



CALIFORNIA STATE UNIVERSITY, LONG BEACH

Subject:	Security Breach of Credit/Debit Cardholder Data		
Department:	Information Security Management and Compliance	Reference No.:	
Division:	Administration and Finance	Issue Date:	September 2007
References:	• Payment Card Industry (PCI) Data Security Standards (DSS) Version 1.1	Revision Date:	
Web Links:	http://daf.csulb.edu/offices/vp/information_security	Expiration Date:	N/A

This document outlines procedures and protocols for campus response to security incidents and breaches involving credit/debit (payment) cardholder data. These procedures and protocols are additional to those outlined in the University [Security Incident Reporting and Breach Notification Procedures](#).

I. BACKGROUND

In response to increasing incidents of identify theft, the major payment card companies – American Express, Discover, MasterCard, and Visa – created regulations to help prevent theft of consumer data. These regulations are known as the Payment Card Industry (PCI) Data Security Standards (DSS). The PCI DSSs are multifaceted and include requirements for security management, policies, procedures, network architecture, software design and other critical protective measures.

The PCI Data Security Standards are not law. Compliance with the PCI DSS is a contractual obligation between the University and each of the payment card companies to proactively protect cardholder data. Each of the major payment card companies has specific and required procedures for providing notification to them in the event of a suspected and/or confirmed unauthorized acquisition of cardholder data.

II. DEFINITIONS

Definitions are included in **Appendix A**.

III. PROCEDURES

A. Immediately Notify Payment Card Companies

Upon notification of a suspected unauthorized acquisition of cardholder data, the Information Security Officer or designee shall immediately notify the following entities:

- MasterCard Compromised Account Team at compromised_account_team@mastercard.com **and** by phone – (636) 722-4100
- Visa USA Fraud Investigations and Incident Management Group – (650)432-2978
- American Express – (800) 528-5200
- Discover Merchant Security Department – (800) 347-3083
- The Merchant Bank
- Los Angeles Office of the U.S. Secret Service – (213) 894-4830

B. Incident Investigation

The Information Security Officer or designee shall conduct an incident investigation within 24 hours to determine the following:

1. Type of cardholder data at risk. Data may include:
 - Cardholder name
 - Cardholder address
 - Cardholder Primary Account Number (PAN)
 - Card expiration date
 - Card Validation Code/Card Verification Value

- Magnetic stripe (track) data
 - PIN
 - PIN blocks
2. Number of cardholder accounts at risk
 3. Incident timeframe for cardholder accounts at risk
 4. Suspected cause of incident

If it is determined that cardholder data has not been compromised, the Information Security Officer or designee shall notify the payment card companies and advise that cardholder data has not been compromised.

C. Confirmed Security Breach

Within 24 hours of knowledge of a confirmed security breach and knowledge that cardholder data has been compromised, the Information Security Officer or designee shall notify the following entities:

- MasterCard Compromised Account Team by email at compromised_account_team@mastercard.com or by phone – (636) 724-1000. Email a detailed written statement about the account compromise, including the contributing circumstances, and a complete list of all potentially or known to be compromised account numbers.
- Visa USA Fraud Investigations and Incident Management Group – (650) 432-2978
- American Express – (800) 528-5200
- Discover Merchant Security Department – (800) 347-3083
- The Merchant Bank
- Los Angeles Office of the U.S. Secret Service – (213) 894-4830

D. Subsequent Notification

Within three (3) business days of the reported compromise, the Information Security Officer or designee shall:

- Provide an *Incident Response Report* to:
 - MasterCard Merchant Fraud Control staff
 - Visa USA Fraud Investigation and Incident Management Group
 - American Express
 - Discover Merchant Security Department
 - The Merchant Bank

Within ten (10) business days, the Information Security Officer or designee shall:

- Provide all compromised Visa, Interlink, and Plus primary account numbers to the merchant bank as instructed by the merchant bank and to Visa Investigations and Incident Management Group.

E. Additional Requirements

Additional requirements are at the sole discretion of the payment card companies and are likely to include the following:

- Depending upon the level of risk and data elements obtained by unauthorized persons, an independent forensic investigation and vulnerability scan of the campus network
- Weekly written status reports addressing open questions and issues, until the audit is considered to be complete
- Completion of a PCI DSS Compliance Questionnaire

IV. PCI RESPONSE TO NON-COMPLIANCE

If investigation of the incident reveals that the University or an auxiliary organization's non-compliance with the PCI DSS contributed to the account compromise or if the University or auxiliary organization was negligent in reporting or investigating the loss of cardholder data, fines and penalties may be assessed.

The payment card companies may take any or all of the following actions:

- Charge up to \$500,000 per security incident if the cardholder information is compromised;
- Prohibit the University and/or auxiliary organization from accepting payment cards for goods or services;
- Fine the University and/or an auxiliary organization up to \$100,000 per security incident for failure to notify of probable or actual violations or compromise of cardholder data

FURTHER INFORMATION

Information Security Management and Compliance

iso@csulb.edu

(562) 985-2283

Card Validation Value or Code	<p>The three-digit value printed on the signature panel area of a payment card, typically used to verify card-not-present transactions.</p> <ul style="list-style-type: none">• CVC2 Card Validation Code 2 (MasterCard payment cards)• CVV2 Card Verification Value 2 (Visa payment cards)• CID Card Identification Number (American Express and Discover payment cards)
Cardholder	<p>The customer to whom a payment card has been issued or the individual authorized to use the card.</p>
Cardholder Data	<p>All personally identifiable data about the cardholder (i.e., primary account number, magnetic stripe, service code, expiration date, data provided by the cardholder, other electronic data gathered by the merchant/agent, and so on). This term also accounts for other Confidential Information gathered about the cardholder (i.e., addresses, telephone numbers, and so on).</p>
Compromise	<p>Intrusion into computer system where unauthorized disclosure, modification, or destruction of cardholder data may have occurred.</p>
Magnetic Stripe Data (Track Data)	<p>The magnetic stripe on the back of all payment cards which contains encoded data used for authorization during a card present transaction. The University may not retain full magnetic stripe data subsequent to transaction authorization. Specifically, subsequent to authorization, service codes, discretionary data/CVV/CVC/CID, and payment card reserved values must be purged; however, account number, expiration date, and name may be extracted and retained.</p>
Merchant Bank	<p>A financial institution that initiates and maintains contractual agreements with merchants for the purpose of accepting and processing payment card transactions.</p>
Payment Card	<p>A phrase used to describe credit and debit cards that contain the American Express, Discover Financial Services, JCB, MasterCard Worldwide and Visa International logos.</p>
PIN	<p>Abbreviation for Personal Identification Number. The four digit security code used to verify the customer is the authorized user of the payment card.</p>
PIN Blocks	<p>Created immediately when a PIN is entered by a cardholder at a Point of Sale. To protect the PIN during electronic transit, it is formatted into a PIN block, the PIN block is encrypted under a transport key and the resulting Encrypted PIN Block (EPB) is sent for verification.</p>
Primary Account Number (PAN)	<p>Is the payment card number (credit or debit) that identifies the issuer and the particular cardholder account.</p>
Security Incident	<p>A collection of related activities or events which provide evidence that confidential information or cardholder data could have been acquired by an unauthorized person.</p>
Security Breach	<p>An unauthorized acquisition of cardholder data.</p>