UCSD Credit Card Processing Policy & Procedure

The Payment Process

UCSD accepts Visa, MasterCard, American Express and Discover credit cards. We accept credit and debit transactions. Note: no debit sales with cash back.

Verify that the signature on ID matches credit card, if cardholder's name does not match name on identification do not accept card for payment, ask for another form of payment. Check the back of the credit card to see if it has been signed and is current. If it has not been signed, the cardholder must show you a current, valid, picture identification card (passport or driver's license).
If the customer is using a chip (EMV) card, there is no need for the cashier to check the card (or to identify the cardholder).

Note: Merchants accepting EMV cards are protected against fraudulent transactions.

Roles and Responsibilities

All UCSD merchants:

Front End Employees, Supervisors and Managers-
All are allowed to process payments
Supervisors and/or Managers-
Approve and process refunds on terminal

Sensitive Authentication Data:

There should not be any credit card information written down or processed at any location without assessment of PCI Administrator and proper process documentation. All paper with credit card information, arrived either by mail or telephone, should be properly destroyed with *cross shredders*. Credit card information should never be stored. Totally outsourced e-Commerce merchants should never process credit card at the merchant locations.

Sensitive authentication data consists of full track data, card security codes, or values (CAV2, CID, CVC2, CVV2) and PIN data must not be stored after authorization, even if it is encrypted.

No credit card information is to be sent via end-user message technologies (such as emails, text, etc.).

BusinessTrack (ClientLine) Reporting Access:

Only supervisors and/or managers should have access to the Bank of America reporting tool – BusinessTrack (Formerly ClientLine) with credit card sales information. All users, regardless of roles, can only access masked Primary Account Numbers (PANs) on BusinessTrack with only the last four digits displayed.

Maintaining Terminal Information

Department is to maintain an updated list of all terminal devices (ex: merchant ID, terminal ID, model of device) and list of authorized personnel who can process a credit card transaction at all time. Any changes to location of terminal, relocation, removing or adding, need to be approved Campus Credit Card Coordinator. No other devices are allowed to be used at any given time. Terminal is to be used for payments for [approved merchant] only. Use of this device for any other merchant activities, or non- UC Regents activities, is prohibited. Merchant is not allowed to change terminal ID, merchant ID, or any other terminal settings without approval of the General Accounting office. General Accounting will review documents on an annually basis.
See "PCI DSS Req. 9.9 Equipment inspection" in the link below for more information.
http://blink.ucsd.edu/finance/cash/credit-debit-cards/pci-dss/index.html#PCI-DSS-Requirement-9.9-Equipme

Tampering of Terminal

This section is to educate employees on what to look for and what to do if a terminal is tampered with.

The department supervisor is required to check the terminal on a daily basis for evidence of tampering. A daily log of inspection completion is to be kept for auditing purposes. The terminals should be placed in an area where the public cannot access them without being noticed.

Criminals use a technique called skimming to capture and transfer payment data to another source. By checking the terminal for any evidence of tampering minimizes the chances of credit card information being stolen. Always be cautious of unannounced service visits. Criminals can use this opportunity to gain access to a terminal and install a skimming device.

- Examples of tampering
    a) Check the terminal for any security stickers placed over screw holes or seams that will act as indicators of the case has been opened. Criminals often remove these labels when compromising terminals and may replace them with their own printed versions. Also, look for any signs that the label may have been removed or tampered with.
    b) Check for changes to terminal connections.
    c) Be aware of any additional, unfamiliar electronic equipment connected to the terminal.

- Examples of theft or loss of terminal to escalate
    a) Identified terminal is missing.
    b) Your location was robbed and terminal is missing.
    c) Lost terminal during a relocation.

- Escalation process if you suspect tampering, theft or loss of terminal:
    1) Disconnect terminal and stop accepting credit card payments
    2) Notify your immediate supervisor
    3) Contact the General Accounting Office
    4) Contact PCI Administrator at Junni Liu jul019@ucsd.edu x20247 or Aurea Webb awebb@ucsd.edu x61784

Theft or Loss of Terminal

If you suspect individuals with suspicious behavior attempting to service terminal without Credit Card Coordinator and/or IT Security authorization, staff is to escalate as indicated in this policy.

References:

UCSD PCI-DSS Blink page
http://blink.ucsd.edu/finance/cash/credit-debit-cards/pci-dss/index.html
UCSD Policy & Procedure Manual PPM300-86
http://adminrecords.ucsd.edu/PPM/docs/300-86.HTML
Computer Incident Response Team (CIRT) Process
https://blink.ucsd.edu/technology/security/services/cirt.html
PCI Security Standards Council – Guidance documents (Skimming Prevention) type "skimming" in search box (Resource Guide, Best Practices for Merchants and Overview of Best Practices for Merchants)
https://www.pcisecuritystandards.org/document_library
P2PE Merchants
https://www.bluefin.com/
https://www.bluefin.com/products/p2pe-point-to-point-encryption/p2pe-manager/
https://www.bluefin.com/products/emv/

AT A GLANCE:
SKIMMING PREVENTION

Skimming Prevention: Overview of Best Practices for Merchants

Skimming is the unauthorized capture and transfer of payment data to another source. Its purpose is to commit fraud, the threat is serious, and it can hit any merchant's environment. With skimming, thieves steal payment data directly from the consumer's payment card or from the payment infrastructure at a merchant location. Both techniques typically require the use of a rogue physical device planted onsite. PCI Security Standards currently contain a number of requirements and recommendations to guard against skimming. In addition, the Council has introduced an overview document for merchants, containing a "deep dive" into skimming with examples, best practices, and tools to thwart its use. This "At-a-Glance" piece provides a snapshot of skimming and introduces areas requiring countermeasures to ensure an appropriate level of security for cardholder data.

MERCHANTS MUST TAKE STEPS TO PREVENT SKIMMING

Skimming equipment can be very sophisticated, small, and difficult to identify (see photos on reverse). Merchants are the first line of defense because skimming gear is frequently deployed at the merchant's point of sale or network. Consequently, it is critical for merchants to become familiar with this category of threats and to take precautions.

Video Resources
- **PCI SSC YouTube Channel**
- **APCA**

Who Does It? Perpetrators skim because it is highly profitable. They may be sophisticated and organized criminals leading complex, effective attacks. Or they may be relatively unsophisticated criminals who use readily available, simple technology to steal cardholder data.

Targets for Attack. There are at least five potential targets for skimming. These include PIN data, often visually captured by people standing near a POS device or by use of fake PIN entry devices; unattended or temporarily unattended terminals; merchants with a high overall transaction volume (allowing a criminal to capture a large amount of data in a short period of time); individual terminals with a heavy volume of usage; and merchants with periods of high-volume sales.

Impact of Skimming Attacks. There is a cost to skimming attacks that is over and above the actual loss of monies, goods, and services: Skimming attacks undermine the integrity of the payment system, employee trust, industry relationships, and consumer trust in the merchant.

USING THE GUIDELINES TO PREVENT SKIMMING

Download the document, *Skimming Prevention: Best Practices for Merchants,* at **https://www.pcisecuritystandards.org/security_standards/documents.php.**

The document provides specific recommendations for the contents outlined in the sidebar below. Please see the document for details, including guidelines and best practices, a risk assessment questionnaire, and evaluation forms.

SKIMMING PREVENTION: BEST PRACTICES FOR MERCHANTS

CONTENTS:

Examples of Terminal Fraud

Criminals use a variety of techniques to skim cardholder data from transactions at the point of sale and through the merchant's payment system. Photos and sidebars below show three examples of devices used to skim at the point of sale. The document has more examples.

Skimming devices hidden within the terminal are invisible, and neither the merchant staff nor the cardholder will know that a card was skimmed.

This picture shows a skimming device inserted in a terminal. The device was hidden by the SIM card cover plate.

Changes to terminal connections can be difficult to spot.

In these images, the criminals completely changed the cable connecting the terminal to the base unit.

The fatter cable housed additional wires required to capture cardholder data.

Handheld skimmers used by corrupt staff are very small, fitting in the palm of a hand.

Despite their size, these devices can store a significant amount of cardholder data.

GUIDELINES AND BEST PRACTICES

Guidelines and best practices mentioned are non-exhaustive. They cover:

Merchant Physical Location. Merchants must address measures affecting terminals, terminal infrastructure, cameras, placement, access, and image storage.

Terminals and Terminal Infrastructure Security. Areas requiring attention include terminal surroundings, IP connectivity, individual terminal data, terminal reviews, terminal purchases and updates, terminal disposal, PIN protection, and wireless terminals.

Staff and Service Access to Payment Devices. Areas affecting people include staff as targets, hiring and staff awareness, outside personnel, and service providers.

Risk Analysis of Terminals and Terminal Infrastructure. The analysis includes identification of assets, threat and probability, and severity. Tools are provided to help with the analysis.

Merchant Acknowledgement

I have read the SAQ for my merchant *and* the Credit Card Processing Instructions and I understand that I must maintain full PCI DSS compliance at all times.

Signed name:_____ Date: _____

Printed name:_____ Title: _____

Merchant name:_____ Merchant ID:_____