frontstream™ payments

Card present six best practices to avoid credit card fraud

Six best practices to avoid credit present fraud

- Criminals are always looking for the weakest link;the unlocked door.
- Advances in credit card security technology have improved with the widespread adoption of EMV chip. EMV saves merchants and consumers billions from counterfeits and unauthorized card use.
- Technology is only one part of the puzzle. Human error at the point of sale continues to remain a costly menace to merchants.
  - When employees aren't trained to detect common fraudulent practices, criminals see a wide-open door to your back pocket.
- Learning to detect the warning signs of fraud will help protect your business. These six best practices will help you avoid Credit Card fraud.

Because nobody wants to be the weakest link!

frontstream™ payments

1. Only accept cards from the authorized user.

- There are no “borrowing privileges” with credit and debit cards. The person whose name is on the front card and signature is on the back is the authorized user.
- Simple due diligence, that takes only seconds, can save you time and money down the road.

frontstream™ payments

2. Accept physically damaged cards at your own risk, or not at all.

- A common Card-Present fraud scheme occurs when cards are defaced so that they cannot be read by either magnetic strip or chip readers. Counterfeit cards are often damaged to bypass anti-fraud features. Swipe or dip every card that is handed to you, no matter how damaged or worn. Be wary of customers who let you know right away that their card won't read.
- It's your business, and you have the right to ask for another form of payment, or to decline the transaction rather than manually key-in information from a damaged card.

frontstream™ payments

3. Beware of fraudulent merchandise returns.

- Handling returns is an important customer service function. Criminals know this and see it as a weak link they can exploit. Making sure that your return policies are fully transparent to both your employees and your customers will minimize this risk.
- Small preventative measures in common sense procedures, and the people that implement them, will pay off big in reduced chargebacks from fraudulent returns.

frontstream™ payments

4.Understanding the how's and whys of payment red flags

- Nobody knows your business as well as you do. When it comes to the payments, credit card processing companies can also help identify red flags. Credit card processors continually monitor your transactions for fraudulent activity.
- If you need to perform any transaction that is out of character for your business, like running a large sale, call ahead to let FrontStream Payments know.
- Understanding why payment red flags are raised will help you manage legitimate transactions that fall outside your regular business patterns.

frontstream™ payments

5. Don’t be Bullied: Reasonable exceptions to “the customer is always right.”

- As you fight to grow your businesses, we live in a mindset where the customer is always right. But there are very appropriate limits.
- A no-tolerance policy for customer bullies is important. Bullies are not just a nuisance to your hard-working staff; they are also not limited to those committing fraud.
- Criminals will often intimidate a cashier by causing a fuss at the point of sale, rushing the purchase, complaining about the service, or anything to keep the cashier’s attention off the authorization of the credit card.
- Don’t be intimidated by bullies. Empower your employees to always make sure the correct procedure is followed when authorizing every credit and debit purchase. Bullying behavior may be a red flag on fraud.

frontstream™ payments

6. A merchant lifeline in cases of suspected credit card fraud: Code 10

- Whenever you encounter doubts about a credit or debit transaction, as a Merchant you have a trusted recourse: calling in for an authorization and informing the credit card processor of a Code 10.
- A Code 10 allows you to call for an authorization without the Customer becoming suspicious. If the card center determines something is amiss, he or she will deny authorization.

frontstream™ payments

6. A merchant lifeline in cases of suspected credit card fraud: Code 10 cont.

- Any time fraudulent activity is suspected is the right time to call in a Code 10. Be aware of cards that don't swipe or dip. Check these cards for other security features.
  - If the card does swipe or dip, make sure the card number and the number that appears on the terminal match.
  - If there is no Bank Identification Number (BIN) above or below the first four digits, that’s a red flag.
  - If the name on the card does not match the signature or there is a misspelling.
  - A Code 10 can be used any time you feel a transaction may not be legitimate.

frontstream™ payments

Conclusion

- Due diligence still matters, even in the age of “frictionless commerce.”
- Merchants seek to provide “frictionless commerce” by serving the needs of your customers wherever and whenever they are, instantly, before they gravitate to the competition.
- In the rush to provide your customers the best possible service, merchants can unwittingly make themselves vulnerable. Avoiding credit card fraud requires merchants to think about balance. Smart merchants invest by training employees who operate Point-of-Sale transactions to spot the red flags of fraud.
- Due diligence matters when it comes to your money. Following these best practices will help take the target off your back by ensuring that your business is not the weakest link.

frontstream™ payments