**Name of Organization**

**Regulatory Notification Requirements**

December 2021

**Revision History**

|  |  |  |  |
| --- | --- | --- | --- |
| Revision Number | Revision Date | Summary of Changes Made | Changed By |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

Instructions

This (Name of Organization) Regulatory Notification Requirements document is designated For Official Use Only (FOUO) and is the property of (Name of Organization). Only (Name of Organization) representatives may distribute this document to individuals on a need-to-know basis. Distribution by other individuals without prior authorization is prohibited. This document is unclassified but contains sensitive information.

**Table of Contents**

[I. Introduction and Purpose 5](#_Toc88584048)

[II. Notification and Communication Requirements 5](#_Toc88584049)

[Interaction with Law Enforcement 5](#_Toc88584050)

[Regulatory Authorities 6](#_Toc88584051)

[Customers 6](#_Toc88584052)

[Public Media Handling 6](#_Toc88584053)

[III. US\_CERT Federal Incident Notification Guidelines 7](#_Toc88584054)

[Submitting Incident Notifications 7](#_Toc88584055)

[IV. Cyber Security and Breach Reporting Sites 8](#_Toc88584056)

[Report Crime, Ransomware, Malware and Incidents 8](#_Toc88584057)

[V. Regulatory Notification Requirements 9](#_Toc88584058)

[Texas Data Breach Notification 9](#_Toc88584059)

[FISMA/NIST 9](#_Toc88584060)

[NERC/CIP 10](#_Toc88584061)

[HIPAA and HITECH 10](#_Toc88584062)

[PCI DSS 10](#_Toc88584063)

[Visa 10](#_Toc88584064)

[MasterCard 12](#_Toc88584065)

[Discover 12](#_Toc88584066)

[American Express 12](#_Toc88584067)

[SOX 12](#_Toc88584068)

[FDIC / OCC 13](#_Toc88584069)

[EU GDPR 14](#_Toc88584070)

# Introduction and Purpose

The (Name of Organization) defines requirements for establishing specific Regulatory Notification and Communication Requirements for responding to, assessment of, and monitoring of threats to organizational information assets. This Regulatory Notification Requirement document builds on the objectives established in the Incident Response Plan and provides specific requirements for notification.

Effective regulatory notification involves every part of the organization, including IT teams, Legal, Technical Support, Human Resources, Corporate Communications, and business operations. It is important that you read and understand your role and the ways you will need to notify internal and external department personnel and agencies.

# Notification and Communication Requirements

Required notification and communication both internally and with third parties (customers, vendors, law enforcement, etc.) based on legal, regulatory, and contractual requirements must take place in a timely manner.

* The Incident Commander must report the incident to the senior leadership.
* The senior leadership must report any potential breaches and/or incidents involving customer data to the Incident Handling Team (IHT) promptly.
* The IHT is responsible for appropriate notification to:
	+ Personnel
	+ Affected customers and/or partners (based on SLA, based on legal or regularity compliance, whichever is shorter).
	+ Local, Texas state or federal law officials as required by applicable statutes and/or regulations.

Depending on the type and scope of breach, consider using the Customer Data Breach Report to inform impacted business entities.

## Interaction with Law Enforcement

Interaction between law enforcement and emergency services personnel should be coordinated by the Incident Commander. The Incident Commander will manage ongoing communication with authorities. It must be noted however that Law Enforcement’s priorities are eventual prosecution of offenders and not necessarily returning the Organization to a functional state in a timely manner. Ensure the Legal department is consulted and provides direction before and while communicating with Law Enforcement.

## Regulatory Authorities

* The Organization is subject to various regulatory oversight, depending on the type and classification of data impacted. If there is the potential that regulated data were breached, it may be necessary to notify the State of Texas, Local Authorities, Payment Card Industry Security Standards Council (PCI SSC), etc. Depending upon the nature of the breach it may be required to contact other federal governmental regulators.
* Only members of the IHT and designates are permitted to discuss the nature and/or details of an incident with anyone including regulatory agencies.
* The IHT should contact regulators as soon as practical.

## Customers

* All customers who are affected by the incident must be notified according to applicable contract language, service level agreements (SLAs), applicable statutes and/or regulations.
* Communications with customers must be consistent, with the same or similar message delivered to each. The message sent to customers will be created by members of the Communications Team.
* Customer service and/or customer account managers will communicate with customers according to the message developed by the Communications Team.

## Public Media Handling

All Information concerning an incident is to be considered confidential, and at no time should any information be discussed with anyone outside of the Organization without approval of executive management and the legal counsel.

Public or media statements must be carefully managed to ensure that any investigation/legal proceedings are not jeopardized, and reputational damage is minimized. Decisions concerning the disclosure and method of disclosure of incident information will only be made by a designated spokesperson assigned by the IHT, likely someone from the Communications Team or a representative coached by the Communications Team.

Inquiries from media agencies must be directed to the designated IHT representative. Employees found to be discussing incidents without approval from executive management/legal counsel will be subject to disciplinary action, up to and including termination.

# US\_CERT Federal Incident Notification Guidelines

Federal Government departments and agencies (D/As): state, local, tribal, and territorial government entities must report information security incidents, where the confidentiality, integrity, or availability of a federal information system of a civilian Executive Branch agency is potentially compromised, to the CISA/US-CERT with the required data elements, as well as any other available information, **within one hour** of being identified by the agency’s top-level Computer Security Incident Response Team (CSIRT), Security Operations Center (SOC), or information technology department.

## Submitting Incident Notifications

The information elements described in steps 1-7 below are required when notifying US-CERT of an incident:

1. Identify the current level of impact on agency functions or services (Functional Impact).
2. Identify the type of information lost, compromised, or corrupted (Information Impact).
3. Estimate the scope of time and resources needed to recover from the incident (Recoverability).
4. Identify when the activity was first detected.
5. Identify the number of systems, records, and users impacted.
6. Identify the network location of the observed activity.
7. Identify point of contact information for additional follow-up.

**Important:** Please refrain from adding sensitive personally identifiable information (PII) to incident submissions.

1. Submit the notification to US-CERT.
2. The following information should also be included if known at the time of submission:
* Identify the attack vector(s) that led to the incident.
* Provide any indicators of compromise, including signatures or detection measures developed in relationship to the incident.
* Provide any mitigation activities undertaken in response to the incident.
1. Within one hour of receiving the report, CISA/US-CERT will provide the agency with:
	* A tracking number for the incident.
	* A risk rating based on the Cyber Incident Scoring System (NCISS).

Reports may be submitted using the CISA/US-CERT Incident Reporting Form; send emails to soc@us-cert.gov or submit reports via Structured Threat Information eXpression (STIX) to autosubmit@us-cert.gov (schema available upon request).

# Cyber Security and Breach Reporting Sites

## Report Crime, Ransomware, Malware and Incidents

[**Internet Crime Complaint Center (IC3)**](https://www.ic3.gov/default.aspx) collects reports of Internet crime from the public. Using such complaints, the IC3’s Recovery Asset Team has assisted in freezing hundreds of thousands of dollars for victims of cybercrime.

[**Cyber Task Forces**](http://www.fbi.gov/about-us/investigate/%20cyber/cyber-task-forces-building-alliances-to-improve-the-%20nations-cybersecurity-1) Cybercrime, including computer intrusions or attacks, fraud, intellectual property theft, identity theft, theft of trade secrets, criminal hacking, terrorist activity, espionage, sabotage, or other foreign intelligence activity

[**Electronic Crimes Task Forces (ECTFs)**](http://www.secretservice.gov/ectf.shtml) **Cybercrime**, including computer intrusions or attacks, transmission of malicious code, password trafficking, or theft of payment card or other financial payment information

[**National Cybersecurity and Communications Integration Center (NCCIC)**](http://www.dhs.gov/about-national-cybersecurity-%20communications-integration-center) Suspected or confirmed cyber incidents that may impact critical infrastructure and require technical response and mitigation assistance.

**CISA** [**Incident Reporting Form:**](https://us-cert.cisa.gov/forms/report) report incidents as defined by [NIST Special Publication 800-61 Rev 2](https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf), to include

* Attempts to gain unauthorized access to a system or its data,
* Unwanted disruption or denial of service, or
* Abuse or misuse of a system or data in violation of policy.

Federal incident notification guidelines, including definitions and reporting timeframes can be found at [http://www.us-cert.gov/incident-notification-guidelines](https://us-cert.cisa.gov/incident-notification-guidelines).

[**Share indicators and defensive measures**](https://us-cert.cisa.gov/forms/share-indicators)**:** submit cyber threat indicators and defensive measures with DHS and the Federal Government (includes sharing under the Cybersecurity Information Sharing Act of 2015).

[**Report phishing**](https://us-cert.cisa.gov/report-phishing/)**:** an attempt by an individual or group to solicit personal information from unsuspecting users by employing social engineering techniques, typically via emails containing links to fraudulent websites.

[**Report malware**](http://malware.us-cert.gov/)**:** malicious code (e.g., viruses, worms, bots) that disrupts service, steals sensitive information, gains access to private computer systems, etc.

[**Report software vulnerabilities or ICS vulnerabilities**](https://www.us-cert.gov/vulnerability-disclosure-policy)**:** defects that allow an attacker to violate an explicit (or implicit) security policy to achieve some impact (or consequence). In particular, defects that allow intruders to gain increased levels of access or interfere with the normal operation of systems are vulnerabilities. Insecure configurations, design choices, and changing environmental conditions can also cause vulnerabilities.

[**Report vulnerabilities in U.S. Government websites**](https://www.kb.cert.org/vuls/report/)**:** defects that may allow an attacker to violate a security policy to cause some impact or consequence, particularly those vulnerabilities that allow increased levels of access or the ability to interfere with the normal operation of the server or site.

# Regulatory Notification Requirements

## Texas Data Breach Notification

Texas law requires certain businesses that experience a data breach of system security to notify affected consumers AND also to provide notice of that data breach to the Office of the Texas Attorney General if the breach affects 250 or more Texans.

Effective September 1, 2021, the notice to the Texas Attorney General must report the number of Texans that your organization has notified of the breach by mail or email. The Attorney General will also post a [listing](https://oagtx.force.com/datasecuritybreachreport/apex/DataSecurityReportsPage) of breach notifications at its website as required by House Bill 3746.

To facilitate this reporting, the Texas Attorney General provides a Data Breach Submission form which you may submit to the Attorney General electronically.

You may [fill out the Data Breach Notice form](https://oagtx.force.com/datasecuritybreachreport/s/) provided and submit it electronically.

Before filling out the form, here is what you need to know:

* The system can NOT save your form, so you will need to complete it in one sitting.
* To prepare, you can [preview the form](https://oagtx.force.com/datasecuritybreachreport/s/).
* Do NOT hit the “back” button on your browser, or your submission will be cleared.
* Your data breach notice is potentially an open record. This means that members of the general public may file an open-records request to obtain a copy of your completed form.
* If you experienced more than one breach, please submit a separate data breach notice for each.

## FISMA/NIST

FISMA is United States legislation intended to protect the security, confidentiality, and integrity of government data systems. A FISMA audit is a test of an organization’s system against the controls outlined in various NIST publications such as NIST SP 800-53, NIST SP 800-171, FIPS 199, and FIPS 200.

* Reporting requirements – A FISMA audit is a test of an organization’s system against the controls outlined in various NIST publications such as NIST SP 800-53, NIST SP 800-171, FIPS 199, and FIPS 200.
* Link – <https://csrc.nist.gov/projects/risk-management>

## NERC/CIP

The NERC Critical Infrastructure Protection (CIP) Standards apply to the cyber security aspects of the Bulk Electric System and its efficient and reliable supply.

* Reporting requirements – Reliability standards require the reporting of cyber security incidents that compromise, or attempt to compromise, a responsible entity’s Electronic Security Perimeter (ESP) or associated Electronic Access Control or Monitoring Systems (EACMS).
* Link – <https://www.nerc.com/pa/Stand/Pages/CIPStandards.aspx>

## HIPAA and HITECH

Any organization that creates, receives, maintains, or transmits electronic protected health information (ePHI) in the United States must meet HIPAA requirements for access control and data sharing.

* Reporting requirements – The HIPAA Breach Notification Rule, 45 CFR §§ 164.400-414, requires HIPAA covered entities and their business associates to provide notification following a breach of unsecured protected health information.
* Similar breach notification provisions implemented and enforced by the Federal Trade Commission (FTC) apply to vendors of personal health records and their third-party service providers, pursuant to section 13407 of the HITECH Act.
* Link – <https://www.hhs.gov/hipaa/for-professionals/breach-notification/index.html>

## PCI DSS

Provides organizations that accept, store or transmit credit card data with guidelines for privilege management and a framework to protect cardholder data.

* Reporting requirements – PCI DSS requires entities have an incident response plan and alert effected parties immediately. PCI DSS 3.2.1, released on May 2018, marks the latest version.
* You may want to set up an arrangement with an independent Payment Card Industry Forensic Investigator (PFI) to call if you need outside expertise.
* Link – <https://www.pcisecuritystandards.org/documents/PCI_SSC_PFI_Guidance.pdf>

## Visa

Taking immediate action

Merchants and service providers that have experienced a suspected or confirmed security breach must take immediate action to help prevent additional damage and adhere to Visa CISP requirements.

Alert all necessary parties immediately:

* Your internal incident response team and information security group.
* Your merchant bank.
* If you do not know the name and/or contact information for your merchant bank, notify Visa Incident Response Manager immediately at U.S. – (650) 432-2978 or usfraudcontrol@visa.com

Loss or theft of account information

Members, service providers or merchants must immediately report the suspected or confirmed loss or theft of any material or records that contain Visa cardholder data.

Forensic Investigation Guidelines

A Visa client/member or compromised entity must engage a Payment Card Industry Forensic Investigator (PFI) to perform a forensic investigation. Visa will NOT accept forensic reports from non-approved forensic companies. It is the Visa client or member’s responsibility to ensure their merchant or agent engage a PFI to perform a PFI forensic investigation. Visa has the right to engage a PFI to perform a further forensic investigation as it deems appropriate and will assess all investigative costs to the appropriate Visa client, in addition to any assessment that may be applicable. PFIs are required to release forensic reports and findings to Visa. All PFIs must utilize Payment Card Industry reporting templates.

Note: For a list of PFIs, please go to: https://www.pcisecuritystandards.org/approved\_companies\_providers/pci\_forensic\_investigator.php

Note: Visa has the right to reject the report if it does not meet the PFI requirements. PFIs are required to address with Visa, the acquirer, and the compromised entity, any discrepancies before finalizing the report.

To preserve evidence and facilitate the investigation:

* Do not access or alter compromised system(s) (e.g., don’t log on at all to the compromised system(s) and change passwords; do not log in as ROOT). Visa highly recommends the 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, shut down switchport, etc.).
* Preserve all evidence and logs (e.g., original evidence, security events, web, database, and firewall logs, etc.)
* Document all actions taken, including dates and individuals involved.
* 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).
* Block suspicious IPs from inbound and outbound traffic.
* Be on high alert and monitor traffic on all systems with cardholder data.

For more information on the forensic investigation guideline, please refer to the document labeled PCI Forensic Investigator (PFI) Program Guide.

## MasterCard

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.

## Discover

To contact Discover regarding Data Security or PCI Compliance:

Data Security: 1-800-347-3083 Call Mon–Fri 8:30am to 12:30pm and 1:30pm to 4:00pm Eastern Time, excluding holidays

Questions on Security or PCI Compliance: AskDataSecurity@discover.com

Report data compromise or cardholder data breach: 1-800-347-3083 Call Mon–Fri 8:30am to 4:00pm Eastern Time, excluding holidays

## American Express

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

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.

Please see the American Express Data Security Operating Policy for all details pertaining to Data Incident Management Obligations.

## SOX

Sarbanes-Oxley (SOX) is designed to reduce corporate fraud by requiring an increase in the strength and granularity of security controls for financial auditing and reporting.

* Reporting requirements – Companies must disclose failure of security safeguards and security breaches to SOX auditors.
* Link – <https://www.sarbanes-oxley-101.com/>

## FDIC / OCC

When a financial institution becomes aware of an incident of unauthorized access to sensitive customer information, the institution should conduct a reasonable investigation to promptly determine the likelihood that the information has been or will be misused.

If the institution determines that misuse of its information about a customer has occurred or is reasonably possible, it should notify the affected customer as soon as possible. However, notice may be delayed if an appropriate law enforcement agency determines that notification will interfere with a criminal investigation.

Under the guidance, a financial institution should notify its primary federal regulator of a security breach involving sensitive customer information, whether or not the institution notifies its customers.

Customer Notification Content

The contents of a breach notification should contain the following elements:

* a general description of the incident and the information that was the subject of unauthorized access;
* a telephone number for further information and assistance;
* a reminder "to remain vigilant" over the next 12 to 24 months;
* a recommendation that incidents of suspected identity theft be reported promptly, and;
* a general description of the steps taken by the financial institution to protect the information from further unauthorized access or use.

Filing a SAR

Banks, bank holding companies, and their subsidiaries are required by federal regulations to file a SAR with respect to:

* Criminal violations involving insider abuse in any amount.
* Criminal violations aggregating $5,000 or more when a suspect can be identified.
* Criminal violations aggregating $25,000 or more regardless of a potential suspect.
* Transactions conducted or attempted by, at, or through the bank (or an affiliate) and aggregating $5,000 or more, if the bank or affiliate knows, suspects, or has reason to suspect that the transaction:
* May involve potential money laundering or other illegal activity (e.g., terrorism financing).
* Is designed to evade the BSA or its implementing regulations.
* Has no business or apparent lawful purpose or is not the type of transaction that the particular customer would normally be expected to engage in, and the bank knows of no reasonable explanation for the transaction after examining the available facts, including the background and possible purpose of the transaction.

A transaction includes a deposit; a withdrawal; a transfer between accounts; an exchange of currency; an extension of credit; a purchase or sale of any stock, bond, certificate of deposit, or other monetary instrument or investment security; or any other payment, transfer, or delivery by, through, or to a bank.

The SAR rules require that a SAR be electronically filed through the BSA E-Filing System no later than 30 calendar days from the date of the initial detection of facts that may constitute a basis for filing a SAR. If no suspect can be identified, the time period for filing a SAR is extended to 60 days.

Use this link to file a SAR: http://bsaefiling.fincen.treas.gov/main.html

## EU GDPR

Any organization dealing with EU citizens' Personally Identifiable Information is obligated to meet standards for effective data protection, adequate security measures, and privacy by design to comply with EUGDPR.

* Reporting requirements – Under GDPR, breach notification is mandatory in all member states where a data breach is likely to result in a risk for the rights and freedoms of individuals. This must be done within 72 hours of first having become aware of the breach. Data processors are required to notify their customers, the controllers, without undue delay after first becoming aware of a data breach.
* Link – <https://www.eugdpr.org/key-changes.html>