Apple Bank

Data Security Incident Response Plan

Effective Date: 5/2021

REVISION HISTORY

Log of Changes

Revision	Date	Initials	Change / Description
1.0	3/2020	MT	Initial version.
2.0	5/2021	JR	Updated to include Business Continuity Officer and FRB notification process as well as emended IS Playbook

Contents

INTRODUCTION 3

1. Purpose 3

2. Scope 3

3. Key Definitions 3

4. Examples of Data Security Incidents 4

5. Plan Authorization, Maintenance, Testing and Reporting 5

INCIDENT RESPONSE TEAM STRUCTURE 6

INCIDENT RESPONSE ACTIVITIES 10

APPENDIX A - CONTACT LIST OF EXTERNAL SUPPORT PROVIDERS AND OTHER CONTACTS . 16

APPENDIX B – DATA SECURITY INCIDENT COMMUNICATIONS GUIDE 18

Attachment 1 to Appendix B - Sample Customer Notice 23

APPENDIX C – SWAT AGENDA & INCIDENT ASSESSMENT GUIDANCE 29

APPENDIX D – IRT INITIAL MEETING AGENDA GUIDANCE 31

APPENDIX E – IRT FOLLOW-UP MEETING AGENDA GUIDANCE 32

APPENDIX F – INCIDENT RESPONSE ACTION ITEM TRACKING FORM 33

APPENDIX G - IRT ROLES AND RESPONSIBILITIES (AS APPLICABLE) 34

APPENDIX H: INFORMATION TECHNOLOGY AND INFORMATION SECURITY RUN-BOOK..... 39

APPENDIX I: SECURITY INCIDENTS HANDLING PLAYBOOK 43

INTRODUCTION

1. Purpose

The purpose of this Data Security Incident Response Plan ("IRP" or "Plan") is to provide a well-defined, organized approach for responding to and resolving Data Security Incidents (as defined below) involving Apple Bank (the "Bank"). This Plan identifies and describes the roles and responsibilities of the Bank's Incident Response Team ("IRT"), including designating a Response Coordinator who is responsible for ensuring that all applicable requirements of this Plan are adhered to in the event of an incident. This Plan also establishes procedures for the Bank's incident response process, including steps for identifying, reporting, investigating, analyzing, resolving and recovering from an incident.

As appropriate, a Bank employee who is assigned responsibilities pursuant to this Plan may delegate his or her responsibilities to one or more Bank employees under his or her direct supervision, provided that final responsibility rests with the delegating employee. Bank personnel must keep information about Data Security Incidents confidential and may only disclose such information on a strictly need-to-know basis. Unless authorized under this Plan or approved by the Legal Department ("Legal"), all Bank personnel, including IRT members, are prohibited from disclosing any information regarding a Data Security Incident (e.g., to customers, other employees, Third-Party Service Providers, business partners, the media, government regulators or any other third party).

2. Scope

This Plan applies to every Data Security Incident (see definition at p. 4 and severity classifications at p. 8).

3. Key Definitions

Bank Information: All information maintained, owned, licensed, possessed or controlled by the Bank, which includes:

- Personal Information (defined below);
- intellectual property, trade secrets, source code, algorithms, interface designs, marketing processes and methods, logistics processes and methods, technical information or know-how, and research and development data;
- proprietary information about the Bank's operations that, if disclosed to an unauthorized person, could cause harm to the Bank, including customer lists and agreements, supplier lists and agreements, joint-venture or partnership agreements, corporate banking information, data compiled for our financial statements and reporting data, business

development and strategic plans, performance data, investor lists, investment and business forecasts, tax records, pricing information, licensing information, marketing and sales plans or analyses, risk assessments, audit reports, employee compensation data, and similar documents or communications that are competitively sensitive regarding the Bank's relationships with customers, employees, Third-Party Service Providers, business partners, government entities or other third parties;

- non-public information pertaining to pending or threatened legal proceedings, regulatory matters or inquiries, investigative demands, enforcement actions, including attorney-client privileged communications, judgment and settlement terms, litigation assessments, regulator correspondences, registration or license applications and/or approvals/denials, confidential supervisory information, and similar non-public documents or communications that, if disclosed to an unauthorized person, could result in loss of privilege, violation of a non-disclosure agreement or other harm to the Bank; and

- information regarding the Bank's computer systems, network infrastructure and information security controls such as system configurations, network architecture maps, user access rights and internal network addresses.

Data Security Incident: Actual or reasonably suspected unauthorized or accidental access to or acquisition, use, disclosure, alteration, loss or destruction of Bank Information. Examples of Data Security Incidents are provided in the section below.

Personal Information: Any information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked (directly or indirectly) with a particular individual or household. Personal Information may relate to a customer, employee, contractor, service provider, supplier, business partner, investor, government representative or any other individual.

Response Coordinator: A senior member of Information Security who is a direct report to the CISO and is assigned responsibility for coordinating the IRT's response to the Data Security Incident.

SME: A subject matter expert, either internal or external to the Bank.

Third-Party Service Providers ("TPSPs"): Any service provider, contractor or supplier that provides services for or on behalf of the Bank.

4. Examples of Data Security Incidents

Examples of Data Security Incidents (a more detailed list can be found in the Incident Response section of the Information Security Policy) include, but are not limited to, any actual or reasonably suspected:

- compromise of the Bank's or its service provider's systems, networks, equipment, devices, hard-copy documents or other media in which Bank Information resides, even if the Bank Information is not known to have been accessed;
- loss or theft of hard-copy documents, electronic media or other media, that may contain Bank Information;
- Bank employees, service providers or other authorized third parties inadvertently sending Bank Information to the wrong recipient;
- Bank employees, service providers or other authorized third parties exceeding the scope of their authorization and accessing Bank Information they are not approved to access;
- exploitation of a cybersecurity vulnerability or configuration issue associated with a Bank service or system that may reasonably result in a compromise to the security of Bank Information;
- accidental or unauthorized loss of a decryption key used to encrypt Bank Information;
- unauthorized use, disclosure, transmission, mailing or destruction (in any medium, including paper) of Bank Information;
- unauthorized wire transfer by the Bank that results from a suspected phishing compromise or other social engineering methods;
- installation or execution of malicious software or code (e.g., virus, worm, Trojan horse, ransomware or other code-based malicious entity) that infects a Bank system and has not been successfully quarantined by anti-malware software;
- receipt of an extortion demand threatening to compromise the confidentiality, integrity or availability of Bank Information;
- unauthorized access to Bank system or online accounts that result from a password replay attack or other method of compromise;
- unauthorized change to or deletion of records, files, webpages or documents containing Bank Information; or
- Denial of Service attack that prevents or impairs the normal authorized functionality of the Bank's networks, systems or applications.

5. Plan Authorization, Maintenance, Testing and Reporting

The Board of Directors has authorized the creation of this Plan to support efforts in responding to any Data Security Incident, and has delegated authority to approve the Plan to the Executive Management Steering Committee ("EMSC"). The Bank's Chief Information Security Officer ("CISO") is responsible for overall maintenance of this Plan. The Plan will be routinely reviewed and tested at least once a year with various scenarios to enhance the Bank's Data Security Incident response capabilities, consider new types of data security threats and incorporate lessons learned from incidents that have occurred since the previous annual review. The CISO will present the

results of the annual review to the Bank's Board of Directors or a designated committee of the Board. In addition, on an annual basis, the CISO will present to the Board of Directors or a designated committee a summary of all Data Security Incidents that occurred during the prior year.

INCIDENT RESPONSE TEAM STRUCTURE

This Plan organizes incident response in a tiered approach based on appropriate escalations. The SWAT team is engaged first in the initial escalation process, to assess and determine if a substantial, organized response is required. As warranted, SWAT thereafter further escalates to the full IRT to determine the appropriate steps necessary to respond to the incident. In such an event, the Response Coordinator will assemble the IRT (see below for members) and coordinate the response to carry out the requirements of this Plan.

The members of the SWAT team are:

Title
Chief Technology Officer
Chief Information Security Officer
Chief Privacy Officer (as warranted for potential privacy issues)
Response Coordinator

The following represents the standing membership of the Incident Response Team (IRT) that reports to the Executive Management Steering Committee:

Title
CEO/Chairman
Chief Technology Officer
Chief Information Security Officer
Chief Privacy Officer
Response Coordinator
General Counsel
Chief Risk Officer
Chief Retail Banking Officer

The following chart lists (non-exclusively) additional personnel who may be called upon to serve on the IRT for a particular incident:

Title
Chief Financial Officer
Chief Compliance Officer
IT Infrastructure and Support Manager
Chief Human Resources Officer
Director of Marketing
Director of Digital Banking
Director of Deposit Operations
Business Continuity Officer
Vendor Management
Head of Financial Crimes Compliance & BSA Officer

The heads of business units listed above shall designate (in advance and in writing with the Response Coordinator) a member of their business function to serve as their delegate in the event the head of the business unit is unavailable at the time of the incident.

Any additional members of the IRT will be determined by the standing members of the IRT on an incident-by-incident basis according to incident type, skill set necessary to appropriately and timely respond to the incident, and availability. The IRT may adjust its roles and responsibilities for the purpose of responding to a particular Data Security Incident, and may add roles and responsibilities from the Bank's other functions or business units, as appropriate. The IRT also may be supplemented with in-house or outside subject matter expertise, including incident response, forensics and public relations functions. Appendix A contains the names and contact information of certain relevant external support providers.

The Bank, through ADP, maintains contact information for the relevant IRT members, which regularly updates the Bank's RPX system to enable emergency communications to be texted to the IRT members as needed.

While the response details are captured below in the Incident Response Activities section, for a detailed list of responsibilities *by role/department*, see Appendix G.

DATA SECURITY INCIDENT SEVERITY CHART

In the event of a Data Security Incident, the CISO (or a designee) will gather initial facts about the incident, analyze known information, identify individuals and entities potentially affected by the incident, and discuss with the SWAT team to render a preliminary assessment of the severity of the Data Security Incident based on the Data Security Incident Severity Classification Chart below.

Data Security Incident Severity Classification Chart			
INCIDENT FACTORS* * An incident does not need to satisfy all the factors listed in this chart to qualify under the relevant severity level (i.e., only one or two factors might be met).	**INCIDENT SEVERITY CHARACTERISTICS**		
	Low *Standard: An event that appears isolated to a small number of individuals, computers or processes that are unlikely to have any meaningful business, operational or legal impact to the Bank.*	**Medium** *Standard: An event that appears likely to have limited or moderate legal, reputational, strategic, operational or financial implications for the Bank.*	**High** *Standard: An event that has or appears likely to have (a) the potential to disrupt business on a large scale across the Bank, or (b) significant legal, reputational, strategic, operational or financial implications.*
Personal Information (PI)	Indication that affected data includes only de minimis (impacting <5 individuals) amounts of PI (or none at all)	Indication that the affected data includes PI about a moderate or sizable number (5-499) of individuals	Indication that the affected data includes PI about a significant number (>500) of individuals
Bank Confidential, Proprietary or Trade Secret Material	Indication that affected data includes only de minimis amounts of Bank confidential, proprietary or trade secret material (or none at all)	Indication that the affected data includes Bank confidential, proprietary or trade secret material (see Nature and Impact factors to distinguish between Medium and High)	Indication that the affected data includes Bank confidential, proprietary or trade secret material (see Nature and Impact factors to distinguish between Medium and High)
Nature of Incident	Single, localized intrusion or phishing attempt. Minimal risk that Bank Information has been accessed or acquired by an unauthorized person for unlawful purposes or other misuse No indication of misuse or adverse impact to Bank Information Indication that the issue was inadvertently or accidentally caused and did not involve criminal activity or malicious intent A small number of insignificant systems, applications or databases are disrupted or unavailable	Reasonable possibility of an incident involving unauthorized access to or acquisition of some unencrypted Bank Information Some indication of misuse, unauthorized disclosure or adverse impact to sensitive Bank Information, or that unlawful activity has occurred Indication that the Bank has been specifically targeted by a nation-state or other sophisticated threat actor Detection of a cybersecurity vulnerability or other security issue associated with a Bank service or system that may reasonably result in a compromise to Bank Information if exploited Detection of larger scale suspicious activity involving critical systems Some systems, applications or databases may be disrupted or unavailable for a meaningful period of time	Credible evidence (e.g., from law enforcement) of an incident involving unauthorized access to or acquisition, use or disclosure of a significant volume of Bank Information Indication that a nation-state actor is reasonably suspected to have infiltrated or conducted surveillance of Bank systems or Bank Information Credible evidence that a cybersecurity vulnerability or other security issue associated with a Bank service or system may reasonably result in a large-scale service or system disruption or compromise to Bank Information A significant system, application or database is disrupted or unavailable, or its integrity or security has been compromised
Potential Impact	No indication that a detected cybersecurity vulnerability or other security issue associated with a Bank service or system has been exploited No meaningful business, operational or legal impact to the Bank appears likely Low expectation that the event could	Reasonable likelihood that incident may have a measurable impact to the Bank's services, internal operations, finances or reputation Indication that media intends to report on the suspected incident or of social media activity regarding the incident	Reasonable possibility of an incident that causes significant risk to the Bank, organization-wide (e.g., incident has or is reasonably likely to halt key services for an extended period of time or cause a significant adverse impact to the Bank's finances, share value or business reputation) Reasonable possibility of significant or widespread media coverage of the incident

	result in the compromise of additional Bank systems or data		
Third Party Service Provider (TPSP)	Reported low-level attacks (e.g. phishing attempts) but no data or connections compromised.	TPSP has suffered a Data Security Incident that has a meaningful business or legal impact on the Bank, but is unlikely to pose a significant risk to the Bank.	TPSP has suffered a Data Security Incident that poses a significant risk to the Bank.

For purposes of this Plan, the incident severity levels and how they are managed/reported are as follows:

Severity Level	Severity Management	Severity Reporting
Low	For a Low severity incident, the IRT will not be convened and the CISO, in coordination with Legal, will work directly with the head of the affected business unit and appropriate IRT members to respond to the incident in accordance with applicable steps set forth in this Plan. Some of the steps in the Plan may be curtailed or omitted for Low severity incidents.	The CISO will provide a summary of Low severity incidents to the Information Security Sub-Committee on a quarterly basis. A summary of Low severity incidents will be reported by the CISO to the Board of Directors in the Annual Information Security Report.
Medium	If the severity is Medium, the IRT will convene and follow the Plan.	As appropriate, Medium severity incidents will be reported by the CISO to the Board of Directors or a designated Committee of the Board. A summary of all Medium severity incidents must nevertheless be provided to the Board of Directors on a quarterly basis.
High	If the severity is high, the IRT will convene and follow the Plan.	High severity incidents will be reported by the CISO to the Board of Directors (or a designated committee of the Board) in a timely manner.

INCIDENT RESPONSE ACTIVITIES

Step #	Owner	Master Incident Response Plan	Completed
1	Multiple (preliminary steps): Employees, MIS Help Desk, Vendors, CISO	**Incident Detection:** The Bank may discover evidence or indicia of a Data Security Incident through a number of different methods, such as IT or monitoring tools or reports from employees, service providers, business partners or other outside third parties (e.g., customers, cybersecurity organizations or researchers, other financial institutions, payment card processors or law enforcement authorities). **Incident Reporting:** When a Data Security Incident has been detected, the Bank personnel who became aware of the incident or the individual's supervisor must immediately report the incident to one of the following incident reporting channels, as appropriate: • Submit a Service-Now ticket. For Ticket Subject, enter "Security/Privacy Incident Report" and provide details about the incident in the Full Description field. Provide contact information for the person most knowledgeable about the incident and capable of providing additional details as needed; • Call/email CISO or Chief Privacy Officer ("CPO") directly o CISO: mtumarinson@applebank.com or (646) 523-2679 o CPO: hamorosana@applebank.com or (860) 378-4304 The Bank's TPSPs and other business partners may be required to notify the Bank of any Data Security Incident affecting Bank Information maintained for or on behalf of the Bank. Upon receipt of such notice, the relevant Bank personnel must relay the notification he or she received from the TPSP or other business partner to one of the incident reporting channels. **Incident Escalation:** Upon being notified of a Data Security Incident, personnel monitoring the relevant incident reporting channel must document the report and notify the CISO (or a designee), who will promptly make an initial determination as to whether a Data Security Incident occurred or is occurring. To do so, the Response Coordinator, at the direction of the CISO, will gather initial facts about the incident, analyze known information, and identify individuals or entities potentially affected by the incident. When necessary, the CISO will consult with Legal to make such initial determinations.	
2	CISO, SWAT, IRT	**Preliminary Severity Assessment:** Upon verifying that a Data Security Incident has occurred, the CISO, in consultation with the SWAT team, as appropriate, will promptly conduct a preliminary assessment of the severity of the incident. In determining the severity level of a Data Security Incident, the CISO (or a designee) will assess the nature of the incident based on all known information about the incident. The severity level will be determined using the Data Security Incident Severity Classification Chart set forth in this Plan, and will be adjusted as appropriate based on additional details that may come to light through further investigation. **Assembling the IRT:** If based on the preliminary assessment, the SWAT team determines that incident is of a Medium or High severity, then it (or a designee) will promptly convene a meeting with the IRT, where reasonably feasible within 24 hours of the CISO becoming aware of an incident.	

<table>
<tr><td></td><td></td><td>To support quick response and collaboration in the event of a Data Security Incident, the Bank has implemented a Bridge Line that can be opened and hosted by any member of the IRT and kept open for ongoing or ad-hoc emergency communications. All IRT members will have immediate access to this bridge, which will support communication while members are in-transit or off-site at time of the critical data/security incident. CISO or its delegate will open the Bridge Line as appropriate and advise relevant IRT members to join the call via email/text/cell phone call (generated via the RPX system).

<table><tr><th>LOCATION</th><th>IRT EMERGENCY BRIDGE TELEPHONE ACCESS</th></tr><tr><td>IRT Virtual Command Center Number</td><td>1 888 726 2010
Access Code = 6469498656
Host Code = 6469498656
Security Code = 8656</td></tr></table></td><td></td></tr>
<tr><td>3</td><td>Response Coordinator, Legal, IRT</td><td>Response Coordinator: In the event of a Medium or High Level severity incident, the Response Coordinator will be responsible for executing this Incident Response Plan. If the incident involves one of the Bank’s TPSPs, the Response Coordinator, in coordination with Legal (and Vendor Management, as appropriate), will work with Business Process Owner who owns the vendor relationship to ensure the general requirements of this Plan are addressed by such TPSP’s response.

Legal and Outside Counsel Support: For every Data Security Incident that is deemed to be High severity and to the extent deemed necessary, or as otherwise appropriate in light of the circumstances, the General Counsel (or its designee) will promptly engage outside counsel to assist the Bank in responding to the Data Security Incident. As appropriate, Legal or outside counsel will direct the Bank’s investigation of the Data Security Incident.

Formation of the IRT: In the event of an incident deemed to be High or Medium severity, or as otherwise appropriate, the standing members of the IRT will assemble the appropriate membership for the IRT to assist in handling the Bank’s response to the Data Security Incident. The size and composition of the IRT will be appropriate to the (1) nature and severity level of the Data Security Incident, (2) relevant Bank business units, services, affiliates and entities impacted by the Data Security Incident and (3) relevant branches or offices impacted by the Data Security Incident. A list of the representatives who may be called upon to serve on the IRT is found in Section II of this Plan.</td><td></td></tr>
<tr><td>4</td><td>CISO</td><td>Forensic and Other External Investigation Support: Based on the nature, scope and severity of the Data Security Incident, the CISO, in consultation with Legal as appropriate, will determine whether external support providers should be engaged to assist the Bank in investigating and remediating the Data Security Incident, such as forensic and technology specialists, cyber threat intelligence firms, security assessment firms, ransom specialists and private investigators. If the CISO determines that external support is appropriate or required, Legal or outside counsel will engage the external support provider and direct the investigation. The General Counsel or its designee (in consultation with outside counsel, as appropriate) will direct the preparation of any documentation relating to a third-party investigation and will determine if and how the findings may be documented.</td><td></td></tr>
</table>

		Notification to Senior Leadership: The IRT will promptly alert the EMSC members who are not part of the IRT of a Data Security Incident deemed to be High severity and may do so, as appropriate, for an incident that represents a Medium severity. The IRT will consult with the EMSC, as appropriate, on the Bank's response to such Data Security Incidents. The CEO, CISO and/or GC will inform the Bank's Board of Directors (or an appropriate committee thereof) of the impact and status of a Data Security Incident deemed to be High severity or as otherwise appropriate in light of the circumstances.	
5	Response Coordinator	**Response Coordinator Assembles the IRT:** The Response Coordinator will assemble a meeting with the assigned members of the IRT promptly, taking reasonable steps to meet within 24 hours of the communication from Response Coordinator. If necessary, the Response Coordinator will open the IRT bridge line to ensure the IRT meets timely. The Response Coordinator will also assess whether setting up a physical or virtual war room is required. As appropriate, the Response Coordinator will assign tasks for members of the IRT to effectively respond to the incident and will develop a working schedule for IRT meetings. As warranted, the Response Coordinator will provide the EMSC ongoing status reports on the IRT's response efforts. **Documentation:** In coordination with Legal, appropriate members of the IRT may document actions, decisions and findings related to the Data Security Incident. In documenting actions and findings related to the Data Security Incident, documentation should be limited to the facts and not include unnecessary assumptions, opinions, interpretations, conjecture or speculation. The General Counsel, or its designee, will advise on the preparation of appropriate documentation. **Business Continuity and Disruption**: To the extent necessary, the Response Coordinator will consult with the Bank's Business Continuity Officer to determine whether a business disruption has occurred or is likely to occur as a result of the Data Security Incident and, if so, whether it is appropriate to initiate the Bank's Business Continuity Plan in response to the Data Security Incident. The Business Impact Analysis (BIA), which is maintained by the Business Continuity Officer and identifies critical business functions and applications, should be referred to during an incident. Additional supporting Business Continuity Plan documents lay out available recovery strategies that the Bank can use in case of an incident that could cause degradation or serious impact to the business.	
6	CISO (or a designee)	**Containment and Remediation:** The CISO (or a designee), in consultation with Legal and outside experts (as appropriate), will determine and oversee the implementation of actions and measures to contain, control and remediate the Data Security Incident, including securing affected Bank systems or information, mitigating harmful effects of the Data Security Incident, and preventing further compromises. The purpose of containment is to limit the scope and magnitude of the incident. Containment usually consists of short-term tactical steps intended to remove access to compromised systems, limit the extent of current damage, and prevent additional damage from occurring. Containment will vary based on incident type. After the Data Security Incident has been contained, additional actions may be necessary to further remediate the incident, such as deleting malware, reconfiguring systems or devices, disabling affected user accounts, and identifying and mitigating vulnerabilities that were exploited in connection with the Data Security Incident. Considerations for determining the appropriate containment and remediation strategies include: • potential damage to and theft of the Bank's systems or information resources (e.g., whether it is necessary to quarantine affected systems, devices or networks);	

		• repairing or rebuilding affected systems, devices and networks; • service and product availability (e.g., network connectivity and services provided to external parties); • time and resources needed to implement the strategy; • availability of appropriate data or system backups; • effectiveness of the strategy (e.g., partial or full containment); • duration of the solution (e.g., a temporary or permanent solution); • implementation of physical security measures (e.g., securing physical areas and facilities, changing locks, and resetting or deactivating access codes or cards); • enhanced monitoring of network or system activities and searches for additional impacted systems; and • identification and elimination of an intruder's means of access to the Bank's systems or devices. For further details, Information Technology and Information Security should consult and may leverage, as applicable, Appendices H and I to this Plan for Information Technology and Information Security Run-Book and Data Flows respectively. **Evidence Preservation:** The containment and remediation strategy must take into account evidence preservation. The strategy should be designed to prevent the corruption or loss of critical evidence (e.g., system logs, volatile memory and persistent storage) necessary to address any legal action that may result from the Data Security Incident. In the course of containing and remediating the Data Security Incident, when feasible and appropriate, affected systems and other information resources should not be shut down or altered in any manner without prior consultation with Legal.	
7	Legal	**Legal Posture:** In parallel with the early containment, remediation and investigation efforts associated with a Data Security Incident, Legal (including outside counsel, as appropriate) will take steps to help preserve the Bank's legal posture, as follows: • The General Counsel (or its designee) or outside counsel will direct and approve relevant documentation and evidence preservation efforts, as appropriate. • The General Counsel (or its designee) will issue legal hold notices applicable to the relevant records, as appropriate. • In the event a Data Security Incident disrupts or potentially compromises the Bank's standard communications systems, the General Counsel (or its designee), in collaboration with the Response Coordinator, will advise on alternative communication methods, protocols and tools in light of evidence preservation and record retention requirements. • As appropriate, Legal will prepare non-disclosure and information sharing agreements with third parties (e.g., law enforcement authorities and regulatory agencies) and affidavits or written agreements that affirm statements of fact made by individuals (e.g., employees or service providers) in connection with the Data Security Incident. • As appropriate, Legal , in consultation with outside counsel as appropriate, will seek to limit the unauthorized disclosure or use of Bank Information that has been exposed in connection with the Data Security Incident (e.g., by issuing takedown requests for Bank Information posted to a website or sending cease and desist letters to individuals who have gained access to Bank Information).	

		• The General Counsel (or its designee), in consultation with outside counsel as appropriate, will document the facts surrounding the Data Security Incident and remedial actions taken by the Bank as required by applicable law, and will advise the IRT regarding the documentation of actions and findings related to the Data Security Incident. **Insurance Coverage:** Legal will pursue insurance coverage for costs associated with the incident to facilitate maximum recovery under the Bank's relevant insurance policies, as appropriate.	
8	Legal	**Notification:** The General Counsel (or its designee), in coordination with the IRT, will work with key stakeholders to determine whether any applicable laws, contracts, or industry requirements or standards require the Bank to notify persons or entities of the Data Security Incident, such as: • Regulators • Customers • Employees • Law enforcement authorities • Business partners • TPSPs • Cybersecurity organizations • Consumer reporting agencies • Payment card brands or processors • Other financial institutions • Insurance carrier(s) and insurance broker • Media • Auditors See the "Communication Guide" attached in Appendix B for additional information about providing notification associated with a Data Security Incident.	
9	Response Coordinator ,CISO, Legal	**Root Cause Analysis:** As appropriate, the IRT, at the direction of the General Counsel (or its designee), will conduct a root cause analysis of the Data Security Incident. In connection with the root cause analysis, the IRT will take appropriate remedial actions to address the Data Security Incident, including without limitation, addressing system vulnerabilities, taking disciplinary actions, or invoking contractual obligations included in agreements with the party responsible for the Data Security Incident. **Lessons Learned Review:** As appropriate, the Response Coordinator will convene a lessons learned meeting with the IRT. This meeting will focus on determining whether improvements should be made to the Bank's security controls and/or the incident response processes. Questions to be considered during the meeting include, as appropriate: • How well did management and personnel perform in dealing with the Data Security Incident? • Were the documented procedures followed? Were they adequate? • What information was needed sooner? • Were any steps or actions taken that might have impeded the recovery? • What would the IRT do differently the next time a similar incident occurs? • What corrective actions can prevent similar incidents in the future? • What indicators should be monitored in the future to detect similar incidents? • What additional tools or resources are needed to detect, analyze and mitigate	

		future incidents? • How could information sharing with other organizations have been improved, if applicable? • Is additional training needed? As appropriate, the IRT will direct relevant Bank personnel and business units to make changes to applicable information security policies, procedures, controls and training based on the lessons learned from the Data Security Incident.	
10	IRT	**Leadership Update:** The IRT will communicate the status and outcome of the Data Security Incident to relevant senior executive management, and Board of Directors, as appropriate.	
11	Legal	**Legal Actions:** Legal will respond to any inquiries or enforcement actions by regulatory authorities in connection with the Data Security Incident. Legal will lead any related litigation activities, whether such activities are proactive (e.g., bringing an action against an allegedly culpable service provider or seeking indemnification from a relevant service provider or business partner) or reactive (e.g., responding to a lawsuit).	

Appendix A - Contact List of External Support Providers and Other Contacts

NOTE: The below contact information is for ease of reference, and does not suggest each point of contact must be involved in the handling of every incident.

Outside Counsel

Hunton Andrews Kurth LLP
Lisa Sotto - LSotto@Hunton.com; (212) 309-1223 (o)
Brittany Bacon - BBacon@Hunton.com; (202) 309-1361 (o)

Insurance Broker

Willis Towers Watson
Tad T. Ojeks , Senior Vice President, Financial Institutions Group
Tad.ojeks@willistowerswatson.com
Direct: +1 212 915 7710, Mobile: 917 622 1222

Forensic Expert
Refer to Hunton Andrews Kurth LLP

PCI Forensic Investigator (PFI)
Refer to Hunton Andrews Kurth LLP

Public Relations Firm

FTI Consulting
Brian Maddox - Brian.Maddox@fticonsulting.com; 646-642-8933 (c), 212-850-5661 (w)
Erica Richardson - Erica.Richardson@fticonsulting.com; 256-527-4336 (c), 202-346-8873 (w)
Danielle Fornabaio - Danielle.Fornabaio@fticonsulting.com: 646-591-7809 (c), 212-850-5731 (w)

Call Center
[Insert name and contact information]

Identity Protection Service
[Insert name and contact information]

Mail House
[Insert name and contact information]

Law Enforcement Contacts

United States Secret Service NY Field Office - 718-840-1000 and the Electronic Crimes Task Force at nyectf@usss.dhs.gov;

FBI NY Field Office: 26 Federal Plaza, 23rd Floor - NY, NY 10278- Phone: (212) 384-1000;

FBI Internet Crime Complaint Center (IC3): http://IC3.gov click link to file a Complaint.

Regulatory Contacts

FDIC: Dan Devlin - ddevlin@fdic.gov

NYS DFS: Reena Mathew – reena.mathew@dfs.ny.gov

FRBNY: Bhavin Patel – bhavin.patel@ny.frb.org

Appendix B – Data Security Incident Communications Guide

This Data Security Incident Communications Guide ("Guide") provides the Bank with a guide for evaluating whether any applicable laws, contracts, or industry requirements or standards require the Bank to notify persons or entities of the Data Security Incident. This Guide applies to all Data Security Incidents, and supplements related incident response documents, including the Bank's Data Security Incident Response Plan. Some steps in the Guide may be curtailed or omitted, as deemed appropriate by the responsible Legal personnel, based on the nature and scope of the Data Security Incident as then understood.

Communication Guide
Regulator Notification Where required by law or as advisable, Legal will provide (or arrange for the provision of) timely written notification of the Data Security Incident to relevant regulatory authorities (e.g., the New York Department of Financial Services, the Federal Deposit Insurance Corporation, state attorneys general, other federal and state financial or consumer protection regulators, and applicable data protection authorities). The General Counsel (or its designee) will take steps to provide notification to regulatory authorities in accordance with the timing, format and content requirements of applicable laws. Steps that may be appropriate, depending on the circumstances, include identifying the jurisdictions in which affected individuals reside, determining the number of affected individuals by jurisdiction, preparing reporting forms or talking points and other correspondence, and seeking assistance from outside counsel on the Bank's regulatory notification obligations. Note: Notice to NYDFS is required no later than 72 hours from a determination that a Cybersecurity Event has occurred that is either of the following (or any other legally required timeframe/criteria): (1) Cybersecurity Events impacting Apple Bank of which notice is required to be provided to any government body, self-regulatory agency or any other supervisory body; or (2) Cybersecurity Events that have a reasonable likelihood of materially harming any material part of the normal operation(s) of Apple Bank. If notice is required to NYDFS, notice shall be provided via the DFS secure portal at https://myportal.dfs.ny.gov/web/cybersecurity by authorized individuals. **NOTE:** *The approval of the General Counsel (or a designee), who will collaborate as appropriate with the Chief Compliance Officer, Chief Privacy Officer and Chief Information Security Officer in the drafting, is required for all notifications to regulators.*
The Institution or its Service Provider must immediately notify the Reserve Banks by telephone at (888) 333-7010, with written confirmation via email at ccc.technical.support@kc.frb.org, of any suspected, threatened or known cyber event, fraud, malware detection, compromise, or other security incident or breach, that relates to or has the

potential to impact an Electronic Connection, Access Control Feature, or the use of a Reserve Bank financial service, including (but not limited to) circumstances in which the Institution or the Service Provider have a reasonable basis to know or suspect that such event:

- impacts or may impact software or hardware that the Institution or Service Provider use to engage or interface with an Electronic Connection or an Access Control Feature;
- impacts or may impact software or data stored on servers or other electronic media shared with Reserve Bank data or applications;
- impacts or may impact hardware, software or data that are used to generate transactions, messages, or other information that will be transmitted through an Electronic Connection;
- caused or may have caused the Institution or its Service Provider to generate an unauthorized transaction;
- causes or may cause the Institution or Service Provider to modify its operations while investigating or mitigating the impact of the event; Operating Circular No. 5 Effective October 15, 2020June 30, 2021 4
- requires notification by the Institution or its Service Provider to its prudential regulator, or by a Service Provider to the Institution, pursuant to any law, regulation, or supervisory requirement;
- resulted in or may have resulted in the loss of, unauthorized access to, compromise of, or tampering with an Access Control Feature; or
- resulted or may have resulted in the unauthorized disclosure or use of Confidential Information.

Law Enforcement Coordination

Depending on the nature and circumstances of the Data Security Incident, the General Counsel or its designee, in consultation with the CISO, may report the incident to relevant law enforcement authorities, as appropriate or required by law, and may cooperate in any criminal investigation related to the incident.

The Bank will file a Suspicious Activity Report (SAR) with the Financial Crimes Enforcement Network (FINCEN) when required by law or as otherwise appropriate (e.g., when it detects a known or suspected violation of federal law, or a suspicious transaction related to a money laundering activity or a violation of the Bank Secrecy Act). SAR filings will be submitted by the Financial Crimes Compliance Department, in coordination with Legal.

The General Counsel or its designee will coordinate with the CISO on whether to inform law enforcement authorities that the Bank intends to provide (or arrange for the provision of) notice to affected individuals. The Bank may delay notification to third parties if requested by law enforcement and the relevant laws permit such delay. Legal will retain the records containing the justification and supporting materials for a law enforcement delay, in accordance with applicable law.

The Response Coordinator shall ensure law enforcement communications are approved by the General Counsel (or a designee).

Affected Individual or Entity Notification

NOTE: *The approval of the General Counsel (or a designee), who will collaborate as*

appropriate with the Chief Compliance Officer, Chief Privacy Officer and Chief Information Security Officer in the drafting, is required for all notifications to impacted individuals or entities or other external communications including talking points.

- Identification of Affected Parties. If Legal determines that a notifiable Data Security Incident has occurred, the General Counsel and the Chief Privacy Officer will coordinate, as appropriate, with the IRT to identify affected individuals and entities and their relevant contact information for notification purposes. If specific affected individuals cannot be identified, the IRT will identify the groups of individuals likely to have been affected (e.g., all individuals whose information was stored on a stolen laptop or in a database that was accessed by an unauthorized party).

- Business Partner Notification. The General Counsel and/or the Chief Privacy Officer will consider whether the Bank has a legal or contractual obligation to notify commercial customers or other business partners of a Data Security Incident. If such third party is to be notified, the General Counsel and/or the Chief Privacy Officer will prepare talking points and other relevant materials in coordination with Marketing / Communications, as appropriate, and will coordinate related activities.

- Notification Content and Method. Once the individuals, entities or groups likely to have been affected by the Data Security Incident have been identified, the Bank will notify the affected individuals, entities or groups in accordance with applicable law. The Bank will provide (or arrange for the provision of) notification to affected individuals and entities in accordance with the timing, format and content requirements of applicable laws. The notice should be clear and conspicuous, and written using easy-to-understand language.

- Substitute Notice. If the Bank cannot identify specific individuals to be notified, or the Bank has insufficient or out-of-date contact information for the affected individuals, substitute notification may be used as an alternative means of notification, as permitted or required by law. The Bank also may provide substitute notification under other circumstances, in accordance with applicable law.

- External Support. When individuals are impacted, Legal may retain and enter into contracts with relevant third-party support providers to assist in the notification process or provide related services (e.g., credit monitoring or identity protection, call center and mail house or email distribution services), as appropriate.

- Talking points: When appropriate, guidance such as scripts or FAQs for inquiries regarding the incident should be timely developed and distributed to the call center, branches and social media areas.

- Additional Customer Communication: If appropriate, set up dedicated web page, email

address, or customer service hotline to answer questions regarding the incident.

Media Communications

Marketing / Communications, in consultation with Legal, will:

- Engage an external communications/public relations firm, as appropriate;
- Develop an external and internal communications plan and coordinate messaging to media (including preparation and implementation of a holding statement, press release and website and social media materials, as appropriate); and
- Determine appropriate Bank representatives to serve as the Bank's spokespersons regarding the Data Security Incident.

In developing talking points for media inquiries, Marketing / Communications should consider the following guidelines:

- Keep the technical level of detail low. Detailed information about the incident may provide enough information for copycat events or even damage the Bank's ability to pursue remedies once the event is over.
- Keep speculation out of media statements. Speculation about the cause of the incident or the motives are very likely to be in error and may cause an inflamed view of the incident.
- Do not allow the media attention to detract from the handling of the event. Always remember that the successful closure of an incident is of primary importance.
- Seek approval for content from the General Counsel (or a designee).

Cybersecurity Organization Reporting

In consultation with Legal, the CISO will determine whether it is appropriate to report cyber threat indicators or defensive measures related to the Data Security Incident to external information security and cybersecurity organizations (such as the FS-ISAC or other information sharing and analysis centers or organizations). Following consultation with Legal, only pertinent and appropriate information on the Data Security Incident may be shared with such external organizations.

Insurance Carrier

- Where required by the Bank's relevant insurance policy(ies) or as otherwise appropriate, the General Counsel (or its designee) will notify the Bank's insurance broker, Willis Towers Watson, of an incident in accordance with the Bank's relevant insurance policy(ies).
- Claims should be emailed to claimcentral@willistowerswatson.com. In turn, Willis will notify the Bank's appropriate insurance carrier(s) about the potential claim(s).
- Proof of "loss," including fees paid to forensic analysts or others in connection with this Response Plan, should be communicated to our insurance carrier(s) as required by the relevant policy.
- If any third-party claims are brought against the Bank following a security incident, General Counsel will consult the coverage terms and notify our insurance broker as required by the

relevant policy(ies).

Payment Card Entity Reporting

If information relating to payment cards (debit, ATM or credit cards) is reasonably believed to have been acquired or accessed by an unauthorized party, Legal will consult with Digital Banking on whether to notify the relevant payment card processing entities or payment card brands in accordance with the Bank's contractual obligations. Digital Banking, in coordination with Legal, will notify the relevant payment card processing entities in accordance with the Bank's contractual obligations, and will comply with applicable payment card brand requirements.

Consumer Reporting Agencies

As required by law or otherwise appropriate, the General Counsel or the Chief Privacy Officer will provide written notification of the notifiable Data Security Incident to the three U.S. nationwide consumer reporting agencies (Equifax, Experian and TransUnion).

Financial Auditors

As required by law or otherwise appropriate, Legal will notify the Bank's financial auditors of a Data Security Incident involving the Bank's internal financial control systems.

Attachment 1 to Appendix B - Sample Customer Notice

Established 1863
Member FDIC

Legal Department

122 East 42nd Street, 9th Floor
New York, NY 10168

[DATE]

Name
Address
City, State
Zip Code

Reference Number: PI-xxxxxxxxxx

Dear [Name]:

At Apple Bank, we take the security of your information seriously and want to let you know about an incident related to your personal information.

Here's what happened and how it affects you
We recently learned that [describe event succinctly - in high-level, non-technical terms; follow state laws for exact required content of the letter]. The personal information involved in the issue may have included [insert relevant elements of personal information affected by the issue].

General Content Requirements: description of event, type of data involved, Bank actions to protect against further unauthorized access or use, contact phone number, reminder to remain vigilant and report incidents of suspected identity theft.

NY requires: the telephone numbers and websites of the relevant state and federal agencies that provide information regarding security breach response and identity theft prevention and protection information, and a description of the categories of information that were, or are reasonably believed to have been, accessed or acquired by a person without valid authorization, including specification of which of the elements of personal information and private information were, or are reasonably believed to have been, so accessed or acquired.

Promptly after learning of the issue, we took steps to secure our systems and determine the nature of the issue. We retained a data security expert to conduct a forensic investigation. **[Verify/Decide if appropriate to include.]** **[If relevant:]** In addition, we are working with law enforcement authorities to assist them in their investigation. Based on our investigation, at this time, we have no evidence that any of the information has been misused as a result of this issue. **[Verify.]**

You can sign up for free monitoring [Offer if required by law due to data elements exposed or as a courtesy (business decision).]

We regret that this issue may affect you. We take our obligation to safeguard personal information very seriously and are alerting you about this issue so you can take steps to help protect yourself. You are entitled under U.S. law to one free credit report annually from each of the three nationwide consumer reporting agencies. To order your free credit report, visit www.annualcreditreport.com or call toll-free at 1-877-322-8228. We encourage you to remain vigilant by reviewing your account statements and monitoring your free credit reports. In addition, we have arranged to offer you [one/two] year(s) of free **[**credit monitoring and identity protected services] through [name credit monitoring services], which helps detect when there are changes to your credit bureau information.

Please see the enclosed reference guide describing how to enroll in the services, as well as the additional steps you can take to help protect yourself.

We hope this information is useful to you. If you have any questions, please call us anytime at [INSERT NUMBER].

Sincerely,

Holly H. Amorosana
Chief Privacy Officer

Enclosed: [vendor] Enrollment Information
Additional Steps to Help Protect Yourself document

Vendor enrollment information – insert instructions from Experian

YOU CAN TAKE ADDITIONAL STEPS TO HELP PROTECT YOURSELF

Order your free annual credit reports

Visit annualcreditreport.com or call 877-322-8228 to get a free copy of your credit reports. Once you receive them:

- Verify that all information is correct.
- Look for discrepancies such as accounts you did not open or creditor inquiries you did not authorize.
- Contact the credit reporting agency if you notice incorrect information or have questions.

Register for Identity Protection and Credit Monitoring Services

We have arranged with **[insert provider]** to help you protect your identity and your credit information for **[one year]** at no cost to you. **[Insert details (or refer to insert) describing the product's features and how to enroll.]**

Manage your personal information

- Carry only essential documents with you.
- Be cautious about sharing your personal information with anyone else.
- Shred receipts, statements, and other documents containing sensitive information.
- Use anti-virus software on your computer and keep it updated.

Monitor your credit and financial accounts

- We suggest you carefully review your credit reports and bank, credit card and other account information on Applebank.com and in statements for any transaction you do not recognize.
- We can provide copies of past statements at no cost to you.
- Call us immediately at [provide number] to report unauthorized or suspicious transactions.
- If you detect any unauthorized transactions in other financial accounts, promptly notify the relevant financial institution or payment card company.
- Work with us to close your Apple Bank account(s) and open new ones with new account numbers.
- Create alerts with your credit card company and bank to notify you of account activity.
- If you detect any incident of identity theft or fraud, promptly report the incident to law enforcement, the FTC or your state Attorney General.

- File an identity theft report with your local police and contact the credit reporting agency that issued the report if you find unauthorized or suspicious activity on your credit report.

Get more information about identity theft and ways to protect yourself

- Visit [insert web info from our credit monitoring vendor]
- Call the Federal Trade Commission (FTC) identity theft hotline at 877-438-4338 (TTY: 866-653-4261) or visit them online at www.ftc.gov/bcp/menus/consumer/data/idt.shtm for additional guidance on the steps you can take to avoid identity theft and for guidance on the steps you should take if you feel you are a victim of identity theft.
- You may also visit the website of the Federal Deposit Insurance Corporation (FDIC) at www.fdic.gov/consumers/consumer/guard/index.html.

Place a 90-day fraud alert on your credit file

An **initial 90-day fraud alert** tells anyone requesting your credit file that you might be at risk for fraud. A lender should verify that you have authorized any request to open a credit account in your name, increase the credit limit and/or get a new card on an existing account. If the lender cannot verify this, they should not process the request.

Contact any one of the credit reporting agencies to set up an initial 90-day fraud alert.

Equifax	**Experian**	**TransUnion**
PO Box 105069	PO Box 9554	PO Box 2000
Atlanta, GA 30348	Allen, TX 75013	Chester, PA 19016
Phone: 800-525-6285	Phone: 888-397-3742	Phone: 800-680-7289
Fax: 770-375-2821	[fill in]	Fax: 714-447-6034
Equifax.com	Experian.com	Transunion.com

Place a security freeze on your credit file

A **security freeze** on your credit file prevents anyone from accessing your credit report and therefore from issuing credit in your name. **However, placing a security freeze also may delay, interfere with, or prevent the timely approval of any requests you make for new loans, credit, mortgage, employment, housing or other services.**

Contact all three of the credit reporting agencies above to set up a security freeze with each of them.

Appendix C – SWAT Agenda & Incident Assessment Guidance

1) Establish factual base line
2) Establish estimated timeline of event
3) Reminder on forensic evidence preservation
4) Confirm record keeping process
5) In assessing the nature and severity of the incident, SWAT may use the following guiding questions:
    - What is the actual or potential size/scope of the incident?
    - When did the Data Security Incident occur and is it potentially ongoing? What appears to be the time window of exposure?
    - What was the cause of the Data Security Incident? Was the incident caused by an accidental, intentional or malicious act?
    - Where did the Data Security Incident occur? Are any TPSPs or other business partners affected by or involved in the incident? If so, what is the impact or involvement?
    - What types of Bank Information were potentially affected? Was the potentially affected information in electronic or hard-copy form? What was the volume of data that was potentially affected?
    - Is there evidence that the relevant Bank Information has been misused or likely will be misused? Is there evidence that the Data Security Incident likely will result in harm to affected individuals, the Bank or its business partners?
    - Was the relevant Bank Information in the Bank's possession or in the possession, custody or control of a third party? If in the possession, custody or control of a third party, is there any evidence that the third party disseminated or disclosed the relevant information to others?
    - Was the data encrypted, pseudonymized or redacted? If the data was encrypted, was the encryption key compromised?
    - What are the intensity, immediacy and potential duration of the incident?
    - What are the actual or potential impacts to Apple Bank in terms of operations, data, reputation, legal or financial standing?
    - Is there a customer impact? If so, are retail customers and/or business customers impacted?

- Who discovered the Data Security Incident and how was it discovered? Who else is aware of the situation?
- Will additional or outside resources likely be required by Apple Bank to deal with this incident?
- Are there any other factors that could cause this incident to grow?
- What is the likelihood of cascading events?
- Does the Bank have any applicable contractual rights or obligations with respect to responding to the Data Security Incident?
- Are there any strategic business considerations to take into account (e.g., an upcoming significant potential partnership, acquisition, merger, capital markets transaction, audit or earnings report)?
- What is the probable "worst case scenario" associated with this incident?

6) Based on their assessment of the incident, SWAT can decide on several actions, including the following options:
   - No action required – this event does not constitute a Data Security Incident;
   - Continue to monitor – information is insufficient to activate the IRT, but the incident requires ongoing monitoring; or
   - Activate the IRT and suggest which additional members should be involved.

Appendix D – IRT Initial Meeting Agenda Guidance

NOTE: The below serves as guidance, and not requirements, for the order and topics to be discussed; fluidity is preferred as every incident is different.

1) Provide initial factual background
2) Reminder on forensic evidence preservation
3) Confirm record keeping process
4) Review incident response requirements and needs – leverage Incident Response Plan, as appropriate.
5) Identify need for ad hoc IRT members or additional resources including outside consultants
6) Identify and deliberate on any strategic issues related to management of the incident and its potential impact on Apple Bank
7) Document outstanding action items that cannot be immediately resolved - leverage tracking form at Appendix E as appropriate
8) Prioritize any critical issues that need to be resolved
9) Confirm communications lockdown, as appropriate, until strategy is developed
10) Determine any extended response requirements
11) Establish expected timeframes/deadlines
12) Set meeting cadence and establish times and outline schedule (24 hours)
13) Other items

Appendix E – IRT Follow-up Meeting Agenda Guidance

NOTE: The below serves as guidance, and not requirements, for the order and topics to be discussed; fluidity is preferred as every incident is different.

1) Conduct incident update/briefing
   a) Response Coordinator
   b) CISO
   c) CTO
   d) Workflow/Status updates – IRT Members
   e) Other Apple Bank staff with current incident information

2) Review / discuss progress on strategy development

3) Identify potential additional Apple Bank impacts

4) Document decisions and next steps

5) Incident communications update - confirm communications strategy, leveraging Appendix B

6) Action items update / new

7) Identify adequacy of staff support and resources including outside consultants

8) Set additional meeting times as appropriate

Appendix F – Incident Response Action Item Tracking Form

Action Item #	Priority*	Action Item Description	Assigned to	Status

*Priority Levels:

Priority 1 – High

Priority 2 – Moderate

Priority 3 – Low

Appendix G - IRT ROLES AND RESPONSIBILITIES (AS APPLICABLE)

In connection with a Data Security Incident, members of the IRT will assume the roles and responsibilities indicated in this Plan. Below is a list of general roles and responsibilities that may be applicable to a Data Security Incident.

Applicable to All Standing Members of Incident Response Team

- Leveraging the Data Security Incident Severity Chart and the guiding questions contained in Appendix D, assess and confirm SWAT team's assessment of the severity and extent of the incident;
- Determine what immediate internal resources – in addition to the IRT – are necessary to deal with the incident;
- Monitor progress of the incident response and provide executive-level support to the Response Coordinator;
- Determine whether regulatory (e.g., FDIC, NYDFS), customer, insurer or other third-party notification of the incident is legally required or appropriate [See Appendix B - Communication Guide];
- Determine whether external resources are required (e.g., external legal counsel, public relations/crisis management firms or forensic investigators) [See Appendix A for contact numbers for external resources];
- As appropriate, make recommendations to mitigate likelihood of similar incidents in the future;
- Determine additional IRT members on incident-by-incident basis according to incident type and skills necessary to appropriately and timely respond to the incident; and/or
- Establish response strategy for each incident and assign tasks to members of the IRT, including setting or approving specific objectives and actions required to mitigate the impacts of the incident.

Response Coordinator

- Coordinate overall response based on directives from IRT; where appropriate, the Response Coordinator will consult with the Business Continuity Officer;
- Ensure compliance with all applicable requirements of the Plan;
- As appropriate, convene IRT meeting; at the initial meeting of the IRT, brief the assembled team on known information about the incident, and what actions have taken place or are underway or are planned to address the issues; as appropriate, lead the IRT through a proposed agenda (see Appendices D through F) modified as necessary to meet the needs of the incident;
- Update and advise IRT on the status of the response;
- In consultation with the General Counsel (or its designee), document relevant actions and decisions related to the incident;

- In consultation with the General Counsel (or its designee), coordinate with external counsel and forensic investigators as applicable;
- Upon request, assist the General Counsel (or its designee) in drafting of notices, if necessary;
- Upon request, assist Marketing, and the General Counsel (or its designee) in coordinating with public relations/crisis management firms to develop internal and external communications on the incident;
- Initiate, complete, and, in coordination with the General Counsel (or its designee), document the incident investigation– see Appendix F for Action Item tracking form; and/or
- Facilitate regular training and practice for the IRT.

Information Security

- Evaluate potential Data Security Incidents to determine need to escalate for SME review in accordance with the Incident Response sections of Information Security Policy and Procedures;
- Escalate potential incidents in accordance with the Plan;
- As appropriate, work with the General Counsel (or its designee) to coordinate with forensic specialist and legal counsel for Data Security Incidents that require forensic evidence to be collected; and/or
- As appropriate, assess need to change Information Security Policies, procedures, security controls, run-books and/or practices based on an incident.

Information Technology

- Follow IT run-books for relevant incident;;
- Take necessary action to block traffic to and from suspected intruders;
- Preserve evidence in accordance with this Plan;
- Create extract files for applicable business units for customer notification or debit card reissuance process; and/or
- Assess need to change IT run-books based on an incident.

Privacy

- Assess incident facts to identify potential notification obligations of the Bank;
- Advise on and help identify privacy issues;
- In coordination with the General Counsel and Chief Compliance Officer, prepare third-party notices in accordance with legal requirements; and/or
- Determine if engagement with identity protection and credit monitoring services is required or appropriate.

Legal

- Serve as main point of contact with outside organizations that have a role in the incident and its resolution;
- Depending on the severity or nature of the incident, update the Board on the current status of the incident, impacts to operations, the efforts to resolve any issues and resume operations, and/or provide other information as may be required based on the nature of the incident;
- Prepare/approve third-party notices in accordance with applicable legal requirements;
- Review all external communications or talking points regarding the Data Security Incident prior to release to ensure consistency with potential disclosures, third-party communications, and legal requirements; and/or
- Advise on litigation avoidance strategy and determine whether affirmative litigation is appropriate.

Compliance

- Track and report customer complaints, if any, related to the incident;
- As appropriate, coordinate with Marketing on communications and messaging;
- In coordination with Legal, oversee messaging on social media and determine if/how/when comments appearing on social media sites regarding Apple Bank, and its handling of the incident, will be answered; and/or
- All rumors will be reported through the IRT to the Chief Compliance Officer, who will recommend and, in coordination with the IRT, implement appropriate actions (media release, briefing, contact with person(s) with rumor information) to correct misinformation.

Human Resources

- Coordinate with the General Counsel and the Chief Compliance Officer, or their designee(s), to draft messages that will provide information to the employees about the incident and any actions that the employees are being requested or directed to take. The Chairman/CEO will approve all bank-wide messages going to employees and, as appropriate, messages to employees will come from the Chairman/CEO; and/or
- Determine best means for information dissemination to employees as the situation dictates.

CustomerLine

- Track and report customer complaints, if any, related to the incident in accordance with the Complaint Monitoring Policy and Procedures, in real time or at a minimum daily; and/or
- Staff phones to address customer questions, leveraging approved scripts provided by IRT.

Financial Crimes Compliance

- Determine whether Suspicious Activity Report (SAR) is required and, if so, file with the SAR in coordination with Legal.

- OFAC encourages victims and those involved with addressing ransomware attacks to contact OFAC immediately if they believe a request for a ransomware payment may involve a sanctions nexus. Victims should also contact the U.S. Department of the Treasury's Office of Cybersecurity and Critical Infrastructure Protection if an attack involves a U.S. financial institution or may cause significant disruption to a firm's ability to perform critical financial services.

    - U.S. Department of the Treasury's Office of Foreign Assets Control
        - Sanctions Compliance and Evaluation Division: ofac_feedback@treasury.gov; (202) 622-2490 / (800) 540-6322
        - Licensing Division: https://licensing.ofac.treas.gov/; (202) 622-2480
    - U.S. Department of the Treasury's Office of Cybersecurity and Critical Infrastructure Protection (OCCIP)
        - OCCIP-Coord@treasury.gov; (202) 622-3000
    - Financial Crimes Enforcement Network (FinCEN)
        - FinCEN Regulatory Support Section: frc@fincen.gov

Senior Branch Operations Officer

- In coordination with Legal and Financial Crimes Compliance, determine whether internal/external fraud or other security investigations are necessary.

Marketing

- In consultation with the General Counsel or his/her designee, create content for internal and external communications on incidents; and/or
- Coordinate communications and messaging with Chief Compliance Officer and outside crisis communication firm.

Corporate Planning & Finance

- Provide any known situational information regarding the incident and advise on potential impact to Apple Bank; and/or
- Identify the need for use of specialized resources.

Accounting / Digital Banking

- Track incident-related expenses; and/or
- For Unauthorized access to Fedline Advantage (refer to Appendix B)
- For Unauthorized access to Wires, and ACH transactions;
  - As appropriate, coordinate with the IRT on closing customer access to retail/commercial banking platforms to limit incident losses;
  - As appropriate, in coordination with Legal, report to clearing firms and others potentially affected by compromised accounts (Note: see the following URL for specific details and a form to report to NACHA on incidents involving ACH transactions - https://www.nacha.org/databreach-form);
  - As appropriate, in coordination with the IRT, notify other applicable vendors to ensure continuity of service notwithstanding an incident;
  - For incidents involving debit cards occurring at external merchant or non-Bank sources (e.g., Home Depot, Target), as appropriate:
    - Determine card reissue process;
    - Initiate debit card blocks; and
    - Determine if lowering dollar limits for Point of Sale (POS) transactions, ATM withdrawals or cash purchases is necessary.

Appendix H: Information Technology and Information Security Run-Book

Step #	Owner	Information Technology and Information Security Run-Book	Completed
1	Response Coordinator	**Incident is Suspected:** Regardless of the severity level of the incident, this Information Technology and Information Security Run-Book may apply as appropriate.	
2	Response Coordinator, or as appropriate, external Forensic Analyst	**Incident Triage** The Response Coordinator will focus on understanding the scope of the attack/incident, including without limitation, the identification of impacted systems, the number of employees or customers affected, and any potential brand impact. In coordination with the IT Department, the Response Coordinator or, depending on the type of incident, a Forensic Analyst engaged by external incident counsel through the General Counsel (or its designee), shall conduct the following investigative aspects of the Incident Triage: 1. Investigate the attack vector; 2. Decipher the scope of the incident; a. Determine if incident is contained (e.g. network is secure versus threat or exposure is ongoing) b. Determine nature of incident (e.g. hacking, loss of device, phishing, ransomware, human error, etc.) c. Determine if countermeasures (e.g. encryption) were enabled when compromise occurred d. Identify system/devices/networks/applications affected i. If incident originated from a vendor: 1. Determine the level of data that supplier had access to (i.e., hosted v. accessible, PI or non-PI) 2. Identify relevant contract terms to determine proper course of action 3. Coordinate response approach with vendor e. Identify who or what originated the incident f. Identify how the incident is occurring (what tools or attack methods) g. Identify what vulnerabilities are being exploited h. Identify nature of data elements involved (name, SSN, Driver's License, account number, etc.) i. Which records (including specific data elements) were viewed or accessed? j. Which records (including specific data elements) were acquired? k. Identify category of data subjects impacted (e.g. customer, employee, etc.) l. Identify residence state of impacted data subjects m. What is the size of the impacted population? n. As the investigation proceeds, if PI is involved, in which states do the impacted customers or employees reside? 3. Determine if data was ex-filtrated or transactions conducted, and if so, how; 4. Identify perpetrator, if possible.	
3	Response	**Containment**	

	Coordinator	Through the IT Department, the Response Coordinator will focus on how to contain the attack vector to minimize impact to the enterprise network, servers, or data. In so doing, the following issues may be considered: 1. Maintain forensic evidence while mitigating the attack; 2. Minimize the attack surface, and quarantine components as necessary; 3. Implement Access Control Lists (Perimeter or Network Backbone) to isolate malicious traffic to prevent further business impact; 4. Update signatures to enable intrusion prevention systems to kill malicious network traffic at the network or host level; 5. Turn off replication of data to the disaster recovery site in attempt to prevent replicated data from overwriting the snapshots of previous data; 6. Disconnect the system that has been compromised from a network to prevent further outbreak which will preserve running processes in memory (potentially useful during forensic investigation); 7. Adjust firewall rules to prevent exfiltration of data from a compromised system; 8. Shut down the system that has been compromised to prevent further outbreak (this should be done only if disconnecting the system from the network is not possible); 9. Ensure backups for affected systems do not get contaminated, which includes ensuring that backups have not been affected in the attack.	
4	Information Technology	**Identification & Eradication Function** Once the incident is contained, the IT Department in coordination with the Response Coordinator shall begin eradication efforts. Eradication involves removing any malicious software, such as viruses, worms or any other malicious code from any affected system(s). This function focuses on cleaning systems and networks. Depending on the circumstance of the incident, this can be accomplished via desktop/server management tools, or a manual process that can clean up the artifacts from end-points. This function should consider the following steps, among others: • Identify attack artifacts (files, registry keys, processes); • Develop removal package and push to end points; • Track number of affected systems and those cleaned until all remediated. Eradication is complete when the vulnerability that caused the incident is found and mitigated. Once systems are cleaned, then containment procedures can be reversed to minimize impact to productivity or delivery of services. The IT Department shall confirm to the Response Coordinator when the threat has been eradicated. <u>Important Notice:</u> It is vital that the backup media that might be used to restore the system to its original state is cleaned of any viruses and other malicious code.	

5	Information Technology	**Recovery Function** In recovery, administrators of impacted devices will focus on restoring systems to normal operation. This function should consider the following steps, among other things: • Clean the system using anti-malware software; • Restore systems from uncorrupted data backups; • Rebuild systems from original media; • Bring up the server from an earlier point in time from the SAN local or remote copy; • Replace compromised files; • Resume processing from disaster recovery site; • Conduct software code review (if required); • Deploy required security patches; • Change credentials (specifically passwords); • Review existing controls to determine which, if any, controls should be strengthened. The IT Department will notify the Response Coordinator when the Recovery Function is complete.	
6	Response Coordinator	**Create Technical Report** The Response Coordinator, in consultation with the IT Department and, if applicable, Forensic Analyst, documents the complete evidence collection and subsequent analysis process thoroughly and in detail in a Technical Report. The Report will include: 1. Detailed information about the event, including actions taken and personnel involved; 2. Detailed information about the investigation; 3. When, where, and from whom the evidence was received (or taken); 4. The physical analysis (visual evaluation), including brand names, model numbers, and serial numbers; 5. The forensic duplication, including how the image was made (for digital evidence), the software and hardware used to make the image, and the hash comparison results; 6. Every step taken in the analysis of media; a. Explain what tools were used and what was or was not discovered as a result of these processes; b. Document other information such as: number of and size of sectors; operating systems; significant software, anti-virus; crash-guard software; etc.; c. All conclusions reached; d. How and when the evidence was returned or the manner in which it was disposed. The Technical Report should adhere to the following principles: • Report only verifiable information.	

		• Capture facts, and avoid stating conclusions unless clearly supported by facts. • Unless critical to the analysis, do not use names of persons, companies or organizations in the report. Instead refer to "subject, "suspect," or "victims." • Be precise. Avoid statements such as "numerous," "many," "multiple hundreds," etc. • Identify the evidence being analyzed as thoroughly as possible.	

Appendix I: Security Incidents Handling Playbook

IS Playbook_52021.doc

AFH Technology Cyber Incident Resp