Incident Response Plan

About This Document

This document contains the incident response plan for the Milestone Computer Incident Response Team (CIRT). This document is for internal use only and is not to be distributed.

Revision History

Version	Date	Author	Description of Change
1.0		GGW	Incident Response Plan Created
2.0	November 2010	GGW	Incident Response Plan Updates
3.0	August 2014	JJB	Updated to PCI DSS v3.0
3.1	June 2015	JDB	Updated to PCI DSS v3.1
3.2	July 2015	MRS	Updated to PCI DSS v3.2
3.2a	June 2020	DT	Review and Update format
3.3	June 2022	MM	Review and update the contact details.
3.4	August 2023	MM	Review and update contact details, Test Scenario Details update.

Contents

Purpose / Scope

This document is designed to help Milestone minimize harm posed to the company that can come as a result of a physical or logical breach of security. By minimizing the time between a security incident being detected and an appropriate response, Milestone can minimize the extent of the security incursion and minimize potential financial and reputational loss incurred as a result of the incident.

Incidents or any suspected incidents regarding the security of the cardholder data network or cardholder data itself must be handled quickly and in a controlled, coordinated, and specific manner. The purpose of the Incident Response Plan is to assist the Milestone Computer Incident Response Team (CIRT) members to identify, respond to, and report a security breach.

The Milestone incident response plan is based on an industry-standard incident response framework consisting of the seven phases listed below.

- Preparation
  - Formation of Computer Incident Response Team
  - Incident response training of CIRT members
  - Technical incident handling training for IT and security staff
  - Contact list for CIRT members, law enforcement, payment card brands and acquiring bank
  - Annual incident response testing
- Identification
  - Observation of anomalous event
- Assessment
  - Determine the scope of the incident
  - Assign severity to the incident
- Containment
  - System isolation
  - Forensically sound system backups
- Eradication
  - Removing unauthorized code
  - Applying patches
  - Installing Security Software
  - Removing unnecessary services
- Recovery
  - Rebuilding of systems
  - Operating system and application hardening
  - Clean backup restoration
- Follow-up/Lessons Learned
  - Forensic review report
  - Re-evaluation of security infrastructure

Card brands and acquiring banks must be notified upon discovery of a data security breach involving cardholder data. Visa and many acquiring banks may require a forensic review of a cardholder data security breach by a Qualified Incident Response Assessor (QIRA), such as SecurityMetrics. The list of Visa approved QIRAs can be found at: http://usa.visa.com/merchants/risk_management/cisp_if_compromised.html.

Preparation

Computer Incident Response Team Requirements

The Computer Incident Response Team is comprised of employees from both management and Information Security with the required skills to identify and control system compromises or other intrusion incidents (See Appendix A).

1. List the members and the roles and responsibilities of the Computer Incident Response Team. (Ref. PCI Security Audit Procedures v3.0 sec. 12.10.1a)
2. Train the members of the Computer Incident Response Team to deal with security breach incidents. (Ref. PCI Security Audit Procedures v3.0 sec. 12.10.4)
3. Ensure the availability of team members at all times (24/7) to respond to alerts, intrusion detection, or other incidents. (Ref. PCI Security Audit Procedures v3.0 sec. 12.10.3)
4. Train members of the Computer Incident Response Team to keep current with technical developments in the industry.
5. Notify the Computer Incident Response Team Leader of any unauthorized activity, critical IDS alerts, or reports of unauthorized critical system or content file changes and determine the need to activate the full Incident Response Plan.

Recommended CIRT Members

CIRT Members	CERT Role
Senior Management	Provide authority to operate and has the authority to make business-related decisions based on information garnered from the other team members.
Information Security	Assess security incidents, perform containment, eradication, and basic forensics. Assist information technology in the recovery role.
Information Technology	Minimize the impact of system end-users. Assist the Information Security team with technical issues and recovery roles.
Audit	Understand the root cause of the incident and any failures of compliance, which may have contributed to the incident.
Physical Security	Assess any physical damage and investigate any physical theft of data. Document chain of custody for any physical evidence.
Legal	Ensure that evidence collected is usable in a criminal investigation. Act as legal counsel to senior management.
Human Resources	Provide advice to senior management if an employee caused the incident.
Public Relations	Work with all members of the CIRT to understand the incident. Coordinate with senior management, acquirers, card brands, and law enforcement to develop a disclosure plan (if any).

Incident Response Plan – Annual Review and Testing

Regular review and testing of the Milestone Incident Response Plan are essential to maintain compliance with the Payment Card Industry Data Security Standard.

The following must be completed at least annually to maintain compliance with the PCI Data Security Standard. Documentation of completion is required. (See Appendix B).

1. Review the Incident Response Plan annually and modify it as necessary to ensure it is up to date according to lessons learned and industry developments. (Ref. PCI Security Audit Procedures v3.0 sec. 12.10.6)
2. Test the Incident Response Plan annually. (Ref. PCI Security Audit Procedures v3.0 sec. 12.10.2)

Identification and Assessment

The Incident Response Plan includes continuous monitoring with the ability to send real-time alerts to appropriate personnel from intrusion detection, intrusion prevention, and file integrity monitoring systems for all critical systems components. (Ref. PCI Security Audit Procedures v3.0 sec. 12.10.1b and 12.10.5)

A detailed process or procedure for monitoring critical security breach indicators (event logs, DS logs, File Integrity report, wireless scans, or wireless IDS logs, wireless access point ID, etc.) must be defined and documented in the IRP. (PCI-DSS Requirement 12.10.5)

All cardholder environment logs will be collected and reviewed daily by Alert Logic. Milestone utilizes Alert Logic Service for 24/7 threat management.

Use the incident response form to help assigned personnel with the identification and initial assessment of security incidents. The form helps incident responders gather information necessary to confirm the existence of an incident. Information gathered allows CIRT members to determine the scope and potential impact of an incident. Any incident involving the compromise or suspected compromise of cardholder information must be reported to impacted card brands, the acquiring bank, and any other entities as required by contract or law.

(See Appendix C – Incident Response Form)

(See Appendix D – Incident contact list)

(See Appendix E – Legal requirements)

Containment

The containment phase allows Milestone incident handlers to regain control of the situation and to minimize the amount of impact caused by an incident. Incident handlers must take careful steps to contain systems storing, transmitting, or processing cardholder information. The following general guidelines should be followed to protect evidence and limit the exposure of cardholder information.

- Perform system backup (backups must be forensically sound to preserve the machine state)
- Remove the system from the network
- Change administrative, application and system passwords
- Create additional firewall restrictions

The business impact must be evaluated before removing a system from a production environment.

Eradication and Recovery

During the eradication and recovery phases of an incident, the root cause of an incident must be determined. Qualified personnel must perform eradication and recovery phase incident response reports. Forensic analysis of system memory, disk storage, and logs must be analyzed to determine the cause of the incident. Administrative tools found on the compromised system should not be used in the event the perpetrator has modified system tools.

Re-installing the operating system and restoring a known clean system backup should perform recovery. The full Milestone systems hardening procedure must be followed before placing the system back into production. Once the system is placed back into production, increased monitoring and testing should be performed to validate that the eradication has been successful and that the root cause of the compromise has not persisted.

Card Association members may require Milestone to contract with a Qualified Incident Response Assessor such as SecurityMetrics. For a list of Visa Inc. QIRAs, go to http://www.visa.com/cisp, under If Compromised section. The file is labeled “Qualified Incident Response Assessor List.” Forensic work performed by a QIRA needs to be coordinated with the card brands and the acquiring bank.

Follow-up and Lessons Learned

Incident response plan tests and live incidents provide valuable insight into the effectiveness of the incident response plan. At the end of the incident response process, there is often a tendency to return to “business as usual” without updating Milestone policies, procedures, and guidelines. A post-mortem examination of the incident should be conducted to validate that Milestone policies, procedures, and guidelines are up to date and being followed. Any changes need to be documented and communicated to relevant personnel.

Appendix A - Assignment of CIRT Member Roles and Responsibilities

As required by the policy in section 12.6 of the Milestone security policy, the following table contains the assignment of management roles for security incident response.

CIRT Member Roles and Responsibilities

Name	Title	Date Assigned	Date Training Received	Email Contact Information	Telephone Contact Information	Description of Role and Responsibility
Ramesh Venkata Achanta	Head of Engineering	05/11/21	06/29/20	ramesh.av@milestoneinternet.com	(213) 357-0347	Provide authority to operate and has the authority to make business-related decisions based on information garnered from the other team members
Mitul Mehta	Associate Director IT	05/05/21	06/29/21	mitul.m@milestoneinternet.com	(213) 357-0565	Understand the root cause of the incident and any failures of compliance, which may have contributed to the incident.
Kishan Nathani	IT Manager	05/05/20	06/29/20	Kishan.n@milestoneinternet.com	(408)-622-9640	Assess security incidents, perform containment, eradication, and basic forensics. Assist information technology in

Kishan Nathani	IT Manager	05/05/20	06/29/20	Kishan.n@milestoneinternet.com	(408)-622-9640	Assess any physical damage and investigate any physical theft of data. Document chain of custody for any physical evidence.
Anil Aggarwal	CEO	05/05/20	06/29/20	Anil@milestoneinternet.com	(408)-200-6861	Ensure that evidence collected is usable in a criminal investigation. Act as legal counsel to senior management.
Vijay Rane	Human Resource	01/12/23	01/12/23	Aditi.m@milestoneinternet.com	(408)-200-7951	Provide advice to senior management if an employee caused the incident.
Gaurav Verma	Marketing	05/02/23	05/02/23	gaurav.v@milestoneinternet.com		Work with all members of the CIRT to understand the incident. Coordinate with senior management, acquirers, card brands, and law enforcement to develop a disclosure plan (if any).

Appendix B - Incident Response Plan – Annual Review and Testing

1. Incident Response Plan will be reviewed annually and modified as necessary to ensure it is up to date according to lessons learned and industry developments. (Ref. PCI Security Audit Procedures v3.1 sec. 12.10.6)
2. The Incident Response Plan will be tested annually. (Ref. PCI Security Audit Procedures v3.1 sec. 12.10.2)

Annual Incident Response Plan Test

Test Date	CIRT Members Involved	Test Scenario	Test Results	Modifications Needed
12 Dec 2021	• Ramesh • Mitul Mehta • Kishan Nathani • Engineering team	Log4J vulnerabilities Assetment.Log4J Vulnerability Assessment	The engineering team responded and checked Milestone product. We are using ASP.Net framework with an IIS webserver to develop a website and product. We are not using J2EE/java technology, so we are not impact by this vulnerability.	Not required
27 June 2022	• IT & Cloud Team • Engineering team	DR Drill for Enterprise customer	IT & Engineering team run DR Mock drill for CMS Product.	Not Required.
29 Aug 2023	• IT & Cloud Team • Engineering team • Product Team • Support Team	Vulnerabilities Assessment on Security Scorecard Tools.	The IT & Cloud team responded and checked. Discus and plan the vulnerabilities impact. Discuss with Engineering team and Product team to step require to remediation the same.	Not Required.

Appendix C - Incident Reporting and Assessment Form

Incident Handler Contact Information

Last Name:		First Name:	
Job Title:		Email:	
Phone:		Alt Phone:	
Mobile:		Fax:	

Incident General Information

Incident #:		Type of Incident:	☐ Malicious Code ☐ Denial-of-Service ☐ Unauthorized Access ☐ Wireless Attack ☐ Rogue Wireless ☐ Network Probes ☐ Others (Specify): ☐ SQL Injection ☐ Physical Theft ☐ Phishing ☐ Cross-Site Scripting ☐ Inappropriate Usage ☐ Privilege Escalation
Source of Incident:	☐ External ☐ Internal		
Date/Time of Incident Occurred:			
Discovered or Reported by:			
Incident location:		Date/Time of Incident Detected:	
Personal Identifiable Information Affected?	☐ Yes ☐ No	Severity Level:	☐ Critical ☐ High ☐ Medium ☐ Low
Credit Card Information Affected?	☐ Yes ☐ No		
Number of Credit Cards Impacted	VISA: MC:	AMEX: DISC:	
Systems and Services Impacted:			

Incident Summary

Comments

Incident Mitigation

Comments:

Recommendation

Comments:

Additional Comments/Notes

Comments:

Appendix D - Incident Contact List

The IRP must include or reference the specific incident response procedures from the payment brands. (PCI-DSS Requirement 12.9.1)

This information must be kept up to date and validated as part of the annual Incident Response procedure review and training.

Organization	Website	Telephone Number	Email Contact Information	Comments
<Acquiring Bank>				
VISA	http://usa.visa.com/merchants/risk_management/cisp_if_compromised.html	(650) 432-2978	usfraudcontrol@Visa.com	Pleasesee current Visa documents on the "What to do if Compromised" webpage.
MasterCard	http://www.mastercard.com/us/merchant/support/security_programs.html	(636) 722-4100	account_data_compromise@mastercard.com	Please see thecurrent MasterCard"Account Data Compromise User Guide" located on the MasterCard website.
American Express	http://www.americanexpress.com/datasecurity	(888) 732-3750 (602) 537-3021	EIRP@aexp.com	Pleaseseethecurrent(AmericanExpressData SecurityOperating Policy for Service Providers or American Express Data Security Operating Policy for U.S. Merchants) document located on the American Express data security website.
Discover	http://www.discovernetwork.com/fraudsecurity/disc.html	(800) 347-3083	N/A	
JCB	http://www.jcbusa.com/contact.html	See website		Pleasecontact the affiliated JCB office in theevent of an accountdata compromise.
Security Metrics	www.securitymetrics.com	(801) 705-5656	forensics@securitymetrics.com	The Qualified Incident Response Assessormust be differentfrom the Qualified Security Assessor.
USSecret Service	http://www.secretservice.gov/field_offices.shtml			See website for the nearest US Secret Service office.

Appendix E – Legal Requirements

PCI DSS Requirement 12.10.1 requires an analysis of legal requirements for reporting compromises.

The following are two examples of state laws:

California Privacy Law SB-1386

Requires notification of affected consumers in the event of an actual or suspected compromise for any business with California residents in their database.

http://info.sen.ca.gov/pub/01-02/bill/sen/sb_1351-1400/sb_1386_bill_20020926_chaptered.html

Massachusetts Privacy Law

201 CMR 17.00: Standard for the Protection of Personal Information of Residents of the Commonwealth of Massachusetts

http://www.mass.gov/Eoca/docs/idtheft/201CMR1700reg.pdf

<Other state, federal and international data security and breach notification laws need to be evaluated in addition to the examples provided.>

Appendix F – Card Brand Requirements

Follow the cardmember requirements listed for each card type listed below. Members of the CIRT are required to understand data breach response requirements outlined by each card brand. Card brands frequently make changes to their incident response guidelines. For complete instructions, please refer to each payment brand's website.

Visa Required Steps:

Please see Visa's "What to Do If Compromised" and "Responding to a Breach" documentation located at http://usa.visa.com/merchants/protect-your-business/data-security/if-compromised.jsp.

- Entities that have experienced a suspected or confirmed security breach must take prompt action to help prevent additional exposure of cardholder data and ensure compliance with the Payment Card Industry Data Security Standard (PCI DSS), PCI Payment Application Data Security Standard (PA- DSS), and PCI PIN Security Requirements.
- Immediately contain and limit the exposure. Minimize data loss. Prevent the further loss of data by conducting a thorough investigation of the suspected or confirmed compromise of information. Compromised entities should consult with their internal incident response team. To preserve evidence and facilitate the investigation:
    - Do not access or alter compromised system(s) (e.g., do not log on at all to the compromised system(s) and change passwords; do not log in as ROOT). Visa highly recommends compromised system not be used to avoid losing critical volatile data.
    - Do not turn the compromised system(s) off. Instead, isolate compromised systems(s) from the network (e.g., unplug network cable).
    - Preserve evidence and logs (e.g., original evidence, security events, web, database, firewall, etc.)
    - Document all actions taken.
    - If using a wireless network, change the Service Set Identifier (SSID) on the wireless access point (WAP) and other systems that may be using this connection (with the exception of any systems believed to be compromised).
    - Be on "high" alert and monitor traffic on all systems with cardholder data.
- Alert all necessary parties immediately:
    - Your internal incident response team and information security group.
    - If you are a merchant, contact your merchant bank.
    - If you do not know the name and/or contact information for your merchant bank, notify Visa Incident Response Manager immediately:
        - U.S. – (650) 432-2978 or *usfraudcontrol@Visa.com*
        - Canada – (416) 860-3090 or *CanadaInvestigations@Visa.com*
        - Latin America & Caribbean – (305) 328-1713 or *lacrmac@Visa.com*
        - Asia Pacific – (65) 96307672 or *APInvestigations@Visa.com*
        - CEMEA – +44 (0) 207-225-8600 or *CEMEAFraudControl@Visa.com*
    - If you are a financial institution, contact the appropriate Visa region at the number provided above.
    - Notify the appropriate law enforcement agency. Contact the Visa Incident Response Manager above for assistance in contacting your local law enforcement agency.
    - The compromised entity should consult with its legal department to determine if notification laws are applicable.
- Provide all compromised Visa, Interlink, and Plus accounts to the Visa acquiring bank or to Visa within

ten (10) business days. All potentially compromised accounts must be provided and transmitted as instructed by the Visa acquiring bank and Visa. Visa will distribute the compromised Visa account numbers to issuers and ensure the confidentiality of entity and non- public information.

Note: If you are an issuer, provide foreign accounts or accounts from other financial institutions to Visa.

- Within three (3) business days of the reported compromise, provide an Incident Report to the Visa client or to Visa. (See *Appendix C,* on page 25, for the Incident Report template.) If you are a financial institution, provide the Incident Report to Visa.

  Note: If Visa deems necessary, an independent forensic investigation by a Visa-approved Qualified Incident Response Assessor (QIRA) will be initiated on the compromised entity.

Key Point to Remember

To minimize the impact of a cardholder information security breach, Visa has created an Incident

Response Team to assist in forensic investigations. In the event of a compromise, Visa will coordinate a team of forensic specialists to go onsite immediately to help identify security deficiencies and control exposure. The forensic information collected by this team is often used as evidence to prosecute criminals.

MasterCard Required Steps

Please see MasterCard's current "Account Data Compromise User Guide" located at: http://www.mastercard.com/us/merchant/support/security_programs.html for MasterCard specific guidelines

- Immediately commence a thorough investigation into the Account Data Compromise (ADC) or Potential ADC event.
- Immediately, no later than within twenty-four (24) hours, identify, contain, and mitigate the ADC event or Potential ADC event, including:
  - Preserve and safeguard all potential evidence pertinent to a forensic examination of a forensic event;
  - Isolate compromised systems and media from the network;
  - Preserve all intrusion detection systems, intrusion prevention systems logs, all firewall, web, database and events logs;
  - Document all incident response actions; and
  - Refrain from restarting or rebooting any compromised or potentially compromised systems or taking other action that would have the effect of eliminating or destroying information that could potentially provide evidence of an ADC event or potential event.
- Within twenty-four (24) hours and on an ongoing basis thereafter, submit to MasterCard all known facts or suspected facts concerning the ADC event or potential ADC event, including, by way of example and not limitation, known or suspected facts as to the cause and source of the ADC event or potential ADC event.
- Within twenty-four (24) hours and continuing throughout the investigation and thereafter, provide to MasterCard, in the required format, all account numbers and expiration dates associated with MasterCard account data that were actually or potentially accessed or disclosed in connection with the ADC event or potential ADC event and any additional information requested by MasterCard. As used herein, the obligation to obtain and provide account numbers to MasterCard applies to any

MasterCard or Maestro account number in a bank identification number (BIN) range assigned by MasterCard. This obligation applies regardless of how or why such account numbers were received, processed or stored, including, by way of example and not limitation, in connection with or relating to a credit, debit (signature or pin based) proprietary, or any other kind of payment transaction, incentive or reward program.

- Within seventy-two (72) hours, engage with the services of a qualified incident response assessor ("QIRA") that was not the entity that provided the Member with its last PCI compliance report, to conduct an independent forensic investigation to assess the cause, scope, magnitude, duration, and effects of the ADC event or potential ADC event.
  Prior to the commencement of such QIRA's investigation, the Member must notify MasterCard of the proposed scope and nature of the investigation and obtain preliminary approval of such proposal by MasterCard or, if such preliminary approval is not obtained, of a modified proposal acceptable to MasterCard.
- Within two (2) business days from the date on which the QIRA was engaged, identify the engaged QIRA to MasterCard, and confirm that the QIRA has commenced its investigation.
- Within three (3) business days from the commencement of the forensic investigation, ensure that the QIRA submits to MasterCard a preliminary forensic report detailing all investigative findings to date.
- Within twenty (20) business days from the commencement of the forensic investigation, provide to MasterCard a final forensic report detailing findings, conclusions and recommendations to the QIRA, continue to address any outstanding exposure, and implement all recommendations until the ADC event or potential ADC event is resolved to the satisfaction of MasterCard. In connection with the independent forensic investigation and preparation of the final forensic report, no Member may engage in or enter into any (or permit any Agent to engage in or enter into) any conduct, agreement or understanding that would impair the completeness, accuracy or objectivity of any aspect of the forensic investigation or final forensic report. The Member shall not engage in any conduct (or permit an Agent to engage in any conduct) that could or would influence, or undermine the independence of, the QIRA or undermine the reliability or integrity of the forensic investigation or final forensic report. By way of example, and not limitation, a Member must not itself, or permit any of its Agents to, take any action or fail to take any action that would have the effect of:
  - Precluding, prohibiting or inhibiting the QIRA from communicating directly with MasterCard;
  - Permitting a Member or its Agent to substantively edit or otherwise alter the forensic report; or
  - Directing the QIRA to withhold information from MasterCard.

Notwithstanding the foregoing, MasterCard may engage a QIRA on behalf of a Member in order to expedite the investigation. The Member on whose behalf the QIRA is so engaged will be responsible for all costs associated with the investigation.

Discover Card Required Steps

- Provide the compromised Discover accounts to Discover Fraud Prevention at (800) 347-3083 within 24 hours of an account compromise event.
- Prepare a detailed written statement of fact about the account compromise including the contributing circumstances.
- Obtain additional specific requirements from Discover Card.

American Express Required Steps

Please see the current “American Express Data Security Operating Policy for Service Providers or American Express Data Security Operating Policy for U.S. Merchants” document located on the American Express data security website www.americanexpress.com/datasecurity.

Appendix G – Backup, Disaster Recovery, and Business Continuity

Please see the Milestone Business Continuity Plan and Disaster Recovery Plan