POS Fraud Prevention Training Manual

evertec®

INTRODUCTION

Fraud in point-of-sale (POS) systems is a serious threat that can compromise the financial security of both our company and our customers. This manual is designed to train employees to recognize signs of fraud—such as skimming devices and suspicious transactions—and to provide clear procedures for responding to potential risks.

External Personnel Identity Verification

There have been reports of individuals fraudulently claiming to represent Evertc in order to gain access to POS terminals.

For your safety:

- Do not allow unauthorized individuals access to your terminal.
- Never hand over your devices, passwords, or sensitive information without first verifying their identity.

What should you do?

1. Request official identification from anyone claiming to represent Evertec.
2. Verify their information by calling our official customer service number: (787) 759-9999

Following this process is essential to prevent fraud.

1. Identifying POS Fraud

Skimming Indicators on POS Terminals

- Presence of external devices or visible modifications to the card reader.
- Loose card reader or parts that appear to have been recently added.
- Repeated error messages during payment processing.
- The need to swipe a card several times before the transaction goes through.

Characteristics of a Fraudulent Transaction

- Multiple failed payment attempts using different cards.
- Unusually large or high-volume purchases.
- Customer avoids entering security codes or providing a digital signature.
- Nervous or evasive behavior by the customer.

2. Procedures in Case of Suspected Fraud

If an employee detects signs of fraud on a POS terminal, they should follow these steps:

Step 1:
Do Not Alert the Suspect

- Stay calm and avoid direct confrontation.
- Do not ask questions that could tip off the suspect

Step 2:
Immediately Inform the Supervisor

- Report the incident to the shift supervisor.
- Clearly describe what happened and the suspicious signs you observed.

Step 3:
Record Incident Details

- Note the date, time, and a description of the suspected fraudulent activity.
- If possible, save images or video of the transaction (in compliance with privacy regulations).

Step 4:
Inspect the POS Terminal

- Physically inspect the POS device for signs of tampering or unfamiliar attachments.
- If tampering is found, disconnect the terminal and notify the security provider.

Step 5:
Report to Financial Institutions

- Inform the affected bank or card provider of the case.
- Provide the necessary information so compromised cards can be blocked if needed.

3. Preventive Measures for Employees and the Company

For Employees

- Regularly inspect the physical condition of POS terminals.
- Avoid sharing confidential information about the payment system.
- Report any suspicious activity without delay.

For the Company

- Use updated software with integrated POS security systems.
- Conduct regular audits of payment devices.
- Offer continuous training programs in fraud detection.
- Encourage internal communication and reporting of suspicious activity.

4. Security Contacts

In case of emergency or questions, employees may contact:

- Shift Supervisor: [Contact]
- Security Team: [Contact]
- POS System Provider: [Contact]
- Associated Bank: [Contact]
- Evertec Customer Service: (787) 759-9999