REFERENCE SHEET

PROTECTING YOUR PAYMENT TERMINAL

Purpose of the document

Help merchants protect themselves from fraud-related risks and provide their clients with a more secure environment. For your security and that of your clients, 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.

How to protect against fraud

Best practices for all merchants

- 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. This technology is very reliable, so 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 3- or 4-digit security code printed on the back.
- 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 transaction. This practice is prohibited. Cash can only be withdrawn on debit card transactions.
- Change your administrative personal identification number (PIN) regularly for your payment terminal (see user guide). Your administrative PIN lets you access restricted features, such as 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 client's name and address.

Telephone or postal orders

Ask the client for the following information:

- Security code (3 or 4 digits) printed on the back of the card
- Cardholder's name, as it appears on the card
- Cardholder's name, as it appears on the card
- Account statement mailing address
- Cardholder's telephone numbers (home and mobile)
- A signature when the order is received, if possible

Online payments

Use the following security features:

- Address Verification Service (AVS) to confirm the card account mailing address
- Security code verification (3 or 4 digits) printed on the back of the card
- Verification options, such as Verified by Visa and Mastercard SecureCode
- Verification of the card in negative databases
- Verification of the card expiry date and the cardholder's name

Fraud prevention tips

5 tips for preventing fraud:

1. **Handing the terminal to the customer.** Hand the client the terminal ONLY after the transaction amount has been entered and confirmed.
2. **Watching the client.** Watch while the client uses the terminal to make sure no information is entered manually.
3. **Chip card.** Make sure 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.

Fraud detection cues

Remain vigilant when:

- An order **seems suspicious. Call the client to confirm the order**; fraudsters often use fake phone numbers
- The **same credit card is used** for multiple orders in a short time span
- **Several orders are delivered to the same address** in a short time span
- **The client's IP address does not match the country that issued** the credit card or the card comes from a country deemed to be high risk
- A client places a **very expensive order** or buys a **very large quantity of a product**

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 close by to the **client when you hand them the terminal for payment at their table.**

Keep your terminal in a **secure place**; never leave it in plain sight in your car.

Place **terminals under the counter or in a secure place before closing up.**

If you suspect fraud

What to do if you suspect fraud:

- Take the customers' card and check the security features.
- Make sure the last 4 digits on the card match the 4 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 steps to take.