FEDERAL DEPOSIT INSURANCE CORPORATION

INSURING AMERICA'S FUTURE

Breach Response Plan

(BRP)

Version 2.6

April 26, 2018

Contents

REVISION HISTORY

Revision History		
Version Number	**Date**	**Change Description**
1.0	12/18/2013	Initial Issue. Consolidated and superseded FDIC's Procedures for Responding to a Breach of Personally Identifiable Information and Procedures for Responding to a Breach of Sensitive Information.
1.1	07/29/2014	Inserted URL to Critical Sensitive Information Inventory. Updated Incident Risk Analysis (IRA) template to match current version in circulation. Clarified definition of an incident and existing procedures for incident closure, IRA completion, and OIG involvement. Updated reference to Chief Information Officer Organization (CIOO) to reflect organization name change.
1.2	08/15/2014	Updated Divisional Incident Response (IR) Points of Contacts (POCs) list to reflect organizational changes.
1.3	12/29/2014	Updated Divisional Incident Response (IR) Points of Contacts (POCs) to reflect organizational changes.
1.4	04/16/2015	Updated URL for Critical Sensitive Information Inventory. Inserted URLs for updated Divisional IR POC listing and downloadable version of IRA template.
1.5	11/09/2015	Updated procedures resulting from a 2013 ISPS Cybersecurity Incident Response facilitated exercise/discussion.
1.6	12/23/2015	Updated procedures to address Office of Management and Budget (OMB) Memorandum M-16-03, Fiscal Year 2015-2016 Guidance on Federal Information Security and Privacy Management Requirements (issued on 10/30/2015).
1.4	02/08/2016	Rescinded versions 1.5 and 1.6 and reissued version 1.4.
1.5	6/06/2016	References added to FISMA 2014, and to OMB M-16-03, Fiscal Year 2015-2016 Guidance on Federal Information Security and Privacy Management Requirements (issued on 10/30/2015). Purpose is to ensure reader is aware of the relevant new requirements while more substantive changes are completed.
2.0	4/07/2017	Reissued as the Breach Response Plan. Clarified definition of when an actual or suspected data breach incident is considered "Major" under OMB M-17-05. Updated to include additional references to Major Incident requirements, where applicable. Added links in a new appendix; deleted the following appendices: Former Appendix B, Critical Agency Sensitive Information Inventory; Appendix C, 'InfoAlert Distribution List'; Appendix F, Incident Prevention/Preparation Supplemental Guidance; Appendix D, Divisional Incident Response (IR) POCS; Appendix G, General Guidance for the Use of FDIC Call Center; Appendix H, Sample Written Notification; Appendix L, Legal Authorities and References; Appendix M, When Is an Incident a Major Incident?; Appendix P, Divisional Data Breach Management Team Members; Appendix Q, Division Incident Response Guidelines.
2.1	10/25/2017	Updated to align with OMB M-17-12, Preparing for and Responding to a Breach of Personally Identifiable Information, and OMB M-18-02, Fiscal Year 2017-2018 Guidance on Federal Information Security and Privacy Management Requirements (which rescinded OMB M-17-05). Changed references from "Information Security and Privacy Staff (ISPS)" to "Office of the Chief Information Security Officer (OCISO)" per reorganization.
2.2	03/09/2018	Updated to include Appendix M: Executive Summary Template.
2.3	03/15/2018	Updated to move previous footnote 26 to become new footnote 24.
2.4	03/27/2018	Updated Appendix M: Executive Summary Template instructions.
2.5	04/13/2018	Added the following sentence to Section 3.2.3 "Reporting to Congress": "The FDIC will,

		as appropriate, supplement the initial Congressional notification and 30-day report with pertinent updates through the closure of the breach."
2.6	04/26/2018	Added the Chief Operating Officer (COO) to the BRT membership to address Office of Inspector General (OIG) audit finding. Inserted provision for delegating BRT responsibilities, and changed references from "Privacy Program Manager (PPM)" to "Privacy Section Chief (PSC)" per Chairman's Designation memo. Added reference to FDIC Emergency Notification System as an option to facilitate convening the BRT in the event normal communication channels are not available.

EXECUTIVE SUMMARY

Protecting personally identifiable information (PII) is critically important to the Federal Deposit Insurance Corporation (FDIC). This Breach Response Plan ("BRP" or "Plan") provides guidance to the Corporation on how to respond to breaches involving PII. This Plan is a subcomponent of the Chief Information Officer Organization's (CIOO) overall Incident Response Plan. This Plan supersedes the Breach Response Plan, Version 2.5, dated April 13, 2018.

This document provides the definition of a breach, as well as the criteria for assessing and mitigating the risk of harm to potentially impacted individuals, in accordance with guidance provided by the Office of Management and Budget.[1] In addition, this Plan establishes and designates the members of the Breach Response Team, as well as specifies the roles and responsibilities of employees, contractors and other personnel for reporting breaches of PII.

[1] *See* OMB M-17-12, *Preparing for and Responding to the Breach of Personally Identifiable Information* (OMB, January 2017).

1 INTRODUCTION

1.1 Background

In fulfilling its mission, the Federal Deposit Insurance Corporation (FDIC) collects and maintains personally identifiable information (PII) about customers, employees, officers and directors of financial institutions, as well as about FDIC personnel and visitors. Under Federal law and policy, the FDIC is responsible for protecting this PII from loss, theft or compromise ("breach"). Failure to adequately protect this PII, as well as to report a breach in a timely manner, could cause significant financial, reputation, or other harm to individuals, the Corporation, or other affected stakeholders.

In today's rapidly evolving threat and risk landscape, Federal information and information systems are increasingly the targets of sophisticated attacks by actors who want to use PII for malicious purposes. The FDIC must ensure it is prepared for and understands how to effectively respond to evolving threats to information and information security. An effective and expeditious response to a breach is critical to the FDIC's efforts to minimize any harm to potentially affected individuals and to maintain the public's trust in the ability of FDIC to safeguard PII.

1.2 Purpose

The FDIC's Breach Response Plan (BRP) sets forth the policy and procedures to prepare for and respond to a breach of PII. It establishes and designates the members of the Breach Response Team, as well as includes the organizational framework for assessing and mitigating the risk of harm to individuals potentially affected by a breach, and provides guidance on whether and how to provide notification and services to those individuals. The purpose of this Plan is to ensure that FDIC responds in a timely, consistent, and appropriate manner to suspected and confirmed breaches, in order to protect FDIC information and assets and to minimize harm to individuals and entities that may be affected by the breach. The BRP is also intended to promote consistency in the way FDIC prepares for and responds to a breach by requiring baseline requirements and procedures.

1.3 Authorities, Scope and Definitions

The BRP is a subcomponent of the FDIC Chief Information Officer Organization's (CIOO) overall Incident Response Plan, and was developed pursuant to Office of Management and Budget (OMB) M-17-12, *Preparing for and Responding to the Breach of Personally Identifiable Information*, and other applicable law and policy. The Plan applies to a breach of FDIC PII in any format (electronic, paper or verbal) as defined below. It does not address incidents involving the loss of classified or agency/business sensitive information (BSI)[2] or

[2] See glossary in Appendix A.

incidents where the FDIC has lost the ability to provide any critical service to system users (matters involving the loss or outage involving a critical system will be referred to FDIC Security Operations Center [SOC] and handled in accordance with the FDIC Cyber Threat and Incident Escalation Guide). Matters involving the loss of Classified National Security Information should be referred to the FDIC Federal Senior Intelligence Coordinator (FSIC) and the FDIC Special Security Officer. Incidents involving the loss or compromise of agency or business sensitive information (BSI) should be handled in accordance with the overarching Incident Response Plan. Incidents involving a combination of both BSI and PII should be handled according to the FDIC Incident Response Plan, with this BRP folding into that overarching process. However, where an incident involves one or more of the aforementioned events and a breach of PII, this Plan will be enacted for the breach portion of the event(s). All FDIC users[3] or other individuals with access to FDIC information and/or information systems must abide by the provisions outlined in this BRP.

KEY DEFINITIONS	
Personally Identifiable Information (PII)	The term PII refers to information that can be used to distinguish or trace an individual's identity, either alone or when combined with other information that is linked or linkable to a specific individual. Because there are many different types of information that can be used to distinguish or trace an individual's identity, the term PII is necessarily broad. To determine whether information is PII, the FDIC shall perform an assessment of the specific risk that an individual can be identified using the information with other information that is linked or linkable to the individual. In performing this assessment, it is important to recognize that information that is not PII can become PII whenever additional information becomes available — in any medium or from any source — that would make it possible to identify an individual.[4]
Incident	An incident[5] refers to an 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. [For purposes of the internal reporting requirements described in this document, an "incident" includes all suspected or known (confirmed) breaches.]
Breach	A breach[6] refers to the 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 personally identifiable information for an other than authorized purpose.
Breach that Constitutes a "Major Incident"	A breach constitutes a "major incident"[7] when it involves PII that, if exfiltrated, modified, deleted, or otherwise compromised, is likely to result in demonstrable harm to the national security interests, foreign relations, or economy of the United States, or to the public confidence, civil liberties, or public health and safety of the American people. An unauthorized modification of, unauthorized deletion of, unauthorized exfiltration of, or unauthorized access to 100,000 or more individuals' PII constitutes a "major incident."

1.3.1 Division-Specific Breach Response Plans

FDIC Divisions must implement and adhere to these BRP provisions, but may develop and implement supplemental, Division-specific breach plans and procedures, so long as they are not less restrictive than and comply with this document. Divisions must review

[3] *See* glossary in Appendix A.
[4] *See* OMB Circular No. A-130, *Managing Information as a Strategic Resource* (OMB, July 2016).
[5] *See* Federal Information Security Modernization Act (FISMA) of 2014.
[6] *See* OMB M-17-12, *Preparing for and Responding to the Breach of Personally Identifiable Information* p. 47 (OMB, January 2017).
[7] *Ibid*.

their plans no less than annually, update them if necessary, and ensure the date of the review is properly documented in their respective plans. As required by OMB M-17-12, any new or substantially revised Divisional plans must be reviewed by the Senior Agency Official for Privacy (SAOP) prior to implementation to ensure consistency with the requirements of the FDIC's BRP, Incident Response Plan, OMB guidance, and applicable law. Divisions should submit their new or substantially revised plans to the FDIC Office of the Chief Information Security Officer (OCISO) for SAOP review at least sixty (60) days prior to the planned date of implementation. New or substantially revised Divisional Breach Response Plans requiring SAOP review should be submitted via email to OCISO Privacy Program Staff at privacy@fdic.gov. Divisions requiring an expedited review or exception to the sixty (60) day timeframe should submit a justification request to privacy@fdic.gov. The Privacy Section Chief (PSC) will review and approve/reject exceptions to the sixty (60) day timeframe.

1.3.2 Elements of Breach Response Plan

The FDIC Breach Response Plan contains the following elements in accordance with Office of Management and Budget (OMB) M-17-12, *Preparing for and Responding to a Breach of Personally Identifiable Information*:[8]

Element	Description	Section
Breach Response Team	Specific FDIC officials who comprise the breach response team, as well as their respective roles and responsibilities when responding to a breach	5
Identifying Applicable Privacy Compliance Documentation	Responsibility to identify any applicable Privacy Act system of records notices (SORNs), privacy impact assessments (PIAs), and privacy notices that may apply to the potentially compromised information	2.3.2
Information Sharing to Respond to a Breach	Potential information sharing within the FDIC, between agencies, or with a non-Federal entity that may arise following a breach to reconcile or eliminate duplicate records, to identify potentially affected individuals, or to obtain contact information to notify potentially affected individuals	2.3
Reporting Requirements	Internal requirements for reporting a breach to FDIC's Security Operations Center (SOC) and the requirements and specific FDIC officials responsible for reporting a breach externally to United States Computer Emergency Readiness Team (US-CERT), law enforcement and oversight entities, and Congress and OIG, when appropriate	3
Assessing the Risk of Harm to Individuals Potentially Affected by a Breach	Factors to consider when assessing the risk of harm to potentially affected individuals.	6
Mitigating the Risk of Harm to Individuals Potentially Affected by a Breach	Whether the FDIC should provide guidance, identity protection, credit monitoring, and/or other services to potentially affected individuals, and what the methods are for acquiring such services	10
Notifying Individuals Potentially Affected by a Breach	If, when, and how to provide notification to potentially affected individuals and other relevant entities	11

[8] *See* OMB M-17-12, *Preparing for and Responding to the Breach of Personally Identifiable Information* (OMB, January 2017).

1.4 Senior Agency Official for Privacy

The head of each agency is required to designate a Senior Agency Official for Privacy (SAOP)[9] who 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.[10] OMB M-17-12 charges the SAOP with, among other things, primary responsibility for developing and implementing the agency's breach response plan, including the policies and procedures for reporting, investigating, and managing a breach of PII. When a breach constitutes a "major incident" or is otherwise designated significant, the SAOP is responsible for chairing the Breach Response Team and appropriately responding to the breach. Within the FDIC, the Chief Information Officer (CIO) has been designated to serve as the SAOP, also referred to as the Chief Privacy Officer (CPO). The FDIC's Chief Information Security Officer (CISO) serves as the Deputy CPO.

1.5 Privacy Section Chief

The Privacy Section Chief (PSC) is responsible for advising the SAOP/CPO and CISO/Deputy CPO in the development, daily operation, and management of the FDIC Privacy Program. In the event of a breach, the PSC shall assist the SAOP/CPO and CISO/Deputy CPO in fulfilling their breach-related responsibilities outlined in OMB M-17-12. Specifically, the PSC shall provide guidance to the Division/Office in assessing the potential risk of harm to individuals, and advise the SAOP and BRT when convened, in coordination with the CISO, on whether notification should be provided to individuals potentially affected by a breach. When the breach is designated as routine (non-significant), the PSC manages the breach to closure. When notification is determined necessary, the PSC will select the method of notification and oversee the notification process on behalf of the SAOP and in coordination with the relevant Division/Office. The PSC shall also assist the SAOP/CPO in reviewing Divisional BRPs and overseeing updates that need to be made to this BRP at least annually. Refer to Appendix C for a complete listing of PSC and other key stakeholders' roles and responsibilities.

2 BREACH PREPARATION AND TRAINING

2.1 Training and Awareness

The FDIC has developed training for all individuals with access to the FDIC's information and information systems on how to identify and respond to a breach, including the internal process at the FDIC for reporting a breach. Training on how to identify, report, and respond

[9] *See* OMB M-16-24, *Role and Designation of Senior Agency Officials for Privacy* (OMB, September 2016).
[10] *See* OMB Circular No. A-130, *Managing Information as a Strategic Resource* (OMB, July 2016).

to a breach is a part of the FDIC's mandatory annual Corporate Information Security and Privacy Awareness training, and also is required prior to any individual accessing Federal information or information systems, including individuals with temporary access such as detailees, contractors, grantees, volunteers, and interns. The training emphasizes the individual's obligation to report not only a confirmed breach, but also a suspected breach, involving information in any medium or form, including paper, electronic, or verbal. In addition to mandatory annual training, FDIC users who have access to or responsibility for High Value Assets (HVAs)[11] containing PII must complete specialized, role-based training that addresses their specific roles and responsibilities for protecting FDIC information and reporting a breach. Targeted, role-based training is also available for those involved in the breach response process. Additionally, FDIC promotes awareness throughout the year, such as by sending periodic email reminders and conducting awareness campaigns.

The SAOP shall ensure that employees and contractors staffing the FDIC SOC and Division of Information Technology (DIT) are properly trained to identify a potential breach and that they understand their responsibilities for escalating a reported breach to the PSC, SAOP, and other appropriate officials.

2.2 Disciplinary Action

FDIC personnel may be subject to disciplinary action for failure to follow FDIC policies related to protection of FDIC Information. Some of the situations for which individuals may be subject to disciplinary action include:

- Unauthorized removal, emailing, sending, disclosing of PII, sensitive, or confidential FDIC information;
- Failure to safeguard PII, sensitive, or confidential FDIC information;
- Accessing/attempting to access PII, sensitive or confidential FDIC information without authorization;
- Using authorized access to PII, sensitive, confidential FDIC information for unauthorized purposes;
- Failure to report violations of data protection rules; and
- Failure to cooperate in FDIC's efforts to remediate effects of violations.

Refer to the LERS Table of Expected Consequences for Violations of FDIC Policies Related to Protection of FDIC Data for more information about the expected consequences for violations of FDIC policies related to the protection of FDIC sensitive information, including PII.

[11] *See* OMB Memorandum M-17-09, *Management of Federal High Value Assets* (OMB, December 2016).

2.3 Documentation and Information Sharing

When responding to a breach, there is often a need for additional information to reconcile or eliminate duplicate records, identify potentially affected individuals, or obtain contact information in order to provide notification. Accordingly, the FDIC may need to combine information maintained in different information systems within the FDIC, share information between agencies, or share information with a non-Federal entity.

In accordance with M-17-12, the SAOP will contemplate the potential information sharing that may be required in response to a breach and address the following, in addition to considerations in the previous section:

- Would the information sharing be consistent with existing or require new data use agreements, information exchange agreements, or memoranda of understanding (MOUs)?[12]
- 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?

To assist the SAOP with this responsibility, the Divisional Information Security Manager or designated Incident Lead, in coordination with the Privacy Section Chief and Legal (FOIA/Privacy Act Group),[13] shall identify and document in CORSICA a preliminary analysis of any relevant data use agreements, MOUs, and information exchange agreements, including a recommendation to address the aforementioned questions. Appendix E provides a template for guiding and documenting this analysis.

2.3.1 Privacy Act Routine Uses Required to Respond to a Breach

OMB M-17-12 requires the SAOP to ensure that all agency Privacy Act system of records notices (SORNs) include routine uses for the disclosure of information necessary to respond to a breach either of the agency's PII or, as appropriate, to assist another agency in its response to a breach.[14] The following routine use will be incorporated in FDIC SORNs:

To appropriate agencies, entities, and persons when (1) FDIC suspects or has confirmed that there has been a breach of the system of records; (2) FDIC has determined that as a result of

[12] Refer to FDIC Circular 3800.10, *Memoranda of Understanding and Interagency Agreements*, for information on MOUs and Interagency Agreements (IAAs) at FDIC.
[13] efoia@fdic.gov
[14] 5 U.S.C. § 552a(b)(3). The publication of appropriate routine uses is required under the Privacy Act and thus would be necessary in order to disclose information for the purpose of executing the FDIC's obligations to effectively manage and report a breach under FISMA. Disclosures pursuant to a routine use are permissive, not mandatory. *See* Privacy Act Implementation: Guidelines and Responsibilities, 40 Fed. Reg. 28,948 (July 9, 1975), *available at* http://www.whitehouse.gov/sites/default/files/omb/assets/omb/inforeg/implementation_guidelines.pdf.

the suspected or confirmed breach there is a risk of harm to individuals, the FDIC (including its information systems, programs and operations), the Federal Government, or national security; and (3) the disclosure made to such agencies, entities, and persons is reasonably necessary to assist in connection with FDIC's efforts to respond to the suspected or confirmed breach or to prevent, minimize, or remedy such harm.

Additionally, the FDIC may have information in its systems of records (SORs) that could assist another agency in its efforts to respond to a breach, such as records that would assist another agency in locating or contacting individuals potentially affected by a breach. To ensure that the FDIC is able to disclose information in its systems of records that may reasonably be needed by another agency in responding to a breach, the SAOP will incorporate the following routine use into each of the FDIC's SORNs as appropriate:

To another Federal agency or Federal entity, when information from this system of records is reasonably necessary to assist the recipient agency or entity in: (1) responding to a suspected or confirmed breach; or (2) preventing, minimizing, or remedying the risk of harm to individuals, the agency (including its information systems, programs and operations), the Federal Government, or national security.

2.3.2 Identifying Applicable Privacy Documentation

When responding to a breach, OMB M-17-12 requires the SAOP to identify all applicable privacy compliance documentation. This information will help identify 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.

For breaches affecting FDIC systems/applications or systems of records (SORs), the Divisional Information Security Manager (ISM) or designated Incident Lead will collaborate with the Incident Coordinator and the Privacy Section Chief to annotate the incident record in CORSICA to address the following as applicable:

- Which PIAs, SORNs, and privacy notices apply to the potentially compromised information?
- If PII maintained as part of a Division's SOR needs to be disclosed as part of the breach response, is the disclosure permissible under the Privacy Act and how will the agency 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?

2.4 Contractors

OMB M-17-12 requires agencies to ensure contract terms necessary for the agency to respond to a breach are included in contracts when a contractor collects or maintains Federal information on behalf of the agency or uses or operates an information system on behalf of the agency. To the extent that a cooperative agreement or other such instrument requires another organization or entity to perform such functions on behalf of the agency, such terms should be included. The FDIC's Chief Acquisition Officer (CAO), in coordination with the SAOP, will ensure that contract provisions to assist with the response to a breach are uniform and consistently included in FDIC contracts. In addition, the SAOP and CIO will ensure that the FDIC's BRP and system security authorization documentation clearly define the roles and responsibilities of contractors that operate Federal information systems that create, collect, use, process, store, maintain, disseminate, disclose, or dispose of PII on behalf of the FDIC. Any such roles and responsibilities should be further defined in the contract so as to ensure contractor compliance with FDIC requirements.

As necessary, the FDIC may require a contractor to notify individuals potentially affected by a breach.[15] The FDIC may also require the contractor to take countermeasures to mitigate the risk of harm to potentially affected individuals and/or to protect PII on behalf of the FDIC, such as operating call centers and providing resources for potentially affected individuals. The FDIC shall ensure that any required countermeasures are consistent with OMB Memorandum M-16-14,[16] which, except under limited circumstances, requires the use of General Services Administration's (GSA's) identity protection services (IPS) blanket purchase agreements (BPAs). GSA has awarded government-wide Federal Supply Schedule BPAs for identity monitoring, credit monitoring, and other related services. These BPAs, the requirements for which were developed jointly with officials from the Office of Personnel Management, the Department of Defense, and other agencies, give Federal agencies access to a vetted pool of well-qualified contractors capable of providing the comprehensive services needed to mitigate the risk of harm to individuals potentially affected by a breach, as well as other personnel security matters.

2.5 Identifying Logistical and Technical Support to Respond to a Breach

Logistical and technical support is often essential to effectively and efficiently respond to a breach. For example, logistical support may be required to prepare and deliver notification and to staff call centers, and technical support is often required to confirm which PII in a given IT system or on a particular device was exposed, accessed, or removed. When a

[15] *See* Section 11 of this Plan for more information on providing notification to potentially affected individuals.
[16] *See* OMB M-16-14, *Category Management Policy 16-2: Providing Comprehensive Identity Protection Services, Identity Monitoring, and Data Breach Response* (OMB, July 2016).

breach potentially affects a large number of individuals or implicates multiple IT systems, this can be a resource-intensive and challenging undertaking.

In accordance with OMB M-17-12, the CIO is responsible for identifying technical support to respond to a breach, including technical remediation and forensic analysis capabilities that exist within the FDIC and which Divisions/Offices are responsible for maintaining those capabilities. Likewise, the SAOP and/or designees (CISO and PSC) are responsible for identifying sufficient logistical support to respond to a breach, including all resource-intensive activities outlined in Appendix K, and considering what capabilities exist within the FDIC, which Divisions/Offices are responsible for executing those capabilities, and whether additional internal and/or external support is needed to effectively and efficiently respond to the breach. In identifying logistical support, the SAOP and/or designees should coordinate closely with the Breach Response Team when applicable and the relevant Division/Office. When a breach involves and/or is caused by a contractor, the Division (via the ISM, Incident Lead or other SME designated by the Division) should coordinate with the Contracting Officer (CO) and Oversight Manager (OM) as appropriate, in consultation with the PSC, Legal, and the BRT (when convened), to discuss and determine the source, issuance and costs associated with providing notification and services to individuals potentially affected by the breach.

As a part of this process, however, the CIO and SAOP (or designees) may identify gaps in the FDIC's technical and/or logistical capabilities and therefore should communicate with the Chief Acquisition Officer (CAO) and other FDIC officials on the need to enter into contracts or to explore other options for ensuring that certain functions are immediately available during a time-sensitive response. Additionally, while the SAOP might not lead the technical team, the SAOP should understand the ability of the FDIC to gather, analyze, and preserve the evidence necessary to support an investigation and identify and assess the risk of harm to potentially affected individuals.

The CIO, in coordination with the SAOP and/or designees, should also consider whether other Federal agencies can support the FDIC in the event of a breach. For example, the FDIC may request technical assistance from US-CERT. In addition, GSA may have BPAs and other guidance for the FDIC to procure technical services to assist with responding to a breach.[17] These issues should be discussed at the initial stages of the breach investigation to ensure the appropriate logistical and technical support is available to effectively and efficiently respond to a breach.

[17] GSA Highly Adaptive Cybersecurity Services (HACS) Special Item Number (SIN) includes 132-45B: Incident Response services help organizations impacted by a cybersecurity compromise determine the extent of the incident, remove the adversary from their IT systems, and restore their networks to a more secure state.

3 REPORTING A SUSPECTED OR CONFIRMED BREACH

3.1 Internal Reporting Requirements

Pursuant to FDIC internal policy,[18] all FDIC personnel, including employees and contractors,[19] and other individuals or entities[20] with access to FDIC information and/or information systems must report a suspected or confirmed breach to the FDIC immediately. This includes a breach in any medium or form, including paper, verbal, and electronic. 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. In order to make it easy for individuals to report a suspected or confirmed breach quickly, the FDIC has established a memorable phone number (1-877-FDIC-999) for reporting breaches to the FDIC Help Desk/SOC.

3.2 External Reporting Requirements

3.2.1 Reporting to US-CERT

FDIC SOC is required to report breaches to the Department of Homeland Security (DHS) United States Computer Emergency Readiness Team (US-CERT) within one hour of identification.[21] US-CERT may help the FDIC assess the circumstances that contributed to the breach and take corrective actions or technical remediation within its scope. However, it is ultimately the FDIC's responsibility to respond to the breach, including full logistical and technical remediation and forensic analysis.

Within one hour of receiving the FDIC's report, the National Cybersecurity and Communications Integration Center (NCCIC)/US-CERT will provide FDIC SOC with a risk rating based on the NCCIC Cyber Incident Scoring System (NCISS). In cases where US-CERT does not provide a risk rating to FDIC, FDIC SOC shall generate a risk rating using the NCISS scoring tool. The contents of FDIC's notification to US-CERT, the NCISS rating, and any additional pertinent information provided to and/or from US-CERT in relation to the incident shall be recorded and maintained in CORSICA by FDIC SOC and included in the Breach Report.

---

[18] *See* FDIC Circular 1360.9, *Protecting Sensitive Information*, and FDIC Circular 1360.12, *Reporting Computer Security Incidents*.

[19] The term "contractor" refers to an individual, corporation, partnership, joint-venture, or other third party entity that enters into a contract with FDIC to provide goods or services. This term is inclusive of contractors, vendors and outsourced service providers.

[20] FDIC employees, contractors, vendors, outsourced service providers, and other persons or entities that handle or otherwise have access to FDIC information or information systems in support of the FDIC's mission or for other FDIC authorized purposes. (Handling includes but is not limited to collecting, receiving, transmitting, processing, using, maintaining, storing or disposing of FDIC information.)

[21] *See* FDIC Circular 1360.9, *Protecting Sensitive Information*; OMB Memorandum M-15-01, *Fiscal Year 2014-2015 Guidance on Improving Federal Information Security and Privacy Management Practices* (October 2014); and *US-CERT Federal Incident Notification Guidelines*, UNITED STATES COMPUTER EMERGENCY READINESS TEAM.

If FDIC determines the breach constitutes a "major incident"[22] pursuant to Section 4.1.2 of this Plan, FDIC SOC will immediately notify and update its initial report to US-CERT.

3.2.2 Reporting to Law Enforcement, the Inspector General, and General Counsel[23]

The FDIC Incident Coordinator (or designated FDIC SOC representative) is responsible for notifying and consulting with the Office of Inspector General (OIG) and General Counsel or designee within the Legal Division on behalf of the FDIC when warranted. When responding to a breach, the Incident Coordinator shall coordinate with the SAOP or designees (CISO and PSC) as needed to ensure that law enforcement, Office of Inspector General (OIG), and General Counsel or designee receive timely notification when notification is appropriate. The Incident Coordinator, in consultation with the SAOP or designees and General Counsel or designee as needed, shall also consider and advise appropriate officials on whether the specific circumstances and type of PII potentially compromised by a breach require the involvement of other oversight entities.

When a breach warrants reporting to law enforcement, the FDIC shall ensure the report occurs promptly, even if the breach is unconfirmed or the circumstances are still unclear. Prompt referral to law enforcement can prevent PII from being further compromised and in some cases can reduce the risk of harm to potentially affected individuals.

The FDIC should work in cooperation with law enforcement and other oversight entities, such as by including them on the Breach Response Team and by promptly and openly sharing information pertaining to the breach with them, as appropriate. The Attorney General, the head of an element of the Intelligence Community, or the Secretary of the Department of Homeland Security (DHS) may direct the FDIC to delay notifying individuals potentially affected by the breach if the notice would disrupt a law enforcement investigation or hamper security remediation actions. In such cases and when directed by law enforcement, the FDIC shall delay notifying potentially affected individuals. However, any delay should not exacerbate the risk of harm to potentially affected individuals.

[22] *See* glossary in Appendix A.

[23] This requirement is separate from the FDIC user requirement to report a theft of their FDIC-furnished equipment to law enforcement, though the Incident Coordinator (or designated FDIC SOC representative) may be responsible for following up and consulting with law enforcement in those situations.

3.2.3 Reporting to Congress

The FDIC must notify[24] the appropriate Congressional Committees pursuant to FISMA[25] no later than seven (7) calendar days after the date on which there is reasonable basis to conclude that a breach that constitutes a "major incident" has occurred.[26] In addition, the FDIC must supplement the initial seven day notification to Congress with a report no later than thirty (30) days after the FDIC discovers the breach. FDIC OIG must also be notified at the same time as Congress. In accordance with FISMA and OMB guidance on reporting a breach to Congress and OIG, this supplemental report must include:

- A summary of information available about the breach, including how the breach occurred, based on information available to FDIC officials on the date when the FDIC submits the report;
- An estimate of the number of individuals affected by the breach, including an assessment of the risk of harm to affected individuals, based on information available to FDIC officials on the date which the FDIC submits the report;
- A description of any circumstances necessitating a delay in providing notice to affected individuals; and
- An estimate of whether and when the FDIC will provide notice to affected individuals.

The FDIC will, as appropriate, supplement the initial Congressional notification and 30-day report with pertinent updates through the closure of the breach. The CIO/CPO (or designee), in consultation with the CISO is responsible for alerting the Chairman when Congressional and OIG notification is required. The Chairman (or designee) is responsible for determining whether a breach constitutes a "major incident" under OMB M-18-02. The Chairman (or designee) must ensure appropriate Congressional and OIG notification is made within seven (7) days from the point when the FDIC had a reasonable basis to conclude that a breach that constitutes a "major incident" has occurred. The content of the Congressional and OIG notification must be coordinated through the following parties prior to release: FDIC Executive Office/ Office of Communications (OCOM), Legal Division, Office of Legislative Affairs (OLA), CIOO, OCISO, and the affected[27] Division/Office.

---

[24] Detailed guidance on meeting FISMA's Congressional and OIG reporting requirements for a breach is provided in OMB M-18-02, *Fiscal Year 2017-2018 Guidance on Federal Information Security and Privacy Management Requirements* (OMB, October 2017).

[25] The committees are the Committee on Oversight and Government Reform, Committee on Homeland Security, and the Committee on Science, Space, and Technology, of the House of Representatives; the Committee on Homeland Security and Governmental Affairs and the Committee on Commerce, Science, and Transportation of the Senate; the appropriate authorization and appropriations committees of Congress; the Committee on the Judiciary of the Senate; and the Committee on the Judiciary of the House of Representatives. *See* 44 U.S.C. § 3553, note ("Breaches"); 44 U.S.C. § 3554 (b)(7)(C)(III)(aa)-(bb).

[26] 44 U.S.C. § 3554 (b)(7)(C)(III)(aa)-(bb).

[27] See glossary in Appendix A.

4 INITIAL RESPONSE TO A BREACH

4.1 Initial Intake of Incident Report

The FDIC SOC is responsible for documenting all incident activity in the FDIC Incident Tracking System (CORSICA).[28] FDIC SOC is also responsible for notifying the appropriate FDIC officials and other authorities about a potential breach and gathering all pertinent information necessary to assess the nature and scope of the incident.

FDIC SOC will work with the incident reporter (user) and affected Division/Office to gather as much relevant information as possible.[29] FDIC SOC will record this information in CORSICA.

4.1.1 Breach Designation and Escalation

Based on the facts available at the time of FDIC SOC's initial intake of information, FDIC SOC, in consultation with the Incident Coordinator and PSC if necessary, will make and document the determination of whether the incident is a breach within CORSICA.

If FDIC SOC marks the incident as a potential breach, an initial informational alert email will be sent to the FDIC InfoAlert Distribution List, the affected Division POCs, and other pertinent FDIC staff and leadership to notify them that FDIC SOC is investigating and/or remediating the breach. This notification will include instructions for accessing the relevant incident record in CORSICA containing all pertinent information known to FDIC SOC at the time.

4.1.2 Potential Breach that Constitutes a "Major Incident" Designation and Escalation

In those circumstances where FDIC SOC has labeled an incident as a potential breach, FDIC SOC will determine (coordinating, as required, with the PSC, CISO, and SAOP) whether the breach **potentially** constitutes a "major incident"[30] or is otherwise significant as defined in the glossary.[31]

---

[28] *See* glossary in Appendix A.
[29] *See* Appendix D, *Breach Report Template*, for all information that FDIC SOC must document within CORSICA for every breach.
[30] *See* OMB M-18-02, *Fiscal Year 2017-2018 Guidance on Federal Information Security and Privacy Management Requirements* (OMB, October 2017) and glossary in Appendix A.
[31] *See* glossary in Appendix A.

If FDIC SOC flags a breach as a potential "major incident" or otherwise significant, FDIC SOC will document this within CORSICA, which will escalate the breach and notify the PSC, CISO, SAOP, and InfoAlert Distribution List. This will alert the SAOP that the Breach Response Team (BRT) must be convened.[32] In the event that normal communication channels are not available to the BRT, the SAOP may use the FDIC Emergency Notification System to facilitate convening the BRT.

4.2 Investigative Responsibilities

The FDIC SOC, with support from other technical resources as needed, is responsible for the investigation and technical remediation of the breach, in accordance with internal OCISO procedures. As needed, the FDIC SOC will coordinate with the Information Security Manager (ISM) and/or designated Incident Response (IR) POCs (Incident Leads) within the affected Division/Office to ascertain the nature of the impacted data and ensure compliance with all FDIC/Divisional policies related to information security and privacy (e.g., FDIC Circular 1360.9). If the FDIC SOC requires Divisional support to investigate or remediate an incident, it will provide sufficient instructions, templates, and guidance to the Division to ensure timely, appropriate, and consistent procedures are followed across the Corporation. The FDIC SOC will coordinate closely with the affected Division to promote appropriate disciplinary action and remediation.

4.2.1 Breach Report

The FDIC has created a model template Breach Report, provided in Appendix D, that includes examples of data elements and information types that can be used to distinguish or trace an individual's identity, either alone or when combined with other information that is linked or linkable to a specific individual. The FDIC Breach Report for a particular incident shall contain, at minimum, the fields shown in FDIC's model template.

For any potential breaches, FDIC SOC shall generate a Breach Report from the incident record in CORSICA. An electronic copy of (or link to) the Breach Report shall be included in the initial FDIC SOC notification. FDIC SOC, with support from other personnel as required, are responsible for ensuring the accuracy and completeness of the CORSICA incident record, updating it in a timely manner to reflect the latest status and findings of the investigation and remediation effort, and facilitating its distribution to the SAOP (or designees), the Breach Response Team when convened, and other relevant stakeholders. The Breach Report will serve as the primary basis for assessing the risk of harm to individuals and determining whether/what countermeasures, notification, and/or services are necessary.

[32] *See* Section 4 of this Plan for more information on the BRT.

4.2.2 Breach Investigation Status Update

Subsequent to issuing the initial notification described in Section 11 of this Plan, FDIC SOC will keep the CORSICA incident record up to date. If at any point during the investigation, the findings indicate that the breach may constitute a "major incident," FDIC SOC shall immediately alert the SAOP, CISO, PSC, and other pertinent staff and management.

4.3 Initial Risk of Harm Assessment[33]

In accordance with OMB M-17-12, the SAOP is ultimately responsible for conducting and documenting an assessment of the risk of harm to individuals potentially affected by a breach. In support of this responsibility, the Division Information Security Manager (ISM) or designee (Incident Lead), with input from the Incident Coordinator, shall perform and document within CORSICA a preliminary assessment of the risk of harm to individuals. This preliminary assessment will be based on the incident details provided in the FDIC Breach Report and will be conducted according to the methodology and procedures provided in Section 6 and Appendix E. This preliminary assessment[34] will also be used to facilitate the final assessment conducted by the BRT (if convened) or the SAOP or designee (Privacy Section Chief).

For significant breaches, the full Breach Response Team will be convened to assist the SAOP with assessing the risk of harm as detailed in the next section. For all other non-significant (routine) breaches, the Privacy Section Chief, at his/her discretion, will convene or consult with any and all consultative officials[35] as needed, including Legal; OCISO Privacy and Security representatives; the Divisional ISM/Incident Lead, Incident Response POCs, and other pertinent staff or management from the affected Division/Office; and applicable FDIC Program Area Specialists (e.g., SEPS, Contracting, etc.).

5 BREACH RESPONSE TEAM (BRT)

5.1 BRT Overview and Purpose

The FDIC's Breach Response Team (BRT) consists of a group of FDIC officials who will be convened to respond to breaches designated as "significant." A breach is significant if it:

[33] *See* Appendix E, *Breach Risk of Harm Assessment Template and Guidance*.
[34] While every effort should be made by the Division/Office to complete a preliminary risk of harm assessment as expeditiously as possible for significant breaches, the convening the BRT shall not be delayed in the absence of, or contingent upon, receiving such a preliminary risk of harm assessment from the Division/Office.
[35] *See* Appendix B, *BRT Core Members and Consultative Officials*.

- Constitutes a "major incident,"[36] or
- Potentially affects a large number of individuals or high-profile individuals;
- Is anticipated to create an overwhelming increase of phone or email traffic; inability or significantly reduced ability to fulfill core FDIC business functions; significant damages or costs associated with breach; and/or
- Has generated or has the potential to generate extensive media attention, Congressional inquiries, or other negative exposure requiring high-level coordinated response.

The SAOP is responsible for convening[37] the BRT for a breach that constitutes a "major incident" and other significant breaches as designated by the PSC, CISO, or SAOP. Once convened, the BRT will: (1) assist the SAOP with assessing the risk of harm to potentially affected individuals; (2) recommend to the SAOP whether the breach constitutes a "major incident" requiring a seven (7) day Congressional and OIG notification under the *Federal Information Security Modernization Act of 2014* (FISMA); and (3) recommend to the SAOP the appropriate course of action to respond to the significant breach, including whether notification, guidance, services or other remediation are required, in accordance with the guidance outlined in Sections 6-11 of this Plan. The BRT also helps to implement the approved course of action, and address the additional concerns and communication issues that may arise from significant breaches.

The SAOP (or designee), in consultation with the CISO, is responsible for providing the BRT's recommendations and findings to the Chairman (or designee). The Chairman (or designee) is responsible for determining whether a breach constitutes a "major incident" under OMB M-18-02 and for ensuring the appropriate Congressional and OIG notification is made within seven (7) days from the point when the FDIC had a reasonable basis to conclude that a breach that constitutes a "major incident" has occurred. The Chairman (or designee) also provides final approval for the recommended course of action, including whether to provide notification, guidance, and/or services to individuals potentially affected by a significant breach. For non-significant (routine) breaches, the PSC, in consultation with any consultative officials when applicable, is responsible for making a recommendation to the CISO and SAOP regarding whether to provide notification, guidance, and/or services to potentially affected individuals. The SAOP reviews the PSC's recommendation, as well as any feedback from the CISO, and has the opportunity to accept, modify, or reject the recommendation. The SAOP is ultimately responsible for making a final decision about whether to provide notification, guidance, and/or services to individuals potentially affected by a non-significant (routine) breach. When a contractor provides notification on behalf of FDIC, such activities shall be in accordance with OMB guidance and the FDIC's Breach

[36] *See* OMB M-18-02, *Fiscal Year 2017-2018 Guidance on Federal Information Security and Privacy Management Requirements* (OMB, October 2017).

[37] In the event that normal communication channels are not available to the BRT, the SAOP may use the FDIC Emergency Notification System to facilitate convening the BRT.

Response Plan and shall be coordinated with and subject to prior written approval by the Chairman or SAOP as applicable.

5.2 BRT Core Membership

The BRT core membership consists of the following representatives who have been designated by the Chairman:

- Senior Agency Official for Privacy (SAOP)/ Chief Privacy Officer (CPO);
- Chief Information Officer (CIO);
- Chief Operating Officer (COO);
- Chief Information Security Officer (CISO);
- Incident Coordinator;
- Privacy Section Chief (PSC);
- General Counsel;
- Office of Communications (OCOM) Director; and
- Office of Legislative Affairs (OLA) Director.

Core members are required for every significant breach; however, the responsibilities of a core member may be delegated in the event of an absence, incapacitation, inability to perform duties, or position vacancy. The SAOP should consider the circumstances of the breach every time the BRT is convened to ensure other consultative officials are included as appropriate.

5.3 BRT Leadership and Working Groups

The BRT is led by the SAOP or designated Breach Commander(s) (CISO, Incident Coordinator, and/or PSC). When the SAOP designates a Breach Commander for significant breaches related to cybersecurity, the CISO or Incident Coordinator assumes the leadership role as the Breach Commander, serving as the central authority for the breach response effort and directly overseeing and coordinating the breach investigation and technical remediation efforts. For significant breaches involving non-cybersecurity matters (e.g., lost/stolen paper records, verbal disclosure, etc.), the CISO or Incident Coordinator will serve as the Breach Commanders by default, unless the SAOP or CISO elects to designate the PSC or another subject matter expert (SME) with technical expertise in these matters to serve as the central Breach Commander in place of the Incident Coordinator or himself/herself. The PSC serves as the Deputy Breach Commander for significant breaches, providing advice and guidance to the BRT in relation to the risk assessment and consumer notification effort. To assist the Breach Commander(s), the BRT may be organized into cross-functional working groups (teams) comprised of a team lead and SMEs who are authorized to take the necessary steps to contain, mitigate and rectify the breach, as well as develop and provide notification, services and guidance to potentially affected individuals upon approval by the BRT (but outside of a meeting of the full BRT). The makeup of the BRT

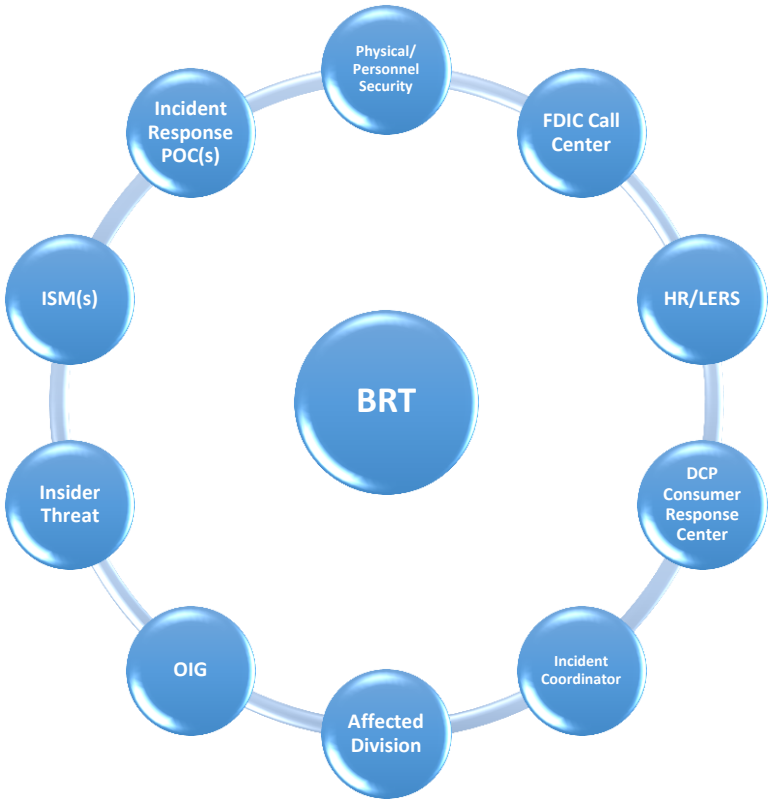
will vary based on the circumstances of the significant breach, since the participants should ensure proper coverage and expertise based on the specific circumstances of the significant breach. The following figure reflects a typical composition of a BRT for significant breaches involving cybersecurity:

5.4 Consultative Officials

In addition to the core members of the BRT, the SAOP may ask representatives of other Divisions/Offices from throughout the Corporation ("consultative officials") to assist in responding to a particular breach. These consultative officials may include, for example; members of the Insider Threat and Counterintelligence Program, Division of Information Technology (DIT), Office of the Chief Information Security Officer (OCISO), Division of Finance (DOF), Division of Administration (DOA) Acquisitions Services Branch (ASB), Library Services, Human Resources (HR)/Labor and Employee Relations (LERS), FDIC Call Center, Division of Consumer Protection (DCP) Consumer Response Center, Office of Inspector General (OIG) Representative(s)[38], the Incident Coordinator, the affected Division/Office

[38] OIG's participation in the BRT is optional and at the discretion of OIG based on the particular circumstances of the breach.

Director (or designee), the Information Security Manager (ISM)/Incident Lead and Incident Response POC(s), as well as management and staff from the affected Division/Office. The BRT may also work closely with other Federal agencies, offices, and teams as necessary and appropriate. The consultative officials engaged by the BRT will vary, depending on the nature of the breach. The following figure reflects examples of consultative bodies or officials that the BRT may call upon for expertise or assistance during the breach response process. A listing of current consultative officials is included in Appendix B, along with their associated roles and responsibilities in Appendix C.



6 METHODOLOGY FOR ASSESSING RISK OF HARM

The FDIC applies the following three-step methodology when assessing the risk of harm to individuals potentially affected by a breach using its Risk of Harm Assessment (RHA) template:

1. **Evaluate key factors** –the factors identified by OMB are assessed in relation to the specific breach (Section 7).
2. **Assign risk factor ratings** – each of the factors is rated with a score from zero to three based on its potential level of risk of high, moderate, low, or none (Section 8).
3. **Determine breach classification** – the breach is categorized into a risk code category (Code Red, Code Blue, Code Green, or Code Orange) based on the total factor rating points (Section 9).

The above methodology was developed in accordance with OMB M-17-12 and provides a flexible and adaptable framework for determining the appropriate breach response activities based upon the specific facts and circumstances of each breach and an analysis of the potential risk of harm to the affected individuals. The response recommendations are a result of the risk analysis process and will vary based on the circumstances of each breach. The methodology ensures the FDIC is able to respond in a timely and consistent manner by assessing each breach based on standardized factors and ratings criteria.

Some of the potential harms that FDIC shall consider when assessing the risk of harm to individuals potentially affected by a breach include the effect of a breach of confidentiality or fiduciary responsibility, the potential for blackmail, the disclosure of private facts, mental pain and emotional distress, financial harm, the disclosure of contact information for victims of abuse, the potential for secondary uses of the information which could result in fear or uncertainty, or the unwarranted exposure leading to humiliation or loss of self-esteem.

Additionally, the Privacy Act requires agencies to protect against any anticipated threats or hazards to the security or integrity of records which could result in "substantial harm, embarrassment, inconvenience, or unfairness to any individual on whom information is maintained." The FDIC will consider all risks relevant to the breach, including risks to the FDIC, FDIC information and information systems, FDIC programs and operations, the Federal Government, or national security as applicable.

The FDIC Breach Report will provide (among other things) an inventory of all compromised data elements, the source of the data, the status of whether it was encrypted, and any other special factors that need to be considered, such as if the data is being used in a criminal or grand jury investigation. The SAOP and BRT when convened will evaluate the Breach Report, using the three-step methodology outlined above, to assess the risk of harm. Refer to Appendix D for the current Breach Report template.

7 EVALUATE KEY FACTORS

In order to respond appropriately to breaches involving PII, OMB recommends the following factors be considered when assessing the likely risk of harm to determine when notification should be provided:

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

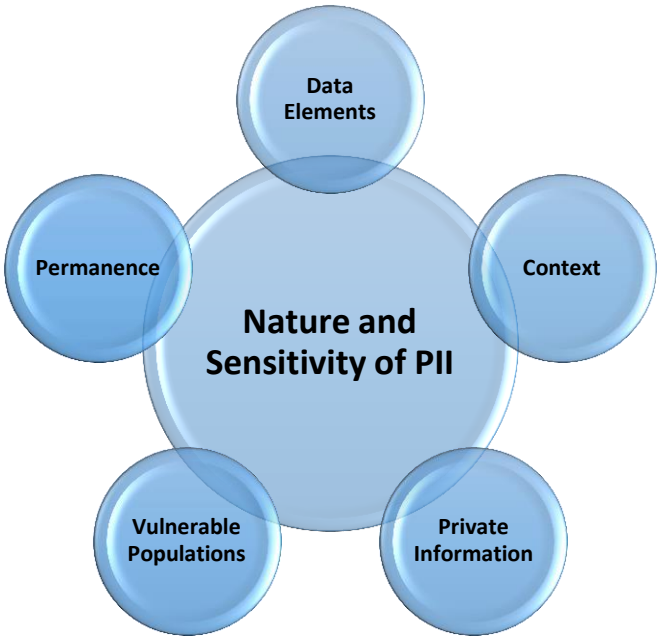
The ability to accurately assess the potential risk and appropriately respond will require the examination of a breach based on specific considerations for each of the key factors.

Key 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, in a given context, may reveal particularly private information about an individual • *Vulnerable Populations,* including the extent to which the PII identifies or disproportionately impacts a particularly vulnerable 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

The FDIC will review each of these factors to complete a risk assessment to determine the potential likelihood of harm to the individuals. Identifying the data elements and assessing the impact of the loss or disclosure are key factors that must be considered in determining if, when, and how notification will be provided to potentially affected individuals.

7.1 Nature and Sensitivity of PII

Risk of Harm takes into account five primary factors, illustrated in the figure below, when assessing the nature and sensitivity of PII potentially compromised by a breach. Each of these factors is detailed in the subsections below.



A. Data Elements, including an analysis of the sensitivity of each individual data element as well as the sensitivity of all the data elements together

Certain data elements are particularly sensitive and may alone present an increased risk of harm to an individual. These data elements include, but are not limited to, social security numbers (SSNs), passport numbers, driver's license numbers, state identification numbers, bank account numbers, passwords, and biometric identifiers. Other data elements, such as date of birth, place of birth, address, and gender may not be particularly sensitive alone, but may present an increased risk when combined with other data elements. The risk assessment should also take into account information that may have been previously compromised, as well as any other available information, that when combined with the information may result in an increased risk of harm to the individuals.

Information related to businesses, such as EIN, name, and address, is considered public information. This type of information does not meet the definition of PII since it is not linked or linkable to an individual. However, personal information disclosed on the officers of a corporation, partners in a partnership, etc., is considered PII since it meets the definition.

B. Context, including the purpose for which the PII was collected, maintained, and used

Consider the purpose for which the PII was collected, maintained, and used. The same information in different contexts can reveal additional information about the affected individuals that may result in increased risk of harm.

C. Private Information, including the extent to which the PII, in a given context, may reveal particularly private information about an individual

Evaluate the extent to which the PII constitutes information that an individual would generally keep private. Information generally kept private may not present a risk of identity theft or other criminal conduct, but may pose other risk of harm such as embarrassment, blackmail, or emotional distress. Examples of private information FDIC may potentially disclose include derogatory personnel or criminal information, personal debt and finance information, or immigration status. Passwords are another example of private information that if involved in a breach may present a risk of harm.

D. Vulnerable Populations, including the extent to which the PII identifies or disproportionately impacts a particularly vulnerable population

Consider whether the potentially affected individuals are from a particularly vulnerable population that may be at greater risk of harm than the general population. Potentially vulnerable populations include, but are not limited to: children, active duty military, government officials in sensitive positions, senior citizens, individuals with disabilities, confidential informants, witnesses, certain populations of immigrants, non-English speakers, and victims of certain crimes such as identity theft, child abuse, trafficking, domestic violence, or stalking.

E. Permanence, including the continued relevance and utility of the PII over time and whether it is easily replaced or substituted

Consider the permanence of the PII; this includes an assessment of the relevancy and utility of the information over time and whether the information will permanently identify an individual. Some information loses its relevancy or utility as it ages, while other information is likely to apply to an individual throughout his or her life. For example, a social security number can permanently identify an individual.

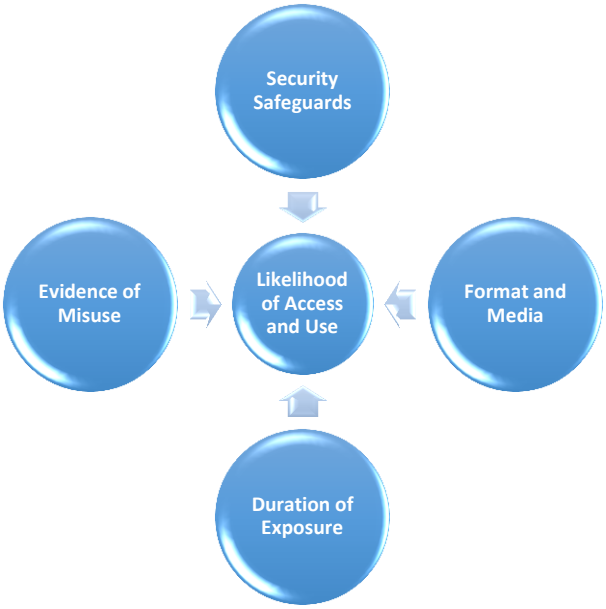
Special consideration, based on the current and potential future uses, is warranted when a breach involves biometric information, such as fingerprints, hand geometry, retina or iris scans, and DNA or other genetic information.

7.2 Likelihood of Access and Use of PII

Another consideration when determining the potential impact of a breach is the likelihood of access and use of the PII involved. OMB guidance clarifies that just because data has been lost or stolen does not mean it has been or can be accessed by unauthorized individuals.[39] This determination must be made by assessing the physical, technological, and

[39] *See* OMB M-17-12, *Preparing for and Responding to the Breach of Personally Identifiable Information* (OMB, January 2017).

procedural safeguards in place. Specifically, an assessment of the likelihood of access and use of the PII must take into account four primary factors, including: (a) security safeguards; (b) format and media; (c) duration of exposure; and (d) evidence of misuse. Each of these factors is detailed in the subsections below.



A. Security Safeguards, including whether the PII was properly encrypted or rendered partially or completely inaccessible by other means

Since security safeguards may significantly reduce the risk of harm to potentially affected individuals, even when the PII is particularly sensitive, consider the security safeguards protecting the information. Whether information has been or is likely to be compromised is best answered after determining what technology was in place to protect the PII. For example, information on a properly encrypted laptop is less likely to be accessed than hard copy documents containing the same information.

Even if the information is encrypted, based on the specifics of the breach and the type, value, or sensitivity of the information, it should be considered whether an individual may have the skills and resources necessary to overcome the safeguards. Refer to Appendix K for additional information on the considerations for evaluating the implementation and effectiveness of security safeguards protecting the information, with focus on encryption protocols.

B. Format and Media, including whether the format of the PII may make it difficult and resource-intensive to use

Consider whether the format or media of the PII may make its use difficult and resource-intensive or if it may be more susceptible to a crime of opportunity. For example, a

spreadsheet on an unencrypted external storage device (flash drive, CD-ROM, DVD) does not require any special skill or knowledge to access and an individual could quickly search and identify fields such as a nine-digit SSN. Conversely, special expertise and equipment would be required to access and use information if it was located within a large volume of unstructured PII, such as information located on a magnetic back-up tape cartridge.

The type, value, or sensitivity of the PII may increase the likelihood of access and use regardless of its format or media because the value of the information may outweigh the difficulty and resources needed to access the information.

C. Duration of Exposure, including how long the PII was exposed

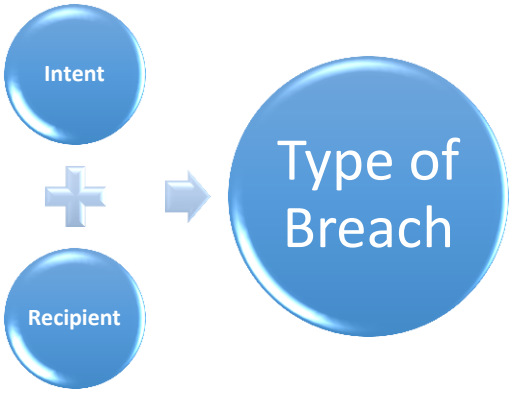
Consider the amount of time that the PII was exposed since PII that was exposed for an extended period of time is more likely to have been accessed or used by unauthorized users. For example, a briefcase containing PII left in a hotel lobby for an hour before being recovered is less likely to have been accessed by an unauthorized user than if it had been left for three days prior to being recovered. Similarly, PII inadvertently published to a public Internet page for an hour before being removed is less likely to have been accessed by an unauthorized user than if it had been available on the public Internet page for a week.

D. Evidence of Misuse, including any evidence confirming that the PII is being misused or that it was never accessed.

Determine if there is evidence of misuse indicating that identity theft has already occurred as a result of the breach or that the PII is appearing in unauthorized external contexts. For example, law enforcement may confirm that PII is appearing on a website dedicated to the sale of stolen PII reflecting strong evidence of misuse. Conversely, FDIC may determine with reasonable certainty that the PII will not be misused. For example, a forensic analysis of a recovered device may reveal that the PII was not accessed.

7.3 Type of Breach

When determining the type of breach, OMB indicates the assessment should take into account whether the information was intentionally compromised (“intent”) and to whom the information was disclosed (“recipient”), such as a contractor, individual with business need for the information, etc. The risk of identity theft or other risk of harm is greater if the compromised data was specifically targeted compared to the risk of data that was inadvertently misplaced or stolen. Even if the information was not the target of theft, it could still potentially be exploited.



A. Intent, including whether the PII was compromised intentionally, unintentionally, or whether the intent is unknown

Consider whether the breach was intentional or unintentional. In some situations the intent is unknown. For example, if an employee realizes a mobile device is missing, it could have been misplaced somewhere or someone could have intentionally stolen it. A package containing PII that never arrives at the intended destination could have been lost or may have been intentionally intercepted.

Some examples of an intentional breach include the theft of assets containing PII from a vehicle or office, the unauthorized intrusion into the FDIC's network that maintains PII, or an employee looking up a celebrity's file in a database without a business need. If a breach was intentional, consider whether the target of the breach was the device itself, like a mobile phone or laptop, and the compromise of the information on the device was incidental. While the risk of harm to individuals may often be lower when the information was not the target, the potential for a significant risk of harm may still exist.

Unintentional breaches are often the result of user error or failure to comply with FDIC policies and procedures. Examples of unintentional breaches include accidentally emailing PII to the wrong email address, storing PII in a shared folder that is not properly access-controlled, mailing documents for two different individuals in the same envelope, or sending PII to an incorrect fax number. The risk of harm to individuals may be lower in these types of situations than if someone intentionally targeted the information, but the breach response must consider the specific facts of the breach to determine the potential risk of harm.

B. Recipient, including whether the PII was disclosed to a known or unknown recipient, and the trustworthiness of a known recipient.

In some cases, the FDIC may know who received the compromised PII and this information may help when assessing the likely risk of harm to individuals. For example, a breach may be reported by a recipient who receives information he or she should not have. This may be

an indication of a lower risk of harm to individuals. Examples of recipients who could pose a lower risk include employees who received information without a need to know, or individuals known to the FDIC who acknowledged receipt of the PII, did not forward or otherwise use the PII and properly disposed of the PII. Even though these types of breaches must be reported and the FDIC will conduct a risk assessment, the risk of harm may be low and the FDIC may not need to notify or provide services to the individual whose PII was compromised.

The risk of harm to the individual is considerably higher if analysis reveals that the PII is under control of a group or person who is either untrustworthy or known to exploit compromised information. In other breaches FDIC may not have any information indicating that compromised or lost PII was ever received or acquired by anyone or the identity may be unknown.

8 RISK FACTOR RATINGS

In accordance with the OMB guidance, FDIC will balance the need for transparency with concerns about over-notifying individuals since notification may not always be beneficial to the potentially affected individuals. When these factors are appropriately reviewed within a fact-specific context, notification will only be given in those instances where there is a reasonable risk of harm and will not lead to the overuse of the notification. The risk levels for each of the factors are described in the following chart.

Assigning Risk Factor Ratings			
Risk Level of Identity Theft or Other Harm	**Factors**		
	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	• SSNs • Financial Information (with passwords) • Passports • Vulnerable population affected • Highly sensitive context	• PII in paper form • PII in electronic form was not encrypted • Evidence information has already been misused • Significant duration of exposure	• Information was specifically targeted • Unknown recipient • Recipient has malicious intent
Moderate = 2	• Financial information (without passwords) • Combination of private data elements but no SSN	• Information was encrypted but not using a NIST approved encryption method • Limited duration of exposure	• Information was not specifically targeted • Incorrect recipient contacted FDIC to advise of error • Correct recipient, but potentially viewed by unauthorized parties
Low = 1	• Public Information • Loan Account Number • Employee Business Information • PII element can be easily	• The PII was properly encrypted using a NIST approved method • Breach occurred in a secure FDIC facility • Affected individual is deceased	• Recipient had a business need for the information but breach was the result of failure to follow FDIC procedures (e.g., proper encryption, etc.)

	changed	• PII was viewed but time of exposure was limited (documents immediately returned, etc.)	• Data was disclosed to an FDIC employee, contractor, or other trusted party
None = 0	• Breach did not involve PII (e.g. business information, account information disclosed to former spouse or to someone with Power of Attorney (POA) for a period that was not authorized, etc.) • FDIC procedures were followed and the breach did not meet FDIC reporting requirements* • Duplicate or non-FDIC Breach • The asset has been recovered with no PII exposure (opened returned mail, emails and fax transmissions are not considered recovered if they have already been viewed)	• Breach did not involve PII (e.g. business info, account information disclosed to former spouse, etc.) • FDIC procedures were followed and the breach did not meet FDIC reporting requirements* • Duplicate or non-FDIC Breach ** • The asset has been recovered with no PII exposure (opened returned mail, emails and fax transmissions are not considered recovered if they have already been viewed)	• Breach did not involve PII (e.g. business information, account information disclosed to former spouse, etc.) • FDIC procedures were followed and the breach did not meet FDIC reporting requirements* • Duplicate or non-FDIC Breach • The asset has been recovered with no PII exposure (opened returned mail, emails and fax transmissions are not considered recovered if they have already been viewed)

** FDIC employee follows all procedures to verify the identity of a caller before disclosing any information; mail sent to last known address in accordance with FDIC secure shipping procedures; employee follows all established procedures for faxing sensitive information, only to later find that the fax number provided by the consumer or authorized representative was incorrect.*

*** FDIC SOC will provide this information within the initial breach notification.*

9 BREACH CLASSIFICATION

The output of the risk assessment is the classification of the PII breach in a risk code category (Code Red, Code Blue, Code Green, or Code Orange) based on the combined total number of points assigned to each of the above factors. The risk assessment classification (code) will only dictate whether or not FDIC will notify the potentially affected individuals. These recommendations are based on the unique circumstances of the PII breach. Each risk code, the total number of points, likelihood of risk, notification decision, and examples are detailed in the table below.

Breach Risk Code	Risk Factor Outputs • Total Points • Likelihood of Risk • Notification	Examples of Common Elements
Code Red	• 8-9 Points • Likely Risk • Implement PII Breach Notification Policy	• Information was targeted • Information was not properly encrypted • SSN or sensitive PII was disclosed to an individual with a higher associated risk (excludes FDIC employee, contractor, approved or trusted recipients, etc.)
Code Blue	• 8-9 Points • Likely Risk • No Notification	• Same as code red but notification would negatively affect: ▪ National security ▪ FDIC financial institution (FI) investigation ▪ Grand jury investigation ▪ Criminal investigation

Code Green	• 1-7 Points • Unlikely Risk • No Notification	• Information was properly encrypted • Information was unencrypted but the recipient had a business need for the information • Data elements compromised not likely to lead to identity theft or other risk of harm • The asset was lost in a secure FDIC facility • Data was disclosed to an FDIC employee, contractor, or trusted party
Code Orange	• 0 Points • Unlikely Risk • No Notification	• Asset does not contain PII, so there is no risk of identity theft or other harm (e.g., business information, account information only disclosed to former spouse, etc.) • Data has been recovered and there was no access or distribution of the information (opened returned mail, e-mails and fax transmissions are not considered recovered if they have been viewed) • FDIC established procedures were followed and the breach does not meet reporting requirements (e.g. FDIC employee follows all procedures to verify the identity of a caller before disclosing any information; mail sent to last known address in accordance with FDIC procedures; employee follows all established procedures for faxing sensitive information, only to later find that the fax number provided by the consumer was incorrect.)

10 MITIGATING THE RISK OF HARM

After assessing the risk of harm to individuals potentially affected by a breach, the FDIC will determine how best to mitigate the identified risks. Because each breach is fact specific, the decision of whether or not to offer guidance or provide services to individuals will depend on the circumstances of the breach. In making this decision, the FDIC will consider the assessed risk of harm (Sections 7 – 9). Decisions regarding whether to offer guidance or provide services to potentially affected individuals will be made in accordance with the procedures provided in this BRP. For any notifications related to significant breaches or those that otherwise are likely to generate leadership or external interest, the SAOP will inform and obtain final approval from the FDIC Chairman prior to issuing notification. For any notifications related to non-significant (routine) breaches, the PSC will make a recommendation (based on the RHA) to the SAOP and give the SAOP the opportunity to accept, modify, or reject the recommendation prior to issuing notification.

The goal of the risk analysis performed is to determine an appropriate course of action that includes strategies to mitigate the risk of harm to individuals whose data was compromised.

The following factors must be considered when determining the need to mitigate any damages:

- Whether any damage occurred;
- The nature of the damage that occurred;
- The amount of damage;
- The type of data that was used or disclosed;
- The reasons for the disclosure; and
- Whether the harm can be mitigated.

The risk analysis is likely to lead to segmenting the breach population. For example, within the same breach, bank customers may be classified into different segments and receive different treatment streams depending on the specific PII pertaining to them and other contextual circumstances.

Actions the FDIC can take to mitigate the risk of harm include:

- ***Countermeasures***, such as expiring compromised passwords or placing an alert in a database containing potentially compromised PII;
- ***Guidance*****,** such as how individuals may obtain a free credit report and whether they should consider closing certain accounts; and
- ***Services*****,** such as identity and/or credit monitoring.

10.1 Countermeasures

When determining how to mitigate the risk of harm to individuals potentially affected by a breach, the FDIC will consider what countermeasures it can take. Countermeasures may not always prevent harm to potentially affected individuals but may limit or reduce the risk of harm. For example, if credit card information is potentially compromised, the FDIC may proactively notify appropriate banks so they can monitor the associated accounts or reissue the lines of credit using new accounts. 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 disability beneficiaries is potentially compromised, the FDIC may consider monitoring beneficiary databases for unusual activity that may signal fraudulent activity, such as a sudden request for a change of address. Similarly, if individuals' passwords are potentially compromised in a breach, the FDIC should require those users to change their passwords.

10.2 Guidance

When determining how to mitigate the risk of harm to individuals potentially affected by a breach, the FDIC will consider what guidance to provide to those individuals about how they may mitigate their own risk of harm. These countermeasures may not always prevent harm, but they may limit or reduce the risk of harm to potentially affected individuals. For example, some of the countermeasures FDIC may advise individuals to take include setting up fraud alerts or credit freezes, changing or closing accounts, and taking advantage of services made available by the Federal Trade Commission (FTC). Where practical, the FDIC will use the information available from the FTC at www.IdentityTheft.gov/databreach as a baseline when drafting guidance. The FTC provides specific guidance for when a breach involves SSNs, payment card information, bank accounts, driver's licenses, children's information, and account credentials. Additionally, the FDIC may advise individuals to change passwords and encourage the use of multi-factor authentication for account access. A summary of possible guidance options are included in Appendix I.

10.3 Services

The FDIC will determine if there are specific services the FDIC can provide to help mitigate the risk of harm. For breaches involving the loss, theft, or disclosure of SSNs or sensitive financial information, the FDIC may issue a letter or notice providing and/or offering various identity theft protection/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 consumer.

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, the FDIC may choose not to provide services to the potentially affected individuals. Choosing not to provide services is a decision separate from the decision to provide notification and there may be circumstances where potentially affected individuals are notified but not provided services. OMB M-17-12 does not set a specific threshold for providing services to individuals.

The 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[40] is paid for by the FDIC. It is free to the individual, but the individual must enroll at his or her option in order to take advantage of the free offering. The notification to the individual includes the offer of the free identity theft protection/credit monitoring product and instructions on how to place a fraud alert on his or her credit file. The FDIC will continue to monitor available services and will update its procedures if additional services become available in the future. For a summary of currently available services refer to Appendix I.

11 BREACH NOTIFICATION POLICY

Because each breach is fact specific, the decision of whether or not to notify individuals will depend on the circumstances of the breach. The assessed risk of harm to individuals (Sections 7 – 9) will inform the FDIC's decision of whether or not to notify individuals. In all cases, the FDIC will carefully evaluate and balance the need for transparency with concerns about over-notifying individuals, since notification may not always be helpful to the potentially affected individuals.

It is the policy of the FDIC to notify potentially affected individuals of a breach of PII in circumstances in which the safeguarding of the PII is the responsibility of the FDIC; the risk analysis (Section 7) resulted in a determination that the potential for harm to the individual is

[40] In accordance with OMB Memorandum M-16-14, the FDIC utilizes where feasible the GSA Identity Protection Services BPAs. For details on the Identity Protection Services BPAs, including task order instructions, offered services, authorized users, order dollar value limitations, the inclusion of agency specific terms, and ordering periods, visit www.gsa.gov/ipsbpa.

likely; notification will not negatively affect national security or an FDIC, criminal or other investigation; and the individuals can be properly identified.

The decision to offer guidance, take countermeasures, or provide services to individuals potentially affected by a breach may require the FDIC to notify those individuals both of the breach and of those steps taken to mitigate any identified risks. The notification may advise the individuals on how to secure any services offered or it may just contain guidance but no services.

11.1 Timeliness of the Notification

The FDIC will provide notification to affected individuals as expeditiously as practicable, without unreasonable delay, and consistent with the needs of law enforcement and national security as applicable. Additionally, it may be necessary and appropriate to delay notification as explained below. The SAOP or designee (PSC), in consultation with the Division/Office, will make a final determination regarding the appropriate timeframe for issuing notification and whether it is necessary to delay the notification timeframe. The Division/Office will record the approved timeframe and any subsequent extension justifications in CORSICA.

Notification should not be issued prematurely, based on incomplete facts (to include not knowing the full scope of the breach), or in a manner that compounds harm to the affected individuals/entities. In addition, the timing of the notification must be consistent with the needs of law enforcement, national security (if applicable), and any measures necessary for the Corporation to contain the incident, reconstruct the breached data, and obtain valid contact information for the potentially affected individuals.

For breaches involving data that could compromise ongoing FDIC or OIG investigations (e.g., FDIC/OIG investigations of Persons of Interest (POI), professional liability claims, etc.), notification may be delayed if disclosure of the investigation pertaining to the breach or to an individual affected by the breach would disrupt or impede the investigation. Additionally, notification to individuals potentially affected by a breach may be delayed at the direction of the Attorney General, the head of an element of the Intelligence Community, or the Secretary of DHS if notification would disrupt a law enforcement investigation, endanger national security, or hamper security remediation actions. Further, before issuing any external notification, the reasonable integrity of the compromised system or data must be restored as necessary. However, any delay should not exacerbate risk or harm to any affected individual(s).

As a practical matter, the FDIC will balance 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. If a technical issue contributed to the breach, the FDIC will also consider whether the issue has been corrected or resolved prior to providing notification.

11.2 Contents of the Notification

The CIOO, in coordination with the affected Division, PSC, Legal, and OCOM (and OLA when the breach is reported to Congress), will issue a breach notification letter to those individuals approved for 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, etc.);
- 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;
- 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, to mitigate losses, and to protect against a future breach; and
- Whom potentially affected individuals should contact at the FDIC for more information, including a telephone number (preferably toll-free), email address, and postal address.

Given the amount of information required in a notification, additional details may be provided in a Frequently Asked Questions (FAQ) format, on the FDIC website or via an enclosure. For a breach that potentially affects a large number of individuals, or as otherwise appropriate, toll-free call centers staffed by trained personnel should be established to handle inquiries from the potentially affected individuals. If the potentially affected individuals are not English speaking, or require translation services, notification should also be provided in the appropriate languages to the extent feasible.

In some instances, it may be necessary to draft different notifications for different populations affected by the same breach. The notification language (and talking points, as needed) shall be prepared by OCISO and the affected Division/Office in coordination with Legal and OCOM. Depending on the circumstances, a third party (such as a financial institution or a vendor) may offer to draft the notification. In such instances, the CIOO will coordinate this effort with the affected Division, Legal, OCOM, and OCISO, and the notification may be drafted jointly with the third party.

11.3 Source of the Notification

The Chairman or designee[41] will serve as the source (i.e., the individual who signs the letter on behalf of the FDIC) of the notification to potentially affected individuals.

When a breach involves FDIC information or information systems operated by a contractor or another entity on behalf of the FDIC, the FDIC will coordinate with the contractor to ensure notification is provided and that the source of the notification is appropriate and understandable from the recipient's perspective. In cases where a contractor provides notification on behalf of the FDIC, such activities shall be in accordance with OMB guidance and the FDIC's BRP and shall be coordinated with and subject to prior written approval by the Chairman as applicable.

The SAOP or designee (PSC) oversees the notification process in coordination with the affected Division. The CIOO, in coordination with the affected Division, is ultimately responsible for implementing the notification process to individuals potentially affected by the breach. When a breach involves and/or is caused by a contractor, the CIOO (via the ISM, Incident Lead or other SME designated by the affected Division) should coordinate with the Contracting Officer (CO) and Oversight Manager (OM) as appropriate, in consultation with the PSC, Legal, and the BRT (when convened), to discuss and determine the source, issuance and costs associated with providing notification and services to individuals potentially affected by the breach.

11.4 Method of Notification

The means for providing notification should be commensurate with the number of individuals/entities affected, what contact information is available about the affected individuals/entities, and the urgency with which they need to receive the notification. For significant breaches, the SAOP, in coordination with the BRT, will decide the appropriate method of notification. For routine breaches, the PSC, in consultation with the affected Division/Office and Legal, will make the final determination about the method of notification. Potential methods of notification include:

> **First-Class Mail**: First-class mail notification to the last known mailing address of the individual in FDIC records is the primary means by which notification is provided. When there is reason to believe the address is no longer current, the FDIC takes reasonable steps to update the address by consulting with other agencies such as the U.S. Postal Service. The notification should be sent separately from any other mailing so that it is conspicuous to the recipient. If the FDIC uses another agency or entity to facilitate mailing, care should be taken to ensure that the FDIC is identified as the sender, and not the facilitating agency or entity. The front of the envelope

[41] The SAOP has been designated by the Chairman to serve as the source of notifications.

should be labeled to alert the recipient to the importance of its contents (e.g., "Data Breach Information Enclosed"), and the sender should be marked as the FDIC to reduce the likelihood the recipient thinks it is advertising mail. Mail returned as undeliverable should be anticipated, and there should be procedures in place for how to provide a secondary notification.

Telephone: Telephone notification may be appropriate in those cases where urgency may dictate immediate and personalized notification or when a small number of individuals are affected. Telephone notification, however, should be contemporaneous with written notification by first-class mail.

Email: Email notification, especially to or from non-government email address, is not recommended due to the high risk of malicious email attacks that are often launched when attackers hear about a breach. Emails often do not reach individuals because they are automatically routed to spam or junk mail folders. Individuals who receive notifications via email are often uncertain of the legitimacy of the email and will not open the notification. While email is not recommended as primary form of notification, in limited circumstances it may be appropriate. For example, if the individuals potentially affected by a breach are internal to the FDIC, it may be appropriate for the FDIC to use an official email address to notify a small number of employees, contractors, detailees, or interns via their FDIC email addresses. A ".gov" email may be used to notify an individual on his or her ".gov" email that his or her PII was potentially compromised by a breach.

Substitute Notification: In those instances where the FDIC does not have sufficient contact information to provide notification, and also as supplemental notification for any breach to keep potentially affected individuals informed, substitute notification may be used. This type of notice may also be beneficial if the FDIC needs to provide an immediate or preliminary notification in the wake of a high-profile breach when notification is particularly time sensitive. A substitute notification should consist of a conspicuous posting of the notification on the FDIC's public homepage (www.FDIC.gov) and/or notification to major print and broadcast media, including major media in areas where the potentially affected individuals reside. Notification to media should include a toll-free phone number and/or an email address that an individual can use to learn whether or not his or her personal information is affected by the breach. In instances where there is an ongoing investigation and the facts and circumstances of a breach are evolving, the FDIC should consider whether it is appropriate to establish an ongoing communication method for interested individuals to automatically receive updates. Depending on the individuals potentially affected and the specific circumstance of the breach, it may be necessary to provide notifications in more than one language.

Existing Government-Wide Services: The FDIC may consider use of Government-wide services to provide support services needed, such as USA Services, including the toll free number of 1-800-FedInfo and www.USA.gov.

Newspapers or other Public Media Outlets: Individual notification may be supplemented with placing notifications in local newspapers or other public media outlets. The FDIC Call Center can be utilized in handling inquiries from the affected individuals and the public.

11.5 Special Considerations

When a breach potentially affects a vulnerable population, the FDIC may need to provide a different type of notification to that population, or provide a notification when it would not otherwise be necessary. For example, when the individual whose information was potentially compromised is a child, the 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.[42] Accommodations may include establishing a Telecommunications Device for the Deaf (TDD) or posting a large-type notice on the FDIC website.

12 LESSONS LEARNED

After completion of a breach that was reported to Congress (and optionally for any other breach at the discretion of the SAOP), the SAOP will schedule a lessons learned meeting with the BRT and all involved parties. The purpose of the meeting is to identify root causes and other issues that need to be addressed, ultimately improving the FDIC's breach response process and data protection measures. The affected Division/Office will assist the SAOP in identifying lessons learned so that business process improvements can be incorporated into the FDIC's security and privacy policies, procedures and practices to help reduce the potential for future breaches. The affected Division/Office ISM(s)/Incident Lead(s) or designee shall record the BRT's and other stakeholders' feedback in the Post-Breach Analysis and Lessons Learned report (Appendix F) during the Lessons Learned meeting(s) and ensure the completed form is recorded in CORSICA in an accurate and timely manner. The lessons learned report should be documented in CORSICA using the template provided in Appendix F and include any salient issues, action items, and resulting recommendations. In addition to providing closure, the lessons learned session could reveal vulnerabilities that may lead to updated breach response policies and procedures, training and resource deficiencies, and/or improved response times. The FDIC will document any changes to the FDIC's breach response plan, policies, training, or other documentation resulting from the lessons learned. Affected Divisions/Offices will take

[42] 29 U.S.C. § 794(d). For additional information about accessibility aids, refer to www.section508.gov.

actions to implement any mitigation strategies identified to prevent or reduce the likelihood of a similar breach in the future and will document in CORSICA any challenges preventing FDIC from instituting any remedial measures. Refer to Appendix F for more information.

In addition to the formal lessons learned meetings for breaches reported to Congress, at the end of each quarter of the fiscal year, FDIC SOC shall provide a report to the SAOP detailing the status of each breach reported to FDIC SOC during the fiscal year. The SAOP will review the report and validate that the report accurately reflects the status of each reported breach.

12.1 Tabletop Exercises

The SAOP will periodically, but not less than annually, convene the FDIC's BRT to hold a tabletop exercise. The purpose of the tabletop exercise is to test the BRP and to help ensure that members of the team are familiar with the plan and understand their specific roles. Testing the BRP is an essential part of risk management and breach response preparation. Tabletop exercises should be used to practice a coordinated response to a breach, further refine and validate the BRP, and identify potential weaknesses in the FDIC's response capabilities.

The SAOP should identify the capabilities that exist within the FDIC to develop, host, and implement the annual tabletop exercise and which Divisions/Offices are responsible for maintaining those capabilities. The SAOP may determine that the FDIC does not have the capability to run the tabletop exercise in any given year, in which case the SAOP will designate an appropriate FDIC official to consult with the DOA Acquisition Services Branch (ASB) to obtain a contract for this service.

12.2 Annual Breach Response Plan Reviews

At the end of each fiscal year, the SAOP will review the reports from FDIC SOC (detailed in Section 13) and consider whether the FDIC should undertake any of the following actions:

- Update its breach response plan;
- Develop and implement new policies to protect the FDIC's PII holdings;
- Revise existing policies to protect the FDIC's PII holdings;
- Reinforce or improve training and awareness;
- Modify information sharing arrangements; and
- Develop or revise documentation such as SORNs, PIAs, or privacy policies.

As part of the review, the SAOP will review the FDIC's BRP to confirm that the plan is current, accurate, and reflects any changes in law, guidance, standards, FDIC policy, procedures, staffing, and/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.

13 REPORTS

13.1 Tracking and Documenting the Response to a Breach

FDIC SOC maintains a formal process to track and document each breach reported to the FDIC. The process ensures that the SAOP is made aware in a timely manner of each report of a suspected or confirmed breach. The SAOP, in coordination with the Incident Coordinator, is responsible for keeping FDIC SOC informed of the status of an ongoing response and for determining when the response to a breach has concluded. When the SAOP determines that the FDIC's response to a breach has concluded, the SAOP shall report that status to FDIC SOC along with the outcome of the response.

As part of the FDIC's formal process for tracking and documenting a response to a breach, the FDIC has developed a standard internal reporting template, provided in Appendix D of this Plan. The Breach Report must be completed and centrally maintained by FDIC SOC for each FDIC breach and include, at minimum, the data elements and information required by M-17-12 and FDIC policy.

The FDIC currently uses CORSICA to track and document each reported breach. Among other things, CORSICA tracks and monitors the following, as required by OMB:

- The total number of breaches reported over a given period of time;
- The status of each reported breach, including whether the breach is open or closed;
- The number of individuals potentially affected by each reported breach;
- The types of information potentially compromised by each reported breach;
- Whether FDIC provided notification to the individuals potentially affected by a breach;
- Whether the FDIC provided services to the individuals potentially affected by a breach; and
- Whether a breach was reported to US-CERT and/or Congress.

13.2 Annual FISMA Reports

FISMA requires the FDIC to submit an annual report on the adequacy and effectiveness of information security policies, procedures, and practices, to include a description of major information security incidents and "major incidents" that involved a breach of PII.[43] In addition to those reporting requirements, the FDIC is required to include in its annual report descriptions of the FDIC's implementation of the requirements in OMB M-17-12.[44] At a minimum, the FDIC shall:

[43] 44 U.S.C. § 3554(c)(1)(A).
[44] 44 U.S.C. § 3554(c).

- Confirm that the FDIC satisfied all requirements in OMB M-17-12 for training and awareness with respect to breach reporting, or if not, explain why the FDIC did not satisfy those requirements in OMB-M-17-12 and what steps the FDIC will take to satisfy those requirements in the next reporting period;
- Submit the number of breaches reported within the FDIC during the reporting period, the number of breaches reported by FDIC SOC to US-CERT, the number of breaches reported by the FDIC to Congress, as well as the number of potentially affected individuals;
- Submit the FDIC's BRP and certify that the plan has been reviewed and updated over the past 12 months, as appropriate;
- Submit the names and titles of the individuals on the FDIC's BRT and identify those individuals who were removed from the team or added to the team over the past 12 months; and
- Confirm that the members of the BRT participated in at least one tabletop exercise during the reporting period, or if not, explain why and what steps the FDIC will take to ensure that the BRT participates in a tabletop exercise during the next reporting period.

Appendix A: Glossary of Terms and Acronyms

GLOSSARY OF TERMS	
Term	**Definition**
Access	The ability or opportunity to gain knowledge of personally identifiable information.
Agency	Any executive department, military department, Government corporation, Government controlled corporation, or other establishment in the executive branch of the Government (including the Executive Office of the President), or any independent regulatory agency, but does not include: the Government Accountability Office; Federal Election Commission; the governments of the District of Columbia and of the territories and possessions of the United States, and their various subdivisions; or Government-owned contractor-operated facilities, including laboratories engaged in national defense research and production activities.[45]
Agency and/or Business Sensitive Information (BSI)	A subset of Sensitive Information that contains identifying information about the Corporation, another government agency, a company, or other business entity that could be used to commit or facilitate the commission of fraud, deceptive practices, or other crimes (*e.g.*, unauthorized sharing of bank account information, trade secrets, or confidential or proprietary business information). Commercial information is not confined to records that reveal basic commercial operations, but it includes any information in which the submitter has a commercial interest, and may include information submitted by a nonprofit entity. Other terms for BSI that must be protected from disclosure are: "confidential business information," "business identifiable information," "confidential commercial information," and "proprietary information."
Breach	An occurrence that involves the loss of control, compromise, unauthorized disclosure, unauthorized acquisition, or any similar occurrence where (1) a person other than an authorized user access or potentially access PII or (2) an authorized user accesses PII for an other than authorized purpose.
Breach Response Plan	The agency's formal document that includes the policies and procedures that shall be followed with respect to reporting, investigating, and managing a breach of PII.
Breach Response Team	The team of specific agency officials, as designated in the agency Breach Response Plan, with responsibility for evaluating the risk to individuals from a Breach and the available options for mitigating that risk. The Breach Response Team through the SAOP serves as the primary advisor to the agency head in making determinations regarding breach notification and the services that should be provided to individuals in the context of a specific breach.
Breach that Constitutes a "Major Incident"	Per OMB M-18-02, a breach constitutes a "major incident" when it involves PII that, if exfiltrated, modified, deleted, or otherwise compromised, is likely to result in demonstrable harm to the national security interests, foreign relations, or economy of the United States, or to the public confidence, civil liberties, or public health and safety of the American people. An unauthorized modification of, unauthorized deletion of, unauthorized exfiltration of, or unauthorized access to 100,000 or more individuals' PII constitutes a "major incident."
Contractor	An individual, corporation, partnership, joint-venture, or other third party entity

[45] 44 U.S.C. § 3502

	that enters into a contract with FDIC to provide goods or services. This term is inclusive of contractors, vendors and outsourced service providers.
CORSICA	The FDIC's system for tracking incidents and breaches. The incident record must contain current, accurate and complete facts about the incident.
Division or Office	A business sector of the FDIC responsible for a program area or line of business (e.g., resolutions and receivership, supervision, etc.) or other defined section of work within the FDIC (e.g., administration, information technology, etc.). Affected Division/Office: The Division/Office that experienced the breach or whose employee/contractor caused the breach. In cases where the Division/Office that experienced the breach is not the same Division as the one that caused the breach, the RHA and other associated breach tasks should be completed by the Division/Office that caused the breach (in consultation with the Division/Office that experienced the breach as needed).
FDIC Information	As defined by the FDIC Records and Information Management Policy Manual, the term information applies broadly to all kinds of documents and data, which may be processed by or stored in any kind of communication, storage, or record-keeping system.
Federal information	Information created, collected, processed, maintained, disseminated, or disposed of by or for the Federal Government, in any medium or form, and includes the definition of "records" in 44 U.S.C. 3301(A) of the Federal Records Act.[46]
Federal information system	An information system used or operated by an agency, by a contractor of an agency, or by another organization on behalf of an agency.[47]
Harm	For the purposes of this document, harm means any adverse effects that would be experienced by an individual or organization (e.g., that may be socially, physically, or financially damaging) whose information was breached, as well as any adverse effects experienced by the organization that maintains the information.
High Value Asset	As defined by OMB M-16-04, those assets, systems, facilities, data, and datasets that are of particular interest to potential adversaries. These assets, systems, and datasets may contain sensitive controls, instructions, or data used in critical Federal operations, or house unique collections of data (by size or content) making them of particular interest to criminal, politically motivated, or state-sponsored actors for either direct exploitation of the data or to cause a loss of confidence in the U.S. Government. Each FDIC Division/Office is responsible for identifying those assets within Division/Office which meet the criteria for a "high value asset" as defined above.
Identity Theft	The act of obtaining or using an individual's identifying information without authorization in an attempt to commit or facilitate the commission of fraud or other crimes. The resulting crimes usually occur in one of the following ways. Identity thieves may attempt to: • Gain unauthorized access to existing bank, investment, or credit accounts using information associated with the person; • Withdraw or borrow money from existing accounts or charge purchases to the accounts; or • Open new accounts with a person's identifiable information without that

[46] *See* OMB Circular No. A-130, *Managing Information as a Strategic Resource* (OMB, July 2016).
[47] *Ibid.*

	person's knowledge
Incident	An occurrence that (1) actually or imminently jeopardizes, without lawful authority, the confidentiality, integrity, 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.[48]
Major Incident	Per OMB M-18-02, any incident that is likely to result in demonstrable harm to the national security interests, foreign relations, or economy of the United States or to the public confidence, civil liberties, or public health and safety of the American people.
Mitigate	To make less severe, to partially remove, or to correct, so that harmful potential effects of an incident are reduced or eliminated.
Personally identifiable information	Information that can be used to distinguish or trace an individual's identity, either alone or when combined with other information that is linked or linkable to a specific individual.[49]
Privacy	The right to be left alone and to control the conditions under which information pertaining to a person is collected, maintained, used, and disseminated. Privacy is the state of being free from unsanctioned intrusion. As an issue, privacy pertains to personal information-data that can be linked to an individual human being. In other words, all personal information requires privacy considerations. When handling personal data of any kind, it is important to take steps to assure privacy of the information. Privacy is both a good practice and mandated by law.
Professional Need to Know	Specific and limited information necessary to complete assigned work, in the case of performing official business.
Routine Breach	A "routine" breach refers to any breach of PII that does not meet the threshold for defining it as a significant breach.
Security	Administrative, physical, and technical safeguards, used to control access and protect information from accidental or intentional disclosure to unauthorized persons and from alteration or destruction, to maintain the integrity of the information.
Security or System Detected Incident	An incident in which FDIC IT Security personnel detect the loss, theft, or compromise of FDIC data via computer monitoring tools, automated security scans, data loss prevention capabilities, etc.
Senior Agency Official for Privacy	The senior official, designated by the head of each agency, who has overall agency-wide responsibility for privacy, including implementation of privacy protections, compliance with Federal laws, regulations, and policies relating to privacy, management of privacy risks at the agency, and a central policy-making role in the agency's development and evaluation of legislative, regulatory, and other policy proposals.[50]
Sensitive Information (SI)	Any information, the loss, misuse, or unauthorized access to or modification of which could adversely impact the interests of FDIC in carrying out its programs or the privacy to which individuals are entitled. Examples of SI include: 1. Information that is exempt from disclosure under the Freedom of Information Act (FOIA) such as trade secrets and commercial or financial information, information compiled for law enforcement purposes, personnel

[48] 44 U.S.C. § 3552
[49] *See* OMB Circular No. A-130, *Managing Information as a Strategic Resource* (OMB, July 2016).
[50] *Ibid.*

	and medical files, and information contained in bank examination reports (*see* FDIC Rules and Regulations, 12 C.F.R. Part 309, for further information); 2. Information under the control of the FDIC contained in a Privacy Act system of record that is retrieved using an individual's name or by other criteria that identifies an individual (*See* FDIC Rules and Regulations, 12 C.F.R. Part 310, for further information); 3. PII about individuals maintained by the FDIC that if released for unauthorized use may result in financial or personal damage to the individual to whom such information relates. Sensitive PII, a subset of PII, may be comprised of a single item of information (*e.g.,* SSN) or a combination of two or more items (*e.g.,* full name along with, financial, medical, criminal, or employment information). Sensitive PII presents the highest risk of being misused for identity theft or fraud; 4. Information about insurance assessments, resolution, and receivership activities, as well as enforcement, legal, and contracting activities; and 5. Any information properly marked as Controlled Unclassified Information.
Significant Breach	A "significant" breach refers to a breach of PII that: • Constitutes a "major incident,"[51] or potentially affects a large number of individuals or high-profile individuals; • Is anticipated to create an overwhelming increase of phone or email traffic; inability or significantly reduced ability to fulfill core FDIC business functions; significant damages or costs associated with breach; and/or • Has generated or has the potential to generate extensive media attention, Congressional inquiries, or other negative exposure requiring high-level coordinated response.
User	Refers to an FDIC employee, contractor, intern, vendor, outsourced provider, or other individual (*e.g.,* non-FDIC government employee) with authorized access to FDIC data, whether in hard copy (paper) or electronic format.
Violation	Infraction of a law; or an action or inaction contrary to established Federal laws or rules.

ACRONYMS	
Acronym	**Meaning**
ASB	Acquisition Services Branch
CISO	Chief Information Security Officer
CIO	Chief Information Officer
CIOO	Chief Information Officer Organization
COO	Chief Operating Officer
CPO	Chief Privacy Officer
SOC	Security Operations Center
FDIC	Federal Deposit Insurance Corporation
LERS	Labor and Employee Relations
OCISO	Office of the Chief Information Security Officer

[51] *See* OMB M-18-02, *Fiscal Year 2017-2018 Guidance on Federal Information Security and Privacy Management Requirements* (OMB, October 2017).

OCOM	Office of Communications
OIG	Office of Inspector General
OLA	Office of Legislative Affairs
NCCIC	National Cybersecurity and Communications Integration Center
NCISS	NCCIC Cyber Incident Scoring System
PII	Personally Identifiable Information
PSC	Privacy Section Chief
SAOP	Senior Agency Official for Privacy
SEPS	Security Emergency Preparedness Section
SSN	Social Security Number
US-CERT	United States Computer Emergency Readiness Team

Appendix B: BRT Core Members and Consultative Officials

Breach Response Team (BRT) Core Members Designated by FDIC Chairman April 16, 2018
Member
Senior Agency Official for Privacy (SAOP) / Chief Privacy Officer (CPO)
Chief Information Officer (CIO)
Chief Operating Officer (COO)
Chief Information Security Officer (CISO) / Deputy CPO
Incident Coordinator
Privacy Section Chief (PSC)
General Counsel
Office of Communications (OCOM) Director
Office of Legislative Affairs (OLA) Director

Consultative Group/Official
Divisional Directors, ISMs, and/or Incident Response POC(s), as applicable
FDIC Insider Threat and Counterintelligence Program Representative(s)
Office of Inspector General (OIG)
DOF Director (or designee)
DOF Risk Management and Internal Control (RMIC)
Chief Acquisitions Officer (CAO)/DOA Acquisitions Services Branch (ASB) Deputy Director (or designee)
DOA Library & Public Information Center (PIC) Assistant Director (or designee)
DOA Call Center Chief; PIC Assistant Director
DOA Security and Emergency Preparedness Section (SEPS) Assistant Director (or designee)
DOA Human Resources/Labor and Employee Relations (LERS) Chief (or designee)
DCP Consumer Response Center (CRC) Chief (or designee)
Federal, State or Local Law Enforcement
DIT Director (or designee)
Office of the Ombudsman (Ombudsman or designee)
Internal Ombudsman (or designee)
Chief Web Master (or designee)
FDIC Program Area Specialists

Appendix C: Roles and Responsibilities Matrix

The following table outlines the roles and responsibilities of key stakeholders (including both individuals and groups) involved in the breach response process. The table is organized in a loosely sequential manner, starting with the roles and responsibilities related to breach reporting; followed by those for investigation, remediation and risk assessment with focus on FDIC SOC, the affected Division/Office, and CIOO/OCISO; and concluding with those pertaining to breach recovery, with focus on the Breach Response Team core and consultative officials.

ROLES	RESPONSIBILITIES
FDIC Users[52]	All FDIC users, including FDIC employees, contractors, or other individuals or entities with access to FDIC information and/or information systems, are responsible for: • Completing FDIC's annual Information Security and Privacy Awareness Training or comparable training, which addresses how to identify, report and respond to a breach; • **Immediately** reporting a suspected or confirmed breach to the FDIC Help Desk/SOC (at *999 or 1-877-334-2999) and immediate Supervisor or Oversight Manager; • Providing all relevant information in the initial notice to the FDIC Help Desk/SOC, including but not limited to: (a) the type of data affected (e.g., name, SSN, address, etc.) and (b) the amount of records or data affected; • Reporting all instances associated with criminal activity, theft, suspicious activity, and lost/stolen property or equipment that occur on FDIC premises to the Security and Emergency Preparedness Section (SEPS);[53] • Reporting to Local Law Enforcement Agency (LLEA) as appropriate if the incident involves a theft or loss of their FDIC-furnished property/equipment; • Obtaining investigation results and submitting it to FDIC SOC; and • Cooperating with and participating in the investigation, hearing, or other inquiry by the FDIC and law enforcement agencies regarding the incident. *Note: The BRP requirements supplement, but do not replace, the procedures set forth in FDIC Circular 1360.12, Reporting Computer Security Incidents, which employees and contractors must review and abide by. For additional guidance, the user should refer to the DIT "Security Incident Reporting" webpage.*
Immediate Supervisor or Oversight	This is the immediate senior FDIC employee to whom the FDIC employee or contractor (user) reports. The Supervisor or Oversight Manager is responsible for: • Ensuring that the user ***immediately*** contacts the FDIC Help Desk/SOC and, in case of theft or loss of equipment, SEPS or LLEA *upon discovery of loss or potential loss* of PII; • Coordinating with FDIC SOC or other FDIC officials in documenting the incident

[52] Not all user requirements listed in this section are applicable to outsourced services providers, office visitors, and government agencies and organization with authorized access to FDIC data; nonetheless, these individuals must immediately report the loss, theft, or compromise of FDIC sensitive information, including PII, to the FDIC. Additional requirements for protecting FDIC-provided data are outlined in applicable contractual and/or sharing agreements between the entity/agency and FDIC.

[53] Individuals should report all security concerns to the guard on duty. After contacting the guard on duty, individuals should inform the Chief, Physical Security Office, SEPS, at 703-562-2276.

Manager	upon request; • Assisting their employees and contractors in identifying and properly securing PII appropriately; and • Participating in the development and/or execution of a corporate response plan in the event of loss or compromise of PII.
FDIC Help Desk	The FDIC Help Desk serves as a central point of contact, available 24 hours a day, seven days a week, for receiving notification of lost or compromised PII. The FDIC Help Desk is responsible for: • Opening a ticket in the FDIC Incident Response Database; and • Collecting basic information from the user in order to populate the FDIC SOC Breach Report.
Security Operations Center (SOC)	The FDIC SOC is a team of information security professionals within the Office of the Chief Information Security Officer (OCISO) that provides centralized technical assistance to investigate, resolve, and close computer security vulnerabilities and other incidents, including but not limited to those involving a breach in any medium or format (verbal, paper and electronic). FDIC SOC is responsible for: • Opening a ticket in the FDIC Incident Response Database (CORSICA) or responding to the ticket generated by the Help Desk; • Collecting facts and required information from the user and documenting them in CORSICA – FDIC SOC may contact the user's immediate Supervisor or Oversight Manager to obtain additional information; • Identifying the affected Division(s); • Assigning a preliminary priority level/risk classification to the breach based on the facts known at the time and adjusting the classification based on the results of the investigation and OCISO and BRT feedback, as applicable; • Notifying the United States Computer Emergency Readiness Team (US-CERT) and applicable internal stakeholders about the breach, highlighting and appropriately escalating those that may be "major" or otherwise significant in nature; • Conducting or supporting the breach investigation and technical remediation as directed by the Incident Coordinator; • Coordinating with the affected Division(s) as needed to ascertain the nature of the impacted data and ensure compliance with all Federal and FDIC requirements; • Coordinating with the Security and Emergency Preparedness Section (SEPS) as applicable if physical loss is involved; • Creating and maintaining a timely, accurate and complete incident record and Breach Report in CORSICA and submitting all collected data to the SAOP, CISO, PSC, affected Division, and BRT when convened, and assisting these FDIC officials in technically analyzing the information about the breach upon request; • Providing a report to the SAOP and designees (CISO and PSC) at the end of each fiscal quarter detailing the status of each breach reported to the FDIC SOC during the fiscal year; and • Participating in the annual tabletop exercise, as required.
AFFECTED DIVISION[54]	

[54] Each Division-specific role identified here may not always be represented for each Division.

Affected Division Director	The Director of the affected Division refers to the FDIC senior-official who heads the FDIC Division or Office that owns or maintains the PII that was involved in the breach and/or whose employee(s) and/or contractor(s) were involved in or responsible for the breach. This may be the same Division in many cases, but is not always the same Division. The affected Division also provides any necessary resources to support the breach investigation, remediation and recovery efforts, as identified by the Incident Coordinator or FDIC SOC, as outlined below and in the BRP. The Director of the affected Division is responsible for: • Participating in or designating a senior-level Divisional official to participate in the BRT, if requested by the SAOP; • Participating in or designating a senior-level Divisional official to participate in, as well as potentially provide feedback on, the annual tabletop exercise, if requested by the SAOP; • Bearing, or designating to a senior-level Divisional official, overall accountability for ensuring the timeliness and effectiveness of the affected Division's breach response and recovery efforts; • As requested, advising the SAOP/CPO, in consultation with the CISO and PSC, on whether breach notification, guidance, services or any further actions are required, including whether a breach constitutes a "major incident" (as defined by OMB); and • Assisting CIOO/OCISO with identifying and ensuring sufficient logistical and technical resources (internal and external) to respond and recover from a breach.
Divisional Incident Lead	The Divisional Incident Lead is the Divisional Information Security Manager (ISM) or another designated Divisional Incident Response (IR) point of contact (POC) who is responsible for supporting the FDIC SOC on behalf of the affected Division. The Incident Lead is responsible for: • Serving as liaison with data/systems owners involved in breach, facilitating Divisional compliance with Federal and FDIC requirements; • Assisting with the investigation/technical remediation as requested by FDIC SOC; • Conducting and documenting a preliminary risk of harm assessment in CORSICA; • Identifying and analyzing, with support from OCISO and Legal, applicable privacy compliance documentation, information sharing agreements, contracts or other artifacts governing or pertaining to the affected Division's breached information systems or information; • Participating in the BRT and annual tabletop exercise, if requested by the SAOP, and taking action on any requested items associated with these (such as providing feedback at the conclusion); • Providing and verifying required information and drafting initial notification, guidance, and/or services to affected individuals in coordination with Legal, OCISO, and OCOM; • When required, taking the lead in preparing, vetting, and issuing (or otherwise facilitating) notification, guidance, and/or services to banks and/or regulators in coordination with Legal, OCISO, and OCOM; and • Participating in and documenting in CORSICA the post-breach analysis of Congressionally-reported breaches.

Divisional Information Security Manager (ISM)	The Divisional ISM is the FDIC employee assigned to facilitate Divisional compliance with FDIC security/privacy circulars, implement business-specific security practices, and serve as the primary liaison between the Office of the Chief Information Security Officer (OCISO) and the ISM's Division/Office. The ISM serves as the Divisional Incident Lead (unless the Division designates another IR POC to serve in the role), and as such, is responsible for completing or assisting with the responsibilities listed in the Incident Lead section above. The ISM is responsible for: • Helping to ensure that PII is adequately protected through his/her participation in FDIC's Information Security Risk Management Program; • Serving as (if designated by the affected Division) or assisting the Divisional Incident Lead and coordinating with any additional Divisional IR POC(s) in the Regions, Field, or Headquarters; and • Participating in the BRT and annual tabletop exercise, if requested by the SAOP.
Divisional Incident Response (IR) Points of Contact (POCs)	Additional Divisional IR POCs may be designated by the Division to assist the Incident Lead with managing the incident to closure. For example, members of the Divisional IT Security Group, Divisional Internal Review Group, or other Regional, Headquarters or Field Office staff may be designated by the Division/Office to serve as the Divisional Incident Lead and/or Divisional IR POCs, so long as they receive sufficient training. Divisional IR POCs may also be required to participate in the BRT and annual tabletop exercise if requested by the SAOP.
Divisional Database Administrator (DBA)	The DBA is the individual responsible for the installation, configuration, administration, monitoring and maintenance of systems/databases for the Division/Office. In the event of a breach, the DBA, in coordination with the Divisional ISM/Incident Lead and other FDIC officials, analyzes the system breach and determines which records may be affected, as well as helps the affected Division as needed in identifying any applicable privacy compliance documentation, information sharing agreements, contracts or other relevant agreements or artifacts governing the impacted systems.
CHIEF INFORMATION OFFICER ORGANIZATION (CIOO)	
Senior Agency Official for Privacy (SAOP)	At the FDIC, the Chief Information Officer serves as the Senior Agency Official for Privacy (SAOP), also referred to as the Chief Privacy Officer (CPO). The SAOP/CPO 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, the SAOP/CPO is responsible for: • Deciding whether the FDIC's response can be conducted at the staff level or whether the BRT must be convened, in consultation with the CISO and PSC; • Convening the BRT as appropriate and ensuring appropriate subject matter experts (SMEs) are included or consulted, based on feedback from the CISO, PSC and Incident Coordinator; • Leading or designating the Breach Commander (CISO or Incident Coordinator) to lead the BRT when convened, as well as to oversee the breach investigation and technical remediation; • Providing the BRT's recommendation to the Chairman of whether a breach constitutes a "major incident" (as defined by OMB) and requires Congressional and OIG reporting, in consultation with the CISO, PSC and BRT when convened; • Coordinating with or designating the CISO and/or Incident Coordinator to coordinate with identified FDIC officials to ensure that law enforcement, OIG, General Counsel, and other oversight entities are involved and/or receive timely notification when appropriate; • With support from the affected Division and PSC, and the BRT when convened,

	conducting and documenting in CORSICA a breach risk of harm assessment and recommended course of action to mitigate the risk of harm, including whether/what countermeasures, notification, guidance and/or services should be provided to individuals potentially affected by the breach; • Notifying the FDIC Chairman/Executive Office (EO) of the BRT's recommended course of action for significant breaches, including whether to provide notification, guidance, or other services to potentially affected individuals, as applicable; • Serving as the source of notification (as designated by the Chairman); • Overseeing or designating the PSC to oversee the notification effort, in coordination with the affected Division and other stakeholders, and selecting the notification method for significant breaches; • Reviewing and concurring or non-concurring with the PSC's recommendation for non-significant (routine) breaches, including the appropriate course of action and whether to provide notification, services, and guidance to potentially affected individuals as applicable; • Determining or designating the Incident Coordinator, with input from the PSC, to determine when the response to a breach has concluded; and • Conducting the post-breach analysis of lessons learned for Congressionally-reported breaches. In addition, the SAOP and/or designees (CISO and PSC) are responsible for: • Conducting an annual tabletop exercise to test the BRP; • Implementing and reviewing, at minimum annually, this BRP to ensure it is current, accurate and compliant with legal, regulatory and internal requirements; • Ensuring that all agency Privacy Act SORNs include routine uses for the disclosure of information necessary to respond to a breach, in coordination with Legal; • Reviewing and updating, as needed, all applicable privacy compliance documentation (e.g., SORNs, PIAs, and privacy notices), in coordination with Legal, the Division/Office, and BRT when convened; • Identifying and ensuring sufficient logistical capabilities to respond to a breach; • Ensuring that FDIC SOC personnel are properly trained to identify a breach, and are duly apprised of the status and outcome of the breach response; • Providing guidance on any exceptions to the requirement to report a suspected or confirmed breach; • Reviewing and validating the quarterly report from FDIC SOC that details the status of each breach reported during that fiscal year; and • Submitting the updated BRP as part of annual FISMA reporting.
Chief Information Officer (CIO)	The CIO is responsible for delivering core IT services consistent with existing service levels; achieving, delivering, and supporting FDIC performance goals, Capital Investment Review Committee projects, and CIO Council projects; managing the IT portfolio to reduce risks and costs while maintaining appropriate service levels; and improving processes used in all of the previously mentioned items. The CIO is responsible for: • Identifying technical remediation and forensic analysis capabilities that exist within the FDIC to respond to a breach, and which offices are responsible for maintaining those capabilities (if gaps are identified, the CIO is also responsible for communicating with the Chief Acquisitions Officer and other FDIC officials

	on the need to enter into contracts or to explore other options for ensuring that certain functions are immediately available during a time-sensitive response); • Considering whether other Federal agencies can support the FDIC in the event of a breach (such as requesting technical assistance from US-CERT, leveraging GSA BPAs and other guidance, etc.); • Participating in or designating a senior-level official to participate in the BRT when convened and the annual tabletop exercise; • Assisting with the assessment of risk of harm to potentially affected individuals; and • Accepting and approving of the risk of not encrypting all FIPS 199 moderate-impact and high-impact information at rest and in transit, if the information compromised was not encrypted to those standards.
CIOO BREACH ADMINISTRATIVE SUPPORT	
SAOP Program/Special Assistant or Other Administrative Personnel	The SAOP Program Assistant and/or Special Assistant (or other administrative personnel designated by the SAOP or designees [CISO and PSC]) are responsible for handling all administrative support to coordinate the BRT meeting. The responsibilities include, but are not limited to: • Scheduling the BRT meeting and handling all associated meeting logistics, including but not limited to reserving a conference room; providing a teleconference number; sending out/updating the meeting invite; obtaining and distributing electronic copies of all relevant BRT briefing materials; preparing and distributing hardcopy materials at the BRT meeting; • Preparing, updating as requested, and distributing BRT meeting minutes, action items and materials; • Preparing executive summaries of discussions; • Scheduling lessons learned meetings; • Vetting communications materials with executives for approval; and • If designated, serving as or assisting the BRT RHA Scribe (refer to the BRT Scribe for more information).
BRT RHA Scribe	The BRT RHA Scribe refers to the CIOO or OCISO Program or Special Assistant or other administrative personnel designated by the SAOP, CISO, or PSC. During a BRT meeting, the BRT RHA Scribe is responsible for documenting the RHA real-time and ensuring it is documented in CORSICA in a timely, accurate, and complete manner. In addition, the BRT RHA scribe is responsible for preparing an executive summary (see Appendix M) of the BRT's risk assessment and assisting the SAOP with vetting it for approval. *Note: If the BRT Scribe does not have access to CORSICA, the BRT Scribe may provide the completed RHA form to the Incident Coordinator and Divisional Information Security Manager (ISM)/Incident Lead for uploading to CORSICA subsequent to the BRT meeting.*
OFFICE OF THE CHIEF INFORMATION SECURITY OFFICER (OCISO)	
Chief Information Security Officer (CISO)	The CISO manages the FDIC's information security and privacy programs, including but not limited to developing the FDIC's security policy and establishing and managing the FDIC's Privacy Program. The CISO serves as the Deputy CPO and assists the SAOP/CPO in fulfilling the breach-related responsibilities outlined in OMB M-17-12, in conjunction with the affected Division, Office of the Chief Information Security Officer, Privacy Section Chief, and the Breach Response Team when convened. Specifically, the CISO is responsible for the following: • Serving as or designating an Incident Coordinator to serve as the Breach

	Commander and lead the breach investigation and remediation effort; • Advising the SAOP/CPO, in consultation with the PSC and Incident Coordinator, on whether to convene the BRT, when notification or any further actions are required, as well as whether a breach meets current OMB criteria for classification as a "major incident;" • Participating in the BRT when convened; • Identifying and ensuring sufficient logistical and technical resources (internal and external) to respond and recover from a breach, in consultation with the PSC, the affected Division, and other relevant stakeholders; • Periodically testing and evaluating the effectiveness of information security/privacy incident handling policies, procedures and practices; • Overseeing the development and execution of the annual tabletop exercise, with support from the Incident Coordinator, PSC, and other CIOO/OCISO personnel as required; and • Participating in the post-breach analysis of Congressionally-reported breaches to evaluate lessons learned, as needed, to provide insight and help identify security control enhancements, process improvements and any other lessons learned to improve the overall incident response capability.
Privacy Section Chief (PSC)	The PSC advises the SAOP/CPO and CISO in the development, daily operation, and management of the FDIC Privacy Program. These efforts include the development, implementation and maintenance of, and adherence to, the FDIC policies and procedures related to privacy and data protection. The PSC leads initiatives to strengthen information privacy protections. The PSC is responsible for: • Reviewing, approving and providing guidance to the Divisional Incident Lead and any other Divisional personnel, Incident Coordinator (or FDIC SOC liaison), and BRT as needed in assessing the risk of harm to individuals potentially affected by a breach (note: this responsibility may be designated to the Head of the affected Division or Office); • Participating in the BRT and serving as the Deputy Breach Commander for significant breaches as requested and in accord with established standard operating procedures; • Coordinating with the CISO on significant breaches to advise the SAOP/CPO regarding (1) whether to convene the BRT, (2) whether breach notification, guidance, services, or other countermeasures are required based on the assessed risk of harm, and (3) whether a breach constitutes a "major incident" (as defined by OMB); • Determining whether any consultative officials should be convened to assist with responding to the breach, and convening/scheduling and leading those consultative officials for routine breaches as applicable; • Providing a recommendation to the CISO and SAOP regarding whether to provide notification, guidance, and/or services to potentially affected individuals based on the assessed risk of harm for routine breaches; • Selecting the notification method and overseeing the breach notification process in consultation with the Division and on behalf of the SAOP/CPO for routine breaches; • Participating in and/or assisting the SAOP/CPO with planning, conducting, and facilitating BRT training and the annual tabletop exercise as requested; • Participating in the post-breach analysis of Congressionally-reported breaches to evaluate lessons learned;

	• Approving breach for closure in coordination with the Incident Coordinator; and • Assisting the SAOP/CPO with overseeing updates to the BRP, at least annually and whenever there is a material change.
Incident Coordinator	The Incident Coordinator is an FDIC employee assigned to ensure that any known or suspected breaches are appropriately managed to closure. The CISO may serve as or designate the Incident Coordinator as required. The Incident Coordinator is responsible for: • Participating in the BRT and serving as the Breach Commander for significant breaches as requested by the CISO; • Acting as a liaison between OCISO/CIOO, FDIC SOC, technical resources, and the affected Division; • Overseeing the incident investigation and ensuring appropriate technical and remedial actions are taken; • Ensuring the timeliness, accuracy, and completeness of the CORSICA incident record and Breach Report; • Reviewing and assisting with the risk of harm assessment and recovery/notification effort as requested by the CISO or PSC; • Keeping the SAOP/CPO, CISO, PSC, and BRT duly apprised of the status of breaches as needed and promptly informing the SAOP/CPO, CISO, PSC, and other relevant stakeholders of any suspected or confirmed breaches that constitute a "major incident" (as defined by OMB) or are otherwise significant in nature; • Reviewing and authorizing breach closure, with input from the PSC; • Participating in and facilitating as requested the post-breach analysis of Congressionally-reported breaches to evaluate lessons learned; and • Helping develop and execute the annual tabletop exercise, as requested.
BREACH RESPONSE TEAM[55]	
Breach Response Team (BRT)	The BRT is led by the SAOP/CPO (or designee) and comprised of FDIC officials who are designated by the Chairman to respond to a breach. The BRT is responsible for: • Assisting the SAOP with assessing the risk of harm of a breach and providing a recommendation to the Chairman via the SAOP of whether a breach constitutes a "major incident" (as defined by OMB) and requires Congressional and OIG notification; • Developing and managing an appropriate course of action to respond to a breach and mitigate harm to individuals, including providing notification, guidance, and services (e.g., identity protection and credit monitoring, call center services, etc.) or taking other countermeasures; • Participating in any required BRT training or tabletop exercises as requested by the SAOP or designee; and • At the direction of the SAOP or designee, reviewing FDIC implementation of this document to capture ongoing changes to resources and business environment.
Chief Operating Officer (COO)	In the event of a "significant breach" or identification of a breach that constitutes a "major incident" (as defined by OMB), the COO participates in the BRT and assists with reviewing Congressional and OIG notification for breaches that constitute "major

[55] Refer to sections above for roles and responsibilities of BRT officials within CIOO/OCISO and affected Division.

	incidents." The COO is also responsible for participating in the annual BRT tabletop exercise, as required.
Legal Division General Counsel	The Legal Division General Counsel is responsible for: • Participating in and coordinating with the BRT in ensuring a Corporate response plan is successfully executed in compliance with federal laws and regulations; • Participating in the annual tabletop exercise, as required; • Ensuring all FDIC SORNs are accurate and complete, as well as assisting with reviewing privacy compliance documentation and information sharing agreements as required by OMB M-17-12; and • In the event of a breach, helping draft, review, and approve breach notification, guidance and communications (e.g., talking points, FAQs, call scripts, website content, etc.), as well as responses to FOIA, Privacy Act, Congressional or other breach-related inquiries and complaints received by FDIC.
Office of Communications (OCOM) Director	The OCOM Director is responsible for: • Participating in the BRT and annual BRT tabletop exercise, as required; • Developing and executing a Corporate-wide breach communications plan for significant breaches or other breaches as directed by the Chairman or designee; • Helping draft and approve external notification and communications (e.g., call center scripts, talking points, FAQs, and official responses to breach-related inquiries and complaints); • As appropriate, overseeing or coordinating with the affected Division regarding the establishment and operation of an official, electronic and centralized mechanism and process for receiving and responding to breach-related inquiries from media and the public; • Assisting with establishing and maintaining a dedicated FDIC-branded website or webpage to provide breach-related guidance or other information to the media and public, as required; and • Responding to media inquiries, and initiating and organizing any press release about the breach, if required.
Office of Legislative Affairs (OLA) Director	OLA serves as the Corporation's congressional liaison and closely monitors and responds to legislation important to the FDIC. The OLA Director is responsible for: • Serving as a central POC in notifying applicable committees and Members of Congress as appropriate about the breach, as well as in responding to requests from various Congressional committees, members, or their staff about the breach; • Participating in the BRT and reviewing external notification and communications for breaches that require Congressional reporting or otherwise bear or may trigger Congressional implications; and • Participating in the annual tabletop exercise, as required.
CONSULTATIVE OFFICIALS[56]	
FDIC Office of Inspector General (FDIC OIG)	The FDIC OIG is an independent unit that conducts audits, investigations, and other reviews of the Corporation's programs and operations, including the Privacy Program. In the event of a breach, particularly if there is suspected violation of criminal law, OIG will be notified by FDIC SOC so that the OIG can conduct an investigation as needed and/or cooperate with the FBI or other law enforcement agencies. OIG representatives

[56] The listing of consultative officials provided in this document is not intended to be exhaustive. Additional officials or bodies may be identified and consulted depending on the specific circumstances of the breach.

	will participate in the BRT and annual tabletop exercise at the discretion of OIG.
Division of Depositor and Consumer Protection (DCP) Consumer Response Center (CRC) Chief	The DCP Consumer Response Center (a part of the Consumer Affairs Program) is responsible for investigating consumer complaints involving FDIC-supervised banks, analyzing consumer complaint data, serving as a resource for examination staff, and educating consumers about consumer protection laws. In the event of a breach, the DCP Consumer Response Center Chief (or designee) is responsible for: • Assisting with managing, triaging, and responding to consumer inquiries and complaints in line with the FDIC-approved communications plan and scripts; • Transferring or forwarding questions deemed to be of a "technical nature" to the appropriate BRT member or other subject matter expert (SME); • Participating in the BRT, if requested by the SAOP, and working with the BRT to update the scripts, canned responses, and other guidance/communications to include new evolving issues or scenarios identified by the CRC; and • Providing CRC activity reports, such as the volume, type and disposition of correspondence or calls received in relation to the breach, and any other information as requested by the BRT.
Division of Information Technology (DIT) Director	DIT is responsible for providing various IT support services to the Corporation, as well as assisting with IT-related products provided by the FDIC to employees (e.g., laptops, mobile phones, software). DIT is also responsible for providing IT-related policy guidance. In the event of a breach involving IT systems or technology, the DIT Director (or designee) will participate in the BRT if requested by the SAOP and work with the BRT to provide DIT operations or technical support (such as root cause analysis, capture and review of large unstructured data sets [e.g., Hadoop], etc.).
Office of the Ombudsman Senior Specialist	The Office of the Ombudsman is an independent, neutral, and confidential resource and liaison for the banking industry and general public to facilitate the resolution of problems and complaints against the FDIC. In the event of a breach, the Ombudsman through the Senior Ombudsman Specialist (or designee) will participate in the BRT if requested by the SAOP and provide facilitation and problem resolution services for complaints or issues that may arise from a reported breach.
Internal Ombudsman	The Internal Ombudsman supports the mission of the FDIC by seeking resolution of work-related questions and concerns raised by all current employees and managers. In the event of a breach, the Internal Ombudsman will participate in the BRT if requested by the SAOP and provide facilitation and problem resolution services for complaints or issues that may arise from a reported breach.
Chief Web Master	In the event a breach involves or impacts the FDIC's public-facing website/webpages, the Chief Web Master (or designee) will work with the BRT as needed to investigate and remediate issues with FDIC's website as applicable; establish a new FDIC webpage; make appropriate updates to FDIC's existing website to provide guidance to potentially impacted individuals as requested; or assist with other web-related tasks as requested by the BRT.
Division of Finance (DOF) Director	DOF is responsible for providing accounting, financial, and employee services to the FDIC. In the event a breach may significantly impact the Corporation's financial operations or budget, the DOF Director (or designee) will participate in the BRT if requested by the SAOP and advise on and help implement any recommended courses of action involving or impacting the Corporation's financial operations or budget.
DOF Risk Management and Internal Control (RMIC) Branch	The RMIC manages internal controls and risks by maintaining partnerships with the Divisions and Offices, providing training, and addressing identified internal control deficiencies. In the event a breach points to a systemic risk that is not sufficiently addressed, the RMIC Branch Deputy Director (or designee) will participate in the BRT if

Deputy Director	requested by the SAOP and will work with the BRT in mitigating that risk.
Division of Administration (DOA) Acquisitions Services Branch (ASB) Deputy Director	ASB is responsible for procuring goods and services on behalf of the Corporation. ASB Contracting Officers (COs) and other ASB personnel work with Oversight Managers (OMs) and Technical Monitors (TMs) to monitor contractor performance, including all security requirements set forth in the contract. In accordance with M-17-12, the ASB Deputy Director or designated Chief Acquisition Officer (CAO), in coordination with the SAOP/CPO or designee(s), shall ensure that contract provisions to assist with the response to a breach are uniform and consistently included in agency contracts. In addition, in the event of a breach involving an FDIC contractor or vendor, or a breach requiring the procurement of new services, the ASB Deputy Director (or designee) will participate in the BRT if requested by the SAOP; provide guidance on any contracting issues raised by the breach; assist with the procurement of new services if applicable; and help advise on and implement any recommended courses of action involving contractor noncompliance or other contracting issues identified by the BRT.
DOA Library & Public Information Center (PIC) Assistant Director	The DOA Library & PIC supports the FDIC's research, reference, and information needs. In the event a breach may require the use of the FDIC/DOA Library Services, the DOA Library and PIC Assistant Director (or designee) will participate in the BRT if requested by the SAOP and will support the BRT by advising on and providing address lookup and verification services for notification purposes.
DOA Call Center Chief	The FDIC/DOA Call Center is the primary telephone point of contact for the banking industry and the general public. Callers reach the Call Center through a toll-free or direct phone number (1-877-ASK-FDIC or 703-562-2222) or a TDD (1-800-925-4618 or 703-562-2289.) In the event of a breach requiring internal call center services, the FDIC Call Center Chief (or designee) is responsible for participating in the BRT, if requested by the SAOP, and: • Ensuring that the FDIC Call Center personnel answer or transfer calls in line with the FDIC-approved communications plan and scripts; • Providing feedback and working with the BRT to update the scripts to address evolving issues or scenarios observed by Call Center personnel; and • Providing call center activity reports, such as the volume, type and disposition of calls received, and any other information as requested by the BRT.
DOA Human Resources/Labor and Employee Relations (LERS) Chief	DOA Human Resources/LERS is responsible for resolving workplace disputes, handling disciplinary and adverse actions, and facilitating employee grievance filings. In the event a breach is a result of employee misconduct or intentional actions, the DOA Human Resources/LERS Chief (or designee) will participate in BRT meetings if requested by the SAOP; work with the BRT to assess the likely risk of harm associated with the employee's actions and intent; and implement appropriate disciplinary actions or other courses of action as necessary.
DOA Security and Emergency Preparedness Section (SEPS) Assistant Director	The Security and Emergency Preparedness Section (SEPS) within the DOA Corporate Services Branch is responsible for personnel security, physical security, emergency operations, transportation, business continuity, insider threat, counterintelligence, and safety of all Corporation personnel. In the event of a breach, the SEPS Assistant Director (or designee) is responsible for: • Participating in the BRT, if requested by the SAOP; • Investigating the physical breach if it took place within FDIC territory; • Recording the breach in the FDIC Incident Reporting Investigation Unit Management System (TRIMS); • Coordinating with FDIC SOC, OCISO, and other relevant stakeholders to ensure all necessary steps are taken to contain and control the breach (e.g., changing

	locks, deactivating PIV cards, etc.); and • Reporting the breach results/fact findings to the authorized designees in CIOO, OCISO, and FDIC SOC.
DOA SEPS Insider Threat and Counterintelligence Program (ITCIP) Manager	The Security and Emergency Preparedness Section (SEPS) within the DOA Corporate Services Branch of the FDIC is responsible for personnel security, physical security, emergency operations, transportation, business continuity, insider threat, counterintelligence, and safety of all Corporation personnel. In the event of a breach, the SEPS Insider Threat and Counterintelligence Program (ITCIP) Manager (or designee) is responsible for: • Participating in the BRT, if requested by the SAOP; • Reviewing the breach for potential insider threat and counterintelligence indicators; • If two or more indicators are present, reporting the breach results/fact findings and applicable indicators to the ITCIP Working Group; • Conducting any required additional FDIC records reviews and interviews as agreed to by the ITCIP Working Group; and • If applicable, conduct and brief the results of an ITCIP assessment on the breach to the ITCIP Working Group and ITCIP Executive Committee. In addition, the ITCIP Manager or designee is responsible for participating in the annual BRT tabletop exercise, if requested by the SAOP.
FDIC EXECUTIVE OFFICE	
Head of Agency (Chairman)	In accordance with OMB M-17-12, the Chairman of the FDIC is responsible for: • Making a final determination, based on the recommendation from the SAOP and BRT when applicable, regarding whether to provide notification, guidance and/or services to individuals potentially affected by a significant breach; • Designating the FDIC officials who will serve on the FDIC's Breach Response Team (BRT); and • Designating, in writing, the SAOP to serve as the source of the notification to potentially affected individuals, when notification is necessary or otherwise required.
Executive Office	In the event of a "significant breach" or identification of a breach that constitutes a "major incident" (as defined by OMB), the Executive Office, in consultation with the Chairman, reviews and provides concurrence or feedback on the recommended course of action identified by the BRT. The Executive Office, in consultation with the Chairman, also reviews, approves and issues Congressional and OIG notification for breaches that constitute "major incidents."

Appendix D: Breach Report Template

This template may evolve and change over time. For the current version of this template, refer to CORSICA. Periodically, the template within this appendix will be updated to reflect the current version in CORSICA.

Federal Deposit Insurance Corporation
Security Operations Center (SOC)

BREACH REPORT

Date Last Updated: _____
Date Exported/Printed: _____
DRAFT / FINAL

SECTION 1 – GENERAL INFORMATION

CINC# (Data Breach Record #) – Affected Division – SOC Priority Level – Breach Type/Summary		
Date and Time Reported to SOC:	Date and Time of Breach:	Date and Time Reported to Division and Privacy:
Location of Breach:	If Date of Breach and Date of Reporting has considerable discrepancy in time (more than 24 hours), explain why.	

SUMMARY OF BREACH AND INVESTIGATION:

Summarize the facts or circumstances of the theft, loss or compromise of PII as currently known, including:

a. A description of what occurred and the parties involved in the breach (include dates and times)
b. The physical or electronic storage location of the information at risk
c. What steps were taken to investigate, contain and mitigate the breach (include dates and times)
d. Whether the breach is an isolated occurrence or a systematic problem
e. Who conducted the investigation of the breach, if applicable
f. Any other pertinent information

TYPE OF BREACH:

MEDIUM OF BREACH:

SECTION 2 – REPORTING

Reported to US-CERT: Y/N (If Yes, complete the following: Date and Time Reported; Name/Title of Reporting Official (*ATTACH US-CERT REPORT TO THIS FORM*)

Reported to Law Enforcement: Y/N (If Yes, complete the following: Date and Time Reported; Name of Law Enforcement Agency/Component; Name/Title of Reporting Official; and Police Report Number, If Applicable)

Reported to FINCEN: Y/N (If Yes, complete the following: Date and Time Reported; Name/Title of Reporting Official)

Reported to OIG: Y/N (If Yes, complete the following: Date and Time Reported; Name/Title of Reporting Official)

Reported to Congress: Y/N (If Yes, complete the following: Date and Time Reported; Name/Title of Reporting Official)

SECTION 3 – PARTIES POTENTIALLY IMPACTED

Category[57] and Number of Individuals Potentially Impacted: _____
Category/Name and Number of Entities Potentially Impacted: _____

SECTION 4 – SIGNIFICANT BREACH/MAJOR INCIDENT DESIGNATION

SIGNIFICANT AND/OR MAJOR INCIDENT DESIGNATION	Yes	No	Potentially
Significant Breach?	☐	☐	☐
Demonstrable harm/affects 100,000 individuals or more?	☐	☐	☐
Otherwise "significant?"	☐	☐	☐

[57] For example, FDIC employees; complainants; customers of BankABC; etc.

Is the incident a major incident per the US-CERT/NCCIC Cyber Incident Severity Schema (NCISS)? Date: _____	☐	☐	☐
NCISS Risk Rating: X points (Priority Level) *(ATTACH DETAILED NCISS SCORECARD AND ANY ADDITIONAL INFO PROVIDED TO/FROM US-CERT.)*			

SECTION 5 – SAFEGUARDS AND ADDITIONAL INFORMATION

SECTION 6 – INFORMATION TYPE AND DATA ELEMENTS

SECTION 7 – REPORTER'S INFORMATION

Reporter's Name	Reporter's Phone Number	Reporter's Current Location
Reporter's Email Address	Reporter's Job Title	
Incident reported via: *(Check One Only)* ☐ Email ☐ Phone ☐ Fax ☐ DLP ☐ Other _____	Is Reporter and Asset User the same person? *(Check One Only)* ☐ Yes ☐ No *(if "Yes," skip next five questions)*	
Asset User's Name	Asset User's Phone Number	Asset User's Current Location
Asset User's Email Address	Asset User's Job Title	
Asset User's Assignment and/or Position Description ☐ End User ☐ Help Desk ☐ ISM ☐Examiner	Asset User's Network ID	
Asset User's Supervisor's Name	Asset User's Supervisor's Telephone Number *(Include Area Code)*	

Asset User's Division or Office *(Check One Only)*

☐ Corporate University (CU)
☐ Division of Administration (DOA)
☐ Division of Depositor and Consumer Protection (DCP)
☐ Division of Finance (DOF)
☐ Division of Information Technology (DIT)
☐ Division of Insurance and Research (DIR)
☐ Division of Resolutions and Receiverships (DRR)
☐ Division of Risk Management Supervision (RMS)
☐ Legal Division
☐ Chief Information Officer Organization (CIOO)
☐ Office of the Chief Information Security Officer (OCISO)
☐ Office of Complex Financial Institutions (OCFI)
☐ Office of Inspector General (OIG)
☐ Office of Legislative Affairs (OLA)
☐ Office of Minority and Women Inclusion (OMWI)
☐ Office of Ombudsman
☐ Office of Communications (OCOM)
☐ Internal Ombudsman
☐ Executive Office (EO)
☐ Other _____

Was Asset User in violation of an FDIC policy? ☐ Yes ☐ No *(If "No," skip remaining questions in this section)*

Which FDIC policy was violated?	Is Asset User a repeat offender? ☐ Yes ☐ No *(If "No," skip next question)*

Provide details (number, date, summary) of past policy violations:

SECTION 8 – BREACH SIGNOFF

REMARKS:

Name of SOC Analyst Completing Report:	Date of Initial Report:	Date Last Updated:

Appendix E: Breach Risk of Harm Assessment Template and Guidance

The following Breach Risk of Harm Assessment template has been designed as a tool to facilitate and document (1) an assessment of the risk of harm to individuals caused by a breach of PII and (2) the actions the FDIC will take to mitigate the identified risks, as required by OMB M-17-12. Instructions and guidance are embedded in the template to assist users with its completion.

This template may evolve and change over time. For the current version of this template, refer to CORSICA. Periodically, the template within this appendix will be updated to reflect the current version in CORSICA.

Federal Deposit Insurance Corporation
Personally Identifiable Information (PII)

Breach Risk of Harm Assessment (RHA)

Date Last Updated: _____
Date Exported/Printed: _____
DRAFT / FINAL

Instructions: *In accordance with OMB M-17-12, the Senior Agency Official for Privacy (SAOP), in coordination with the Breach Response Team (BRT) when applicable, is responsible for the completion and approval of the Breach Risk of Harm Assessment (RHA). The BRT RHA scribe[58] will document their analysis using this form and enter it real-time into CORSICA during the BRT meeting.[59] The Divisional ISM/Incident Lead is responsible for completing a preliminary Breach Risk of Harm Assessment in CORSICA and submitting it electronically for OCISO and SAOP approval. Upon recommendation from the SAOP, the FDIC Chairman will provide final approval/disapproval for providing notification, guidance, and/or services to individuals potentially affected by a significant breach.*

SECTION 1 – GENERAL INFORMATION

SOC INC#:	<<INC#>>	**Affected Division:**	<< Division >>
Date(s) of BRT Risk Assessment:		**BRT RHA Scribe:**	

SECTION 2 – ASSESSING THE RISK OF HARM TO INDIVIDUALS

A. Nature and Sensitivity of PII: ☐ High (3) ☐ Moderate (2) ☐ Low (1) ☐ None (0)

Provide brief summary of evaluation of this factor. In the evaluation, consider the following items:

- *Data Elements (the sensitivity of each individual element of data as well as the sensitivity of all the data elements together)*
- *Context (the purpose for which the PII was collected, maintained, and used)*
- *Private Information (the extent to which the PII, in a given context, may reveal particularly private information about an individual)*
- *Vulnerable Populations (the extent to which the PII identifies or disproportionately impacts a particularly vulnerable population)*
- *Permanence (the continued relevance and utility of the PII over time and whether it is easily replaced or substituted)*

Refer to Section 7.1 of the BRP for additional guidance.

B. Likelihood of Access and Use of PII: ☐ High (3) ☐ Moderate (2) ☐ Low (1) ☐ None (0)

Provide brief summary of evaluation of this factor. In the evaluation, consider the following items:

- *Security Safeguards (whether the PII was properly encrypted or rendered partially or completely inaccessible by other means)*
- *Format and Media (whether the format of the PII may make it difficult and resource-intensive to use):*
- *Duration of Exposure (how long the PII was exposed)*
- *Evidence of Misuse (any evidence confirming that the PII is being misused or that it was never accessed)*

Refer to Section 7.2 of the BRP for additional guidance.

C. Type of Breach: ☐ High (3) ☐ Moderate (2) ☐ Low (1) ☐ None (0)

Provide brief summary of evaluation of this factor. In the evaluation, consider the following items:

- *Intent (whether the PII was compromised intentionally, unintentionally, or whether the intent is unknown)*
- *Recipient (whether the PII was disclosed to a known or unknown recipient, and the trustworthiness of a known recipient)*

Refer to Section 7.3 of the BRP for additional guidance.

[58] CIOO or OCISO Program/Special Assistant or other designated administrative personnel responsible for recording the SAOP and BRT's analysis and recommendations in this form real-time during the BRT meeting and ensuring it is documented accurately, timely, and completely in CORSICA.

[59] Alternatively, the BRT RHA scribe may provide the completed form to the Incident Coordinator and Divisional Information Security Manager (ISM)/Incident Lead for uploading to CORSICA subsequent to the BRT meeting.

Breach Classification

(Refer to Section 9 of the BRP for examples and guidelines for determining the breach classification.)

☐ **Code Red/Likely Risk (8-9 Points-Notification)** ☐ **Code Blue/Likely Risk (8-9 Points-No Notification)**

☐ **Code Green/Unlikely Risk (1-7 Points-No Notification)** ☐ **Code Orange/Unlikely Risk (0 Points-No Notification)**

SECTION 3 – RECOMMENDATION FOR MITIGATING THE RISK OF HARM

A. Countermeasures *(Refer to Section 10 of the BRP for guidance.)*

Are additional[60] countermeasures required? ☐ Yes ☐ No ☐ Potentially / TBD

If yes, describe: _____

B. Notification *(Refer to Section 11 of the BRP for guidance.)*

Based on the breach classification, select all to whom notification[61] is recommended.

☐ **Individuals** ☐ **Congress** ☐ **Financial Institutions (FIs)** ☐ **Regulators** ☐ **Other Entities (Specify.)**

Chairman Concurrence ☐ Yes ☐ No **Date:** _____

C. Services and Guidance *(Refer to Sections 10.2 and 10.3 of the BRP for guidance.)*

Select all services and guidance that are recommended.

☐ **Offering identity protection and/or credit monitoring services**
- Number of Individuals to be Provided Service: << >>
- Estimated Cost: << >>

☐ **Establishing a dedicated call center to handle inquiries about the breach**
- ☐ FDIC/DOA Call Center
- ☐ DCP Consumer Response Center
- ☐ Contracted Service Provider: << >>

☐ **Establishing a dedicated website/webpage addressing the breach**
- ☐ FDIC Site (Link: ____) ☐ Third-Party Site (Link: ____)

☐ **Issuing a press release addressing the breach**

☐ **Establishing a dedicated FDIC email inbox to respond to inquiries about the breach**
- ☐ FDIC (POC: << >>)
- ☐ Vendor (POC: << >>)

☐ **Offering guidance to potentially affected individuals** (Method of providing guidance << >>)
- ☐ Setting up fraud alerts or credit freezes
- ☐ Changing or closing accounts
- ☐ Taking advantage of services made available by FTC
- ☐ Changing passwords
- ☐ Encouraging use of multi-factor authentication for account access
- ☐ Other (Specify: _____)

☐ **Other** << Explain >>

Chairman Concurrence ☐ Yes ☐ No **Date:** _____ **Summary of Feedback (if applicable):** _____

SECTION 4 – COMPLIANCE DOCUMENTATION *(Refer to Section 2.3.2 of the BRP, and consult with Legal (FOIA/Privacy Act Group) and OCISO/Privacy as needed for guidance.)*[62]

1. Which systems of records notices (SORNs), privacy threshold analyses (PTAs), privacy impact assessments (PIAs), and/or privacy notices apply to the potentially compromised information? << >>	**3. Does any PII maintained as part of a system of records need to be disclosed as part of the breach response?** ☐ Yes ☐ No << If yes, is the disclosure permissible under the Privacy Act? How will the FDIC account for the disclosure? >>
2. Are the relevant SORNs, PTAs, PIAs, and/or privacy notices accurate and up-to-date?[63] ☐ Yes ☐ No	**4. Is any additional PII necessary to contact or verify the identity of individuals potentially affected?** ☐ Yes ☐ No << If yes, does that information require new or revised SORN(s) or PIA(s)? >>

SECTION 5 – INFORMATION SHARING *(Refer to Section 2.3 of the BRP, and consult with Legal and OCISO as needed for guidance.)*[64]

[60] Refer to Breach Report for countermeasures that have already been taken and/or are in process to mitigate the risk of harm.
[61] Divisional Incident Lead and IR POCs responsible for drafting and vetting notification.
[62] Contact privacy@fdic.gov for assistance with identifying and consulting with current Legal and Privacy POCs.
[63] As the data owner, the Division is responsible for ensuring its privacy compliance documentation is current, accurate, and complete. Whenever this is a material change impacting privacy, Divisions must reassess and submit revised privacy compliance documentation to Privacy (privacy@fdic.gov) for review. However, OMB M-17-12 requires additional due diligence and specific, documented confirmation that these artifacts have been reassessed to address the questions in Section 4 when there is a breach.
[64] Contact privacy@fdic.gov for assistance with identifying and consulting with current Legal and Privacy POCs.

To respond to the breach, will information sharing[65] with any of the following will be necessary? Check all that apply and specify systems, agencies or other entities with which information will be shared.

☐ With other systems within the FDIC (Specify: ____) ☐ With another agency (or agencies) (Specify: ____)
☐ With any non-Federal entities/third parties (Specify: ____)

If any of the above are checked, answer the following:

- Is the information sharing consistent with existing data use agreements, information exchange agreements, and/or memoranda of understanding? ☐ Yes ☐ No (Explain: ____)
- Will the information sharing require new or modified data use agreements, information exchange agreements, or memoranda of understanding? ☐ Yes ☐ No (Explain: ____)
- 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?

SECTION 6 – LESSONS LEARNED

Did the response to this breach result in any lessons learned or changes to the FDIC or Divisional BRPs, policies, training, or other documentation? ☐ Yes ☐ No **<<** If yes, document any lessons learned or changes based on lessons learned. **>>**

Date and Summary[66] of Post-Breach BRT Lessons Learned Meeting (only required for breaches reported to Congress): _____

SECTION 7 – ADDITIONAL COMMENTS

[65] When responding to a breach, the FDIC may need additional information to reconcile or eliminate duplicate records, identify potentially affected individuals, or obtain contact information in order to provide notification. The FDIC may need to combine information maintained in different information systems within the FDIC, share information between the FDIC and another agency, or share information with a non-Federal entity.

[66] In lieu of a summary, a copy of the Post-Breach Analysis and Lessons Learned Report may be attached/uploaded into CORSICA. Refer to Section 12 and Appendix F of the BRP for a template and guidance.

Appendix F: Post-Breach Analysis and Lessons Learned Template and Instructions

This template may evolve and change over time. For the current version of this template, refer to CORSICA. Periodically, the template within this appendix will be updated to reflect the current version in CORSICA.

FDIC Post-Breach Analysis and Lessons Learned Report

Date Last Updated: _____
Date Exported/Printed: _____
DRAFT / FINAL

Instructions: *This Post-Breach Analysis and Lessons Learned Report template is to be completed for all breaches that have been reported to Congress after the breach response has concluded. The SAOP shall convene the Breach Response Team (BRT) and all applicable stakeholders to evaluate and complete this form for single or multiple breaches reported to Congress, as appropriate. The affected Division/Office ISM(s) or designee shall record the BRT and other stakeholders' feedback in this form during the Lesson Learned meeting(s) and ensure the completed form is recorded in CORSICA in an accurate and timely manner.*

SECTION 1 – GENERAL INFORMATION

SOC INC#:	<<INC#>>	**Affected Division:**	<< Division >>
Lesson Learned Meeting Date(s):		**Division ISM(s)/Incident Lead(s) or Designee:**	

SECTION 2 – LESSONS LEARNED AND CURRENT/PLANNED MITIGATION ACTIVITIES

A. Technical

1. Did this breach raise any potential "lessons learned," in terms of improving the breach handling process and/or enhancing technical privacy/security controls over PII?	**Yes**	☐
	No	☐
<< Document any potential lessons learned, recommendations, and/or action items. >>		
2. Did the response to this breach result in any current or planned changes to the technical security or privacy controls? If not, were/are there specific challenges preventing the changes from occurring?	**Yes**	☐
	No	☐
<< Document any current or planned changes to technical controls based on lessons learned, and any challenges preventing the changes from occurring if applicable. >>		

B. Administrative

1. Did this breach raise any potential "lessons learned," in terms of improving the breach handling process and/or enhancing administrative privacy/security controls over PII?	**Yes**	☐
	No	☐
<< Document any potential lessons learned, recommendations, and/or action items. >>		
2. Did the response to this breach result in any current or planned changes to administrative security or privacy controls (i.e., the BRP, policies, training, or other documentation)? If not, were/are there specific challenges preventing the changes from occurring?	**Yes**	☐
	No	☐
<< Document any current or planned changes to administrative controls based on lessons learned, and any challenges preventing the changes from occurring if applicable. >>		

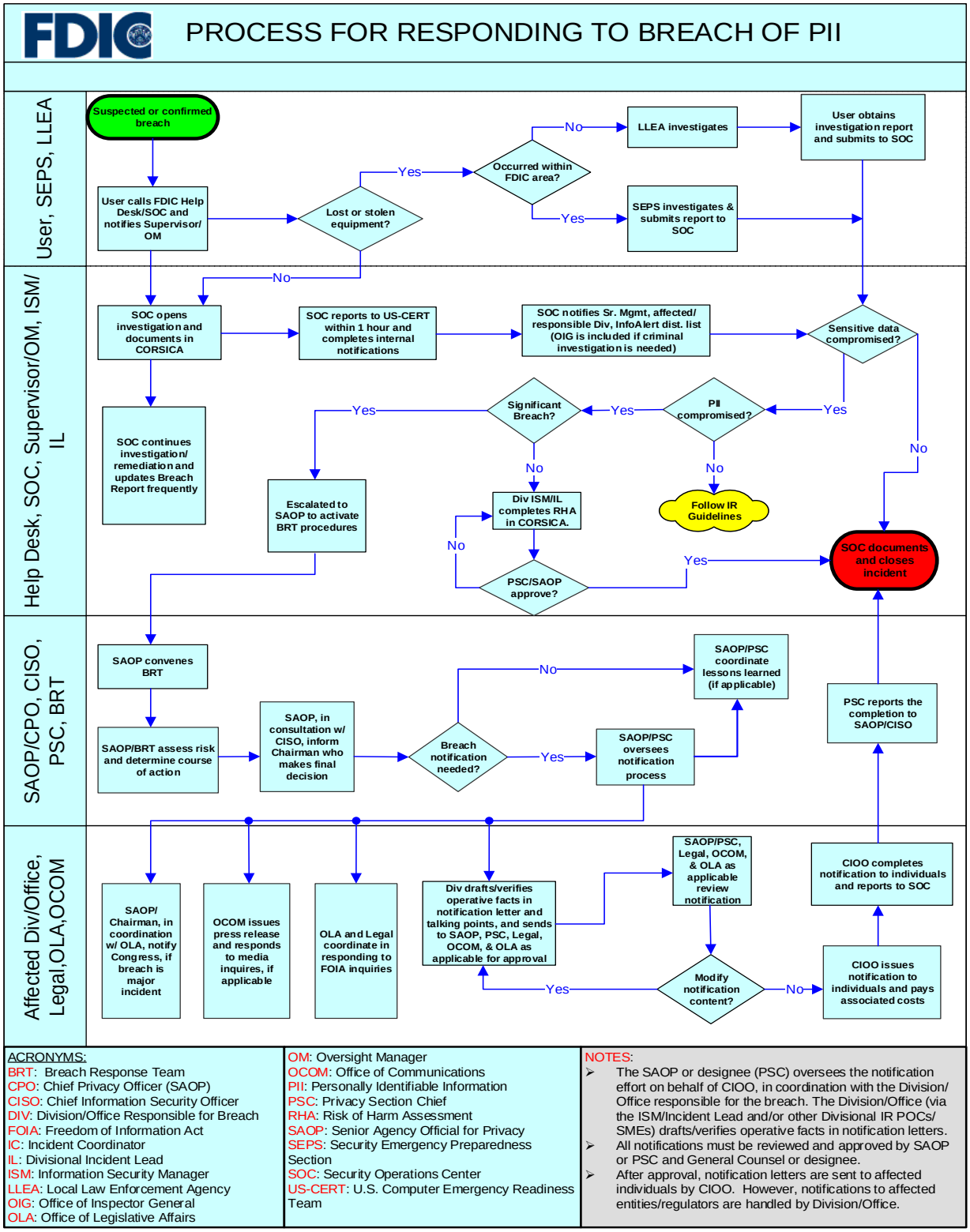
C. Physical

1. Did this breach raise any potential "lessons learned," in terms of improving the breach handling process and/or enhancing physical privacy/security controls over PII?	**Yes**	☐
	No	☐
<< Document any potential lessons learned, recommendations, and/or action items. >>		
2. Did the response to this breach result in any current or planned changes to physical security or privacy controls? If not, were/are there specific challenges preventing the changes from occurring?	**Yes**	☐
	No	☐
<< Document any current or planned changes to physical controls based on lessons learned, and any challenges preventing the changes from occurring if applicable. >>		

SECTION 3 – ADDITIONAL COMMENTS

Sensitive Information – For Official Use Only

Appendix G: High-Level PII Breach Summary Flowchart



ACRONYMS:
BRT: Breach Response Team
CPO: Chief Privacy Officer (SAOP)
CISO: Chief Information Security Officer
DIV: Division/Office Responsible for Breach
FOIA: Freedom of Information Act
IC: Incident Coordinator
IL: Divisional Incident Lead
ISM: Information Security Manager
LLEA: Local Law Enforcement Agency
OIG: Office of Inspector General
OLA: Office of Legislative Affairs
OM: Oversight Manager
OCOM: Office of Communications
PII: Personally Identifiable Information
PSC: Privacy Section Chief
RHA: Risk of Harm Assessment
SAOP: Senior Agency Official for Privacy
SEPS: Security Emergency Preparedness Section
SOC: Security Operations Center
US-CERT: U.S. Computer Emergency Readiness Team

NOTES:
- The SAOP or designee (PSC) oversees the notification effort on behalf of CIOO, in coordination with the Division/ Office responsible for the breach. The Division/Office (via the ISM/Incident Lead and/or other Divisional IR POCs/ SMEs) drafts/verifies operative facts in notification letters.
- All notifications must be reviewed and approved by SAOP or PSC and General Counsel or designee.
- After approval, notification letters are sent to affected individuals by CIOO. However, notifications to affected entities/regulators are handled by Division/Office.

Appendix H: Exceptions to the Breach Reporting Requirement

Because there are many different types of occurrences involving PII that may result in a risk of harm to individuals or to the FDIC, the term breach is inherently broad. In limited circumstances, however, an occurrence may meet the technical definition of a breach but not result in any risk of harm to the affected individuals or to the FDIC. Accordingly, the FDIC may institute very narrow exceptions to the requirement that individuals with access to FDIC information or information systems report a suspected or confirmed breach to the FDIC SOC for those limited circumstances where: 1) there is no risk of harm to the potentially affected individuals or to the FDIC, and 2) the failure to report the occurrences would not violate law or regulation. These occurrences will always be context-dependent and FDIC-specific and will require the SAOP to conduct an assessment of the risk of harm, in accordance with the FDIC's BRP.

In accordance with OMB M-17-12, the following table provides examples of the limited circumstances under which the requirement to report a suspected or confirmed breach to FDIC SOC is not triggered. The SAOP has assessed each of these circumstances and determined that while they meet the technical definition of a breach, they warrant exemption from the requirement to report because the risk of harm to potentially affected individuals is negligible, and the failure to report these occurrences does not violate law or regulation.

Examples of Non-Reportable Breaches	
1	An employee discards a document with the author's name on the front into an office bin.
2	An employee loses a copy of an office directory that contains individuals' names and work phone numbers.
3	An employee emails a file with non-sensitive, publicly available PII about a specific individual (e.g., newspaper article, public post on social media).

Appendix I: Examples of Guidance FDIC May Offer to Affected Individuals

In addition to, or in lieu of offering credit monitoring and identity protection services, following are examples of guidance and resources FDIC may offer to potentially affected individuals, depending on the nature and circumstances of the breach:

Active Duty Alert: Service members who deploy can place an active duty alert on their credit reports to help minimize their risk of identity theft. An active duty alert on a credit report means businesses have to take extra steps before granting credit in your name. Active duty alerts last for one year, and can be renewed to match the period of deployment.

Credit Freeze: A credit freeze restricts access to an individual's credit report. Because access to a credit report is usually required by creditors, a credit freeze can prevent creditors from approving a new account.

Credit Freezes for Children*:* When the individuals potentially affected by a breach are children, their guardians are sometimes able to place a freeze on their credit, even if the children do not yet have a credit history. Several states mandate that all credit bureaus provide this option. Outside those states, the option may still be possible depending on the credit bureau. In these instances, parents and guardians may have to provide additional information about themselves as well as the child in order to show the relationship.

Closing or Changing Accounts: Consumers should immediately dispute any unauthorized charges to existing accounts, including closing or changing account information so that unauthorized activity does not continue. This will not prevent new unauthorized accounts of which individuals may be unaware.

Obtaining a Free Credit Report: Individuals can obtain a free credit report yearly from each of the three national credit bureaus (Equifax, Experian, and TransUnion), from annualcreditreport.com, or by calling the credit reporting agencies' toll-free numbers. Individuals should review their credit reports for any accounts they do not recognize.

Cyber Hygiene: Resources include: DHS's *Stop.Think.Connect*. Campaign at: https://www.dhs.gov/stopthinkconnect or https://www.onguardonline.gov; US-CERT's tips on protecting privacy at: https://www.us-cert.gov/ncas/tips/ST04-013; and US-CERT's tips on preventing online identity theft at: https://www.us-cert.gov/ncas/tips/ST05-019.

Deceased Alerts*:* Deceased individuals can be at heightened risk for identity fraud that may impact the deceased individual's estate. This creates liability for a surviving spouse if, for example, his or her name is on joint accounts. To prevent this, death certificates can be sent to the IRS as well as the major credit bureaus, which place a "deceased alert" on the account to prevent new activity.

Fraud Alert: A fraud alert tells creditors that they must take reasonable steps to verify the identity of the individual who is applying for credit. A fraud alert also allows individuals to order one free copy of the individual's credit report from each of the three national credit bureaus. To place this alert, individuals can contact one of the three national credit bureaus, who must notify the others. The initial fraud alert stays on the credit report for 90 days and can be renewed.

FTC.gov/idtheft: The FTC's website provides free identity theft resources for individuals as well as community leaders, businesses, advocates, and law enforcement to share in their communities. The website includes resources on proactive steps individuals can take to monitor and protect their information and educate themselves on the different types of identity theft and the resources available to protect against and recover from identity theft.

IdentityTheft.gov: This is the Federal government's one-stop resource for identity theft victims. Individuals can use the website to report identity theft and get a personalized recovery plan that walks them through each step, updates the plan as needed, and pre-fills letters and forms. It also advises individuals on steps they can take to prevent identity theft when they receive notice that their PII has been compromised. The website is integrated with the FTC's complaint system, which makes the complaint information available to law enforcement across the country through Consumer Sentinel, a secure online database only available to law enforcement.

Tax Fraud*:* The FDIC may consider recommending individuals file an IRS Identity Theft Affidavit (Form 14039) to prevent an identity thief from using compromised PII to falsely claim the individual's tax refund.

Appendix J: Considerations for Identifying Logistical Support to Respond to a Breach

Sufficient logistical support is essential to respond effectively and efficiently to a breach. For example, logistical support may be required to prepare and deliver notification and to staff call centers. When a breach potentially affects a large number of individuals or implicates multiple IT systems, this can be a resource-intensive and challenging undertaking and can require hundreds or even thousands of hours to complete.

In accordance with OMB M-17-12 and FDIC policy, the SAOP and/or designees (CISO and PSC) in coordination with the Breach Response Team (BRT) when convened and the affected Division/Office, shall identify and ensure sufficient logistical support to respond to a breach. This includes considering what capabilities exist within the FDIC, which Divisions/Offices are responsible for executing those capabilities, and whether additional internal and/or external support is necessary to effectively and efficiently respond to the breach. At minimum, consideration shall be given to the following resource-intensive activities that may be necessary to provide notification, offer guidance, and provide services to individuals potentially affected by a breach:

- Procuring, updating and managing contracts and tasks related to identity protection and credit monitoring vendor(s);
- Establishing and maintaining dedicated website(s), webpage(s), and/or shared email box(es);
- Establishing, staffing and providing scripts/training to call center staff (both internal and external);
- Providing translation services;
- Recreating, maintaining, and analyzing unstructured and structured breached data;
- Identifying and compiling lists, counts, and type of impacted PII of potentially affected individuals;
- Performing address verification and lookup services;
- Developing, vetting and updating communications materials (e.g., press releases, FAQs, call center scripts, talking points, official written notifications to potentially affected individuals, financial institutions, regulators or other stakeholders, Congressional notification, official reports, etc.);
- Creating, reviewing and approving proofs of mailings;
- Printing and mailing notification letters;
- Processing and tracking credit monitoring issuance, mailings, activation/redemption, costs, and other pertinent notification information; and
- Triaging and responding to breach-related complaints and inquiries.

As a part of this process, the SAOP and/or designees (CISO and PSC), in coordination with the BRT when convened and the affected Division/Office, should identify any gaps or constraints in the FDIC's logistical capabilities and communicate with the Acquisitions Services Branch (ASB)

and other applicable FDIC groups or officials regarding the need to enter into contracts or to explore other options for ensuring that certain functions are immediately available during a time-sensitive response. These issues should be discussed at the initial stages of the breach investigation to ensure the appropriate logistical support is available to effectively and efficiently respond to a breach.

In addition, consideration shall also be given to administrative responsibilities implicit in and underlying many of the aforementioned logistical efforts, such as scheduling BRT meetings; preparing, updating and distributing meeting minutes, action items and materials; preparing executive summaries of discussions; scheduling lessons learned meetings; vetting communications materials to executives for approval; etc. A CIOO/OCISO special or program assistant(s) or other administrative and/or project management personnel shall be designated by the SAOP or designees (CISO and PSC) to serve as the BRT scribe and support these and other assigned administrative functions related to breach response.

Appendix K: Additional Considerations for Security Safeguards

When assessing the likelihood of access and use of PII potentially compromised by a breach, the CIO shall evaluate the implementation and effectiveness of security safeguards protecting the information. Security safeguards may significantly reduce the risk of harm to potentially affected individuals, even when the PII is particularly sensitive. The CIO shall consider each of the employed security safeguards on a case-by-case basis and take 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.

Encryption:

When evaluating the likelihood of access and use of encrypted PII potentially compromised by a breach, the CIO, in coordination with the SAOP[67] and CISO, shall confirm:

- 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.

There are many ways to encrypt information and different technologies provide varying degrees of protection. Encryption can be applied at the:

- Device-level;
- File-level; and
- To information at rest or in transmission.

The protection provided by encryption may be undermined if keys, credentials, or authenticators used to access encrypted information are compromised.

Federal agencies are required to use a NIST-validated encryption method.[68] The SAOP shall consult with the agency's CISO and other technical experts, as appropriate, to ascertain whether information was properly encrypted. For additional information, refer to National Institute of Standards and Technology Federal Information Processing Standards Publication 140, Security Requirements for Cryptographic Modules at: http://csrc.nist.gov/publications.

The PII potentially compromised by a breach also may be rendered partially or completely inaccessible by security safeguards other than encryption. This may include redaction, data

[67] At the FDIC, the CIO also serves as the SAOP.

[68] OMB Circular A-130 requires agencies to encrypt all FIPS 199 moderate-impact and high-impact information at rest and in transit, unless encrypting such information is technically infeasible or would demonstrably affect the ability of agencies to carry out their respective missions, functions, or operations; and the risk of not encrypting is accepted by the authorizing official and approved by the agency CIO, in consultation with the SAOP (as appropriate).

masking, and remote wiping of a connected device. Physical security safeguards such as a locked case securing documents or devices may also reduce the likelihood of access and use of PII. For example, PII in a briefcase left temporarily unattended is less likely to have been accessed and used if the briefcase was securely locked.

Appendix L: RACI (Responsible, Accountable, Consulted, and Informed) Matrix

RACI Matrix - FDIC PII Breach Response Process

PII Breach Activity	Key FDIC PII Breach Stakeholders																								
	User	DOA Security Emergency Preparedness Section	Local Law Enforcement Agency	Help Desk	Security Operations Center (SOC)	User's Supervisor or Oversight Manager	SAOP/CPO	CIO	Incident Coordinator	CISO	Privacy Section Chief	Breach Response Team	Legal Division	OLA	OCOM	Executive Management of Affected Division/Office	Incident Lead (ISM/IR POC of Affected Division)	FDIC Chairman or Executive Office	Office of Inspector General	OCISO Security and Engineering Section	Ombudsmen	US Congress	Affected Users/Entities	BRT RHA Scribe	US CERT
User Reports Incident to HelpDesk	R/A	I	I	I		I																			
HelpDesk Provides Notification As Appropriate	C			R/A	I																				
Triage, Record Incident in CORSICA, Complete Breach Report, and Provide Notification	C			C	R/A	C		I	I	I	I		I	I	I		I/C		I	I	I				I
Identify Incident Lead and Notify OCISO					I				I		I						R/A								
Lead investigation/technical remediation and coordinate with Division and other resources as needed					R/A	I/C			R/A								I/C								

As part of investigation, provides secure staging area for breached data when applicable; coordinates with Division to obtain, recreate, and review data to confirm nature of data, number/type of records involved, number of individuals potentially affected, and other info necessary to complete Breach Report.					**R/A**				**R/A**		**I/C**						**I/C**								
Verifies nature of data and compiles breach notification list(s), as applicable.					**I/C**				**I/C**		**I/C**					**I/C**	**R/A**								
Continues to coordinate w/ Div as necessary and provides frequent updates on findings of investigation/remediation.					**R/A**				**R/A**	**I**	**I**					**I**	**I/C**								
Performs preliminary RHA in CORSICA and immediately alerts PSC and key stakeholders if assessment indicates breach may be significant.					**I**				**I/A/C**		**I/A/C**					**I/C**	**R/A**								
Reviews Incident Lead's preliminary RHA and recommends to CISO and SAOP/CPO to convene BRT (if significant) or manage to closure at staff level (non-significant)								**C/I**	**I/A**	**C/I**	**R/A**						**C/I**								
For non-significant breach, approves final RHA; coordinates with other consultative officials if required; and routes final RHA for CISO and SAOP/CPO approval.							**I/C**	**I/C**	**I/A/C**	**I/C**	**R/A**		**I/C**	**I/C**	**I/C**	**I/C**	**I/A/C**								
For significant breach, convenes / schedules BRT					**I**	**I/A**	**R/A**	**I/A**	**I/A**	**I/A**	**I/A/C**	**I/A**	**I/A**	**I/A**	**I/A**		**I/A**		**I**	**I/C**	**I/A**				
Performs RHA real-time during BRT mtg					**I**	**A**	**R/A**	**A/C**	**A/C**	**A/C**	**A/C**	**R/A**	**A/C**	**A/C**	**A/C**		**A/C**	**A/C**	**I**	**I/C**					

Documents RHA real-time during BRT mtg and ensures it is documented in CORSICA in a timely and accurate manner					I		I/C		I/A/C	I/C	I/C						I/A/C								R/A	
Notifies FDIC Chairman of BRT Recommendation as applicable							R/A	I	I	I/A/C	I		I			I	I	I/C								
Makes final decision to provide notification, guidance or services to affected individuals							R/A[69]	I/C		I/C	I/C					I/C	I/C	R/A[70]								
Notification to Congress if Breach constitutes Major Incident							A/C	C	C	C	C		C	C	C	C	C	R/A	I			I				
Draft Individual Notification Letters/FAQs; and Bank/Regulator talking points/notification							R/A		I/C		R/A/C		A/C		C/I	R/A/C	A/C									
Draft Responses to Inquiries from FIs and Consumers							R/A		I/C		A/C		A/C		A/C	R/A	I/C									
Establish/Monitor Central Shared Mailbox, If Applicable									I/C		I/C		I/C		C/I	R/A	I/C									
Develop/Maintain Public-Facing Website, If Applicable									I/C		I/C		I/C		R/A	I/C	I/C									
Draft/Issue Communications Plan and Press Release, If Applicable									I/C		I/C		I/C		R/A	I/C	I/C									
Bear Costs and Assign Resources to Facilitate Notification and Credit Monitoring Issuance							R/A		I/C	I/C	A/C					I/A/C	I/C									
Provide Notification/Credit Monitoring Services							R/A		I/C		A/C		I/C		I/C		I/A/C							I		
Press Releases and Public/Media Inquiries								I/C	I/C	I/C	I/C		I/C	I	R/A	I	I	I/C	I		I			I		
Identify and Document Lessons Learned					I/C		I/A/C	I/C	I/C	I/C	I/C	I/C	I/C	I/C	I/C	R/A	I/A/C			I/C						
Privacy Act or FOIA Inquiries									I/C	I/C	I/C		R/A	I/C	I/C	I/C	I/C									

[69] For non-significant breaches, PSC prepares and provides recommendation to CISO and SAOP for review. SAOP considers PSC recommendation and any feedback from CISO, and concurs/non-concurs.
[70] For significant breaches, Chairman or designee makes final determination.

Congressional Inquiries							A/I		I/C	I/C	I/C		R/A	R/A		I/C	I/C		I/C							
Draft Close-Out Recommendation									I/C		I/C						R/A									
Review and Approve Close-Out Request					I				A/C		R/A						I									
Officially Close Breach Record in CORSICA					I/R/A		I		R/A	I	I						I									

RACI Definitions:

Responsibility = person or role responsible for ensuring that the item is completed

Accountable = person or role responsible for actually doing or completing the item

Consulted = person or role whose subject matter expertise is required in order to complete the item

Informed = person or role that needs to be kept informed of the status of item completion

Appendix M: Executive Summary Template

FDIC PII Breach Executive Summary

Incident Number: CINC_____

Instructions: *The BRT RHA Scribe is responsible for preparing an Executive Summary of the BRT's risk assessment and recommendations, and assisting the SAOP with vetting it for approval and recording the date(s) of SAOP and Chairman concurrence or non-concurrence with the BRT recommendation, along with the rationale for any points of non-concurrence. The SAOP (or designee) shall provide the updated Executive Summary and supporting RHA to the BRT, at minimum within one business day of receiving a final determination from the Chairman (or designee) and at the conclusion of the breach response process. This Executive Summary will be stored in CORSICA (the official system of record) upon completion. Any disagreements, and the manner in which they will be resolved (i.e., elevated to the Chairman, etc.) will be documented within this summary.*

Summary

[Example (Ex): The reporting employee is an Examiner in RMS/Kansas City Regional Office. A hardcopy document was inadvertently faxed to an unauthorized individual on February 22, 2017. CSIRT was notified of the incident on March 14, 2017.
The faxed document contained sensitive PII about bank customers including: SSNs, names, home addresses, and bank account information. There were 200 potentially affected individuals.]

BRT Risk Assessment

Asset Type	# of Potentially Impacted		Data Element Assessment
	Individuals	Businesses	SPII (Yes/No)
[Ex: Hardcopy Document]	*[Ex: 200]*	*[Ex: 0]*	*[Ex: Yes]*

Compromise Assessment			
Encryption (Yes/No)	Encryption Type	Likelihood of Harm Assessment	Level Classification
[Ex: N/A]	*[Ex: N/A]*	*[Ex: Likely]*	*[Ex: Red]*

BRT Recommendation(s)

[Ex: Because the disclosure to an unauthorized individual contained sensitive PII data in unencrypted format, with a risk level classification of Red, the BRT recommends the following actions to mitigate the risk of harm to individuals:]

#	BRT Recommendation *(Date)*	SAOP Concurs? *(Date)*	Justification for Non-Concurrence *(If Applicable)*
1	*[Ex: Written notification and guidance should be provided to the potentially impacted individual(s) (200 Bank of X customers). (03/19/17)]*	*[Ex: Yes (03/20/17)]*	*[Ex: N/A]*
2	*[Ex: Credit monitoring should be provided to those potentially impacted individuals whose sensitive PII presents a risk of identity theft (100 of 200 Bank of X customers). (03/19/17)]*	*[Ex: Yes (03/21/17)]*	*[Ex: N/A]*
3	*[Ex: Notification via telephone should be provided to the impacted institution (Bank of X) prior to releasing notification to the bank's impacted customers. (03/19/17)]*	*[Ex: No (03/21/17)]*	*[Ex: Notification to impacted institution could disrupt an ongoing examination.]*

FDIC Chairman Decision(s)

Date Exec Summary Provided to Chairman	Chairman Concurs with BRT Recommendations? *(Date)*	Justification for Non-Concurrence *(If Applicable)*
[Ex: 03/22/17]	*[Ex: Yes (03/22/17)]*	*[Ex: N/A]*