BREACH RESPONSE PLAN

June 2025

FDIC

FEDERAL DEPOSIT INSURANCE CORPORATION

Table of Contents

1. INTRODUCTION

1.1 Purpose and Scope

The purpose of this Breach Response Plan (Plan) is to describe the activities the Federal Deposit Insurance Corporation (FDIC) undertakes to respond to a breach of personally identifiable information (PII). It describes the breach response process, details the framework for assessing the risk of harm to individuals potentially affected by a breach, and provides guidance on whether and how to provide notification and offer mitigation services to affected individuals. It also assigns roles and responsibilities for responding to a breach.

The Office of Management and Budget (OMB) Memorandum M-17-12, Preparing for and Responding to a Breach of Personally Identifiable Information, establishes policy for Federal agencies to prepare for and respond to a breach of PII. Among other things, it requires agencies to establish a breach response plan. OMB defines an "incident" as:

> "[a]n occurrence that (1) actually or imminently jeopardizes, without lawful authority, the integrity, confidentiality, or availability of information or an information system; or (2) constitutes a violation or imminent threat of violation of law, security policies, security procedures, or acceptable use policies."[1]

Additionally, OMB defines a "breach" as:

> "[t]he loss of control, compromise, unauthorized disclosure, unauthorized acquisition, or any similar occurrence where (1) a person other than an authorized user accesses or potentially accesses personally identifiable information or (2) an authorized user accesses or potentially accesses personally identifiable information for an other than authorized purpose."[2]

A breach is a subset of an incident. It may include the inadvertent disclosure of PII on a public website, an oral disclosure of PII to an individual who is not authorized to receive that information, or an authorized user accessing PII for an unauthorized purpose.

This Plan applies to all breaches involving PII at the FDIC. The PII can be in any format (i.e., electronic, paper, or verbal). FDIC applies the OMB definition of PII to determine whether the compromised information falls into that definition.[3]

The Plan is a component of FDIC's Office of the Chief Information Security Officer (OCISO) Incident Response Plan (IRP). The IRP is the roadmap for implementing the Corporation's

[1] OMB Memorandum M-17-12, Preparing for and Responding to a Breach of Personally Identifiable Information, §III.C. (Jan. 3, 2017).
[2] OMB M-17-12, §III.C.
[3] *See* OMB Circular No. A-130, Managing Information as a Strategic Resource, §10(a)(57) (2016).

incident response capability. The Breach Response Plan documents the FDIC's procedures for reporting, investigating, and managing a breach. The FDIC uses the Plan to effectively and efficiently respond to a breach, no matter the size. For all incidents not constituting a breach, the FDIC uses to the IRP, the Corporation's incident handling guide.

1.2 Authorities

The FDIC is required to protect PII and to respond to breaches. The FDIC has authority to respond to breaches and has derived its response plan from several sources, including:

- The Federal Information Security Modernization Act of 2014 (FISMA), Title 44, U.S.C., Chapter 35, Subchapter II, "Information Security"
- Office of Management and Budget (OMB) Circular No. A-130, Managing Information as a Strategic Resource (July 28, 2016)
- OMB Memorandum 16-24, Role and Designation of Senior Agency Officials for Privacy (September 15, 2016)
- OMB Memorandum 17-12, Preparing for and Responding to a Breach of Personally Identifiable Information (January 3, 2017)
- OMB Memorandum 25-04, Fiscal Year 2025 Guidance on Federal Information Security and Privacy Management Requirements (January 15, 2025) or successor publication
- FDIC Directive 1360.12, Reporting Information Security Incidents
- FDIC Directive 1360.20, Privacy Program

1.3 Supplemental Guidance

FDIC Divisions and Offices may develop and implement supplemental Division- or Office-specific breach plans and procedures, so long as they comply with and are not less restrictive than this document. As required by OMB M-17-12, any new or substantially revised Division or Office breach plans and procedures must be reviewed and approved by the Senior Agency Official for Privacy (SAOP) prior to implementation to ensure consistency with the requirements of this Plan, other FDIC guidance, applicable OMB guidance, and applicable law.

1.4 Review Cadence

The SAOP reviews this Plan at least once in the 12 months preceding the annual submission of the FDIC FISMA Report to confirm that the plan is current, accurate, and reflects any changes in law, guidance, standards, agency policy, procedures, staffing, or technology.

The SAOP is responsible for documenting the date of the most recent review and submitting the updated version of the Plan to OMB when requested as part of annual FISMA reporting. FDIC Divisions or Offices must annually submit their breach plans and procedures to the SAOP for review. Division or Office breach plans and procedures must clearly detail the relationship between the Division or Office breach plans and procedures and this Plan.

2 ROLES AND RESPONSIBILITES

The following section details the roles with primary responsibility during any incident involving PII.

2.1 Head of Agency (Board of Directors)

The Board of Directors, or duly authorized officers or agents, are responsible for determining whether a breach constitutes a major incident[4] and for ensuring the appropriate congressional and Office of Inspector General (OIG) notification has been made according to governing directives. In the event of a breach that constitutes a major incident, the Board of Directors, or duly authorized officers or agents, also provide final approval for the recommended course of action, including whether to provide notification, guidance, or services to individuals potentially affected by a breach.

2.2 Chief Information Officer (CIO)

The CIO assists in determining the impact of the breach by evaluating the implementation and effectiveness of security safeguards protecting the information (e.g., identify technical remediation and forensic analysis capabilities and which offices are responsible) and provides guidance regarding any information technology needed to respond to the breach. The CIO, in coordination with the SAOP, Chief Information Security Officer (CISO), and other technical experts, confirms whether encryption was in effect; the degree of encryption; at which level the encryption was applied; and whether decryption keys were controlled, managed, and used. The CIO also considers other security safeguards employed, on a case-by-case basis, taking into account whether the type, value, or sensitivity of the information might motivate a malicious actor to put time and resources towards overcoming those safeguards.

2.3 Senior Agency Official for Privacy

The SAOP has agency-wide responsibility and accountability for ensuring compliance with applicable privacy requirements, developing and evaluating privacy policy, and managing privacy risks consistent with the agency's mission.[5]

The SAOP maintains primary responsibility for developing and implementing FDIC's Plan, including the policies and procedures for reporting, investigating, and managing a breach. The SAOP, or designee, convenes and leads the Breach Response Team (BRT) when there is a suspected or confirmed major incident that is a breach. The SAOP responds to the breach and

[4] OMB defines "major incident" in an annual guidance memo on federal information security and privacy management requirements.

[5] *See* OMB Circular A-130, Managing Information as a Strategic Resource (July 28, 2016).

presents the BRT's recommendations and findings to the Board of Directors, or duly authorized officers or agents.

Pursuant to the SAOP Designation Memo, the SAOP is responsible for making a final decision about whether to provide notification, guidance, or services to individuals potentially affected by a routine breach. The SAOP and is the principal point of coordination for all requests related to delayed notification.[6]

2.4 Chief Information Security Officer

The CISO serves as the designated senior agency information security officer,[7] responsible for developing and maintaining FDIC's information security and privacy programs. The CISO is responsible for developing and maintaining the FDIC's information security policies, procedures, and controls to address all applicable requirements, training, and overseeing personnel with significant responsibilities for information security, and establishing and managing the FDIC's Privacy Program.

2.5 Privacy Program Chief (PPC)

The Privacy Program Chief (PPC) is responsible for advising the SAOP and CISO in the development, daily operation, and management of the FDIC Privacy Program. In the event of a breach, the PPC assists the SAOP and CISO in fulfilling their breach-related responsibilities as outlined in this Plan and OMB M-17-12. The PPC provides guidance to the impacted Division or Office and system or business owner(s) in assessing the potential risk of harm to individuals. The PPC serves as a principal advisor to the SAOP and BRT, in coordination with the CISO, on decisions regarding notification and breach mitigation. The PPC, on behalf of the SAOP, is also responsible for keeping the Enterprise Security Operations Section (ESOS) informed of the status of an ongoing response, for determining when the response to a breach has concluded, and for reporting the completed status and the outcome of the response.

When a breach does not require the convening of the BRT, the PPC, on behalf of the SAOP, manages these routine breaches to closure. When notification is determined necessary, the PPC selects the method of notification and oversees the notification process on behalf of the SAOP in coordination with the relevant Division or Office. The PPC also assists the SAOP in reviewing Division- or Office-specific breach plans and procedures and overseeing updates that need to be made to this Plan at least annually.

[6] Memorandum, Designation of Senior Agency Official for Privacy as Source of Notification Letter for Breaches (October 26, 2017).
[7] *See* 44 U.S.C. § 3554(a)(3)

2.6 Incident Response Coordinator

The Incident Response Coordinator works within the ESOS, which includes the Security Response Team (SRT). The Incident Response Coordinator is accountable for all FDIC incident response activities and provides centralized technical assistance to investigate, resolve, and contain security incidents. The Incident Response Coordinator shall ensure that the PPC, on behalf of the SAOP, is made aware in a timely manner of each report of a suspected or confirmed breach.

2.7 Breach Response Team

The BRT is comprised of FDIC officials who support the agency response to breaches that may constitute major incidents as defined by OMB. In a memo dated September 20, 2018, the FDIC Chairperson, considering the skills and expertise that may be required to effectively and efficiently respond to a breach, designated the officials identified in Appendix B to serve on the BRT.[8] When convening the BRT, the SAOP, or designee, considers the circumstances of the breach to ensure appropriate subject matter experts are also included.

3 BREACH RESPONSE PROCESS

3.1 Initial Breach Reporting

Before gaining access to federal information or information systems, and annually thereafter, all FDIC personnel, including employees and contractors, and other individuals with access to FDIC information or systems, must successfully complete FDIC training on how to identify, respond to, and report breaches. This training directs them to report a suspected or confirmed breach to the FDIC Service Desk as soon as possible and without unreasonable delay. Individuals must not wait for confirmation that a breach has in fact occurred before reporting, as such delay may undermine the FDIC's ability to apply preventative and remedial measures to protect the PII and reduce the risk of harm to potentially impacted individuals.

Individuals must report a suspected or confirmed breach regardless of whether they are in the office, teleworking, or located at any remote location, including during domestic and international travel. Individuals may call FDIC's Service Desk phone number to report a breach. FDIC requires all suspected and confirmed breaches to be reported.[9]

[8] Memorandum, Designation of FDIC Breach Response Team (September 20, 2018).
[9] FDIC Directive 1360.12, Reporting Information Security Incidents.

3.1.1 Breach Report

After a suspected breach is reported, SRT collects the fact pattern of the incident from which the Privacy Program creates a Breach Report. The Breach Report provides the factual information gathered by SRT and other stakeholders related to the suspected breach.

3.2 Breach Designation

Based on the facts available at the time of initial intake of information, the Incident Response Coordinator identifies potential incidents involving PII, and PPC makes the determination as to whether an incident involves PII. If the incident involves PII, then the PPC or designee will determine whether to process the incident as a breach that appears to meet the criteria for a major incident, a routine breach, or resolve as a non-breach. The Privacy Program tracks and documents each breach (or suspected breach) reported to the FDIC.

3.2.1 Non-breach

After a review of the facts, the PPC may decide to close the incident as a non-breach. The PPC documents this determination in FDIC's incident case management system. This may be done for a variety of reasons, such as the information does not belong to FDIC; the incident does not involve PII; the incident involves PII, but a review of the facts determines that the PII was authorized to be released; or synthetic or dummy data was mistaken for real PII.

3.2.2 Routine Breach

FDIC defines a routine breach as a breach that does not meet the definition of major incident, as defined by OMB guidance. In processing a routine breach, the PPC at their discretion may convene or consult with the Legal Division, the Office or Division whose data was impacted, and other relevant stakeholders to conduct a Risk of Harm Assessment. Section 4 addresses the methodology and process of assessing the risk of harm to individuals potentially affected by a breach. If the routine breach matches a fact pattern from a previous breach, as a matter of discretion, the PPC may process the breach following the same decision-making process as in the previous breach.

3.2.3 Major Incident

As soon as the PPC becomes aware of a breach that may constitute a major incident, the PPC notifies the SAOP or designee. The SAOP or designee, in consultation with the PPC, determines whether the breach constitutes a suspected major incident. For all suspected major incidents involving breaches, as defined by OMB, the SAOP or designee convenes the BRT. The BRT, led by the SAOP or designee, makes a recommendation to the Chairperson, the duly authorized

officer of the Board of Directors**,** whether to declare a Major Incident. The Chairperson, acting on behalf of the Board of Directors, makes all major incident declarations for FDIC.

3.3 Other Reporting Requirements

3.3.1 Major Incident Reporting Requirements

Law and OMB guidance require agencies to provide formal notifications in the event of a major incident. The table below contains a summary of FDIC's notification requirements, timelines, and the FDIC official responsible for conducting each notification for a major incident that is a breach.

NOTICE RECIPIENT	TIMEFRAME	FDIC RESPONSIBILITY
Cybersecurity Infrastructure Security Agency (CISA)	Within 1 Hour of Determining a Major Incident Has Occurred	Incident Response Coordinator
OMB Office of Federal Chief Information Officer (OFCIO)	Within 1 Hour of Determining a Major Incident Has Occurred	SAOP
FDIC OIG	No later than 7 Days After FDIC has Reasonable Basis to Determine a Major Incident Has Occurred	Incident Response Coordinator
Congress	No later than 7 Days After FDIC has Reasonable Basis to Determine a Major Incident Has Occurred, Supplement 30 Days After	Director, Office of Legislative Affairs

3.3.2 Cybersecurity and Infrastructure Security Agency

When the PPC determines that a breach has occurred, the FDIC SRT notifies CISA of a breach consistent with FDIC's Incident Response Plan and CISA's Federal Incident Notification Guidelines.[10] In addition, when FDIC determines a breach constitutes a "major incident," as defined by OMB guidance, the Incident Response Coordinator reports that designation directly to CISA within one (1) hour of determining a major incident occurred. Similarly, the Incident Response Coordinator updates CISA within one (1) hour of determining that a previously reported breach constitutes a major incident.

3.3.3 Office of Management and Budget Office of Federal Chief Information Officer

[10] Cybersecurity & Infrastructure Security Agency, CISA Federal Incident Notification Guidelines, https://www.cisa.gov/federal-incident-notification-guidelines.

When a breach has been declared a major incident, the SAOP notifies OMB OFCIO within one (1) hour of determining a major incident occurred as required by FISMA and in accordance with OMB guidance. Similarly, the SAOP updates the OMB OFCIO within one (1) hour of determining that a previously reported breach constitutes a major incident.

3.3.4 Inspector General and Law Enforcement

When responding to a breach, the Incident Response Coordinator (or designated SRT staff acting on behalf of the Incident Response Coordinator) coordinates with the SAOP (or the CISO or PPC acting on the SAOP's behalf) to ensure that OIG receives timely notification when notification is appropriate. When a breach has been declared a major incident, the Incident Response Coordinator notifies OIG no later than seven (7) days after the date on which there is a reasonable basis to conclude that a breach that constitutes a major incident has occurred.

Notification to OIG constitutes notification to law enforcement. When a breach warrants reporting to law enforcement partners, the FDIC OIG ensures that the report occurs promptly, even if the breach is unconfirmed or the circumstances are still unclear. The SAOP also considers and advises the Board of Directors, or duly authorized officers or agents, on whether the specific circumstances require the involvement of other oversight entities.

3.3.5 Congress

The Office of Legislative Affairs Director notifies appropriate congressional committees no later than seven (7) days after the date on which there is a reasonable basis to conclude that a breach that constitutes a major incident has occurred. FDIC also supplements this initial notification to Congress with pertinent updates within a reasonable period of time after additional information relating to the incident is discovered. Further, FDIC then supplements previous reports with an additional report to Congress no later than 30 days after FDIC discovers the breach. The details of each supplemental report will include all the required elements as set forth in the annual FISMA guidance memorandum issued by OMB.

3.4 Identifying Applicable Privacy Documentation

When responding to a breach, the PPC, on behalf of the SAOP, identifies all applicable privacy compliance documentation to help determine what information was potentially compromised, the population of individuals potentially affected, the purpose for which the information had originally been collected, the permitted uses and disclosures of the information, and other information that may be useful when developing the agency's response.

As part of the process, the SAOP, or the CISO or PPC acting on the SAOP's behalf, considers the following:

- Which Privacy Impact Assessment(s) (PIA), System of Records Notice(s) (SORN), and privacy notices apply to the potentially compromised information?
- If PII maintained as part of a system of records needs to be disclosed as part of the breach response, is the disclosure permissible under the Privacy Act and how will FDIC account for the disclosure?
- If additional PII is necessary to contact or verify the identity of individuals potentially affected by the breach, does that information require new or revised SORNs or PIAs?
- Are the relevant SORNs, PIAs, and privacy notices accurate and up to date?

3.5 Documentation and Information Sharing

During a breach response, there may be a need for additional information. Accordingly, FDIC may need to exchange information with other agencies or non-Federal entities.

When contemplating potential information sharing in response to a breach, the SAOP, or the CISO or PPC acting on the SAOP's behalf, considers the following:

- Would the information sharing be consistent with existing or require new data use agreements, information exchange agreements, or memoranda of understanding (MOUs)?[11]
- Whether Privacy Act information will be shared, and if so, under what authority?
- How will PII be transmitted and protected when in transmission, for how long will it be retained, and may it be shared with third parties?

3.6 Tracking and Documenting the Response to a Breach

ESOS maintains an incident case management system to track and document each breach reported to FDIC. The PPC, on behalf of the SAOP, updates this incident case management system with the status of an ongoing response and determines when the response to a breach has concluded. FDIC's process for internal tracking includes documenting the following:

- The total number of breaches reported over a given period of time;
- The status for each reported breach, including whether FDIC's response to a breach is ongoing or has concluded;
- The number of individuals potentially affected by each reported breach;
- The types of information potentially compromised by each reported breach;

[11] *See* FDIC Circular 3800.10, Memoranda of Understanding and Interagency Agreements, for information on MOUs and Interagency Agreements (IAAs) at FDIC.

- Whether FDIC, after assessing the risk of harm, provided notification to the individuals potentially affected by a breach;
- Whether FDIC, after considering how best to mitigate the identified risks, provided services to the individuals potentially affected by a breach;
- Whether the breach constituted a major incident;
- Whether a breach was reported to OIG, CISA, and Congress; and
- Key dates and times related to the items being documented.

4 ASSESSING THE RISK OF HARM

Once the PPC has confirmed that a breach has occurred, the SAOP or designee, in coordination with the BRT when applicable, conducts and documents a Risk of Harm Assessment for the purpose of determining the risk of harm to the individuals who are potentially affected by the breach. Assessing the risk of harm to individuals assists FDIC in determining whether or not to notify individuals. As part of the Risk of Harm Assessment process, FDIC will also consider any and all risks relevant to the breach, such as risks to FDIC, the Federal Government, or national security.

The Risk of Harm Assessment considers, at a minimum, the following three factors, as well as any information externally provided to FDIC (e.g., law enforcement):

1. Nature and Sensitivity of the PII potentially compromised by the breach, including the potential harms that an individual could experience from the compromise of that type of PII;

2. Likelihood of Access and Use of PII, including whether the PII was properly encrypted or rendered partially or completely inaccessible by other means; and

3. Type of Breach, including the circumstances of the breach, as well as the actors involved and their intent.

The following table lists the considerations for each factor.

RISK OF HARM ASSESSMENT FACTORS	
FACTOR	**CONSIDERATIONS**
NATURE AND SENSITIVITY OF PII	• *Data Elements,* including an analysis of the sensitivity of each individual data element as well as the sensitivity of all the data elements together • *Context,* including the purpose for which the PII was collected, maintained, and used • *Private Information,* including the extent to which the PII constitutes information that an individual would generally keep private. • *Vulnerable Populations,* including whether the potentially affected individuals are from a particularly vulnerable population that may be at greater risk of harm than the general population. • *Permanence,* including the continued relevance and utility of the PII over time and whether it is easily replaced or substituted
LIKELIHOOD OF ACCESS AND USE OF PII	• *Security Safeguards,* including whether the PII was properly encrypted or rendered partially or completely inaccessible by other means • *Format and Media,* including whether the format of the PII may make it difficult and resource-intensive to use • *Duration of Exposure,* including how long the PII was exposed • *Evidence of Misuse*, including any evidence confirming that the PII is being misused or that it was never accessed
TYPE OF BREACH	• *Intent,* including whether the PII was compromised intentionally, unintentionally, or whether the intent is unknown • *Recipient,* including whether the PII was disclosed to a known or unknown recipient, and the trustworthiness of a known recipient

4.1 Assign Risk Factor Ratings

Once FDIC reviews the risk factors associated with the breach, it then assigns a risk rating to each factor. The risk levels for each of the factors are described in the table below.

Risk Level of Identity Theft or Other Harm	Factors & Considerations		
	Nature & Sensitivity of PII *(Data Elements, Context, Private information, Permanence, and Vulnerable Population)*	***Likelihood of Access & Use of PII*** *(Security Safeguards, Format and Media, Duration of Exposure, and Evidence of Misuse)*	***Type of Breach*** *(Intent and Recipient)*
High = 3	• Social Security number (SSN), including truncated SSNs (e.g., last four digits) • Financial account information (with account access information or passwords) • Vulnerable population affected • Highly sensitive context	• PII lost was contained on storage media but was not encrypted • PII transmitted unencrypted or via a non-NIST-approved encryption method • PII in paper form was lost outside a trusted mailing facility, or was recovered with evidence of compromised packaging • Evidence information has already been misused (potential for indefinite or permanent exposure) • Potential duration of exposure is indefinite (e.g., unencrypted email through a commercial webmail provider)	• Demonstrated malicious intent or is a known malicious actor • Recipient unknown to FDIC
Moderate = 2	• Financial account information (without account access information or passwords) • Combination of private PII data elements but no SSN	• PII lost was contained on storage media, and encrypted, but not using a NIST-approved encryption method • PII transmitted via NIST-approved encrypted channels, but was viewed and downloaded • PII transmitted in paper form and lost in a trusted mailing facility • PII misdelivered in physical form, and not returned in a timely manner	• Known recipient with no facts indicating malicious intent • Incorrect recipient contacted FDIC to advise of error • Correct recipient, but potentially viewed by unauthorized parties
Low = 1	• Loan Account Number • PII data element(s) that can be easily changed • Employee ID Number	• PII lost was contained on storage media, and encrypted using a NIST-approved method • PII transmitted via NIST-approved encrypted channel, but viewed only • Breach occurred in a secure FDIC facility or remained on the FDIC network • PII contained in format and media requiring special expertise and equipment for access and use • Potential duration of exposure was insignificant (documents immediately returned or deleted)	• Disclosed to an FDIC employee, contractor, or other trusted party (e.g., unintended recipient was a bank official) on a trusted network • Disclosed to reputable but unauthorized third-party websites (e.g., leading webmail providers)

4.2 Determine Appropriate Mitigation

The output of the risk assessment is the determination whether FDIC should provide notification or other services to affected individuals, as discussed further in Section 6. If the point total is 8 or 9, notification is recommended. If the point total is 7 or below, notification is generally not recommended. When determining whether to provide notification, FDIC balances the need for transparency with concerns about over-notifying individuals, among other factors.

5 MITIGATING THE RISK OF HARM

After assessing the risk of harm to individuals potentially affected by a major incident, the SAOP or designee, in coordination with the BRT, when applicable, is responsible for advising the Board of Directors, or duly authorized officers or agents, on how to best mitigate the identified risks; whether and when to provide notification; as well as the decision of whether to take countermeasures, offer guidance, or provide services to individuals. For routine breaches, the SAOP or designee decides on the appropriate actions to mitigate the risk of harm to individuals without engaging the Board of Directors.

5.1 Countermeasures

Countermeasures may not always prevent harm to potentially affected individuals, but may limit or reduce the risk of harm. If the information is only useful in a specific context, there may be context-specific countermeasures that can be taken to limit the risk of harm. For example, if information related to corporate credit cards is potentially compromised, FDIC may consider monitoring corporate credit cards for unusual or fraudulent activity, such as a sudden request for a change of address, or reissue the corporate credit card. Similarly, if individuals' passwords are potentially compromised in a breach, FDIC may require those users to change their passwords.

5.2 Guidance

The SAOP or designee determines what guidance FDIC will provide to potentially affected individuals about how they may mitigate their own risk of harm. When choosing guidance to mitigate the risk of harm, the SAOP considers the guidance options included in Appendix II of M-17-12. Likewise, FDIC uses the information available from the Federal Trade Commission (FTC) at www.IdentityTheft.gov/databreach as the baseline when drafting guidance, particularly when a breach involves Social Security numbers (SSN), payment card information,

bank accounts, driver's licenses, children's information, and account credentials. Additionally, FDIC may advise individuals to change passwords and encourage the use of multi-factor authentication for account access, when appropriate.

5.3 Services

The SAOP determines if there are services FDIC can provide to help mitigate the risk of harm. For breaches involving the loss, theft, or disclosure of SSNs or sensitive financial information, FDIC may issue a letter or notice offering various identity theft protection or credit monitoring services. The level of protection offered should be commensurate with the type of breached data, the level of risk related to the breach, and the direct risk to the individual.

Services are not always available to mitigate the potential harms resulting from the evolving threat and risk landscape. If no service is currently available to mitigate a specific risk of harm, FDIC may choose not to provide services to the potentially affected individuals. Choosing not to provide services is a decision separate from that of providing notification; there may be circumstances in which potentially affected individuals are notified but not provided services. In accordance with OMB M-16-14, FDIC has an established process to provide an identity theft protection/credit monitoring product to potentially affected individuals if there is a risk of identity theft. The identity theft protection/credit monitoring product is paid for by FDIC at no cost to the individual. However, the individual must enroll to take advantage of the product. FDIC will continue to monitor available services and will update its procedures if additional, appropriate services become available in the future.

6 NOTIFICATION PROCESS

The Risk of Harm Assessment is used to make notification decisions. In order to make a notification recommendation, the PPC facilitates a meeting with key stakeholders including the responsible FDIC division or office, the Incident Response Coordinator, and the Legal Division. In the meeting, the parties review the facts of the breach and the PPC obtains consensus on the overall risk score. Breaches with overall risk scores of 8 or more generally require the PPC to make a notification recommendation to the SAOP. If notification is recommended, the PPC will draft the notification letter, which will be reviewed by the responsible FDIC division or office, the Legal Division, and the CISO. After obtaining consensus on the overall risk score, the PPC will make a recommendation (based on the Risk of Harm Assessment) to the SAOP, and the SAOP will determine whether to accept, modify, or reject the recommendation prior to issuing any notification.

6.1 Source of the Notification

Pursuant to the authority delegated to the SAOP by the Chairperson of the Board of Directors, the SAOP signs the notification letters sent to the individuals potentially affected by the breach.[12] When a breach involves FDIC information held by or information systems operated by a contractor or another entity on behalf of FDIC, FDIC will coordinate with the contractor/entity to ensure notification is provided and that it is appropriate and easily understandable. In cases in which a contractor/entity provides notification on behalf of FDIC, such notification shall be coordinated with, and subject to, prior written approval by the Board of Directors, or duly authorized officer or agent.

6.2 Timeliness of the Notification

FDIC provides notification to affected individuals as expeditiously as practicable without unreasonable delay. The FDIC works to avoid providing multiple notifications for a single breach and balances the timeliness of the notification with the need to gather and confirm information about a breach and assess the risk of harm to potentially affected individuals.
The Attorney General, the head of an element of the Intelligence Community, or the Secretary of the Department of Homeland Security (DHS) may delay notifying individuals potentially affected by a breach if the notification would disrupt a law enforcement investigation, endanger national security, or hamper security remediation actions.[13] Any instruction to delay notification must be sent in writing to the Board of Directors. Absent a formal, written request to delay notification in accordance with OMB Memorandum M-17-12, FDIC will, by default, provide notification.

6.3 Contents of the Notification

The notification letter must be concise, use plain language, and include:

- A brief description of what happened, including the date(s) of the breach and of its discovery;
- To the extent possible, a description of the types of PII compromised by the breach (e.g., full name, SSN, date of birth, home address, account number);
- A statement of whether the information was encrypted or protected by other means, when it is determined that disclosing such information would be beneficial to potentially affected individuals and would not compromise the security of the information system;

[12] Memorandum, Designation of Senior Agency Official for Privacy as Source of Notification Letter for Breaches (October 26, 2017).
[13] 44 U.S.C. § 3553.

- Guidance to potentially affected individuals on how they can mitigate their own risk of harm, countermeasures the FDIC is taking, and services the FDIC is providing to potentially affected individuals, if any;
- Steps the FDIC is taking, if any, to investigate the breach, mitigate losses, and protect against a future breach; and
- Who potentially affected individuals should contact at the FDIC for more information, including a telephone number (preferably toll-free), email address, or postal address.

Given the amount of information required in a notification, additional details may be made available to affected individuals via a set of Frequently Asked Questions (FAQs).

6.4 Method of Notification

The SAOP will select the method for providing notification in accordance with M-17-12, which should be commensurate with the number of individuals or entities affected, the contact information available about those affected, and the urgency with which they need to receive notification.

6.5 Special Considerations

When a breach potentially affects a vulnerable population, FDIC may need to provide a different type of notification to that population, or provide a notification that would not otherwise be necessary. For example, when the individual whose information was potentially compromised is a child, FDIC may provide notification to the child's parent or legal guardian(s). In addition, if FDIC becomes aware an individual is visually or hearing impaired, FDIC will give special consideration to providing notice to those individuals consistent with Section 508 of the Rehabilitation Act of 1973, as amended.[14]

7 TRACKING AND DOCUMENTING

At the end of each annual FISMA reporting period, the SAOP shall review the reports detailing the status of each breach reported during the fiscal year and consider whether FDIC should undertake any of the following actions:

- Update its breach response plan;
- Develop and implement new policies to protect the agency's PII holdings;
- Revise existing policies to protect the agency's PII holdings;
- Reinforce or improve training and awareness;
- Modify information sharing arrangements; and

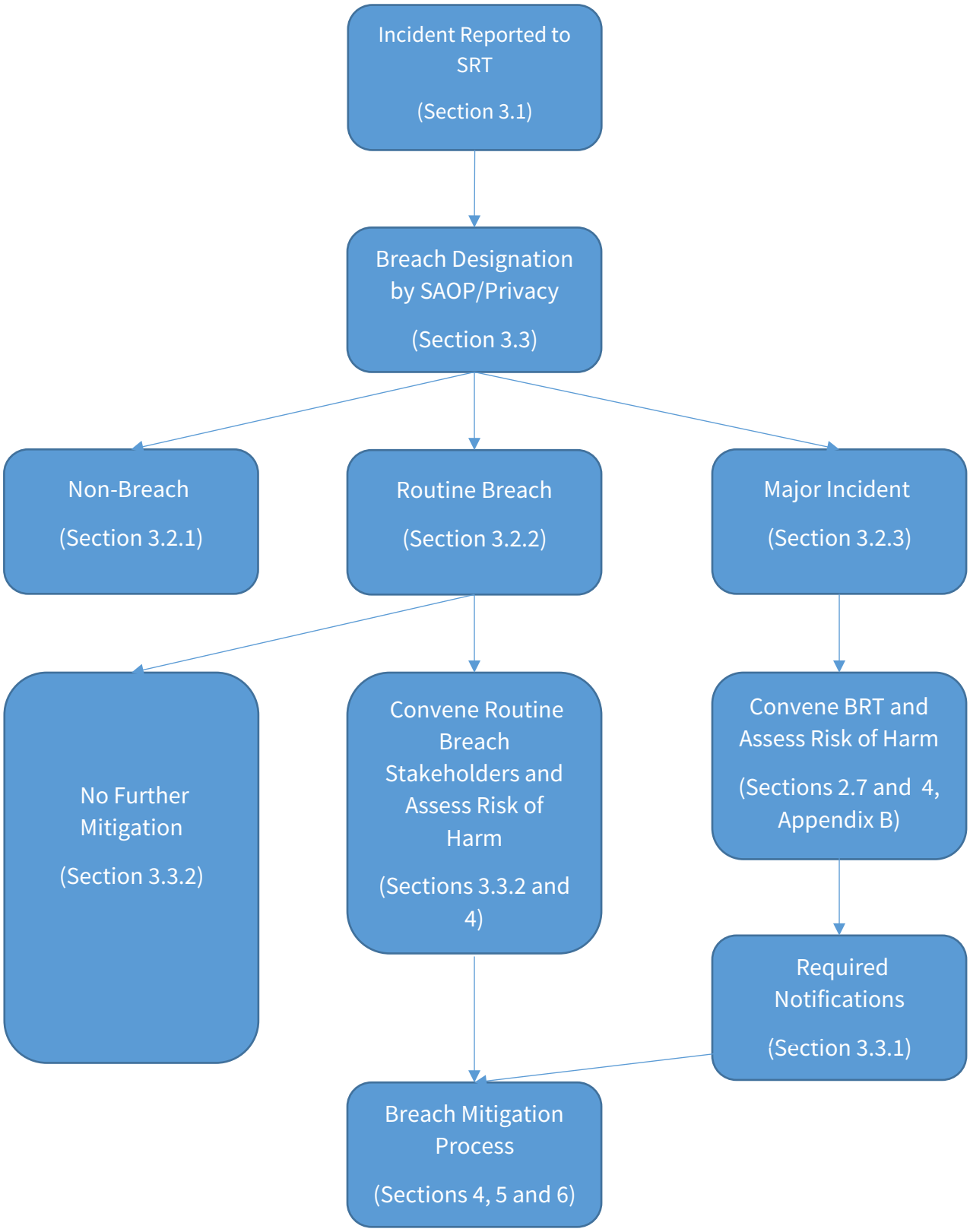
[14] 29 U.S.C. § 794(d); for additional information about accessibility aids, *see* www.section508.gov.

- Develop or revise documentation such as SORNs, PIAs, or privacy policies.

After the FDIC reports a major incident that is a breach in accordance with Section 3.2.3, the SAOP will convene the FDIC BRT to formally review the agency's response to the breach and identify any lessons learned. The FDIC will use lessons learned to implement specific, preventative actions, and will document any resulting changes to its breach response plan, policies, training, or other documentation. If there are specific challenges preventing FDIC from instituting remedial measures, FDIC will also document those challenges.

The SAOP will hold a breach tabletop exercise annually to test the FDIC's ability to respond to breaches and ensure each member of the BRT understands their role. Any lessons learned from the exercise will be appropriately documented. For any year in which the SAOP convened the FDIC BRT to consider whether a breach that constitutes a major incident has occurred, the annual exercise is not required.

Appendix A: Breach Response Process Flow



Appendix B: Breach Response Team (BRT) Membership Roles and Responsibilities

BRT Core Membership

Roles	Responsibilities
Chief Information Officer (CIO)	The Chief Information Officer (CIO) is primarily responsible for FDIC's privacy and data protection policies as well as delivering core FDIC IT services. The CIO will assist with the assessment of risk of harm to potentially affected individuals in the event of a breach.
Senior Agency Official for Privacy (SAOP)	The SAOP has agency-wide responsibility and accountability for the FDIC's privacy program and is responsible for overseeing, coordinating and facilitating the FDIC's privacy compliance efforts. In the event of a breach that constitutes a major incident, the SAOP, or designee, is responsible for convening the BRT; serving as or designating, the BRT lead; providing the BRT's recommendation to the Board of Directors, or duly authorized officers or agents; coordinating with internal and external officials; and serving as the source of notification when required. The SAOP is also responsible for conducting a breach risk of harm assessment, consulting with CISO and other technical experts, overseeing the notification effort, recommending the course of action to mitigate the harm, and conducting the post-breach analysis of lessons learned for congressionally-reported breaches. In addition, the SAOP, or the CISO or PPC acting on her behalf, is responsible for convening the BRT to hold annual tabletop exercises, review of the Plan and related privacy policies, and ensuring compliance with all privacy documentation and FISMA reporting.
Chief Operating Officer (COO)	In the event of a major incident, the Chief Operating Officer (COO) is responsible for serving as a special advisor to the Chairperson regarding incident and breach-related activities and courses of action that impact the functional areas of the Corporation under the COO's span of responsibility. The COO is also responsible for assisting with the review of congressional, OMB OFCIO, and OIG notifications, as appropriate, for major incidents.

Chief of Staff (COS)	In the event of a major incident, the COS is responsible for serving as a special advisor to the Chairperson regarding incident and breach-related activities and courses of action that impact the functional areas of the Corporation under the COS' span of responsibility. The COS is also responsible for assisting with the review of Congressional and OIG notifications, as appropriate, for major incidents and breaches.
Chief Information Security Officer (CISO)	The CISO serves as the designated senior agency information security officer, responsible for developing and maintaining FDIC's information security and privacy programs.
Incident Response Coordinator	The Incident Response Coordinator is an FDIC employee under ESOS, who is assigned to ensure that Privacy is made aware in a timely manner of suspected or confirmed breaches, as well as appropriately managing these breaches to closure. The Incident Response Coordinator is also responsible for notifying CISA and the OMB OFCIO when there is a major incident that is a breach.
Privacy Program Chief	The Privacy Program Chief (PPC) is responsible for advising the SAOP and CISO in the development, daily operation, and management of the FDIC Privacy Program. In the event of a breach, the PPC assists the SAOP and CISO in fulfilling their breach-related responsibilities outlined in OMB M-17-12.
General Counsel	The Legal Division's General Counsel is responsible for ensuring a Corporate response plan is successfully executed in compliance with federal laws and regulations. In the event of a breach, the General Counsel helps draft and review breach notification, guidance, and communications (e.g., talking points, FAQs, call scripts, website content), as well as responses to FOIA, Privacy Act, congressional or other breach-related inquiries and complaints received by FDIC.
FDIC Office of Legislative Affairs Director (OLA)	OLA serves as the Corporation's congressional liaison and closely monitors and responds to legislation important to FDIC. The OLA Director is responsible for serving as a central POC in notifying applicable committees and Members of Congress about major incidents and breaches, as well as in responding to requests from various congressional committees, members, or their staff about the incident or breach.

FDIC Office of Communications Director (OCOM)	The OCOM Director is responsible for developing and executing a Corporate-wide communications plan for breaches as directed by the Board of Directors, or duly authorized officers or agents. OCOM helps draft external notification and communications (e.g., call center scripts, talking points, FAQs, and official responses to breach-related inquiries and complaints), establishes and maintains a dedicated FDIC-branded webpage to provide breach-related guidance, and responds to media inquiries, initiating and organizing any press release about the breach, if required.
Deputy to the Chairperson for External Affairs (DCEA)	In the event of a major incident, the DCEA is responsible for serving as an advisor to the Chairperson regarding FDIC incident- or breach-related communications and ensuring the coordination of efforts, as appropriate, between the Office of Communications, the Office of Legislative Affairs and the External Ombudsman. The DCEA is also responsible for assisting with the review of congressional, OMB OFCIO, and OIG notifications, as appropriate for breaches that constitute major incidents.