| | | |
|---|---|---|
| | **Credit and Debit Card Processing Policy** | |
| | **Responsible Administrative Unit:**<br>Controller's Office | **Policy Contact:**<br>Noelle Sanchez, Controller<br>nsanchez@mines.edu |

## 1.0 BACKGROUND AND PURPOSE

The Colorado School of Mines ("Mines") is committed to complying with the Payment Card Industry Data Security Standards (PCI DSS). PCI DSS requirements apply to all transactions surrounding the payment card industry and the merchants/organizations that accept these cards as forms of payment. Mines must show evidence of/maintain compliance with PCI DSS, in order to accept credit or debit card payments. As part of this commitment Mines has promulgated this policy and procedures to help prevent loss or disclosure of customer information, including credit or debit card numbers.

## 2.0 POLICY STATEMENTS

In order to accept credit and debit card payments each department/area must be approved as a Merchant Department by the Controller's Office.

All Merchant Departments must comply with payment card industry standards and this policy and procedures.

Student organizations and clubs are prohibited from obtaining a merchant account with any bank.

Only Mines approved payment card processing devices can be used by campus.

Student organizations and campus departments are NOT ALLOWED to accept monies via Paypal, Venmo, Square or other method, which requires funds to flow through personal bank accounts.

## 3.0 RESPONSIBILITIES

All faculty, staff, students, organizations, third-party vendors, individuals, systems and networks involved with the transmission, storage, or processing of Cardholder Data (including systems that can impact the security of payment card data) must comply with this policy and procedures. Any business conducted on behalf of Mines, is subject to this policy.

All persons with physical and logical access to Mines Cardholder Data Environment, whether employees, third-parties, service providers, contractors, temporary employees, students, and/or other staff members, must be trained by the Controller's Office on their

role in protecting Mines from threats to help safeguard Mines finances, operations, and brand name.

A PCI Oversight Committee has been created to enforce PCI DSS and to educate entities in Mines' payment environment about these standards. The PCI Oversight Committee is comprised of the Controller, Chief Information Officer (CIO), Chief Information Security Officer (CISO), and Privacy Compliance Director.

Each Merchant Department must designate and have in place a Merchant Department Responsible Person (MDRP) at all times. It is the responsibility of the MDRP and the MDRP's direct supervisor to ensure this role is filled. The direct supervisor must record and track any change in MDRP's and provide the MDRP's contact information to the Bursar's Office.

## 4.0 COMPLIANCE/ENFORCEMENT

PCI compliance is an ongoing process, not a one-time event. PCI DSS emphasizes "Business as Usual," performing continuous compliance activities in an ongoing manner 24 hours a day, 7 days a week, 365 days a year. Any failures to protect customer information may result in financial loss for customers, suspension of payment card processing privileges, fines, and damage to the reputation of Mines.

Failure to meet the requirements outlined in this policy will result in suspension of the physical and, if appropriate, electronic payment capability with payment cards for affected units. Additionally, if appropriate, any fines and assessments, which may be imposed by the affected payment card company will be the responsibility of the impacted unit. In the event of a breach or a PCI violation the payment card brands may assess penalties to Mines' bank which will be passed on to Mines. A one-time penalty of up to $500,000 per breach can be assessed as well as on-going monthly penalties.

Persons in violation of this policy, whether intentionally or unintentionally, are subject to sanctions, including loss of computer or network access privileges, disciplinary action, suspension and termination of employment. The appropriate Vice President will authorize sanctions. Some violations may constitute criminal offenses under local, state or federal laws. Mines will carry out its responsibility to report such violations to the appropriate authorities.

## 5.0 DEFINITIONS

**Cardholder Data** means the elements of payment card information that are required to be protected. These elements include Primary Account Number, Cardholder Name, Expiration Date and the Service Code.

**Cardholder Data Environment (CDE)** means the people, processes, and technologies that store, process, or transmit data, including cardholder or sensitive authentication data. Technology components include network devices, servers, computing devices, and applications.

**Cardholder Name** means the name of the Cardholder to whom the card has been issued.

**CAV2, CVC2, CID, or CVV2** means the three- or four-digit value printed on or to the right of the signature panel or on the face of a payment card used to verify card- not-present transactions.

**Expiration Date** means the date on which a card expires and is no longer valid. The expiration date is embossed, encoded or printed on the card.

**Magnetic Stripe (i.e., Track)** means data encoded in the magnetic stripe or equivalent data on a chip used for authorization during a card-present transaction. Entities may not retain full magnetic-stripe data after transaction authorization.

**Merchant Department** means any Mines department or unit (can be a group of departments or a subset of a department) which has been approved by Mines to accept payment cards and has been assigned a merchant identification number.

**Merchant Department Responsible Person (MDRP)** means the individual within a department who has primary authority and responsibility for that department's payment card transactions.

**Payment Card Industry Data Security Standards (PCI DSS)** mean the security requirements defined by the Payment Card Industry Security Standards Council and the five major Payment card Brands: Visa, MasterCard, American Express, Discover, JCB to provide specific guidelines for safeguarding cardholder information.

**PIN/PIN Block** means the personal identification number entered by cardholder during a card- present transaction, and/or encrypted PIN Block present within the transaction message.

**Primary Account Number (PAN)** means the number code of 14 or 16 digits embossed on a bank or payment card and encoded in the card's magnetic strip. PAN identifies the issuer of the card and the account, and includes a check digit as an authentication device.

**Response Team** means the team that will respond and review PCI incidents. The Response Team will consist of the Controller, CIO, CISO, and the Privacy Compliance Director. The Computer Incident Technical Team (CITT), as defined in the security incident response procedures, will be utilized, as needed.

**Security Breach/Incident** means a suspected or confirmed event where there has been unauthorized access, loss, or theft (to a system, network, material, or records) to Cardholder Data. This includes systems, networks, or physical locations where Cardholder Data is collected, processed, stored, or transmitted.

**Sensitive Authentication Data** means the elements of payment card information that are also required to be protected but never stored. These include Magnetic Stripe (i.e., Track) data, CAV2, CVC2, CID, or CVV2 data and PINs/PIN Block.

**Service Code** means the code that permits where the card is used and for what.

## 6.0 RESOURCES or ATTACHMENTS

- PCI Security Standards Council Web site: https://pcisecuritystandards.org/
- For questions or concerns not addressed in this policy, please email pci@mines.edu
- Mines Help Center service ticket
- PCI Compliance Website https://www.mines.edu/controllers-office/pci/
- Mines' PCI Roles
- PCI Calendar of Activities
- PCI FAQs
- POS Tampering Checklist
- Process Flowcharts:
    - Adding a person or device for card processing
    - PCI Change to CDE/ Software acquisition process

***KEY WORDS***
*PCI, PCI DSS, Payment Card Industry, credit card, processing, compliance, breach, security*

## 7.0 HISTORY AND REVIEW CYCLE

The policy will be reviewed at least annually or as needed by the Responsible Administrative Unit.

Issued: July 30, 2020

## EXHIBIT 1 - PROCEDURES

### 1.0 PROCEDURES PURPOSE

These procedures provide the requirements for processing, transmitting, storage and disposal of Cardholder Data related to payment card transactions, to help reduce the institutional risk associated with the administration of credit and debit card payments accepted by Mines departments and to ensure proper internal control and compliance with PCI DSS.

### 2.0 PROCEDURES

**2.1 Merchant Department Responsible Person (MDRP).** Merchant Departments must identify a person to be responsible for payment card activity for the department/unit. MDRP Responsibilities include, but are not limited to, the following:

A. Ensure agents of Mines, with access to or who can affect the security of payment card data, complete the PCI Training program upon hire and annually.
B. Ensure job descriptions, for agents of Mines that will have access to more than one payment card at a time, include a background check prior to hire. The background check is completed by Mines' Human Resources Department.
C. Ensure only dedicated, approved hardware/software is utilized to process card payments. Hardware/software utilized in the processing of card information must be configured and managed according to the standards laid out herein.
D. Provide the IP address of the any hardware utilized in card processing to ITS to ensure that address is included in any scans carried out by an ASV.
E. Ensure no hardware used for card processing is ever connected to Mines WiFi network.
F. Be aware of all payment processes and practices within their Merchant Department. All changes to processes and practices must be reviewed and approved through the PCI Change Management process in Team Dynamix.
G. Ensure Cardholder Data is never stored.
H. Ensure all agents of Mines receive, and are trained on, the MDRP Payment Card Procedures (See PCI Compliance website; MDRP Payment Card Procedures) upon hire and annually. Ensure these department specific procedures are adhered to.
I. Ensure that all payment card transactions are reviewed and reconciled to daily merchant reports. These transactions must be turned into the Bursar's Office within two business days.
J. Ensure all Point of Sales (POS) devices, including cellular based stand-alone swipe terminals and point of sale systems, are maintained under a state of consistent control and supervision. The Bursar's Office has a cellular card swipe terminal for loan to agents of Mines that have completed the PCI Training Program.
K. Ensure POS devices/terminals (cash registers, stand-alone swipe terminals etc.) are physically secured.
    - For Merchant Account Requests, the MDRP must follow the processes noted in the client process set-up procedures (See PCI Compliance website;

MDRP Payment Card Procedures). These steps must be made and completed prior to engaging in payment activity.

- All devices that process payment cards must be stored in a locked space with limited access when not in use. Access to deployed units while in use must be limited to the department merchant users and must not be left unattended.

L. Perform a daily visual inspection of devices that capture payment card data
M. A monthly physical inspection must be performed, documented and retained.

**2.2 Authorization.**

A. Limit access to system components and Cardholder Data to only those individuals whose job requires such access.
B. The level of access is determined by job requirements; based on the least privilege model.
C. Sufficient controls are in place to identify individuals entering and exiting software and system.
D. Each Merchant Department must maintain a current list of employees and review monthly to ensure the list reflects the most current access needed and granted.

**2.3 Payment Card Acceptance and Handling.** In the course of doing business it may be necessary for a department or other unit to accept payment cards. The opening of a new merchant account for the purpose of accepting and processing of payment cards is done on a case by case basis. Any fees associated with the acceptance of payment cards in that unit, will be charged to the unit (including but not limited to; infrastructure, security and management, i.e., firewall, switch, network cables).

A. See Transmitting for acceptable methods of payment card acceptance.
B. To request a merchant account, please submit a ticket through the Mines Help Center. See PCI Compliance website; Process Flowcharts, for an overview of the process.

**2.4 Transmitting**.

A. Employees must be discreet and use common sense when handling Cardholder Data.
B. Payment cards may be accepted in the follow manner:
    - In person (card present).
    - Direct telephone contact (telephone order) should only occur on an encrypted phone line; the constituent on the telephone should verify the payment card information twice, agents of Mines should not read the payment card data back to constituent.
    - Through a PCI DSS compliant system that is entirely hosted by a PCI DSS compliant third-party organization (e-commerce) and approved by the PCI Oversight Committee and where the device is on the subnet.
    - Cardholder data must be encrypted in transit at all times (including voice communication and from point of data entry to the processor's site). Encryption technologies used must meet or exceed current campus standards (see the document "System and Communication Procedure,

sections 5.1.8, 5.1.10, 5.1.16 for current standards). Together with the prohibition against storage ensures that there is never Cardholder Data on campus.

- Devices participating in the transmission of card data must be configured and maintained in accordance with [PCI Workstation Configuration document, PCI Workstation Compliance Assurance document].
- Participating devices may only be connected to the CDE subnet configured and maintained by ITS solely for this purpose. This subnet must use a default-deny policy (in and out). In accordance with the process described in "System and Communication Procedure – Appendix Firewall Policy Process" the Controller and CIO must authorize any exceptions.
  - The CDE subnet may not include any wireless component.
  - The CDE subnet must be scanned using a network protocol scanner at least monthly by both internal and external entities to ensure there is no unintended exposure.

C. Payment card may **not** be accepted in the following manner:
- Sent via end user messaging technologies, text message, SMS, chat etc.
- Constituent Cardholder Data must not be accepted or sent via fax. If a fax is received with Cardholder Data, immediately shred in a crosscut shredder.
- Email is not a secure form of transmission. In the event card information is received via email the email must be deleted from the inbox and deleted folder.
- Notify the PCI Oversight Committee with the name, date, location the Cardholder Data was received. Follow up with the constituent and advise this method of transmitting Cardholder Data is not secure. Advise the constituent we cannot process the payment and educate him/her on the appropriate methods of conveying a card payment. See above for appropriate acceptance methods.

D. In the rare instance that an agent of Mines is offered payment card information during an off-site visit, the agent will process the payment on a Mines approved point-to-point (P2P) encryption device (i.e. online donation site, phone). For compliance and security Mines employees must not store or take possession of Cardholder Data while off-site.

E. All equipment used to collect payment card data must be secured against unauthorized use or tampering in accordance with the PCI Data Security Standard. See PCI Compliance website; POS Tampering Checklist.

F. In the event that a non-merchant department has a customer who wants to pay with a credit or debit card, the department should complete the steps below:
- Create a departmental deposit in CASHNet and provide their customer with the deposit number.
- The customer will call the Cashier's Office, provide the deposit number, and the Cashier will take the payment over the phone, on an encrypted line and entering the card number directly into a Mines approved P2P device.
- The Cashier will email a receipt of payment directly to the customer and the department.

G. In the case of emergency, a merchant department can write the card number down and keep it in a secure, locked, location. The payment must be processed within 24 hours of the emergency being mitigated. Once the payment is

processed, the card information must be cross-cut shredded. Non-merchant departments are not authorized to write any card information down.

**2.5 Processing.**

A. Cardholder Data received for manual processing (mail, hand delivered) must be processed with a University approved card payment terminal the same day it is received if possible; but absolutely no later than one business day (excluding calendar and fiscal year end periods). Cardholder Data in written form is redacted immediately following authorization in the payment gateway. Acceptable form of redaction is crosscut shred, so that Cardholder Data cannot be reconstructed.
B. Refunds must be processed using the same card for the transaction within six months of the payment. A different card may not be used.
C. Physical security controls must be in place to prevent unauthorized individuals from gaining access to the buildings, rooms, or cabinets that store the equipment, documents, or electronic files containing card holder data.
D. Mask the Primary Account Number when displayed (the first six and last four digits are the maximum number of digits to be displayed), such that only personnel with a legitimate business need can see the full PAN.

**2.6 Storage.**

A. Mines does not store authorized Cardholder Data (media), in hardcopy or electronic form.
B. Mines does not store Sensitive Authentication Data; including the PAN, Expiration Date and Service Code (CVV).
C. Cardholder Data that is collected but has not yet been processed (pending authorization in payment gateway), in addition to any USPS mail that hasn't been opened, must be stored in a secure location (locked safe, locked file cabinet), see Processing above. Only authorized staff shall have access to the keys/combination.
D. Cardholder Data may not be stored on any portable devices including but not limited to USB flash drives, cellular phones, personal digital assistants and laptop computers.
E. Cardholder Data may not be stored in logs (for example, transaction, history, debugging, or error), history files, trace files or database contents.

**2.7 Disposal.** Cardholder Data must be disposed of in a certain manner that renders all data un-recoverable. This includes paper documents and any electronic media including computers, hard drives, magnetic tapes, or USB storage devices. As storage of Cardholder Data is not allowed on campus, disposal procedures apply only to emergency situations, as described within this policy. In those situations, Cardholder Data must be disposed of in a certain manner that renders all data unrecoverable. The approved method of disposal for hardcopy media is cross-cut shredding.

**2.8 Physical Security and Skimming Prevention of Payment Card Processing Devices.** The Controller's Office will maintain a list of all devices that capture payment card data, for which the list is to include the following:

A. Make, model, serial number (or other method of unique identification) and location of device
B. Ensure that the list of devices is updated when devices are added, relocated, decommissioned
C. Physically secure all devices that capture payment card data

**2.9 Security Awareness Program.** Upon hire and at least annually, all users connected to Mines Cardholder Data Environment (in any way), are to complete the Mines PCI Training program. Read and acknowledge compliance with the Mines Credit and Debit Card Processing Policy. Training Completion logs for those who completed PCI training, must be kept by the PCI Oversight Committee.

**2.10 Security Breach/Incident.** In the event of a breach or suspected breach of security, the reporting department must immediately execute each of the relevant steps detailed below:

A. The MDRP or any individual suspecting a Security Breach must immediately notify the Response Team of an actual breach or suspected breach of payment card information.
   - Notification can occur through email to pci@mines.edu or directly to any of the *Response Team* members.
   - The initial notification should include the best contact information for the Incident Response Team to reach the reporting party. Details of the breach should not be disclosed in email correspondence.

B. The MDRP or any individual suspecting a Security Breach must ensure the department head of the unit experiencing the suspected breach is informed.

C. The MDRP or any individual suspecting a Security Breach involving e-commerce also must immediately ensure that the following steps, where relevant, are taken to contain and limit the exposure of the breach:
   - If the incident involves a payment station (PC used to process credit cards):
     - Do NOT turn off the PC.
     - Disconnect the network cable connecting the PC to the network jack. If the cable is secured and you do not have the key to the network jack, simply cut the network cable.
   - Prevent any further access to or alteration of the compromised system(s). (i.e., do not log on at all to the machine and/or change passwords)
   - Preserve logs and electronic evidence.
   - Document every action you take from the point of suspected breach forward, preserving any logs or electronic evidence available. Include in the documentation:
     - Date and time
     - Action taken
     - Location
     - Person performing action
     - Person performing documentation
     - All personnel involved
     - Be on HIGH alert and monitor all e-commerce applications
   - Assist the Response Team as they investigate the incident.

If a suspected or confirmed intrusion / breach of a system has occurred, the Response Team will alert the merchant bank, the payment card associations, local authorities, Mines Police Department, and the Executive Vice President of Finance Administration and Operations.

The PCI Oversight Committee will maintain a detailed incident response plan (**Exhibit 2**).

**2.11 Student Organizations.** All money collected from fundraisers or dues must be deposited directly into the organization's university account. No organizational money should ever be deposited into a personal banking account. Student Organizations must contact the Student Activities, Involvement, & Leadership (SAIL) Office for possible payment processes. The MDRP for all Student Organizations must be a full-time employee for SAIL.

Please direct questions regarding the use of payment card services, by Student Organizations and Clubs, to SAIL.

**2.12 Third Party Processor Procedures.** When deciding on a third-party processor make sure to include the PCI Oversight Committee. New processors must be approved through the PCI Oversight Committee before they can be used on behalf of Mines. Ensure contracts include language that states that the service provider or third-party vendor is PCI complaint and will protect all Cardholder Data. Mines will not work with vendors who are not PCI compliant. In addition, the contract must be approved through the Contract Approval Process by Procurement. Third-party processors must have a completed and current Attestation of Compliance form on file with Mines. Mines will annually audit the PCI compliance status of all service providers and third-party vendors. A lapse in PCI compliance could result in the termination of the relationship. See PCI Compliance website; [Process Flowcharts] for the Process Flowcharts.

**2.13 Service Provider Management.**

A. Service Providers (third parties) must be contractually required to adhere to the PCI DSS requirements. Due diligence must be exercised before engaging with any service providers that may affect or have a relationship or function associated with Mines CDE. The written agreement shall include an acknowledgement by the service providers of their responsibility for securing Cardholder Data and breach liability language, which will be evaluated by Procurement.

   Note: This also includes companies that provide services that control or could impact the security of Cardholder Data. Examples include managed service providers that provide managed firewalls, IDS and other services as well as hosting providers and other entities.

B. The Controller's Office must obtain the appropriate PCI compliance documentation, from Service Providers, on an annual basis prior to Expiration Date of the current documentation.

C. Service Providers must provide a valid Attestation of Compliance including the specific requirements Service Provider is attesting to.
D. The PCI Oversight Committee will maintain a collective, current and accurate list of Service Providers with the following information:
    - Service Provider Name
    - Service being provided (description)
    - PCI Validation Required
    - Validation Date
    - Expiration Date
    - Assessor
    - Functional Area

**2.14 Security Measures.**

Mines ITS employs up-to-date security measures in firewall configuration, network administration, and other areas that could affect our PCI compliance.

## EXHIBIT 2 - MINES' PCI INCIDENT RESPONSE PLAN ("INCIDENT RESPONSE PLAN")

### Purpose

The PCI Incident Response Plan governs the process when payment card information is or may be breached. It can be supplemented by the Mines' security incident response plans and/or the privacy incident response plans.

One of the Payment Card Industry Data Security Standards (PCI DSS) requires that merchants create a Response Team and document an Incident Response Plan.

This document defines those responsible, the classification and handling of, and the reporting/notification requirements for incident response plan at Mines. This process will be reviewed and tested on an annual basis.

### Scope/Applicability

Any area on campus accepting credit or debit card payments.

### Mines PCI Incident Response Team ("Response Team")

Communication for the Response Team can be sent to pci@mines.edu.

An 'incident' is defined as any suspected or confirmed event where there has been unauthorized access, loss, or theft (to a system or network) to Cardholder Data. This includes systems, networks, or physical locations where Cardholder Data is collected, processed, stored, or transmitted.

In the event of a suspected or confirmed incident:

1. All incidents or suspected incidents must be immediately reported to the Response Team through any of the various mechanisms, described in the policy.
2. The Response Team will confirm receipt of the notification and immediately coordinate a response.
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 in volved.
5. The Response Team will notify the PCI Oversight Committee immediately if an incident has been confirmed.
6. The PCI Oversight Committee will determine the communication plan to relevant Mines' stakeholders and community partners (Executive Leadership, General Counsel, departments, public relations, HR, campus police, local law enforcement, etc.), as necessary. The CIO will be responsible for communications to executive leadership and determining technology being taken offline and reconstituted. They will also report the incident and findings to the appropriate parties (credit card associations, credit card processors, bank, cardholders, etc.), as necessary and in accordance with applicable state statutes.

7. The Response Team will determine action steps (e.g., training, updating policies and processes) to avoid a similar incident in the future.

*CITT Procedures*
After being notified, if a system is compromised or suspected of compromise, the CITT 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 and alerts.
3. Assist department in analysis of locally maintained system and other logs, as ne eded.
4. Conduct appropriate forensic analysis of compromised system.
5. If an incident of unauthorized access is confirmed and card holder data was potentially compromised, the CITT will notify the Response Team of the nature of the data and the details of the compromise.
6. Assist card industry security and law enforcement personnel in investigative process.

*Breach Notification Plans*

***Cardholder Notification***
Breach notification to impacted cardholders will follow the Privacy Incident Response procedures.

***Bank Notification***
The payment card companies have specific requirements the Response Team must address in reporting suspected or confirmed breaches of Cardholder Data. For Visa and MasterCard it is Mines' responsibility to notify their own bank (the financial institution(s) that issues merchant accounts to Mines) and Mines' bank will be responsible for notifying Visa and MasterCard, where applicable.

***Credit Card Company Notification***

a) Mines Acquiring Bank(s), the Acquiring Bank will be responsible for communicating with the card brands (VISA, MasterCard)
   i. See Wells Fargo Breach Response Plan
   ii. See Visa – Responding to a Breach
   iii. See Mastercard – Responding to a Breach
b) If American Express payment cards are potentially included in the breach Mines is responsible for notifying and working with American Express
   i. For incidents involving American Express cards, contact American Express Enterprise Incident Response Program (EIRP) within 24 hours after the reported incident.
      1. Phone number: (888) 732-3750 or 1-602-537-3021
      2. Email: EIRP@aexp.com.
   ii. For more detail see American Express – Responding to a Breach

c) If Discover Network payment cards are potentially included in the breach Mines is responsible for notifying and working with Discover Network.
   i. If there is a breach in your system, notify Discover Security within 48 hours. Phone Number: (800) 347-3083
   ii. For more details see Discover Network – Fraud Prevention FAQ
d) United States Secret Service Electronic Crimes Task Forces (ECTF)
   i. www.secretservice.gov/investigation/
   ii. The ECTF focuses on investigating financial crimes and can assist with incident response and mitigation of a Compromise Event.

***Wells Fargo Breach Response Plan***


**Merchant Steps and Requirements for Compromised Entities**

Merchants that have experienced a suspected or confirmed Security Breach must take prompt action to help prevent additional damage and adhere the Visa CISP and MasterCard SDP requirements listed below:

**1) Immediately contain and limit the exposure.** Prevent the further loss of data by conducting a thorough investigation of the suspected or confirmed compromise of information. 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 SSID on the AP and other machines that may be using this connection with the exception of any systems believed to be compromised.

**2) Alert all necessary parties immediately.** Be sure to contact:

- Your internal information security group and incident response team
- Your local US Secret Service office
- Wells Fargo "Association Compliance":

Monica Bourgeois
Wells Fargo Merchant Solutions
1655 Grant Street 3rd Floor
Concord Ca. 94520

WFMSCompromiseInvestigations@wellsfargo.com
(925) 483-9456

- Consult with your legal department to determine if notification laws are applicable.

**3) Be prepared to provide all compromised accounts numbers to Wells Fargo's Association Compliance Group.** An encrypted .txt file that contains all potentially compromised accounts must be provided to Wells Fargo Association Compliance (contact listed above)

**4) Be prepared to engage a PCI Forensic Investigator (PFI) from the following list**

| **Sikich LLP** | **Verizon** | **Security Metrics** |
|---|---|---|
| Bran Lutgen (USA)<br>brad.lutgen@sikich.com<br>1-888-403-3438 | Chris Novak (N. Amer & Lat. Amer.)<br>Chris.Novak@verizonbusiness.com<br>1-914-574-2805 | Jason Leland (USA)<br>PFI@securitymetrics.com<br>1-801- 705-5656 |

**Or you may choose a PFI from the list maintained by the PCI Council at:**
https://www.pcisecuritystandards.org/approved_companies_providers/pfi_companies.php

**5) Within three business days of the reported compromise:**

Provide an Incident Report document to Wells Fargo's Association Compliance

**Incident Report**

This template is required when initiating / responding to a MasterCard, Visa and Discover Common Point of Purchase (CPP) / Account Data Compromise (ADC) Event.

| **Overview** | **Response** |
|---|---|
| Date of Report | |
| Merchant Name | |
| Contact Name | |
| Contact Phone Number | |
| Merchant ID | |
| Provide a high-level description of the incident | |
| **Entity Description** | **Response** |

| | |
|---|---|
| Entity Name | |
| If a merchant, location of merchant (city, state) | |
| If a merchant, are there additional merchant locations? If answered yes, please provide a list of merchant locations. | |
| Name of current acquirer | |
| Current Acquirer ICA | |
| If a merchant, date merchant first processed with acquirer. | |
| If applicable, last processing date with acquirer: | |
| Entity PCI Level (i.e.; Level 1-4): | |
| Number annual incoming credit/debit/POS PIN/ATM transactions: | |
| Is the entity PCI Compliant? (If answered as yes, please provide PCI compliance documentation): | |

| **Potential Compromise Description** | **Response** |
|---|---|
| What is was the first known date of incident/compromise: | |
| How did the compromise occur (if known)? | |
| When was the compromise identified? | |
| What evidence of intrusion, if any, has been discovered? (i.e.; Suspicious email traffic, suspicious processes running on network systems, suspicious files). | |
| What was the duration of the compromise? | |
| What is the transaction date range associated with the compromised accounts? | |
| How many MasterCard accounts were affected? | |
| How Many Visa Cards were affected? | |
| How Many Discover Cards were affected? | |

| | |
|---|---|
| What credit card data was exposed / at risk?<br>▪ Primary Account Number<br>▪ Expiration Date<br>▪ Full Track 1<br>▪ Full Track 2<br>▪ CVV2<br>▪ Cardholder Name<br>▪ Social Security Number<br>▪ Date of Birth | |
| Is there any video surveillance and has it been reviewed? | |
| Can all PEDs be accounted for at all times? | |
| Are any of the POS PEDs in use listed on the June 2010 Security Alert available at: http://usa.visa.com/download/merchants/bulletin_compromised_ped_listing_mandatory_sunset_dates.pdf | |
| **If Confirmed Breach, Please Provide the Following** | **Response** |
| 1. List vulnerabilities that allowed the compromise to take place<br>2. Details of hacker's activity<br>3. List malicious IPs<br>List malware information | |
| Has the compromise been contained? If so, how? | |
| Was the entity storing Cardholder Data? If so, indicate the type of data?<br>▪ Primary Account Number<br>▪ Expiration Date<br>▪ Full Track 1<br>▪ Full Track 2<br>▪ CVV2<br>▪ Cardholder Name<br>▪ Social Security Number<br>▪ Date of Birth | |
| How many MasterCard accounts were affected? | |
| How Many Visa Cards were affected? | |
| How Many Discover Cards were affected? | |
| How Many American Express Card were affected? | |

| | |
|---|---|
| ▪ What credit card data was compromised? What data elements are at risk? Primary Account Number<br>▪ Expiration Date<br>▪ Full Track 1<br>▪ Full Track 2<br>▪ CVV2<br>▪ Cardholder Name<br>▪ Social Security Number<br>Date of Birth | |
| **Network and Payment Application Description** | **Response** |
| Does the entity have connectivity to the Internet? If so, name the type of connection (i.e.; cable modem, DSL) | |
| Does the entity have wireless/remote access connectivity? If so, please list persons with such access: | |
| Is remote access always on or is it enabled upon request? | |
| What type of remote access software is used? | |
| Is the terminal PC-based or is it connected to a PC-based environment? | |
| What are the names of compromised Point of Sale (POS) systems? | |
| What software and what version was the entity running at the time of the event? | |
| Is this a corporate-mandated payment application and version? | |
| Are the payment applications in use PCI PA-DSS compliant? Visit https://www.pcisecuritystandards.org/approved_companies_providers/vpa_agreement.php for a list of PA-DSS compliant payment applications. | |
| Is entity using a compliant PED? Visit www.pcisecuritystandards.org/pin for a list of compliant PEDs. | |
| Is entity using a compliant PED? Visit www.pcisecuritystandards.org/pin for a list of compliant PEDs. | |
| Was the entity storing Track 1 or Track 2 data? | |
| Was the entity storing CVV, CVC 2 data? | |

| | |
|---|---|
| How long is the data stored on the system? | |
| Have there been any recent changes to the network and host such as:<br>▪ Upgrade to the payment application<br>▪ Installation of a firewall<br>▪ Installation of anti-virus program<br>Changes to remote access connectivity | |
| | |
| Provide a transaction flow for credit and debit, as well as remote access to the network. The data flow must include:<br>▪ Installation of anti-virus program<br>▪ Cardholder Data sent to a central corporate server or data center<br>▪ Upstream connection to third-party service providers<br>▪ Connection to entity bank/acquirer<br>Remote access connection by third-party service providers or internal staff | |
| **Third-Party Connectivity** | **Response** |
| Does the entity send transactions to a processor(s)? If so, who is the processor(s)? | |
| Name of payment application vendor | |
| Name of reseller, if applicable | |
| Is the entity hosted? If so, who is the hosting provider? | |
| **If an e-commerce merchant, please answer the following:** | |
| Provide the affected website(s) URL address | |
| If a merchant, what is the entity's web hosting company? | |
| If a merchant, was the entity's e-commerce website on a shared or dedicated server? | |
| Does the web hosting company have access to payment card data? | |
| If a merchant, what shopping cart application is being used? | |
| If a merchant, who is the entity's payment processor or gateway provider? | |

| | |
|---|---|
| Is card payment data stored on the server, the database, shopping cart, or the payment gateway? | |
| **Other Information** | **Response** |
| Was law enforcement notified, and if so, which department/agency? | |
| What steps have been taken to remediate the risk/vulnerabilities? | |
| Please include any additional information you can provide on the investigation and the remediation of your systems you feel necessary. | |

***Visa – Responding to a Breach***
Follow the steps set forth in the resource:
https://usa.visa.com/dam/VCOM/download/merchants/cisp-what-to-do-if-compromised.pdf

a) Initial Steps and Requirements for Visa Clients (Acquirers and Issuers) - A full description of the steps is available at the link listed above.
b) Notification
    i. Immediately report to Visa the suspected or confirmed loss or theft of Visa Cardholder Data. Clients must contact the Visa Risk Management group immediately at the appropriate Visa region at USFraudControl@visa.com or 1-844-847-2106.
    ii. Within 3 days, advise Visa whether the entity was in compliance with PCI DSS and, if applicable, PCI PA-DSS and PCI PIN Security requirements at the time of the incident. If so, provide appropriate proof.
c) Preliminary Investigation
    i. Perform an initial investigation and provide written documentation to Visa w ithin three (3) business days. The information provided will help Visa understand the potential exposure and assist entities in containing the incident. Documentation must include the steps taken to contain the incident.

***MasterCard – Responding to a Breach***
The MasterCard Account Data Compromise User Guide sets forth instructions for MasterCard members, merchants, and agents, including but not limited to member service providers and data storage entities regarding processes and procedures relating to the administration of the MasterCard Account Data Compromise (ADC) program. https://www.mastercard.us/en-us/merchants/safety-security/suspect-fraud.html

a) Initial Steps and Requirements for MasterCard Clients - A full description of the steps is available at the link listed above
b) Notification
    i. Immediately report to MasterCard the suspected or confirmed loss or theft of Cardholder Data. Clients must submit a Report of Potential Account Data Compromise in the MasterCard Connect site.

c) Investigation
    i. Perform an investigation and provide written documentation to MasterCard within fifteen (15) business days. The information provided will help MasterCard understand the potential exposure and assist entities in containing the incident. Documentation must include the steps taken to contain the incident.

***American Express – Responding to a Breach***

Merchants must notify American Express immediately and in no case later than twenty-four (24) hours after discovery of a Data Incident.

a) You must engage a PCI Forensic Investigator for Data Breaches involving 10,000 or more unique American Express Card account numbers.
   The investigation must begin within 5 days of notification of the breach.
b) The final investigation report must be submitted within in 10 days of completion.
c) To notify American Express, please contact the American Express Enterprise Incident Response Program (EIRP) toll free at (888) 732-3750/US only, or at 1-(602) 537-3021/International, or email at EIRP@aexp.com. Merchants must designate an individual as their contact regarding such Data Incident.
d) For more complete language on the obligations of merchants and service providers see the following 2 documents:
    i. American Express® Data Security Operating Policy United States and Its Territories
    ii. https://www.amerianexpress.com/content/dam/amex/us/merchant/merchant-channel/April_2019_DSOP_US_EN_Final.pdf