Credit Card Security Incident Response Plan

Bradley University has a thorough data security policy [1]. To address credit cardholder security, the major card brands (Visa, MasterCard, American Express, Discover & JCB) jointly established the PCI Security Standards Council to administer the Payment Card Industry Data Security Standards (PCI DSS) that provide specific guidelines for safeguarding cardholder information. One of these guidelines requires that merchants create a security incident response team and document an incident response plan. The Bradley University Credit Card Security Incident Response Team (Response Team) is comprised of the Director of Information Security, the Senior Accountant, the Assistant Controller, the Director of System Integration, and the System Administrator (see below for names and contact information). The Bradley University security incident response plan is as follows:

1. Each department must report an incident to the Director of Information Security (preferably) or another member of the Response Team.
2. That member of the team will report the incident to the entire Response Team.
3. The Response Team will investigate the incident and assist the compromised department in limiting the exposure of cardholder data.
4. The Response Team will resolve the problem to the satisfaction of all parties involved, including reporting the incident and findings to the appropriate parties (credit card associations, credit card processors, etc) as necessary.
5. The Response Team will determine if policies and processes need to be updated to avoid a similar incident in the future.

Bradley University Credit Card Security Incident Response Team (Response Team)

Director of Information Security	David Scuffham	(309)677-3041	david@bradley.edu
Senior Accountant	Ellen Keenan	(309)677-3116	efm@bradley.edu
Assistant Controller	Ryan Schmidgall	(309)677-3130	rschmidgall@bradley.edu
Director of System Integration	Ramona Hutchison	(309)677-2962	rkh@bradley.edu
System Administrator	Steve Herrera	(309)677-2336	sherrera@bradley.edu

Incident Response Plan

[1] Bradley University Data Security Policy:
http://www.bradley.edu/irt/policies/

Prior to proceeding with any of the following steps, the department must:

1. Contact a member of the Response Team.
2. Assess the threat with the Response Team.
3. In conjunction with the Response Team, determine if an account compromise event has occurred or a security breach has occurred wherein there is a suspected or confirmed loss or theft of any material or records that contain credit cardholder data.
4. If it is determined that a security breach has occurred that may have compromised credit cardholder data, proceed as indicated below. A formal Incident Response Report may need to be completed.

IT Security Incident Response Procedures

The Bradley University Credit Card Security Incident Response Team must be contacted by a department in the event of a system compromise or a suspected system compromise. After being notified of a compromise, the Response Team, along with other designated university staff from Information Technology (IT), will implement their incident response plan to assist and augment departments' response plans.

In response to a systems compromise, the Response Team and IT will:

1. Ensure compromised system is isolated on/from the network.
2. Gather, review and analyze all centrally maintained system, firewall, file integrity and intrusion detection/protection system logs.
3. Assist department in analysis of locally maintained system and other logs, as needed.
4. Conduct appropriate forensic analysis of compromised system.
5. Contact the Controller's Office, University Police and/or other law enforcement agencies as appropriate (See Appendix B).
6. Make forensic and log analysis available to appropriate law enforcement or card industry security personnel.
7. Assist law enforcement and card industry security personnel in investigative process.

The credit card companies have individually specific requirements the Response Team must address in reporting suspected or confirmed breaches of cardholder data. See Appendix A for these requirements.

APPENDIX A

MasterCard Specific Steps:
See Account Data Compromise User Guide at:
https://www.mastercard.com.cn/content/dam/mccom/zh-cn/merchants/documents/AccountDataCompromiseUserGuide.pdf

1. Within 24 hours of an account compromise event, notify the MasterCard Compromised Account Team at account_data_compromise@mastercard.com
2. Provide a detailed written statement of fact about the account compromise (including the contributing circumstances)
3. Provide the MasterCard Merchant Fraud Control Department with a complete list of all known compromised account numbers.
4. **Within 72 hours of knowledge of a suspected account data compromise (ADC),** engage the services of a PCI SSC Forensic Investigator (PFI) to conduct an independent forensic investigation to assess the cause, scope, magnitude, duration, and effects of the ADC Event or Potential ADC Event.
5. Provide weekly written status reports to MasterCard, addressing open questions and issues until the audit is complete to the satisfaction of MasterCard.
6. Promptly furnish updated lists of potential or known compromised account numbers, additional documentation, and other information that MasterCard may request.
7. Provide finding of all audits and investigations to the MasterCard Merchant Fraud Control department within the required time frame and continue to address any outstanding exposure or recommendation until resolved to the satisfaction of MasterCard.

Once MasterCard obtains the details of the account data compromise and the list of compromised account numbers, MasterCard will:

1. Identify the issuers of the accounts that were suspected to have been compromised and group all known accounts under the respective parent member IDs.
2. Distribute the account number data to its respective issuers.

VISA U.S.A. Specific Steps:

(Excerpted from VISA U.S.A. Cardholder Information Security Program (CISP), What To Do If Compromised, October 2019)

Refer to documentation online at
https://usa.visa.com/dam/VCOM/download/merchants/cisp-what-to-do-if-compromised.pdf

In the event of a security beach, the **Visa U.S.A. Operating Regulations** require entities to immediately report the breach and the suspected or confirmed loss or theft of any material or records that contain cardholder data. Entities must demonstrate the ability to prevent future loss or theft of account information, consistent with the requirements of the VISA U.S.A. Cardholder Information Security Program. If VISA U.S.A. determines that an entity has been deficient or negligent in securely maintaining account information or reporting or investigating loss of this information, VISA U.S.A. may require immediate corrective action.

If a merchant or its agent does not comply with the security requirements or fails to rectify a security issue, VISA may:

- Fine the Member Bank
- Impose restrictions on the merchant or its agent, **or**
- Permanently prohibit the merchant or its agent from participating in VISA programs.

VISA has provided the following step-by-step guidelines to assist an entity in the event of a compromise. In addition to the following, VISA may require additional investigation. This includes, but is not limited to, providing access to premises and all pertinent records.

Steps and Requirements for Compromised Entities

1. Immediately contain and limit the exposure.

   To prevent further loss of data, conduct a thorough investigation of the suspected or confirmed loss or theft of account information within 24 hours of the compromise. To facilitate the investigation:
   - Do not access or alter compromised systems (i.e., don't log on at all to the machine and change passwords, do not log in as ROOT).
   - Do not turn the compromised machine off. Instead, isolate compromised systems from the network (i.e., unplug cable).
   - Preserve logs and electronic evidence.
   - Log all actions taken.
   - If using a wireless network, change Service Set Identifier (SSID) on the access point and other machines that may be using this connection (with the exception of any systems believed to be compromised).
   - Be on HIGH alert and monitor all VISA systems.

2. Alert all necessary parties, including:

   - Internal information security group and Incident Response Team, if applicable
   - Legal department
   - Merchant bank
   - VISA Fraud Control Group at USFraudControl@visa.com in the U.S.
   - Local FBI Office, U.S. Secret Service, or RCMP local detachment, if VISA payment data is compromised.

3. Provide the compromised Visa account to VISA Fraud Control Group at USFraudControl@visa.com within 24 hours.

   - Account numbers must be securely sent to VISA as instructed by VISA. It is critical that all potentially compromised accounts are provided. VISA will distribute the compromised VISA account numbers to Issuers and ensure the confidentiality of entity and non-public information.

4. Requirements for Compromised Entities
    - All merchant banks must:
        - Within 48 hours of the reported compromise, provide proof of Cardholder Information Security Program compliance to VISA
        - Provide an incident report document to VISA within four business days of the reported compromise
        - Provide an additional incident report document to VISA no later than fourteen days after initial report (See template: Appendix C)
        - Depending on the level of risk and data elements obtained, complete within four days of the reported compromise
            - An independent forensic review
            - A compliance questionnaire and vulnerability scan upon VISA's discretion

Steps for Merchant Banks

1. Contact Visa USA Fraud Control Group immediately at USFraudControl@visa.com

2. Participate in all discussions with the compromised entity and VISA USA

3. Engage in a VISA approved security assessor to perform the forensic investigation

4. Obtain information about compromise from the entity

5. Determine if compromise has been contained

6. Determine if an independent security firm has been engaged by the entity

7. Provide the number of compromised VISA accounts to Visa Fraud Control Group within 24 hours

8. Inform Visa of investigation status within 48 hours

9. Complete steps necessary to bring entity into compliance with CISP according to timeframes described in "What to do if Compromised"

10. Ensure that entity has taken steps to prevent future loss or theft of account information, consistent with the requirements of the VISA USA Cardholder Information Security Program

Forensic Investigation Guidelines

Entity must initiate investigation of the suspected or confirmed loss or theft of account information within 24 hours of compromise.

The following must be included as part of the forensic investigation:

1. Determine cardholder information at risk

    a. Number of accounts at risk, identify those stored and compromised on all test, development and production systems
    b. Type of account information at risk
    c. Account number
    d. Expiration date
    e. Cardholder name
    f. Cardholder address
    g. CVV2
    h. Track 1 and Track 2
    i. Any data exported by intruder

2. Perform incident validation and assessment

    a. Establish how compromise occurred
    b. Identify the source of the compromise
    c. Determine timeframe of compromise
    d. Review entire network to identify all compromised or affected systems, considering the e-commerce, corporate, test, development, and production environments as well as VPN, modem, DSL and cable modem connections, and any third-party connections
    e. Determine if compromise has been contained

3. Check all potential database locations to ensure that CVV2, Track 1 and Track 2 data are not stored anywhere, whether encrypted or unencrypted (e.g., duplicate or backup tables or databases, databases used in development, stage or testing environments data on software engineers' machines, etc.)

4. If applicable, review VisaNet endpoint security and determine risk

5. Preserve all potential electronic evidence on a platform suitable for review and analysis by a court of law if needed

6. Perform remote vulnerability scan of entity's Internet facing site(s)

Discover Card Specific Steps

1. Within 24 hours of an account compromise event, notify the Discover Data Security Team at (800) 347-3803

2. Prepare a detailed written statement of fact about the account compromise including the contributing circumstances

3. Prepare a list of all known compromised account numbers

4. Obtain additional specific requirements from Discover Card

American Express Specific Steps

1. Within 24 hours of an account compromise event, notify American Express Merchant Services at (800) 528-5200 in the U.S.

2. Prepare a detailed written statement of fact about the account compromise including the contributing circumstances

3. Prepare a list of all known compromised account numbers

4. Obtain additional specific requirements from American Express

APPENDIX B-Incident Response Notification

Escalation Members (VP Level of Management)

Escalation – First Level

Director of Information Security
Senior Accountant
Assistant Controller
Director of Systems Integration
System Administrator

Escalation – Second Level

Chief Information Officer
Executive Director, Enterprise Services & Strategic Initiatives
Associate Controller

Auxiliary Members (as needed)

Chief Financial Officer
University Police Chief
Executive Director Public Relations/University Spokesperson

External Contacts (as needed)

Merchant Provider
Card Brands
Internet Service Provider (if applicable)
Internet Service Provider of Intruder (if applicable)
Communication Carriers (local and long distance)
Business Partners
Insurance Carrier
External Response Team as applicable (CERT Coordination Center[2], etc)
Law Enforcement
- Local Police Force (jurisdiction is determined by crime)
- Federal Bureau of Investigation (FBI) (Especially if a federal interest computer or a federal crime is involved)
- Secret Service

Notification Order

[2] The CERT/CC is a major reporting center for Internet security problems. Staff members provide technical advice and coordinate responses to security compromises, identity trends in intruder activity, work with other security experts to identify solutions to security problems, and disseminate information to the broad community. The CERT/CC also analyzes product vulnerabilities, publishes technical documents, and presents training courses. For more detailed information about CERT/CC, see http://www.cert.org

Incident Response Team
Information Technology Department
System Administrator(s) of area affected by incident
Manager of the area affected by incident
Associate Controller
Campus Police
Chief Financial Officer and President (when impact of incident has been determined)
Executive Director Public Relations/University Spokesperson
Business Partners
Human Resources

Escalation Member Notification List

Incident Response Team Members

Title	Member	Office Phone	Alternative Number	E-mail
Director of Systems Information Security	David Scuffham	(309)677-3041	(309)677-2950	david@bradley.edu
Senior Accountant	Ellen Keenan	(309)677-3116	(309)677-3117	efm@bradley.edu
Assistant Controller	Ryan Schmidgall	(309)677-3130	(309)677-3117	rschmidgall@bradley.edu
Director of Systems Integration	Ramona Hutchison	(309)677-2962	(309)677-3117	rkh@bradley.edu
System Administrator	Steve Herrera	(309)677-2336	(309)677-2950	sherrera@bradley.edu
Chief Information Officer	Zach Gorman	(309)677-3100	(309)677-3440	zgorman@bradley.edu
Exec. Dir., Enterprise Serv/Strategic Initiatives	Sandy Bury	(309)677-2808	(309)677-2950	sandy@bradley.edu
Associate Controller	Dennis Koch	(309)677-3119	(309)677-3117	dmk@bradley.edu
Chief Financial Officer	Jeffrey Blade	(309)677-3117		jblade@bradley.edu
University Police Chief	Brian Joschko	(309)677-2000		bjoscho@bradley.edu
Executive Director PR	Renee Charles	(309)677-3260	(309)677-3245	rcharles@bradley.edu

APPENDIX C

Visa Incident Report Template

This report must be provided to VISA within 14 days after initial report of incident to VISA. The following report content and standards must be followed when completing the incident report. Incident report must be securely distributed to VISA and Merchant Bank. Visa will classify the report as "VISA Secret"*.

I. Executive Summary
    a. Include overview of the incident
    b. Include RISK Level(High, Medium, Low)
    c. Determine if compromise has been contained

II. Background

III. Initial Analysis

IV. Investigative Procedures
    a. Include forensic tools used during investigation

V. Findings
    a. Number of accounts at risk, identify those stores and compromised
    b. Type of account information at risk
    c. Identify ALL systems analyzed. Include the following:
        - Domain Name System (DNS) names
        - Internet Protocol (IP) addresses
        - Operating System (OS) version
        - Function of system(s)
    d. Identify ALL compromised systems. Include the following:
        - DNS names
        - IP addresses
        - OS version
        - Function of System(s)
    e. Timeframe of compromise
    f. Any data exported by intruder
    g. Establish how and source of compromise
    h. Check all potential database locations to ensure that no CVV2, Track 1 or Track 2 data is stored anywhere, whether encrypted or unencrypted (e.g., duplicate or backup tables or databases, databases used in development, stage or testing environments, data on software engineers' machines, etc.)
    i. If applicable, review VisaNet endpoint security and determine risk

VI. Compromised Entity Action

VII. Recommendations

VIII. Contact(s) at entity and security assessor performing investigation

*This classification applies to the most sensitive business information, which is intended for use within VISA. Its unauthorized disclosure could seriously and adversely impact VISA, its employees, member banks, business partners, and/or the Brand.