as these criminals often pretend to work for POS companies or say that they are attending to other official business.

Any attempt to repair your terminal should be reported to the police, and no replacement terminals should be accepted. The safest thing you can do is to be cautious and report any suspicious happenings immediately by calling into the Global Payments Help Desk. They will help you verify whether your device has been scheduled for pick up and repair and as well as the authorized repair dealer.

Fraudulent Returns

Believe it or not, fraudulent returns are a major problem associated with fraud and theft. Staff members have been caught returning items that were never purchased and pocketing the money. In some cases, merchants don't even realize they have been victimized until it is too late. Make sure your employees take the necessary steps to ensure this doesn't happen in your business.

- Keep your point-of-sale terminal passwords confidential and stored in a safe place
- Change your password often to protect yourself in case someone does get into your system
- Don't share your terminal
- Make sure to follow the proper procedures when it is time to shut down your POS terminal at the end of each business day
- Keep a record of your balances each day so you can identify a problem as soon as it occurs

International Credit Cards

Take extra care when accepting international credit cards. Thieves use foreign cards because cashiers are not as familiar with them. The criminal searches for a busy merchant who may overlook irregularities in a card issued by a foreign bank rather than become suspicious.

Inspect the card thoroughly, checking to make sure the card is valid, and always swipe it. The security features of the card – logo, hologram, clear embossing, and so on – should be the same despite where the card originated. Check to make sure the signature matches the name on the card, and that once swiped, the number on the terminal matches the number on the card. Also, watch out for customers who check out the cashiers first before getting in line – criminals often look for an inexperienced clerk or someone who may be easily intimidated. If anything seems suspicious during the transaction, call in a Code 10.

Office Products Scams

Watch out for companies trying to sell office products such as copy paper, ink cartridges, stationery, and other supplies to your business. They may try to appear as if they are working for a reputable company. In reality, they will overcharge you for inferior merchandise. Deceptive telemarketing is a violation of the law – report any suspicious persons immediately.

Phone Fraud

Like the paper scammers, you may not see the phone fraud coming until it is too late. Of course there are the telemarketers who use the phone to further their illegitimate businesses and scam money. But what about the criminals that aren't selling anything at all? These crooks still use the phone to swindle merchandise from the retailer. Most of the time the criminal will phone a store, telling the clerk he has picked out the items he wants but cannot come to pick them up for some reason or another. He will ask the clerk to run his credit card through and assure the clerk that a courier will be by to pick up the merchandise. Once the merchandise has left the store, there is no way of knowing to whom it actually went or where it was going. Often these phone fraudsters pose as respected individuals with high profile jobs and qualifications. It is not uncommon, however, to find out the person has stolen a credit card and is using someone else's identity to receive the desired merchandise.

There is no real way of knowing if the card is legitimate in a situation where the cardholder is not able to show up. It is safest to stick to the rules in these situations – don't take credit card numbers over the phone, and reject a credit card that is not being handed to you by its lawful owner.

The Last Minute Shopper

Be on the lookout for the shopper who is purchasing expensive items just before closing time, or someone who is hurriedly filling a shopping cart with this type of item, without paying much attention to price, size or quality. These are the shoppers whose transactions need to be handled with your utmost attention.

Counterfeit Cards

Stolen and counterfeit cards are a huge problem for merchants and credit card issuers alike. Because of the technology available to them, counterfeiters are able to reproduce false cards that are high quality, even without the benefit of the original. All they really need is personal information and technology to produce credit cards, debit cards, and smart cards. The result is a huge financial loss to businesses around the globe.

Protect your business by teaching your staff to recognize the signs of a false credit card by checking the card security features every time you make a credit card sale. Call in a Code 10 if you suspect that the card presented to you seems suspicious.

Don't Hesitate! Call In a Code 10

Any time you have doubts about something – a fraudulent card, a signature or even a customer's behavior – call in a Code 10. A Code 10 allows you to call for an authorization without the customer becoming suspicious. After dialing the authorization center, inform the operator that you have a Code 10. The operator will put you through to the correct person, who will ask you a series of "yes" or "no" questions. Hold onto the card if possible while making the call. If the operator decides something is amiss, he or she will deny authorization. The operator may even request to speak with the cardholder to ask account information questions that only the true owner of the card would know.

A Code 10 can be used any time you feel a transaction may not be legitimate, even if you have already gotten approval on a transaction or if the customer had already left the premises. Following are potential reasons to call in a Code 10:

- If the embossing on the card is illegible
- If the last few numbers are not embossed on the hologram or if these numbers do not match the account number on the sales draft or at the terminal
- If there is no Bank Identification Number (BIN) above or below the first four digits
- If the name on the card does not match the signature or there is a misspelling
- If the hologram is not clear or the picture in the hologram does not move
- If the card does not have an expiration date
- If the card does not start with the correct numeric digit – all Visa cards should start with a 4, all cards from MasterCard® with a 5
- Be aware of cards that don't swipe – check these cards for other security features
- If a card does swipe, make sure the card number and the number that appears on the terminal match
- If you receive any message other than "approved" or "declined"

Defeating Fraud Helps You and Your Customers

Whether it's a different twist on an old scam or a new scam altogether, there will always be someone who tries to pull the wool over your eyes. If you and your staff are well prepared, however, with the skills to recognize suspicious transactions, and know how to correct the situation, then you're beating them at their own game. Take the extra steps to stop fraud before it starts. After all, it is the merchant – not the consumer – that stands to lose the most from credit card fraud. The most important thing you can do is stay educated on the ways fraud occurs and follow your instincts when you find yourself in a suspicious situation. The majority of the time, plain old common sense can prevent losses. Prevention is the most important step you can take. But should you suspect you have been the victim of a fraudulent activity, call Global Payments. We're here to help you and want to protect your interests.

**By following the information in this guide and working together,
we increase the chances of successfully protecting your business
against fraud!**