QUICK REFERENCE

Protecting your payment terminal

Document purpose

The purpose of this document is to help merchants protect themselves from fraud-related risks and provide their customers with a more secure environment. For your security and that of your customers, it's important to follow the guidelines for transactions, whether they're carried out in person, online, over the phone or by mail.

This document outlines best practices that you should use to prevent fraud.

This document is for: Merchants

Last updated: June 2018

How to protect against fraud

Best practices that all merchants should be using

- Take the customer's card and verify it—it's your responsibility.
- Make sure all your employees are trained on how to use the payment terminal, that they know the methods for accepting cards, and that they use the chip reader as their standard method. Chip technology is very reliable; if a chip can't be read, it should raise suspicions.
- Make sure the credit card has all the security features: embossed card number, first four digits of the number printed above or below it, and a printed three- or four-digit security code.
- If you need to swipe or manually enter the card number, compare the signature on the back of the card with the signature on the receipt.
- If you need to swipe the card, compare the first and last four digits of the embossed card number with what appears on the receipt.
- **NEVER** authorize a cash withdrawal on a credit card. This practice is prohibited. Cash can only be withdrawn during debit card transactions.
- Regularly change your administrative personal identification number (PIN) for your payment terminal (see user guide). Your administrative PIN lets you access restricted features, like cancelling or refunding transactions.
- Never provide a refund using a different card than the one used for the original purchase.
- For online transactions, you can always contact the card issuer to confirm the customer's name and address.

Phone or mail orders

Ask for the customer for the following:

- Security code (three or four digits) printed on the card
- Name of the cardholder as it appears on the card
- Expiry date as it appears on the card
- Card account mailing address
- Cardholder's telephone numbers (home and cellular)
- Signature upon delivery, if possible

Online payments

Use security features such as:

- Address Verification Service (AVS), to confirm the card account mailing address
- Security code verification (three or four digits) printed on the card
- Verification options likes Verified by Visa and Mastercard SecureCode
- Verification of the card in a negative database
- Verification of the card expiry date and the cardholder's name

Tips for preventing fraud

5 tips to protect against fraud

1. **Giving the terminal to the customer**. Hand the terminal to the customer ONLY after you've entered and confirmed the transaction amount.
2. **Watching the customer**. Watch the customer when they use the terminal, to make sure they don't enter any information manually.
3. **Chip card only**. Make sure that the transaction is carried out with the chip and not the magnetic stripe.
4. **Refunds**. Set up an administrative PIN on your terminal to prevent fraudulent refunds to debit and credit cards.
5. **Administrator PIN**. Regularly change your administrator PIN for the terminal and only give this password to trustworthy employees.

Tips for detecting fraud

Here are some tip-offs that there might be fraud:

- **An order seems suspicious**. Call the customer to confirm the order; fraudsters often use fake phone numbers.
- The **same credit card is used** for several orders in a short period of time.
- **Several orders for delivery to the same address** are made within a short period of time.
- **The customer's IP address doesn't match the credit card's issuing country** or is from a high-risk country.
- A customer makes a **very expensive order** or buys a **large quantity of an item**.

How to protect your terminal

In-store terminals	Mobile terminals
Attach your terminal to a specially designed stand to prevent theft and vandalism.	If possible, attach your tablet or smartphone to a stand.
Keep a constant eye on the terminal, because criminals often work as a team—one creates a distraction while the other works on the terminal.	Never leave your device unattended.
Stay by your customers when you hand them the payment terminal at their table.	Keep your terminal in a secure location; never leave it in sight in your vehicle.
Put your terminals under the counter or in a secure location before closing up for the day.	

Suspect fraud?

What to do if you suspect fraud:

- Take the customers' card and check the security features.
- Make sure the last four digits on the card match the four digits printed on the transaction receipt.
- Ask for two pieces of photo ID to identify the cardholder and check their signature, if applicable. However, you may not record their personal information.
- If you still suspect fraud, call your payment terminal provider to find out what to do next.