Cyber Incident Response Policy

Document Classification:	
Document Ref.	
Version:	**1**
Date:	
Document Author:	
Document Owner:	

Revision History

Version	Date	Revision Author	Summary of Changes

Distribution

Name	Title

Approval

Name	Position	Signature	Date

Purpose

This policy is established to clarify roles and responsibilities in the event of a cyber incident. The availability of cyber resources is critical to the operation of the organization and a swift and complete response to any incidents is necessary in order to maintain that availability and protect information.

Scope

The scope of this policy is applicable to all Information Technology (IT) resources owned or operated by $COMPANY$. Any information, not specifically identified as the property of other parties, that is transmitted or stored on $COMPANY$ IT resources (including e-mail, messages and files) is the property of $COMPANY$. All users ($COMPANY$ employees, contractors, vendors or others) of IT resources are responsible for adhering to this policy. The policy will be accessible via $COMPANY$ $DOCUMENT LOCATION$.

Responsible Executive

The head of $COMPANY$ shall be the Responsible Executive.
The responsibilities of the executive include, but are not limited to:

- receiving initial notification and status reports from the Incident Response Manager
- public notification, involvement of the organization’s attorney and notification of law enforcement
- preparing and delivering press releases
- updating appropriate staff on priorities for response and recovery
- advising the Incident Response Manager on priorities
- Engage PCI Forensic investigator

Incident Response Manager

$COMPANY$ designates that the Incident Response Manager has responsibility for preparing for and coordinating the response to a cyber incident. Responsibilities include, but are not limited to:

- training users to recognize and report suspected incidents annually or as needed.
- developing and testing response plans annually or as needed. Submit test results to Executive Management and as necessary external compliance entities.
- insuring incident response plans are executed correctly
- being the point of contact should any employee or official believe an incident has occurred
- involving the identified technical support to address the incident
- notifying the appropriate executives that an incident has occurred if significant
- advising executives and appropriate staff regarding notification of payment brands, PCI forensic investigators, law enforcement and the corporate attorney if appropriate
- providing information to the individual (s) responsible for notifying the press and public
- coordinating the logging and documentation of the incident and response
- making recommendations to reduce exposure to the same or similar incidents
- Track incident response performance
- Update the Incident Response Plan/Procedures annually or as needed
- Responsible for disseminating policy/procedures to identified roles

Technical Support Staff

$COMPANY$ operations shall provide technical support to the Incident Response Manager. Responsibilities include, but are not limited to:

- assessing the situation and providing corrective recommendations to the Incident Response Manager
- helping the Incident Response Manager make initial response to incidents
- responding to the incident to contain and correct problems
- reporting to the Incident Response Manager on actions taken and progress
- participating in review of the incident and development of recommendations to reduce future exposure
- consulting with other executives and appropriate staff on public notification, involvement of the small business/agency attorney, and notification of law enforcement
- assisting with preparation of press releases
- consulting with appropriate staff on priorities for response and recovery
- advising the Incident Response Manager on priorities

Legal Counsel

The attorney shall provide advice as called upon.

General $COMPANY$ Employees

It is the responsibility of all $COMPANY$ staff to adhere to corporate security policies and procedures. They are required to promptly report information security incidents to $COMPANY$ Incident Response Team for evaluation.

Notification/Reporting Requirements

Incidents are tracked in the $COMPANY$ Ticketing/Knowledge management systems. Reports to customers and management are generated from these systems. External communications to customers, law enforcement, press and attorneys are reviewed by executive management prior to submission.

Any Severity Level 5 incident (disaster) will immediately trigger execution of the Disaster Recovery Plan. Levels 3 and 4 will require an immediate meeting of the $COMPANY$ Incident Response Team and Management will be informed immediately. Level 2 incidents will require a report to the $COMPANY$ Incident Response Team and further review in the next regularly scheduled meeting. Level 1 incidents will be included in monthly reports to the $COMPANY$ Incident Response Team and Management.

The Incident Response Manager is responsible for reporting to any customers/external agencies.

In the case of emergencies employees are trained to utilize the call try located in the $COMPANY$ $DOCUMENT LOCATION$.

Types of Incidents

The $COMPANY$ Incident Response Team will classify all incidents into one of three types:

- Disclosure Incidents: These are incidents which, because of some statute or regulation, require $COMPANY$ to notify customers, law enforcement or examiners. $COMPANY$ must comply with all applicable laws and regulations, including state and federal laws.
- Security Incidents: These are incidents related to the confidentiality and integrity of information. They can include technical incidents such as malware (virus, worm, and Trojan horse) detection, unauthorized use of computer accounts and computer systems, but can also include non-technical incidents such as improper use of information assets.
- Negative Incidents: These are incidents related to the availability of information assets or other risks such as legal risks, strategic risks, or reputational risks that do not directly impact the confidentiality or integrity of information. For example, installing an

unlicensed application on a $COMPANY$ System that does not impact confidentiality, integrity, or availability, but this policy still requires the $COMPANY$ Incident Response Team to track it.

Incident Detection

- The primary means of technological intrusion detection is to leverage a suite of tools that monitor network traffic, logs, processes, and various other information points to detect exploitation attempts. Alarms are generated via security system dashboard or automated alerts
- $COMPANY$ Team members are trained to notify the $COMPANY$ Incident Response Team at Incident Response Team@wildcardcorp.com in the event that they detect a potential security issue.
- The $COMPANY$ Incident Response Team generates a ticket and explores the issue to determine if it is a true incident.

Response Guidelines

Below is a list of general methods to respond to a reported incident. These guidelines may be tuned at the Incident Response Manager’s discretion.

- Evaluation/Classification: $COMPANY$ Incident Response Team assesses the reported incident and classifies it based on pre-defined list of intrusion types.
- Containment: Upon incident confirmation, this phase is implemented with the purpose of limiting the attack. Essential to containment is assignment of severity rating as well as decisions to shut down system, limit network access, continue to monitor, or other provisions. Notification occurs during this phase.
- Eradication: Once an incident has been contained the cause is eradicated. Here is where malware, viruses, etc are removed from the system/network
- Recovery: this phase is where a system is returned to normal operations.
- Follow-up: Includes regular status updates, documentation of new controls and a lessons learned session. The lessons learned are documented in the $COMPANY$ knowledge base $DOCUMENT LOCATION$. Lessons learned will be incorporated into policy/procedures, training, and testing.

Response Metrics

Below is a list of general metrics that will be captured during the incident response process. This is not an exhaustive list and may be modified as needed throughout daily operation:

- Detection Time
- Dwell Time
- False Positive Rates
- Percent of Incidents detected by automated tools

Severity Rating Assignment

For Security and Negative Incidents, to simplify the response process, $COMPANY$ Incident Response Team members will assign one of five severity ratings to incidents as they are reported.

Level 1) Minor Incident

No interruption in data processing operations.

All incidents that will not affect operation of business but need reported in monthly written reports.

Level 2) Reportable Incident

Some computer facility and/or computer equipment damage or an interruption in critical services is observed, but operations can be resumed within 12 hours. Any incident which has disabled or will disable, partially or completely the central computing facilities, and/or the communications network for a period of 12 hours or less.

OR Any security incident which has been successfully responded to and which does not have the potential, over time, to affect inherent operational or reputational risk.

Level 3) Major Incident:

Moderate damage to the computer facility and/or the computer equipment or an interruption in critical services is observed, but operations can be resumed within 12 to 40 hours. User departments would experience two or less working days delay of updated information. Any incident which has disabled or will disable, partially or completely the central computing facilities, and/or the communications network for a period of more than 12 to 40 hours.

OR Any security incident which it is clear that a person has been specifically targeting for the purpose of breaching security.

Level 4) Critical Incident:

Any incident which has disabled or will disable, partially or completely the central computing facilities, and/or the communications network for a period of more than 12 to 48 hours.

AND/OR Any security incident which it is clear that a person has breached security or for some other reason the Information Security Officer determines that the Management may want to consider involving law enforcement.

AND/OR Any event that may increase reputational or legal risk if not addressed immediately.

AND/OR Any security incident in which protected customer information has been breached.

Level 5) Disaster:

Any Level 3 incident which has disabled or will disable, partially or completely the central computing facilities, and/or the communications network for a period of more than 48 hours.

Level 3 incidents or higher must be responded to immediately. Level 2 and below must be responded to in under 8 hours.

Information Spillage Detection and Response

$COMPANY$ has put in place automated systems capable of detecting sensitive information and alerting the Incident Response Team whenever sensitive data is transferred to unauthorized devices and systems.

Upon detection, the Incident Response Team will assess if a spill has occurred and report the potential spillage to the information owner. If the impacted system involves e-mail, $COMPANY$ instant messaging is used for communication. If the impacted system involves instant messaging then communication is conducted via e-mail.

The information owner will evaluate the report and delegate the appropriate personnel to coordinate remediation of the spillage. The information owner is responsible for putting in place controls that allow personnel to continue to perform their role despite the spillage of information. The information owner must assess if legal needs to be involved. The Incident Response Team will then isolate the system and contain to minimize the spillage and preserve evidence. Affected devices/systems immediately take on the classification of the data that is spilled limiting exposure of unauthorized personnel to the data. Upon completion of investigation, the Incident Response Team will eradicate the data from the device/system and return it to its proper classification level.

Incident Response Training

The Incident Response Manager is responsible for conducting a gap analysis on the skills of the Incident Response Team in regard to the current threat landscape. Formal or informal training will be conducting to bridge the gap as needed. During employee annual reviews, an assessment of skills will be conducted and a path to increasing Incident Response Team personnel capabilities will be outlined.

Training on Incident Response Team incident response policy/procedures will be conducted during employee onboarding, as needed (i.e. changes in system, changes in policy/procedure, etc), and annually.

Incident Response Testing

The Incident Response Manager builds and schedules the annual incident response exercise plans. The Incident Response Manager is responsible for disseminating the test plan to executive management, 3rd parties, and necessary personnel. The tests are designed to baseline the response time of the incident response team and validate that proper procedures are followed to minimize the organization’s time to recover from an incident. Annual incident response testing occurs every $TIME$.

Appendix A:

	American Express	Discover	JCB	MasterCard	Visa
Notification	Immediately send an email to EIRP@aexp.com no later than 24 hours after the incident is discovered. Complete the Merchant Data Incident - Initial Notice Form and attach it to your email. For data incidents involving 10,000 or more unique American Express Card account numbers (or otherwise at American Express's request), a PCI Forensic Investigator (PFI) must conduct this investigation	Within 48 hours of an incident.		Must notify MasterCard immediately when the Customer becomes aware of an ADC (Account Data Compromise) Event or Potential ADC Event in or affecting any system or environment of the Customer or its Agent. Must report an ADC Event within twenty-four (24) hours of becoming aware of the Event or Potential Event, and on an ongoing basis thereafter to MasterCard all known and or suspected facts concerning the ADC Event or potential ADC Event.	Within three (3) business days of a suspected or confirmed account data compromise, provide the Visa Initial Investigation Report to the acquiring bank or directly to Visa.
Forensic Investigation	May Require PCI forensic investigator			Within seventy-two (72) hours, engage the services of a PFI to conduct an	Visa may require a compromised entity to engage a PFI to perform an independent

				independent forensic investigation to assess the cause, scope, magnitude, duration, and effects of the ADC Event or Potential ADC Event. The PFI engaged to conduct the investigation must not have provided the last PCI compliance report concerning the system or environment to be examined. Prior to the commencement of such PFI's investigation, the Customer 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.	forensic investigation. Visa will not accept forensic reports from non-approved PFI forensic organizations. PFIs are required to provide forensic reports and investigative findings directly to Visa.
Forensic Investigator Timeframe	The unedited report must be provided to American Express,			Within five (5) business days from the	Provide Visa with the initial forensic (i.e. preliminary)

	within 10 business days after completion.			commencement of the forensic investigation, ensure that the PFI 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 all findings, conclusions, and recommendations of the PFI, 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.	report within ten (10) business days from when the PFI is engaged (or the contract is signed) Provide Visa with a final forensic report within ten (10) business days of completion of the review.
Contact Information	Report a data incident at 1-888-732-3750 or EIRP@aexp.com	Call Discover® Global Network Security at 1-800-347-3083 to report a		Must report an ADC Event or Potential ADC Event through the Manage My Fraud and Risk Programs application.	Contact Visa at (650) 432-2978 or usfraudcontrol@visa.com

		data security breach. If you have questions, email AskDataSecurity@discover.com		account_data_compromise@mastercard.com	
Compromised account reporting				Via My Fraud and Risk Programs application. Within twenty-four (24) hours and continuing throughout the investigation and thereafter, provide to MasterCard, in the required format, all PANs associated with 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.	Visa CAMS (Compromised Account Management System)
Indemnification	American Express will not seek indemnification from your organization for an incident (a) involving less than			MasterCard may charge Operational Reimbursement (OR) and Fraud Recovery (FR) fees based on the	To qualify an account data compromise event under the GCAR (Global Compromised Account Recovery)

	10,000 unique Compromised Card Numbers or (b) if: You notified American Express of the Data Incident pursuant to AMEX policy, § You were in compliance at the time of the Data Incident with the PCI DSS (as determined by the PFI's investigation of the Data Incident) and § The data incident was not caused by your wrongful			number of compromised or potentially compromised accounts. In the event that the compromised entity is an e-commerce merchant where only PAN, expiration date, and/or the CVC code have been compromised, only OR will be invoked. Based on the totality of known circumstances surrounding an ADC Event or Potential ADC Event, including the knowledge and intent of the responsible Customer, MasterCard (in addition to any assessments provided for elsewhere in the Standards) may assess a responsible Customer up to US$ 100,000 for each violation of a requirement of the PCI SSC. If the Customer fails to comply with the procedures set forth in section	program, Visa must determine all of the following criteria have been met: 1. A PCI DSS or PCI PIN Security or PIN Security Program Guide violation has occurred that could have allowed a compromise of Primary Account Number (PAN) and Card Verification Value (CVV) magnetic-stripe data and/or PIN data. 2. Primary Account Number (PAN) and Card Verification Value (CVV) magnetic-stripe data, and/or PIN data, is exposed at the compromised entity during the intrusion access window. 3. 15,000 or more eligible accounts were sent in one or more CAMS (Compromised Account Management System) IC (Internet Compromise) or RA (Research & Analysis) alerts and/or Visa Account Bulletin (VAB) alerts indicating Primary Account Number (PAN) and Card Verification Value (CVV)

				10.2 of the Security Rules and Procedures Manual, MasterCard may impose an assessment of up to USD 25,000 per day for each day that the Customer is noncompliant and/or disqualify the Customer from participating as a recipient of ADC OR reimbursement and FR disbursements, whether such disbursements are made in connection with the subject ADC Event or any other ADC Event, from the date that MasterCard provides the Customer with written notice of such disqualification until MasterCard determines that the Customer has resolved all compliance issues under this section 10.2.	magnetic-stripe data is potentially at risk. 4. A combined total of US$ 150,000 or more recovery for all issuers involved in the event. 5. Elevated magnetic-stripe counterfeit fraud was observed in the population of eligible accounts sent in the CAMS alert(s) associated with the Account Data Compromise Event. Under the GCAR program, Visa uses a basic set of rules to calculate an acquirer's liability for issuer incremental counterfeit fraud losses and a predetermined amount to cover operating expenses associated with accounts at risk in the compromise event. These calculations are based on eligible CAMS-alerted accounts and issuer-reported counterfeit fraud that occurred during the alert Fraud Window for one or more event alerts. Visa also may impose a liability cap for compromises that

					meet specified criteria to be deemed catastrophic, based on a balancing of the overall interests of the system. For merchant compromises where other criteria are met, the cap on the acquirer's liability is calculated based on the annual Visa sales volume of transactions submitted by acquirers for entities owned or controlled by the legal owner of the compromised entity. This will include Visa sales at all entities owned by the legal owner of the compromised entity

For additional information refer to the following websites:

AMEX

- https://merchant-channel.americanexpress.com/merchant/en_US/data-security
- https://icm.aexpstatic.com/Internet/NGMS/US_en/Images/DSOP_Merchant_US.pdf

Discover:

- https://www.discovernetwork.com/en-us/business-resources/fraud-security/pcirules-regulations/discover-information-security-compliance

JCB

- http://www.global.jcb/en/products/security/data-security-program/

MasterCard

- https://www.mastercard.us/en-us/merchants/safety-security/securityrecommendations/site-data-protection-PCI.html
- https://www.mastercard.us/content/dam/mccom/en-us/documents/SPME-ManualSept-2017.pdf
- https://www.mastercard.us/content/dam/mccom/en-us/documents/account-datacompromise-manual.pdf
- https://globalrisk.mastercard.com/online_resource/member-alert-to-control-highrisk-merchants-match-compliance-program/

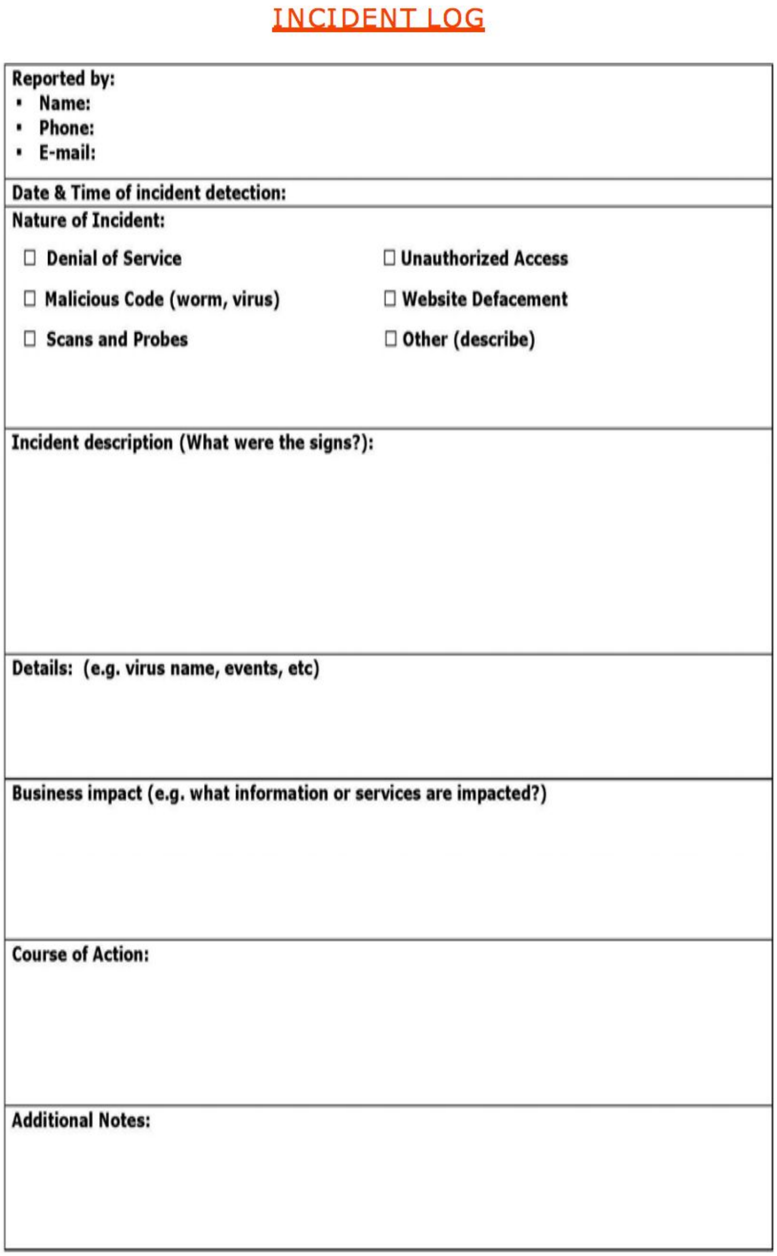
Visa

- https://usa.visa.com/support/small-business/security-compliance.html
- https://usa.visa.com/dam/VCOM/download/merchants/cisp-what-to-do-ifcompromised.pdf
- http://paymentworld.com/docs/training/visa/what-every-merchant-should-knowgcar-vol-091213-final.pdf
- https://usa.visa.com/dam/VCOM/download/about-visa/visa-rules-public.pdf

Contacts

Contact	Phone	e-mail
Visa	650 432 2978	usfraudcontrol@visa.com
United States Secret Service Electronic Crimes Task Forces (ECTF)	202 406 5708	

Sample Incident Log



INCIDENT LOG

Reported by:
- **Name:**
- **Phone:**
- **E-mail:**

Date & Time of incident detection:

Nature of Incident:

☐ Denial of Service	☐ Unauthorized Access
☐ Malicious Code (worm, virus)	☐ Website Defacement
☐ Scans and Probes	☐ Other (describe)

Incident description (What were the signs?):

Details: (e.g. virus name, events, etc)

Business impact (e.g. what information or services are impacted?)

Course of Action:

Additional Notes: