Credit Card Data Compromise: Incident Response Plan

Purpose

It is the objective of the university to maintain secure financial transactions. To comply with state law and contractual obligations, the division of finance and administration and the division of information technology are responsible for a unified response to a breach or potential compromise of credit card data. This incident response plan provides guidance for identification, containment, notification, verification, communication, investigation, and remediation of such incidents.

Roles and responsibility

Any university employee or any other person or entity accepting credit card payments on behalf of the university who believes a breach or potential compromise (electronic or physical) of any type or form of cardholder data (personally identifiable information associated with a specific cardholder) has occurred is required to adhere to the steps outlined in this plan. In the case of a suspected data breach the entities identified below should, at a minimum, unless more stringent guidelines are noted in contract language, follow the guidelines outlined:

Merchant

- Immediately contact Kent State's PCI-DSS Lead as identified in this document.
- Does not access or alter confirmed or suspected compromised system(s).
- Does not turn off the confirmed or suspected compromised system(s).
- Isolates the confirmed or suspected system(s) from the network by unplugging the network cable only, or the phone cable if the POS appears to have been tampered with.
- Follows this plan through to resolution of the issue.

Information Security Team

- Monitor all systems within cardholder data environment.
- Determines if participation of KSU's Cyber Security Incident Response Team is needed.

PCI-DSS Incident Response Team

- Participates in the division of Information Technology Cyber Security Incident Response Team, if needed.

PCI-DSS Lead

- Coordinates, and maintains communications with the acquiring bank.
- In coordination with University General Counsel, Information Security, and PCI-DSS Incident Response Teams, determines the official line of notification.

Acquiring Bank

- Assesses the information supplied by the PCI-DSS Lead to determine if a payment card industry forensic investigator should be contacted.

Payment Card Industry Forensic Investigator

- Drives and performs all aspects of the forensic investigation.
- Completes investigation report in a secure and timely manner.

Identification

Identification of a breach or potential compromise of data is the first step in an incident response. Identification can occur by, but is not limited to, the following:

(1) Report from a third party (such as a cardholder, vendor, and merchant),
(2) Anonymous complaint of unauthorized use or misuse of data,
(3) Alerts from security monitoring systems including, but not limited to, intrusion-detection, intrusion prevention, firewalls, file-integrity monitoring systems, and network infrastructure devices that detect rogue wireless access (wireless access points physically connected to the network that are used to intentionally subvert University policy and/or security controls)
(4) Routine monitoring (examination of activity and/or access logs),
(5) Vulnerability scans, or
(6) Suspicious circumstances beyond normal processes.

Identification is reliant on timely and credible information being provided by various reporting parties and mechanisms. Identification is dependent on notification from partnered or contracted third parties and a preliminary substantiation of this information.

Containment

Containment is the next critical step to limit exposure, preserve potential evidence, and prepare for an investigation of the incident. Containment steps include:

(1) If an electronic device:

    (a) Do not access or alter the compromised device,
    (b) Do not power off the device,
    (c) Do terminate its network connection (unplug network connection from the device or disable the wireless adapter),
    (d) Isolate the device from access by others,
    (e) Document how the event was detected and the state of the device at that time, and
    (f) Document steps taken to contain and isolate the device.

(2) If data is believed to have been compromised by loss of physical property, follow the steps outlined in the section for Response Team Notification below.

Response Team Notification

In the event of a breach or potential compromise of data, notification of the appropriate internal personnel will ensure a coordinated and unified response in determining the scope of the breach, business continuity, internal and external communications, and remediation. Notification must be made to the division of information technology data center at 330-672-2552. An email notification should also be sent to PCICompliance@kent.edu.

(1) If the data breach involves loss of physical property (theft of physical media or a device containing credit card data), report this to the law enforcement agency having jurisdiction where the loss occurred.

(2) Cross reference each notification. Provide law enforcement with contact information used for internal university notification. Include law enforcement department and report number in notification to university.

PCI-DSS Response Team (Response Team)

The recipient(s) of a notification of a breach or potential compromise of data should immediately contact the team lead of the Response Team, comprised of the members noted below. The Team Lead will immediately contact the members of the Response Team to begin the requisite response activities. The Response Team will be comprised of the following positions:

- Associate Vice President for Business and Administration Services – Team Lead
- Chief Information Security Officer, or delegate
- Manager of Cashiering, Bursar's Office
- Representation from public safety/police services, only if the breach or potential compromise of data occurs on any Kent State University owned or leased property or until such jurisdiction is determined.

In the absence of the Response Team Lead responsibility for contacting the PCI-DSS Response Team will fall to the members of the team in the order listed. The Response Team will convene immediately to initiate a response and will involve others in the university community as circumstances warrant.

Verification

(1) The division of information technology will lead preliminary efforts in verifying a breach of electronic data. The division of finance and administration will lead efforts in verifying a breach of non-electronic

data. If and upon the discovery of evidence indicating a criminal offense was committed, the department of public safety / police services will be notified. Police services may collaborate with other federal, state, and local law enforcement agencies as appropriate. A criminal investigation may be conducted in parallel, supersede, or require authorization for any further action taken by the university.

(2) The theft of physical media or a device containing credit card data will be reported to the appropriate law enforcement agency. A criminal investigation will be at the discretion of said agency. The division of information technology will be responsible for attempts to determine the type and scope of cardholder data potentially compromised. Additionally, the division of information technology in conjunction with the person having control over the device will determine the availability of remote access to the device.

Internal Notification

Communication strategies begin upon the verification of a data breach or compromise. The following institutional members will all be informed of a breach or compromise of data. These members will also be provided with periodic updates of significant findings from the Response Team during the investigation and remediation processes:

- Senior Vice President for Finance and Administration. The SVP for Finance and Administration will notify the President and the President will determine if notification of Trustees is warranted based on the circumstances.
- Vice President for Information Technology,
- Vice President or executive responsible for functional area of breach,
- General Counsel,
- Director of Public Safety / Police Services,
- Vice President of University Relations
- First Data / Card Brand(s) representatives
- Associate Vice President of Compliance and Risk Management

Depending on the type and circumstances of the breach, additional institutional members may need to be contacted. See Appendix B for additional contact information.

Investigation

The investigation will be the responsibility of the division of information technology, the appropriate law enforcement agency, or a combination of both. The investigation will include, but is not limited to, the following:

(1) Interview of the person or entity learning of or discovering the breach or compromise of data.

(2) Collect and preserve evidence:

(a) Photograph or video record the scene as is,
(b) Collect affected hardware,
(c) Acquire activity and/or access logs and network logs for device,
(d) Acquire recent history of users of device,
(e) Retain documentation of any associated alerts from security monitoring systems,
(f) Obtain video surveillance history and key swipe logs of area accessed without authorization, and
(g) Maintain chain of custody records for evidence collected.

(3) Minimize scope:

(a) Determine if breach or compromise is likely to be duplicated,
(b) Determine if breach or compromise is beyond a single device,
(c) Cease operation of certain hardware or physical areas where there is a reasonable belief the breach or compromise could be repeated, and
(d) Provide alternatives to affected area to maintain business operations.

(4) Forensics:

(a) Forensics should support the overall investigation in determining the origination of the breach or compromise, the devices and or systems affected, the data compromised, and the possibility of re-occurrence.

(b) A forensic consultant may be contracted at the discretion of the division of information technology and the division of finance and administration in the absence of or in conjunction with a criminal forensic process. The need for a forensic consultant will be determined based on the type and scope of the breach or compromise or may be contractually required by one or more of the involved credit card brands.

Recovery, External Notification, and Remediation

The information gathered during the investigation will allow for assessment of functional impact, informational impact, and remediation.

(1) The division of finance and administration will be responsible for the following:

(a) Formal documentation of event.
(b) Notifying the cyber liability insurance carrier and coordinating the services provided under the policy with internal stakeholders.
(c) In consultation with the office of general counsel, notification and delivery of documentation will be made to the relevant card processors, banks, and credit card brands as appropriate based on the nature and magnitude of the breach (see appendix A for card brand guidelines).
(d) In consultation with the division of university relations, prepare notification in the form deemed most appropriate and expedient to be sent to affected individuals, including available mitigation and support services.
(e) If deemed appropriate by legal statute or otherwise decided, prepare to offer free credit report resources to affected users.
(f) Coordinate regular update meetings during the investigative process and a debriefing meeting approximately two to four weeks post event.
(g) In conjunction with the division of information technology monitor and collaborate with the investigative and notification remediation processes of contracted third party vendors and merchants.

(2) The division of information technology will be responsible for the following:

(a) Remediate any compromise to network or device security.
(b) Identify and assess data backups and processes.
(c) Document cardholder data including names and contact information of affected cardholders.
(d) Backup and provide any necessary network, log, scan, and device data to any investigative body within the legal requirements.
(e) Aid in providing resources necessary for the university to coordinate communication to all entities listed within this plan (for example: website, call center, email development and support).
(f) In conjunction with the division of finance and administration monitor and collaborate with the investigative and notification remediation processes of contracted third party vendors and

merchants.

(3) The division of university relations will assume responsibility for disseminating information to the media in consultation with the division of finance and administration and the division of information technology.

(4) The division of information technology with guidance from the office of general counsel will assume responsibility for the review and compliance of applicable domestic and international laws related to data breaches.

Incident Response Plan Distribution and Review

(1) The Incident Response Plan will be available on the office of security and access management website at https://www.kent.edu/it/policies-and-procedures

(2) The Response Team will meet annually to review and test the Incident Response Plan. The Response Team Lead will coordinate and document this annual event.

(3) As part of the annual event, response team members will assess the content, structure, and usability of the plan.

(4) The division of finance and administration will maintain current information on Payment Card Industry (PCI) standards as well as current contact information for the payment card brands.

(5) The incident response plan annual review process, training, assessment, and current information from the PCI Security Standards Council and the payment brands, will be used to appropriately modify existing controls and the incident response plan as needed.

Review and Revision History

- Original document 3/25/15
- Revised 6/30/15
- Revised 12/20/16
- Revised 10/17/17
- Revised 11/29/18
- Revised 12/17/19
- Revised 12/11/20

Appendix A: Payment brand guidelines and contact information.

MasterCard:https://www.mastercard.us/en-us/merchants/safety-security/security-recommendations/site-data-protection-PCI.html

Visa: https://usa.visa.com/support/small-business/security-compliance.html?ep=v_sym_cisp#5
1-650-432-2978 or e-mail usfraudcontrol@visa.com

Discover: https://www.discovernetwork.com/en-us/business-resources/fraud-security/
1-800-347-3083

AmericanExpress: https://www.americanexpress.com/us/merchant/us-data-security.html?linknav=merchant-nsnu-policy-datasecurity
1-888-732-3750 or email EIRP@aexp.com

Appendix B: Additional Institutional Members, Included as Needed

Division of Finance and Administration
Division of Information Technology – Other
Provost and Academic Affairs
Office of Student Affairs
University Communications and Marketing
Office of Public Safety
Regional Campus Administration
Regional Campus IT Support
Merchant Representatives, Cashiering Office
WKSU
KSU Foundation
Internal Audit