Credit and Debit Card Fraud and Security Procedure

Western Illinois University

Introduction

Credit and Debit Card security is a shared responsibility. Merchants accepting cards must be on guard against credit and debit card fraud. Basic steps are to be taken to protect both consumers and the University from fraudulent card transactions.

Examples of Credit and Debit Card Fraud

Altered Cards. On an altered card, the name, expiration date, account number, and/or the magnetic stripe have been changed in some way.

Altered Equipment. Be aware of any potential altering or tampering of credit and debit card machines or devices.

Counterfeit Cards. Counterfeit cards bear a valid account number. A valid card number may appear on the front of the card, in the magnetic stripe on the back of the card, or in both places.

Lost/Stolen Card. A card is stolen from the cardholder and used fraudulently to purchase goods or services from a legitimate merchant.

Mail Order/Phone Fraud. Someone other than the authorized cardholder obtains an account number (often with the expiration date of the account and card validation code from the back of the card) and uses it to purchase goods or services by mail or by phone.

Online Order Fraud. Someone other than the authorized cardholder obtains an account number (often with the expiration date of the account and card validation code from the back of the card) and uses it to purchase goods online.

What is Not Credit and Debit Card Fraud?

There are many legitimate reasons that a credit or debit card transaction may be declined. Some examples follow.

- A payment on the account is overdue
- A technical malfunction has occurred during transaction processing
- An international purchase has been recently made with the card
- The card issuer has put a hold on the card
- The card was exposed to a potential security threat
- The customer has reached their credit card limit
- The card is expired

Point of Sale Credit and Debit Card Checklist for Employees

Become familiar with new card designs. Some cards are un-embossed. These cards may look different – they have no raised (embossed) numbers, so you cannot make a manual imprint – but the brand behind them is the same. Credit card chip technology adds an additional layer of security protection.

Check the embossed numbers on the front of the card. If an account number is embossed, the embossing should be clear and uniform in size and spacing. These numbers should not be chipped away. And no "halos" of previous numbers should appear under the embossed account number.

Examine the hologram. A hologram may be on the front or back of the card. The three-dimensional hologram should reflect light and appear to move when the card is rotated.

Compare signatures. The back of the card must be signed, and the signature should reasonably compare to the cardholder signature on the sales receipt. Check to make sure that it has not been taped over, mutilated, erased or altered in any suspicious manner. The word "Void" on the signature panel indicates that the signature panel has been tampered with.

Look at the magnetic stripe. The magnetic stripe on the reverse of the card should appear smooth and straight, with no signs of tampering.

Examine the expiration date. The card should not be accepted after the last day of the "expires end" or "valid thru" date embossed on the card. Merchant sales assistants must validate the card expiration date.

For unsigned Credit and Debit Cards. Ask the customer to sign the credit card and supply an official government ID. Verify that that the signature on the credit card and ID match.

Contact a Supervisor. If card verification steps have been followed and suspicious activity is suspected, remain calm, keep hold of the card, inform the customer that additional card verification is required, and contact a supervisor.

Supervisor Approval of Credit or Debit Card Transactions

Be observant of the customer's behavior, does it seem normal, or does the person appear uneasy? For your and your staff's safety, do not, under any circumstances, confront or try to apprehend the customer. If safety is a concern, call 911.

To verify that the customer using the card is the actual cardholder. You may request a form of ID, however the customer has the right to not show an ID if the credit card is signed, or if they cancel the purchase transaction.

To obtain a voice authorization code. Call the Authorization Center of the credit card company, or the Merchant Bank of the debit card and request an Authorization Code.

For Credit Cards

- American Express Assistance Center 1-800-528-2121
- Discover Assistance Center 1-800-347-1111
- MasterCard Assistance Center 1-800-622-7747
- VISA Assistance center 1-800-847-2911

For Debit Cards

- Call the number on the back of the customer's debit card

Other Options

- Call your own Merchant Provider's Voice Authorization Number

If a fraudulent activity is suspected. Contact the following for assistance.

- If safety is a concern, call 911
- WIU Business Services – 309-298-1811