<<<< BANK NAME >>>>

Incident Response Plan

(Includes Security Breach Notification)

December 2016

Document Name: Incident Response Plan (IRP)

Summary

The following document provides a detailed description of the <<<< BANK NAME >>>> response to information incidents. The Incident Response Plan (IRP) is utilized to identify, contain, remediate and respond to system, network alerts, events, and incidents that may impact the confidentiality, integrity or availability of confidential (i.e. customer) information. These are events that could threaten the integrity, health, and survivability of the organization. The IRP includes procedures for notification of customers in the event of a security breach causing potential misuse of customer sensitive information (aka nonpublic Personally Identifiable Information (NPI)). The procedures are also designed to meet the requirements set forth by GLBA in providing security breach notification.

Failure to comply with this IRP may undermine the organization's ability to identify, contain, and eradicate threats to the integrity, confidentiality, and availability of systems and data and remain compliant to GLBA Section 501b. This can also impact the process of prosecuting any individual responsible for an incident. Failure to comply with this plan may result in disciplinary actions up to and including termination of employment, agreements, and possible prosecution.

Our monitoring tool Aristotle Insight (www.aristotleinsight.com) will detect events and activities outside a baseline that it is able to track that may indicate a cybersecurity incident based on threat intelligence that needs to be followed up using the planning, verification and triage documented in this plan.
Examples may include:

- advance persistent threats (APT),
- anomalies and unusual behavior that does not meet baseline,

- potential breaches of acceptable use policy,
- misuse and abuse of applications, by percentage of use or out of baseline activity,
- inappropriate use of key words and phrases in searches, emails, or word documents,
- potential of data loss by use of USB, DVD/CD or other media,
- potential of data loss by excessive printing,
- new applications, new user and new workstations,
- correlation of events in firewall other network traffic and user activity on operating systems,
- downloads and installation of plug-ins, screen savers, any unapproved application or data,
- use of ports, protocols that are not normally used,
- login/out activity during business hours and outside business hours,
- access to folders, changes to security rights,
- use of privileged accounts; administrative privileges, active directory, VM and Core,
- Others

These Aristotle Insight detected activity will be tracked and if necessary further documented using the forms and procedures in this Incident Response Plan, otherwise only notation of the event can be made and history of the event and forensic evidence retained in the Aristotle Insight DataVault.

Our network support vendors utilize threat intelligence as a means of analyzing and acting on cybersecurity threats. If a zero-day threat becomes an incident, the ISO, IT Management or the Network Administrator may deviate from normal procedures to contain and control the incident. The measures may include but are not limited to; shutting down systems or applications, reconfiguring firewalls, disabling system access or other means of containing the threat. Containment is highly dependent on the type and scope of the incident. Once contained, the ISO will assess any potential exploitations of the threat and continue the response process accordingly. Senior Management will be notified of the deviation and the deviation will be included in the incident report.

Record of Changes

Revisions to this document will be issued periodically to reflect changes to policy, procedures, or responsibilities that do not warrant an update to the entire document. Changes will be issued by replacing entire Chapters, Sections, or pages. A complete list of revisions will be issued with each new change to ensure all documents are kept current. Changes should be entered in the document and recorded in the Table below.

Document Change Control Log:

Revision	Date	Author	Change Description
DRAFT	1/1/2016	Ken M. Shaurette	Initial version of document draft format by FIPCO.
FINAL	1/1/2016	na	Board Approved

Table of Contents

1.0 IRP Overview

IRP Introduction

In order to coordinate response to and resolution of incidents, <<<< BANK NAME >>>> has established an Incident Response Plan (IRP). The plan gives the Incident Response Team (IRT) the flexibility to implement procedures vital to the confidentiality, availability and integrity of company assets especially nonpublic personally identifiable information (NPI). An IRP is required in order to bring needed resources together in an organized manner to deal with an adverse event related to the safety and security of Bank information resources. The IRP provides guidance for an orderly response to incidents such as malware (aka viruses), suspected hacking events and compromises, improper disclosure of confidential information, breach of NPI and any other event that puts protected information at risk. In addition it outlines the authority that the IRT has for putting the plan into action when responding to a crisis situation.

The IRT will be led by an IRT Coordinator (or alternate). The IRT will be brought together on an incident by incident basis appropriate to the incident and will consist of appropriate staff from within the bank. This group will form the incident team appropriate for handling each specific incident.

Scope

This IRP applies to all hard copy, computer systems, networks, and devices connected that make up the Bank's business computing environment. It also applies to information in any format including electronic, printed or spoken. Any vendor or other third party requiring access to Bank computer resources is required to comply with the IRP as well as other standards, procedures, plans and policies.

Intended Audience

The Board of Directors is responsible for review and approval of the plan for purposes of meeting GLBA Section 501b compliance. The intended audience for executing on this plan is the core IRT and any associated staff that may be called upon to perform the duties as IRT members in order to gather data or remediate an incident.

INCIDENT DEFINITION

A cybersecurity incident is any adverse event whereby some aspect of information technology could be threatened: loss of data confidentiality, disruption of data or system integrity, or disruption or denial of availability. The following categories and examples are considered an incident:

- **Compromise of integrity**, such as when a virus infects a program, the discovery and compromise of a serious application vulnerability, or changes to system hardware or software characteristics without the Bank’s knowledge, instruction or consent(i.e. Ransomware);

- **Denial of service**, such as when an attacker has disabled a system by saturating the network with data in such a way that bandwidth is not available for legitimate access;
- **Misuse**, such as when an intrude (or insider) makes unauthorized use of an account or unauthorized use of technology resources for processing, copying, deleting or storing data;
- **Damage**, such as destructive Malware;
- **Intrusions**, such as when an intruder or Malware penetrates or attempts to penetrate system security; and
- **Unauthorized acquisition** of data that compromises the security, confidentiality or integrity of personally identifiable and/or sensitive, confidential information maintained by the Bank.

SENSITIVE CUSTOMER INFORMATION

Sensitive customer information is a customer’s name, address or telephone number in conjunction with the customer’s Social Security number, driver’s license, account number, credit or debit card number, or a personal identification number or password that would permit access to the customer’s account. It also includes medical information and any combination of components of customer information that would allow someone to log on to or access the customer’s account, such as user name and password or password and account number. Refer to the <CONMPANY> Data Security Standard for more information.

2.0 IRP Roles and Responsibilities

The responsibilities for response team coordination will be assigned to the IRT Coordinator (or alternate) as defined by the Information Systems Policy.

Incident Response Team (IRT)

The base IRT consists of the members of the Information Systems Steering Committee as defined by the Information Systems Policy (Refer to the Appendix for team members and contact information).

The IRT is tasked with providing a quick, coordinated response to alerts, events, and incidents across the Bank. The authority to make decisions and implement necessary measures is given to the primary and alternate IRT Coordinators.

IRT Coordinator (or alternate)

If necessary <<<< BANK NAME >>>> may chose to assign the specific IRT Coordinator (or alternate) duties to a different <<<< BANK NAME >>>> Staff member (technical staff or outsourced vendor if appropriate) for a specific alert. Every declared Incident will have a primary

IRT Coordinator (or alternate), this could be a designated staff member responsible for follow through on the specific incident, but must be a person trained in the IRP.

The IRT Coordinator (or alternate) is charged with the responsibility of researching the potential impact of an incident and coordinating the response activities.

The IRT Coordinator (or alternate) will:

- Develop and deliver the initial Incident report to management and the Board.
- Communicate all updates and changes in status to the IRT Coordinator or management.
- Develop and deliver required updates to the initial report at applicable times, depending on the severity of the incident.
- Develop and deliver the final Incident report.
- Coordinate any Computer Forensics activity.
- Coordinate and Data Recovery activity.
- Participate from beginning to end in the Incident.

The IRT Coordinator (or alternate) must follow the IRP and will be a key member of the IRT throughout the investigation.

The IRT Coordinator and alternate have responsibility to:

- Subscribe to various Computer Security Alert Services to remain abreast of relevant threats, vulnerabilities, or alerts from actual incidents for other organizations or in other industries.
- Maintain the IRP.

  The IRP provides documentation that helps establish the criteria of incident severity determination along with detail IRP Standard Operating Procedures (Appendix A) to assist with an overall IRP, customer notification on potential data breach and the coordination of corporate communications flow during any given response activity.

- Protect the confidentially, integrity and availability of the organization's information assets as required by organization policy, laws and regulations (i.e. GLBA, Security Breach - Wisconsin Statute § 134.98).
- Provide a point of contact during incident activity for the dissemination of and reporting of appropriate information.
- Minimize the negative impact that an information event or incident might have on business operations, financial state, and/or public image.
- Minimize legal implications generated by an information event or incident, including compromise of customer data.

- Establish employee awareness of incident reporting and when appropriate these procedures for investigating and gather data about an incident.
- Provide timeliness in reporting of incidents as necessary to customers in the event that non-public personal information is compromised.
- Coordinate and protect the collection of necessary data and evidence for event and incident resolution, eradication, and if necessary prosecution.
- Test the plan at least annually with the IRT.

3.0 Assumptions

The following assumptions have been made and approved by all involved parties to expedite the start to finish management of all alerts, events, and incidents:

- Executive management has given the support and authority to the IRT Coordinator and alternative coordinator to make appropriate executive decisions or seek necessary advice during a response scenario. This includes keeping appropriate management informed from start to finish.
- The IRT has the necessary resources readily available for completing a security investigation, including appropriate resources and third party contact list for reputable computer forensic investigators and law enforcement authorities.
- Out-of-band communication channels are established and available.
- Processes or technology that provides the ability to securely (i.e. encrypted) communicate electronically when necessary will be established.
- Internal public relations points of contact are available, as required.
- Responsible parties and applicable vendors immediately and accurately report suspected alerts, events, and incidents to the IRT Coordinator (or alternate).

4.0 Exceptions to Plan

This document identifies standard operating procedures for responding to an incident. Deviations from the standard process must be reported and approved by the IS Committee. All deviations must be documented so the IRP can be updated in the future. This documentation will be reviewed during the post-mortem phase of an incident for permanent change consideration. The plan will be presented after major changes or at least annually to the Board of Directors for approval.

5.0 Notification

The IRT Coordinator (or alternate) will be the central point for contact to report an alert, event or incident. Anyone who suspects an event or incident has occurred should contact the IRT Coordinator (or alternate) as quickly as practical. Other areas that can be contacted include the

Help Desk or any member of the Information Systems Steering Committee (refer to Appendix for list of names). Documented support numbers and notification procedures are documented in the Appendix.

When possible a follow-up e-mail containing applicable information regarding the suspected activity is also requested. The follow-up email can be sent to the IRT Coordinator (or alternate).

6.0 Incident Response Plan

7.0 Identification

The initial source from where an Incident is identified is immaterial. Potential Incidents can be reported from a variety of sources. A key source for detection of unusual behavior will be our activity tracking and behavior analytics tool Aristotle Insight. The following list is not all-inclusive, but contains some potential means of identifying Incidents:

- Alert or alerts from intrusion detection and monitoring tools
- Advance Persistent Threats
- Use of Privileged Access that does not match to Change Management
- Excessive use of the Internet based on Aristotle Insight parameters
- Use of Inappropriate keywords or phrases as documented in Aristotle Insight
- Log files from systems, servers, firewalls, or other network equipment
- A report of a person recently terminated and threatening retaliatory action(s)
- A web administrator’s report of the defacement of a company web site
- Customers or other 3rd parties including vendor service providers
- User reporting a virus infection to the Help Desk
- Customer reporting suspected or unusual activity that might signify an incident has occurred including suspected identify theft
- Law enforcement, examiners or state/federal agencies

- Public reports that a fast-spreading virus or worm is causing severe problems for specific systems, networks, applications or databases, this includes information from trusted alert services

- A report of the theft of computer hardware

The IRT Coordinator (or alternate) upon notification must determine the risk of continuing operations using any affected system or process. In addition determination must be made quickly whether the potential incident will have legal ramifications. This must be done in order to ensure that evidence is properly gathered and preserved in case of possible criminal prosecution.

If there is a need for Containment; the steps outlined in the Containment Section of this IRP must be followed. Network and computer logs of the system must be gathered immediately. Other logs that need to be collected and reviewed include the logs of systems that regularly connect to the affected system and logs of routers and other network devices to determine if the compromised system was used as a launch point to attain access to other parts of the Bank's network or other company's networks. It may be necessary to contact the Bank's outsourced network vendor, but caution should be exercised in case that there are possible confidentiality considerations required about the incident. (For example; a high ranking employee is involved in the event and this could be embarrassing or something the Bank needs to carefully manage release of information.)

A SAR Reporting form (www.fincen.gov/forms/files/f9022-47_sar-di.pdf) could be used to begin gathering information about the incident depending on the type of incident involved. Otherwise in the appendix there is the Incident Identification & Gathering Form along with the Computer System Data Gathering form that can also be used appropriate to the type of incident and information to be gathered. These may be more appropriate for use to capture initial information about the incident from a computer perspective including the following information:

- Method Incident was reported
- System date and time
- As much information as can be gathered about the applications, databases, systems, network, people involved; that can be gathered near the time that the incident was reported to have occurred
- A list of users currently logged on
- A list of current or recent connections from other systems

Once an incident has been reported, or suspected, the IRT will analyze all symptoms and available data gathered during the Triage Phase to ensure whether or not an incident has truly occurred. The Triage Phase is described later in this document.

8.0 Verification

Identifying an Incident may result in the need to employ a large amount of Information Security resources. The importance of eliminating any security threat is critical. During the identification and verification process, all team members will adhere to the following:

- **Assumptions -** Do not assume anything. Network Events are volatile by design and must be recognized as such. Fraudulent activity could have legal ramifications, requires extreme confidentiality and improper handling could alert the perpetrator or result in evidence tampering.
- **Data Collection -** Collect as much information as possible on the system or device including the Operating System (OS) type, the OS version number, applications running on the system, system configuration, etc.. Obtain any hard proof of the event. Identify names of any people that may have been involved or suspected of having information pertaining to the incident.
- **Information Gathering -** If an individual gathers the incident information, gather all information that is available from the involved party such as times and location where the event is believed to have occurred, how the incident was noticed, names of other people

who may have information etc... Ensure a detailed description of symptoms and the times symptoms were noticed are included in the report.

- **Logging** – A detail log of activities, processes followed; the findings and who performed them along with the date and time must be maintained from initial alert to post-mortem of the incident.

9.0 Notification

Once an Incident is confirmed, the IRT Coordinator (or alternate) will distribute notifications to the necessary contact list. Note that the handling of Incidents is not necessarily improved by an increased number of people that are aware an incident has taken place.

At initiation of an Incident, the IRT Coordinator (or alternate) will ensure the IRT enforces a strict "Need-To-Know" policy in order to control communication channels. Notifications will vary based on the type of incident that has taken place. All notifications will be documented on an IRP Processing Log. Samples are provided in the Appendix.

10.0 Triage Phase

The IRT Coordinator (or alternate) assembles the IRT staff to gather preliminary details about the Incident. The IRT Coordinator (or alternate) will activate the full IRT, this team may include all or part of the IS Committee depending on the incident and personnel needing to be involved in gathering information.

The IRT will:

- Evaluate the need to use forensic procedures. This decision must be made before any response is performed, as it will affect the techniques and tools that can be used in the response. Internal staff must **NOT** attempt any forensic procedures without instructions received directly from a computer forensics expert of the IRT Coordinator (or alternate).

- Allocate resources and personnel to the IRT, based on initial analysis and identification of the incident. This may require contact to Sergeant Laboratories for assistance gathering digital evidence from the Aristotle Insight DataVault or in more extreme cases; activation of an engagement letter/contract with Computer Forensics experts. Potential Vendors & Contact information are included in the Appendix.

- If an Incident is declared for any occurrence of hardware theft. Interviews with personnel originally responsible for the equipment will be conducted to qualify the severity of the threat.

- External organizations may need to be contacted. Authority to make this decision resides with the IRT Coordinator (or alternate).

  These organizations could include:

  - FDIC, Federal Reserve, State DFI
  - Federal Trade Commission (FTC)

- Computer Forensics Consulting Experts (see appendix)
- The Internet Service Provider providing access to the compromised system.
- Credit Reporting Agencies (Equifax, Experian, TransUnion)
- Local Law Enforcement Computer Crime division (see appendix)
- Local FBI (typically contacted on recommendations from local law enforcement)
- Media outlets – The

11.0 Triage Summary

From the beginning of the Incident, an IRT Coordinator (or alternate) must take step-by-step notes consisting of actions taken, by whom, including dates, and times. Keep these notes in chronological order and stick to the facts. Sample forms are supplied in Appendix C of this document.

Reminder: NEVER ASSUME ANYTHING!

Use the logging templates provided in this document for assistance. Make sure the logging is accurate. Make note of even the smallest or seemingly inconsequential things. Always note the time of discovery any notes and the person who took them. It may become necessary at a future date to testify in court or in a formal review by management or an external source (i.e. computer forensic experts).

When beginning the triage check for simple mistakes first. System configuration errors, program errors, recent software upgrades, hardware failures and human error can all become misinterpreted as a security breach.

12.0 Containment

Depending on the severity of the event, the affected system(s) may be taken off-line until the root cause of the event is eradicated. The recommendation to remove the affected system from the network will be made by the IRT Coordinator (or alternate) and submitted to the IRT for discussion and final approval. The IRT Coordinator (or alternate) is responsible for ensuring timely approval to take the system offline.

If the decision is made to remove the system from the network for eradication, containment, and/or investigative purposes, the network cable will be removed from affected system. **DO NOT REBOOT OR MAKE ANY CHANGES TO THE SYSTEM ITSELF.** The physical area where the incident occurred must be physically secured. Care must be taken not to alert any person(s) that may have been involved in the event/incident to the actions that are being taken by the IRT.

If the system is a mission critical asset, activate the appropriate components of the Disaster Recovery Plan to use alternate or redundant backup systems until the necessary computer forensic evidence procedures can be completed and the system can then be restored to a secure, production ready state.

Preparation for a backup system should be planned in advance to accommodate the need to replace the system functionality even if in a temporarily degraded state.

Isolating network services or servers may significantly affect continued business functionality and customer service. Input from the appropriate business areas with regard to the impact to business must be considered. Always consult with senior business area management and the IRT before shutting down major services. Communications with appropriate team members is critical.

During any investigative process, the IRT Coordinator (or alternate) must maintain constant communication with the IRT or other experts and business areas in order to make recommendations and decisions that may not be specifically outlined in this IRP.

13.0 Eradication

The goal of eradication is to eliminate or mitigate whatever factors led to the compromise of the system(s). A security problem cannot be fixed without an understanding of what happened, but risks could be reduced and the system can be further monitored for additional or ongoing activity by the perpetrator at the discretion of the IRT Coordinator (or alternate). If ongoing tracking of a situation regarding computer use is necessary, network system logs may need to be carefully reviewed or consideration given to a more robust monitoring tool such as Aristotle from Sergeant Laboratories to track user and computer activity.

When it is felt that necessary data has been gathered from mission critical systems they must be put back into production as soon as possible. Before being put back into service the system should be rebuilt from a trusted backup, hardened, and restored using applicable backups of system data.

The IRT will analyze all of the information gathered in an attempt to determine the method of compromise. The system may also need to undergo thorough vulnerability assessment testing. It is highly possible that methods or vulnerabilities exploited by an intruder resulting in system compromise may never be known. As a result special due diligence must be taken to analyze known vulnerabilities (internal and external) and mitigate appropriately to reduce the potential that the same intrusion methods could be reused.

The IRT should at this point have the evidence required to perform an investigation of the incident. The information gathered during the Triage Phase may be sufficient to determine the cause and effect. If there is insufficient evidence to arrive at an exact understanding of the attack and how the attacker exploited a weakness; team members should document all realistic possibilities based upon the available information. This will provide the team collectively with information that could help develop realistic scenarios to explain what has occurred. It can help the team make an informed analysis and judgment of what occurred and helps identify new controls that may be necessary or controls that require reinforcement.

Compromised non-mission critical systems will not be allowed to reestablish network connections until the team has a reasonably full understanding of the potential cause of the incident and can direct specific mitigation procedures or implement compensating controls.

14.0 Recovery

Affected systems must be restored to their pre-incident condition. This may require rebuilding the system from a trusted backup or from scratch.

Completing the following steps will assist in the recovery process:

- Reinstall, harden, and recover data for the system. The IRT Coordinator (or alternate) can approve the restore of a system from backup media. If this option is taken, make every effort to ensure that the restore is from a backup made before any potential timeline of the compromise or beginning of the incident.
- Validate the system. Once the system has been restored, verify that the operation was successful and the system is back to its normal condition.
- Harden the system using the latest system hardening techniques.
- Consider performing a vulnerability assessment of the involved systems and the overall network after the affected system(s) have been restored.
- Decide when to restore operations. The final decision rests with the IRT Coordinator (or alternate) in conjunction with the IRT.
- Monitor the systems. If the event was the result of a malicious code outbreak; back doors and sophisticated malicious code can be well hidden and may end up being restored from the backup. It is important to continue monitoring the system for reoccurrence of events that may indicate that root cause of the incident may have escaped detection and eradication. If this is the case it may be necessary to repeat the eradication steps.
- Depending on the severity of the incident consideration should be given to regular vulnerability assessment testing of the internal and/or external network and systems. The frequency must be determined based on the potential of recurrence and could be as often as monthly for at least 90 days after the incident to minimize that something may have gone undetected or could be introduced that would result in another incident.

15.0 Post-Mortem/Lessons Learned

The postmortem phase provides a mechanism to learn from the event and update the incident response plan and procedures. Lessons learned that are not captured in a reasonable time after the event may be lost.

Refer to notes, logs from the event, and other data gathered during the investigation. A postmortem report, including lessons learned, is the accepted method of protecting the knowledge so that it can be used in the future. This phase can help improve response for future events.

Some useful tips that might aid in conducting the postmortem phase are:

- Hold a “Lessons Learned Meeting” with the IRT as soon as practicable after the event has been resolved. It is suggested that no more than 5 days elapse following the conclusion of the incident. The meeting should focus on recreating the incident using a tabletop exercise. The exercise would review successes and identify areas for improvements.

- Reviewed during the post-mortem should be the logging that was performed, the overall IRP, any forms that were completed and the recap of forensic analysis, if it was completed.
- Consider timeliness and adequacy of the method used for initial reporting, quality of information gained and whether staffs were properly responsive.
- Review the input from all interested parties that may have participated in the Incident. Comments, opinions and insights should be maintained as part of the post-mortem report draft.
- Build an Executive Summary report that would include a summary of the outcome from the incident, any estimated costs both from the actual incident as well as in resources, or that were deployed to resolve the incident. Establish and get approval of timelines and resources if any are necessary to mitigate outstanding issues.
- Present the Executive Summary to the Board of Directors at the next available board meeting.
- Send recommended changes to Bank management along with a cost estimate, high-level schedule, and if known the impact of implementing or not implementing any recommended actions.
- Ensure that budget is adequate and approved to make the required improvement(s) and management commits to meet established timelines. This may require board level involvement.

Appendix A: IRP Standard Operating Procedures

The following steps should be executed in sequence when possible, but could be executed out-of-order or even simultaneously without impacting the results of incident follow-up, depending on the situation.

Not all emergencies are the same, but these steps represent industry accepted practices. The steps provide a high level flow of the incident for the IRT Coordinator (or alternate) and team to follow. They are followed by the detail actions that should be taken or at least considered during the incident.

Emergency Procedures

1. **Remain Calm**

   Secure communications and coordination within the IRT are critical. Your composure will help everyone else remain calm. DO NOT communicate or make any assumptions about the situation outside the IRT. At this point, it is necessary to be very careful how the team proceeds. The team may need to react quickly. Be careful to avoid making changes to any system that could compromise further investigation in the future or damage evidence that may be needed if the incident is determined to be criminal activity. Caution must be exercised not to alter logs, erase evidence or alert potential perpetrators of the event that the incident has been discovered.

2. **Take Valuable Notes**

   All information and events must be tracked and recorded. Even miniscule details must be included. Date and time stamps must be entered with each log entry. All members of the IRT must log their actions with a time and date stamp, regardless of whether they are physically present at the potential incident site. Keep in mind that notes may have to be used as evidence in court. Even a camera can be handy to capture the state of computer screens and pictures can be a helpful reminder of the activities that occurred during the incident.

   Evidence logs must be kept secured with a precise chain of custody, if there is strong suspicion that a crime has been committed using computers, contract with a Digital Forensic Expert for advice and assistance as quickly as possible. At minimum the following information should be recorded:

   a. Dates and times when events were discovered, reported and/or occurred
   b. Date and times of any communications related to the incident
   c. Personnel and actions performed during the IRP
   d. Systems, accounts, services, data, and networks that may have been affected by the incident. Any remote or outside IRT members must also keep accurate notes.
   e. Details describing the circumstances and parties involved in any non-computer related incident.

3. Identification

Gather all information that is available from various involved parties. Interview the person who identified the possible incident as well as the system administrator for the suspect system(s). Include in the IRP logs a detailed description of symptoms and what time the symptoms were noticed.

Once an incident has been reported, or suspected, the IRT must analyze all symptoms and available data gathered during the Triage phase to ensure whether or not an incident has truly occurred.

This step is likely the first point in the process where identification of a breach of access to NPI or Sensitive Customer Information may have occurred, and the extent to which a breach extends. When a breach of NPI or Sensitive Customer Information has been identified it is necessary to begin the Customer Notification Procedure (Appendix B) as soon as practicable.

4. Enforce a "Need to Know" Policy

Once an incident is reported to security personnel, there is no need to discuss the incident with individuals not involved in the IRP process. This is an important item to remember since the source of the incident may be an internal staff member and discussion may alert them to the investigation. Unnecessary discussion will also reduce speculation and rumor based on incomplete information or constantly changing theories by the IRT regarding the source and extent of the incident. Remind the IRT that they are trusted individuals and that the company is counting on their discretion. Avoid speculation about the incident.

5. Use Out-of-Band Communications

The communications methods used during an incident must be secure and timely. Since we won't know the extent, type, or threat involved in an intrusion until proper analysis is done, all standard, insecure forms of communications must be suspect even from the beginning. It is recommended for communications to be out-of-band with regard to company services to ensure an intruder would not be able to intercept any communications (i.e. email, intercompany mail) and become aware of the investigation, the plans and IRT responses.

During any given IRP process there are personnel permanently responsible for IRP as well as temporarily assigned resources that may differ depending on the incident. Any transfer of files over the Bank's internal network or over the Internet must be performed securely. Encrypt files or use a secure portal to share information.

It must be assumed that an intruder might have a sniffer on the internal network and any unsecured information traveling the network may be intercepted. This includes all e-mail, attachments and file transfers. Insecure communication could compromise the IRT planned responses as well as plans for analysis of the incident. An interception of our communication could alert the intruder causing tampering with any evidence in an attempt to cover their tracks or activities could immediately become more malicious including deleting or destroying critical files, evidence or databases.

6. Containment

Proper steps must be taken to ensure that the problem will not get any worse. This could include actions like installing filters to block a denial of service attack, disconnecting the company from Internet connectivity, or isolating the impacted system from the rest of the company Network. ONLY the IRT Coordinator (or alternate) along with the IRT is authorized to make this decision and will likely not be making the decision alone. It will be necessary to ensure that disconnecting the system is feasible as a business, technical, or legal matter and that disconnecting the system does not create a worse problem than the effects of the actual incident. The original intent of the event might have been to get the system taken offline in order to have an impact on the business.

Attempts to remove an attacker could result in more damage to the network and eliminate any chance of catching the perpetrator. Attacks from outside the company tend to have a low identification rate. Caution must be used to avoid encouraging the attacker to cause more damage to the systems as well as erase data including what was done, how access was gained, system log files, and other evidence that may be left behind. The IRT Coordinator (or alternate) may decide to leave the system and connection as is, and monitor the attack to gather evidence rather than shutting off the attack. This should never be done if access is suspected to a system containing customer information.

7. Backup the System

Typically the best evidence on any incident is the analysis of the system's state when the incident was first detected.

The best way to maintain evidence and get a system back up and running quickly is to swap out the systems hard drive with a replacement drive and secure the original hard drive(s) (ensure evidence of proper chain of custody) of the system until appropriate forensic duplication can be completed. Be sure to maintain a chain of custody. Performance of Computer Forensics activities must only be performed by experienced and trained forensics professional if the Bank expects to use the data to prosecute a criminal case or use the evidence in a court proceeding. It is critical to maintain accurate and detail activity logs. Ensure date and time stamps are associated with every action performed.

Eradicate the Problem

Once the system has been isolated and a good forensic backup taken, the system must be prepared to return to production. At this point, the system must be rebuilt. The <<<< BANK NAME >>>> System Administrator will ensure that the current hardening procedures are performed on the system. After the system and associated applications are working properly it is recommended that a vulnerability assessment be performed of the computing environment, consider both internal and external. This is important especially for impacted system and systems that it interfaces with. If this was suspected as being an attack using technical exposure, vulnerability scanning is strong encouraged.

It is necessary to make the system as secure as possible until the final cause of breach, or a strong theory, is known. Detail logging and active monitoring of the system is a must during this stage. Until the breach method is known, the system should be monitored very carefully for further breaches. Also, carefully inspect and watch other systems especially any that the compromised system regularly interfaces with and users who regularly interface with the compromised system.

8. **Resume Business**

   After receiving approval from the IRT Coordinator (or alternate), the system can be returned to the production environment. Continue to carefully monitor the restored system to ensure it is performing its tasks properly. Once the system is reconnected to the network; monitor the compromised system for a minimum number of days (two weeks recommended) to ensure that system stability and suspected activities do not recur. Daily and weekly system log reporting must continue to be performed during and at the end of this two week monitoring period.

Detail Computer IRP Procedures

The procedures documented below assume the event being handled is associated with computer processing equipment.

When following the detail procedures if you are unclear about a particular step or if it is felt that it might be necessary to deviate, contact the IRT Coordinator (or alternate) or have discussion with the entire IRT. Anyone assigned to handle an Alert, Event or Incident should make sure that each step is at least considered during the IRP process.

1. **Immediately remove the system suspected of compromise from the network.** Remove by unplugging the network cable. DO NOT reboot the machine. DO NOT halt or freeze the system at this point. Consider severity of the system and whether the DR/BC Plan needs to be initiated to continue processing.
2. **Begin completing the Incident Identification Log.** The IRT Coordinator (or alternate) will ensure each entry is time/date stamped. Notes should be as detailed as possible and based on fact to the extent possible. Suspicions or opinions can be included, but should

be labeled as such. Record all activity, actions, and communications between all personnel involved in the situation or outside the specific alert/event/incident.

> **NOTE:** IRT Coordinator (or alternate); Remember, it may be necessary to testify in court based on the accuracy of notes taken and the notes will provide a way potentially several months later to recall the activity that occurred during the situation. The incident notes may be the only things allowed in court during testimony to refresh your memory.

3. **Ensure all appropriate forms are completed.** The IRT Coordinator (or alternate) ensures that appropriate IRP forms (samples included in Appendix C) are completed.
4. **Properly handle all potential criminal evidence.** Evidence of a potential crime (including media, photos, team logs, etc) must be handled properly (i.e. chain of custody). *Only trained Computer Forensics personnel are authorized to perform gathering of information from computer systems once suspicion of a crime has been determined.* Any pictures that are taken of the crime scene, the system, and anything on the console screen immediately after the incident is reported may become evidence and must be protected from tampering.
5. **Secure the Incident scene.** Limit the amount of activity on the system to as little as possible. Limit the staff that can perform any actions on the computer, preferably to only a single individual. If this individual is a third party, be sure that an internal Bank member is monitoring their actions and evidence of their actions can be formally documented. Record the current state of the computer and log any access by personnel to the room where it is stored. Record what was on the screen at the time of the incident, if anything and take photographs where possible. Take photographs of the computer and the immediate area where the computer is physically located.
6. **Activate the IRT.** The IRT Coordinator (or alternate) will notify and determine the necessary makeup of the IRT then assemble the permanent IRT members for this incident and assign other members of the team from staff and outside consultants (e.g. outsourced network resource) as necessary to help respond to the specific incident including outside entities such as law enforcement or computer forensics experts.

   If the incident is suspected to have high visibility or to be very invasive, a member that must be included on the IRT team should be the Bank President or a representative who is responsible for public and/or media contact. The Wisconsin Bankers Association media department may be called on to assist with handling of any release of information to the media.
7. **Interview the System Administrator.** Gather any facts possible including date the system was last patched, most current backup, etc. If the System Administrator might have involvement in the incident ensure that they are not allowed access to the system, either physically or remotely after verification of the incident.
8. **If Computer Forensics is Necessary.** Contract with a trusted computer forensics company or individual who is trained in gathering forensic information; refer to Appendix for possible companies. Internal staff must not begin to perform data gathering activities

unless there evidence is not expected to be needed to establish a legal or criminal case or evidence will not be needed to support employee termination.

9. **Gather and analyze system software and configuration files.** Check for the presence of attacker tools such as network sniffers, rootkits/backdoors, unapproved registry changes or evidence that might point to Trojans or keystroke loggers. **Check for tools and data that might be out of place and left behind by an attacker.** Check for Vulnerability Exploits and other Intruder tools, which can probe other systems, launch denial of service attacks or widespread network probes, warez files, or tools that can use corporate resources. Also, check for the output of these tools, or evidence of these tools in the logs and network connections.

10. **Review log files.** Remember that the attacker may have modified system log files stored on the compromised system. It is possible that deleted portions of the log will be recovered during the forensic process. Identify anything that seems out of the ordinary.

11. **CRITICAL ERROR POINT! Never assume anything at this point.** There will likely be pressure, possibly from high-level people, to provide answers. Unless verification is complete and there is evidence to back up a claim simply respond with facts or that evidence does not support any conclusion at this time.

12. **Check connected or dependent systems.** Check other systems on the network, especially those associated with the compromised system for possible upstream or downstream compromises.

13. **Review all information gathered.** Check all gathered information to determine if systems outside the company network which may have been affected or used in the compromise. Monitor performance of the system and network traffic for anomalies. The IRT can analyze system logs, possible hacker output files, and any other files created, modified, or used during the time of the intrusion to determine whether the source of the incident can be identified or any other systems were affected.

14. **Contact network or Internet Service Providers (ISP).** Coordinate with any outsourced network or ISP's used by the compromised system especially if the system has direct exposure outside the Bank, i.e. Profit Stars for web server. This is especially relevant in the case of a Distributed Denial of Service (DDOS) attack against the network.

15. **Notify appropriate officials, external to <<<< BANK NAME >>>>.** Notify the appropriate officials at the discretion of the IRT Coordinator (or alternate). Involve the IRT in any decision to contact external sources. This could include law enforcement, a national or regional Computer Emergency Response Team (CERT), and other agencies (FBI InfraGard, FS-ISAC) that may be able to help with the problem, or could help other companies avoid a similar situation.

16. **Install a clean version of the operating system.**

17. **Harden the system.** Work with a hardening expert to disable unnecessary services and install security patches. Review the current Security Implementation hardening procedures for the system**.**

18. **Restore the system.** If data must be restored from backups, ensure that the backup is not from a compromised system. Pay close attention to the data that is restored. It might be possible to reintroduce malicious code or other exploits when restoring data, especially when restoring user type directories.

19. **Change system passwords.** Ensure all passwords are changed for all Bank employees, consider both network and if separate passwords are used for critical applications. Ensure company's password complexity rules are followed when changing all passwords.

20. **Re-connect the system to the network.** The IRT Coordinator (or alternate) in cooperation with IRT will make the decision when to put a restored system back into production. Place the system back to a normal operational state when this approval is received.

21. **Finalize the investigation process.** IRT will continue the investigation if the method of compromise has not been determined.

22. **Finalize/complete IRT Coordinator (or alternate) responsibilities.** During the post-mortem phase of IRP, the IRT Coordinator (or alternate) will:

    - Ensure appropriate forms are completed properly and stored for future reference
    - Ensure that copies of the IRT Coordinator's (or alternate) notes, logbook, any pictures, and other evidence are properly copied (ensure chain of custody) and forwarded to the IRT and appropriate members of Executive as necessary.
    - Finalize and deliver the Incident Report

23. **Conduct post-mortem lessons learned analysis.** The IRT will conduct a lessons learned meeting and analyze events. The intention is to gather data to help update and improve controls, policies and procedures. This process may also identify control deficiencies and identify additional resources needed to minimize future events or reduce impact of future incidents.

24. **Securely archive all incident information.** All documents, forms, reports, correspondence, and copies of all media will be collected into a file that will be securely stored for future analysis. The file should include:

    - A technical explanation and executive summary of what occurred
    - Copies of e-mail correspondence and forensic analysis reports
    - Copies of IRT Coordinator (or alternate) and team notes, forms, and other gathered evidence

25. **Update the IRP.** Update the IRP policy and procedures (i.e. these procedures) to incorporate lessons learned from the incident.

Internal Security Violation Procedures

For insider security violations, the Bank will take at minimum the following actions:

1. For minor offenses, issue a verbal warning to employee(s) violating Bank policy.

2. Warn in writing and/or reassign or demote an employee(s) who repeatedly violates Bank policy.

3. Counsel, terminate or take legal action against employee(s) who repeatedly violate Bank security directives or who commit a serious offense.

Communications with the Media

The **<<<< POSITION NAME >>>>** or their appointed representative is solely responsible for all public statements regarding the Bank, including breaches of sensitive customer information.

Bank staff is instructed not to give any statements to the media. This includes press release, press conference or other types of radio, newspaper or television communication.

Information provided to the media is to be on a need to know basis and may include the following:

1. Description of the event.

2. Immediate and long-term affect on customers and Bank staff.

3. Approximate time frame in which affected operations or services will be secured and returned to normal operation or access.

4. Assurance that customer assets are secure and being protected; that the event is being addressed and is under control.

When Customer Notice Is NOT Required

The Bank is not required to give notice when it becomes aware of an incident of unauthorized access to customer information, and the Bank, after an appropriate investigation, can reasonably conclude that misuse of the information is unlikely to occur and takes appropriate steps to safeguard the interests of affected customers. For example, it would not be required for the Bank to notify affected customers in connection with the following types incidents, Management could still determine that notices will be given:

- The Bank is able to retrieve sensitive customer information that has been stolen, and reasonably concludes, based upon its investigation of the incident, that it has done so before the information has been copied, misused or transferred to another person who could misuse it;

- The Bank determines that sensitive customer information was improperly disposed of, but can establish that the information was not retrieved or used before it was destroyed properly;
- A hacker accessed files that contain only customer names and addresses; or
- A laptop computer containing sensitive customer information is lost, but the data is encrypted and may only be accessed with adequately secure authentication that was very unlikely to have been compromised.

When to provide Customer Notice!

The following are a few typical incidents that would generally signify a likely breach of information:

- An employee or other individual has obtained unauthorized access to sensitive customer information maintained in either paper or electronic form;
- A cyber intruder has broken into any Bank or vendor's system that contains NPI;
- Computer equipment such as a laptop computer, cell phone, floppy disk, CD-ROM, backup tape or other electronic media containing sensitive customer information has been lost or stolen;
- The Bank has not properly disposed of customer records containing sensitive customer information (includes workstations, servers, laptops, any electronic storage media); or
- The Bank's third party service provider has experienced any of the incidents described above, in connection with NPI.

Along with the documented emergency and detail response procedures identified by this incident management plan the Bank is required to notify affected customers when it is aware of incidents involving potential of compromised NPI unless the Bank, after an appropriate investigation, can reasonably conclude that misuse of the information is unlikely to occur and takes appropriate steps to safeguard the interests of affected customers. If this determination should occur it is important that formal documentation is created, retained and approved by Management and the Information Security Officer. Communication should still be provided to the Board of Directors of the incident.

Appendix B. GLBA Customer Data Breach Notification Procedure

Customer Data Security Breach Response Procedures

1. Notify the bank's primary Federal regulator (i.e. FDIC and DFI) as soon as practicable.
2. File a SAR Report
3. Ensure that appropriate steps have been taken to contain and control the incident to prevent further compromise of customer information. This shall include notifying all appropriate bank management and other security officers of the incident.
4. If warranted, appropriate customers shall be notified in a timely manner.

If it is determined that customer information has been compromised the IRT Coordinator shall ensure that the following corrective actions are recommended:

Corrective Measures

At minimum, appropriate Bank personnel are to conduct the following procedures in the event an incident involving unauthorized access to NPI (some of the following may already be documented in base IRP procedures) to mitigate substantial harm or inconvenience to affected customers:

1. Flag Affected Accounts. Accounts of customers whose information may have been compromised will be identified. These affected accounts are to be monitored for unusual activity, and appropriate controls monitored to prevent the unauthorized withdrawal or transfer of funds from customer accounts;

2. Secure Affected Accounts. All identified accounts, in addition to affected Bank services used to access such accounts, associated with the breach of customer information are to be secured by administrative, physical, technical, or other means to prevent further unauthorized access or use until such time as the Bank and the customer agree on a course of action;

3. Notify Affected Customers and Provide Assistance. It is the responsibility of the IRT Coordinator (or alternate) to notify affected customers through appropriate means (i.e., letter, telephone, e-mail, etc.), written notice is required, when the Bank becomes aware that sensitive customer information about them is the subject of unauthorized access.

   Customer notification by the Bank is to be limited to those persons specifically identified as those affected by the security breach. If specific customer identification is unattainable, the Bank is to notify each customer likely to be affected by the incident.

The notice should consider the following:

A. A general description of the incident that was the subject of unauthorized access or use of customer information in a clear and conspicuous manner. Describe the incident in general terms and include the type of customer information that may have been the subject of unauthorized access or use. Generally describe what action has been taken to protect further unauthorized access.
B. A designated customer service number at the Bank that customers can call for further information and assistance;
C. A reminder that customers need to remain vigilant, over the next twelve to twenty-four months, and to promptly report incidents of suspected identity theft to the Bank, credit reporting agencies, etc.;
D. Steps customers can take to obtain and review their credit reports and to file fraud alerts with nationwide credit reporting agencies as required by the Fair Credit Reporting Act, and other sources of information designed to assist individuals in protecting against identity theft:

   - Notify each nationwide credit reporting agency to place a fraud alert 18 in the customer's consumer reports;

   - Periodically obtain credit reports from each nationwide credit reporting agency and have information relating to fraudulent transactions deleted; and

   - Inform the customer of the right to obtain a credit report free of charge, if the customer has reason to believe that the file at the consumer reporting agency contains inaccurate information due to fraud, together with contact information regarding the nationwide credit reporting agencies.

E. Inform each affected customer about the availability of the Federal Trade Commission's (FTC) online guidance regarding measures to protect against identity theft and to encourage the customer to report any suspected incidents of identity theft to the FTC. The FTC's website address is http://www.ftc.gov/idtheft, and the toll free number for the identity theft hotline is 1–877–IDTHEFT (1-877-438-4338).
F. Consistent with SAR regulations, notify appropriate regulatory and law enforcement authorities. The FDIC and DFI along with appropriate law enforcement agencies are to be notified by the IRT Coordinator (or alternate) regarding the incident, in addition to the completion and submission of a Suspicious Activity Report (SAR) when the incident meets the requirements for official SAR filing it must be formally filed.

Appendix C. IRP Forms

The forms that follow include samples for tracking information on the Incident. Not all forms are necessary for every incident, but may be very valuable as a reminder of actions to take and data to gather.

The IRT Coordinator (or alternate) is responsible for making the determination of when it is necessary to formally file a Suspicious Activity Report (SAR) based on the incident. The Bank uses the following link for a SAR Reporting form. http://www.fincen.gov/forms/files/f9022-47_sar-di.pdf

16.0 Incident Identification & Reporting Form

Use this form to report an incident:

CONTACT INFORMATION

Name____Title______________________________
Organization____ Direct-
Dial Phone_______________________________E-mail____________________________

Legal Contact Name______________________________Phone______________________________
Location/Site(s) Involved____
Street Address____
City_______________________________________State_____________ZIP_____________ Main
Telephone___________________________________Fax______________________________ ISP
Contact Information____

INCIDENT DESCRIPTION

□Denial of Service	□Suspected attack probe or scan
□Intrusion External Hack	□Electronic Monitoring (sniffer)
□Misuse of Systems (internal or external)	□Website Defacement
□Malicious Code (virus, worm, Trojan)	□Corporate Policy Violation
□Suspected illegal Activity	□Violation of Acceptable Use
□Network or System Slowdown	

Other (specify) ____

____

DATE/TIME OF INCIDENT DISCOVERY

Date: ________________________ Time: _______________________________________

Estimated Duration of Incident: ____

IMPACT

□Loss/Compromise of Data	□System Downtime
□Damage to Systems/Data	□Network/System Slowdown
□Financial Loss (estimated amount: $_________________________)	□Other Organizations’ Systems Affected
Damage to the Integrity or Delivery of Critical Goods, Services or Information	

SEVERITY OF ATTACK, INCLUDING FINANCIAL LOSS OR INFRASTRUCTURE

□High □Medium □Low □Unknown

SENSITIVITY OF DATA

□High □Medium □Low □Unknown

Describe how the incident was detected and the location of available evidence supporting the incident, include contact information for people who may have reported the incident or are involved in the incident directly or indirectly.

Has corporate legal or law enforcement been contacted about this incident? If so indicate who & when?

Has the incident been resolved? Describe resolution steps that were taken

Has a post incident review been completed to identify mitigation steps to prevent reoccurrence? Describe results of post incident review or location where the information can be found.

17.0 Sample Customer Notification Letter

MODEL LETTER FOR COMPROMISE OF NPI

The following letter is a model for notifying people whose names and NPI such as Social Security numbers or bank account numbers have been compromised. In cases of stolen Social Security numbers or account numbers, it is important that people place a fraud alert on their credit reports. A fraud alert may hinder identity thieves from getting credit with stolen information because it is a signal to creditors to contact the consumer before opening new accounts or changing existing accounts. Potential victims of a theft also should be reminded to review their credit reports regularly to track whether their information is being misused. For some victims, weeks or months may pass between the time the information is stolen and the time it is misused.

Dear _____________:

We are contacting you about a potential problem involving identity theft.
[Describe the information compromise and how you are responding to it.]

We recommend that you place a fraud alert on your credit file. A fraud alert tells creditors to contact you before they open any new accounts or change your existing accounts. Call any one of the three major credit bureaus. As soon as one credit bureau confirms your fraud alert, the others are notified to place fraud alerts. All three credit reports will be sent to you, free of charge, for your review.

Equifax 800-685-1111	Experian 888-397-3742	TransUnion 800-680-7289

Even if you do not find any suspicious activity on your initial credit reports, the Federal Trade Commission (FTC) recommends that you check your credit reports periodically. Victim information sometimes is held for use or shared among a group of thieves at different times. Checking your credit reports periodically can help you spot problems and address them quickly.

If you find suspicious activity on your credit reports or have reason to believe your information is being misused, call [insert contact information for law enforcement] and file a police report. Get a copy of the report; many creditors want the information it contains to absolve you of the fraudulent debts. You also should file a complaint with the FTC atwww.ftc.gov/idtheft or at 1-877-ID-THEFT (877-438-4338). Your complaint will be added to the FTC's Identity Theft Data Clearinghouse, where it will be accessible to law enforcers for their investigations.

We have enclosed a copy of Take Charge: Fighting Back Against Identity Theft, a comprehensive guide from the FTC to help you guard against and deal with identity theft.

[Insert closing] Your Name

18.0 Computer System Data Gathering Form

Task	Completed By	Date/Time Completed
Notification & Identification		

Date:	**Month DD, YYYY**	**Alert ID:**	**20__-xxx**
Point of Contact:	**Name:** **Office:**	**E-mail:** **Cell:** mailto:bryon.miller@bcbsga.com	
Title:			
Impact:	□Low □Medium □ High □ Critical		

Assign Tracking Number		
Notify IRT Coordinator (or alternate): Time E-mail Was Sent:__________ Time Called:__________		
Complete Incident Identification Form		
Initiate IRP Activity Recording On IRP Chronological Logs.		
Identify All Involved Systems.		
Determine extent of Customer information involved in loss and whether there is a need to perform Security Breach notification procedures.		
Send Incident Notification Report To Executive Management, Through IRT Coordinator.		
Containment:		
Deploy The IRT		
Annotate IRT Members On The IRP Processing Log.		
Remove The Affected Machine(s) From The Network		
Physically Secure The Area Where The Incident Occurred		
Backup The System Using NEW Media		
Store Backup Media In A Secure Location		
Change Passwords On The Affected System		
Change Passwords On Connected Systems		
Collect All Available System Information		

Affected System(s)	
IP Address:	
Hostname:	
Network Location:	□Internal □ DMZ
User's Name/Network ID:	
User's Manager:	
Technical Details	
Technical Description:	<Enter Technical Description>
Recommendations:	<Enter Recommendations>
Patch Availability:	<Enter Location or information on the Patch or Virus Definitions>

Eradication:		
Isolate the attack and determine how it was executed.		
Implement Appropriate Protection Techniques (Firewall/Router Changes, Vulnerability Patches, Etc.)		
Perform Scans On The Affected System To Ensure The Vulnerability Has Been Removed.		
Perform A Subnet Scan To Identify Other Systems That May Have The Same Vulnerability As The Affected System.		
Recovery:		
Reload The Affected System.		
Restore The Affected System.		
Perform The Latest IT Security Hardening Procedures.		
Monitor The System For 14 Days After Final Incident Resolution.		
Postmortem:		
Create A Draft Incident Report – Sample form included in Appendix C of IRP.		
Conduct A Postmortem Meeting With All IRP Team Members.		
Finalize Incident Report		
Send Incident Report To IRT Coordinator For Distribution.		

Reporting	
Reporting Incident:	Incident reporting form
Remediation Plan Due:	<Enter Due Date For Remediation Plan>

19.0 Eradication Form

Date		**Incident Tracking #**	YYYY-Sequence#

List the names of all persons who performed forensics on affected system(s):

Was the vulnerability identified? Describe:

List the validation procedures used to ensure the cause of the Incident was eradicated:

20.0 Processing Log

#:	**Date/Time:**	**Item Description/Comments:**

1		
2		
3		
4		
5		

21.0 Photographic Evidence Log

#:	Date/Time:	Description:	Location:	Photographer:
1				
2				
3				
4				
5				

22.0 Electronic Evidence Log

#:	Date/Time:	Description:	Location:	Recorder:
1				
2				
3				
4				
5				

23.0 Information Technology Steering Committee

Commented [kms1]: INSERT BANKS ACTUAL IT COMMITTEE NAME

Contact	Contact Information

24.0 Miscellaneous Other Important Contact Numbers

Contact	Contact Information
FDIC – OCC – NCUA – FRB - ????	

Wisconsin State DFI	Tim Sinz, Asst. Director WI DFI Madison (608) 267-6830
Federal Reserve	Federal Reserve Bank of Chicago 230 South LaSalle St. Chicago, IL 60604 (312) 322-5322
FBI InfraGard	Local Wisconsin InfraGard chapters website: www.infragard.net/chapters/wisconsin/
FS-ISAC, Financial Information Sharing and Analysis Center	Financial Services - Information Sharing and Analysis Center (888) 732-2812 (toll free) (703) 948-4044 (Direct) www.fs-isac.org
Federal Trade Commission (FTC)	Internet Fraud & Safety www.ftc.gov/bcp/menus/consumer/tech/privacy.shtm Identity Theft www.ftc.gov/bcp/edu/microsites/idtheft/ Privacy and Data Security www.ftc.gov/privacy/
Better Business Bureau Report a Scam	Report A Scam IMPORTANT: You will not receive an individual response from BBB concerning your BBB Scam Tracker report. https://www.bbb.org/scamtracker/us/reportscam
Internet Crime Complaint Center	https://www.ic3.gov/faq/default.aspx
OTHER BANK IMPORTANT CONTACT INSERTED HERE AS APPROPRIATE	
Internet Services Provider	**BANK CONTACT FOR SERVICE PROVIDER**
Outsourced Network Services	**BANK CONTACT FOR ANY OUTSOURCED NETWORK OR SYSTEM SERVICES**

25.0 Computer Forensics and Data Recovery Contact Numbers

Commented [kms2]: INSERT VENDORS WHO HAVE BEEN VETTED FOR THE BANKS PUPOPSES AND APPROPRIATE TO BANKS GEOGRAPHIC REGION IF DESIRED

- The vendor contacts are listed below in alphabetical order.

These vendors have been separated into two distinct groups. While some of the vendors provide services in both area they have been listed in both categories. The two areas are services Digital

Forensics and legal investigation and the second being vendors that can recover data on damaged electronic devices such as hard drives or other storage media include cameras and cell phones.

Computer (Digital) Forensics	Vendor Contact Information
Sergeant Laboratories – Aristotle Insight ***(if using a DataVault, may offer Digital Forensics support with contract their base license agreement for AristotleInsight)***	866.SGTLABS (748.5227) info@provecompliance.com Local – 608.788.9143 200 Mason St. Onalaska, WI 54650
Digital Intelligence, Inc. ***(Recommended for Digital Forensics)***	Douglas G. Elrick Director of Forensic Services Digital Intelligence, Inc. 17165 W. Glendale Dr. New Berlin, WI 53151 (866) 344-4683 (toll free) (262) 782-3332 (phone) www.DigitalIntelligence.com
Gillware Inc. ***(Recommended for Digital Forensics)***	Cindy Murphy President Gillware Inc. 10 Terrace Court Suite 103 Madison, WI 53718 (877) 624-7206 (toll free) (608) 237-8780 (phone) gillware@gillware.com https://www.gillware.com/forensics/
Kroll Ontrack - Legal Discovery	Kroll Ontrack Inc. 9023 Columbine Rd. Eden Prairie, MN 55347 (800) 347-6105 (toll free) (952) 937-5161 (phone) http://www.krollontrack.com/
Data Recovery Vendors	**Vendor Contact Information**
Kroll Ontrack - Data Recovery	Kroll Ontrack Inc. 9023 Columbine Rd. Eden Prairie, MN 55347 (800) 872-2599 (toll free)

	(952) 937-5161 (phone) http://www.ontrackdatarecovery.com/

26.0 Law Enforcement

Contact with law enforcement is not recommended unless an incident has been verified to have criminal elements, however it is recommended to involve law enforcement as quickly as possible if there is any chance of an event having criminal or legal impacts.

This would typically mean that Digital Forensics has also been completed to gather appropriate evidence.

In any incident where there is suspicion of child pornography law enforcement must be contacted as quickly as practicable.

Name	Contact Information
LOCAL Police Department	ADDDRESS AND PERTINENT PHONE NUMBERS
LOCAL County Sheriff's Department	ADDDRESS AND PERTINENT PHONE NUMBERS
Local FBI Office if available	ADDDRESS AND PERTINENT PHONE NUMBERS
FBI Wisconsin Division Headquarters	Plaza East Building 330 E. Kilbourn Ave, Suite 600 Milwaukee, WI 53202 (414) 276-4684 (phone) (414) 291-2400 (fax)

27.0 Media Contacts

Name	Contact Information
LOCAL MEDIA OUTLETS, PAPER, RADIO, TELEVISION	ADDDRESS AND PERTINENT PHONE NUMBERS
LOCAL MEDIA OUTLETS, PAPER, RADIO, TELEVISION	ADDDRESS AND PERTINENT PHONE NUMBERS
Wisconsin Bankers Association Media Department	Wisconsin Bankers Association 4721 S. Biltmore Lane Madison, WI. 53718 (608) 441-1200 (phone) (608) 661-9381 (fax) www.wisbank.com

Appendix D - Definitions

The three key areas of security response are alert, event, and incident. To distinguish between these three areas, the IRP Team has developed the following definitions and examples of criteria for each response:

- **Alert:** A Alert is a response sent by the IRP Team to notify individuals that information has been received concerning threats to which <<<< BANK NAME >>>> assets may be vulnerable. Examples of Alert criteria include operating system vulnerabilities, external viruses, and a minimal number of network probes or scans.
- **Chain of Custody** refers to the chronological documentation or trail, showing the seizure, custody, control, transfer, analysis, and disposition of any evidence gathered whether physical or electronic. It may become necessary for evidence to be used in court for criminal incidents. As such the evidence must be handled in such a way to that it can be illustrated that the evidence could not have been tampered with and consists of the original untainted information. The for recording chain of custody is to establish that the information gathered is in fact associated with the potential crime that the incident tracked. It is important for there to be trusted physical custody of a piece of evidence.
- **Computer Security Alert Services**: Sample alert networks/services to consider include services available from the following sites/organizations:
  - **Bugtraq,** http://www.securityfocus.com/
  - **Computer Emergency Response Team,** www.cert.org/certcc.html
  - **Financial Services Information Sharing and Analysis Center,** http://www.fsisac.com/
  - **Google Safe Browsing Alerts for Network Administrators,** http://safebrowsingalerts.googlelabs.com/
  - **InfraGard,** http://www.infragard.org/
  - **Internet Fraud Alert Service,** https://www.ifraudalert.org/
  - **Microsoft Technical Security Notifications,** http://technet.microsoft.com/en-us/security/dd252948.aspx
  - **United States Computer Emergency Readiness Team,** http://www.us-cert.gov/current/
- **Data Breach (aka Security Breach):** Includes the loss of control, compromise, unauthorized disclosure, unauthorized acquisition, access for an unauthorized purpose, or other unauthorized access, to data, whether physical or electronic. Unauthorized access can include access by employees not authorized by their job role for access to data.
- **Event:** An event that indicates or produces an actual or potential negative consequence to WBA Inc computing resources with the ***potential to compromise*** the confidentiality, availability, or integrity of those resources or the data stored on these devices. Examples of Event criteria include internal viruses, significant number of network probes or scans, and non-impacting penetration or denial of service attacks.

- **FBI InfraGard**, www.infragard.com, refers to the private public partnership for protection of critical infrastructures that is coordinated by the FBI. Regional Wisconsin based representatives are in place for InfraGard out of both the Madison and Milwaukee FBI Field offices.

- **FS-ISAC**, www.fsisac.com/, refers to the industry forum for collaboration on critical security threats facing the financial services sector.

  When attacks occur, early warning and expert advice can mean the difference between business continuity and widespread business catastrophe. Members of the Financial Services Information Sharing and Analysis Center (FS-ISAC) receive timely notification and authoritative information specifically designed to help protect critical systems and assets from physical and cyber security threats

- **Identity Theft**: The act of obtaining 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 individual.
  - Withdraw or borrow money from existing accounts or charge purchases to the accounts
  - Open new accounts with an individual's personally identifiable information without that individual's knowledge
  - Obtain driver's licenses, social security cards, passports, or other identification documents using the stolen identity

  Resources for identity theft information include www.identitytheft.info and the Federal Trade Commission (FTC) at www.ftc.gov/bcp/edu/microsites/idtheft/.

- **Incident:** A Incident is any occurrence of unauthorized access to or use of <<<< BANK NAME >>>> computer and network resources that causes a ***confirmed compromise*** of the confidentiality, availability, or integrity of those resources or the data stored on those devices. The term "incident" throughout this document implies harm, attempt to harm, or threat of harm to any portion of or the entire enterprise that results in the compromise of system and/or information. Examples of Incident criteria include unauthorized use of another user's account, unauthorized use of system privileges, and execution of malicious code to gain unauthorized levels of access to and/or destroy data.

- **Incident Response Team Coordinator (or alternate) (IRT Coordinator)**: This position is responsible for the coordination and response to any incident from initial alert to post mortem. The role is assigned as identified in the Roles and Responsibilities section of the Incident Response Plan.

- **Incident Response Team (IRT)**: This group can be formed dynamically based on the specific incident's expertise requirements, individual business area or the confidentiality requirements that may be determined necessary for an incident. The team is responsible for supporting the IRT Coordinator's response to any incident from initial alert to post mortem. The team is defined as identified in the Roles and Responsibilities section of the Incident Response Plan.

- **Nonpublic Personally Identifiable Information (NPI) (aka Sensitive Customer Information, Information Resources, Confidential Data):** The bank includes a definition of NPI for the purpose of maintaining a level of standard definition concerning sensitive information with the information security industry using US government agency based definitions. Information which can be used to distinguish or trace an individual's identity, such as their name, social security number, biometric records, etc. alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc. OMB Memorandum 07-16, *Safeguarding Against and Responding to the Breach of Personally Identifiable Information*, dated May 22, 2007.

  Information about an individual, including, but not limited to, education, financial transactions, medical history, and criminal or employment history and information which can be used to distinguish or trace an individual's identity, such as their name, social security number, date and place of birth, mother's maiden name, biometric records, etc., including any other personal information which is linked or linkable to an individual. OMB Memorandum 06-19, *Reporting Incidents Involving Personally Identifiable Information and Incorporating the Cost for Security in Agency Information Technology Investments*, dated July 12, 2006.

  The above definitions have been developed by OMB. Please note that the items listed in those definitions are meant to serve as examples and do not represent a comprehensive list of personally identifiable information.

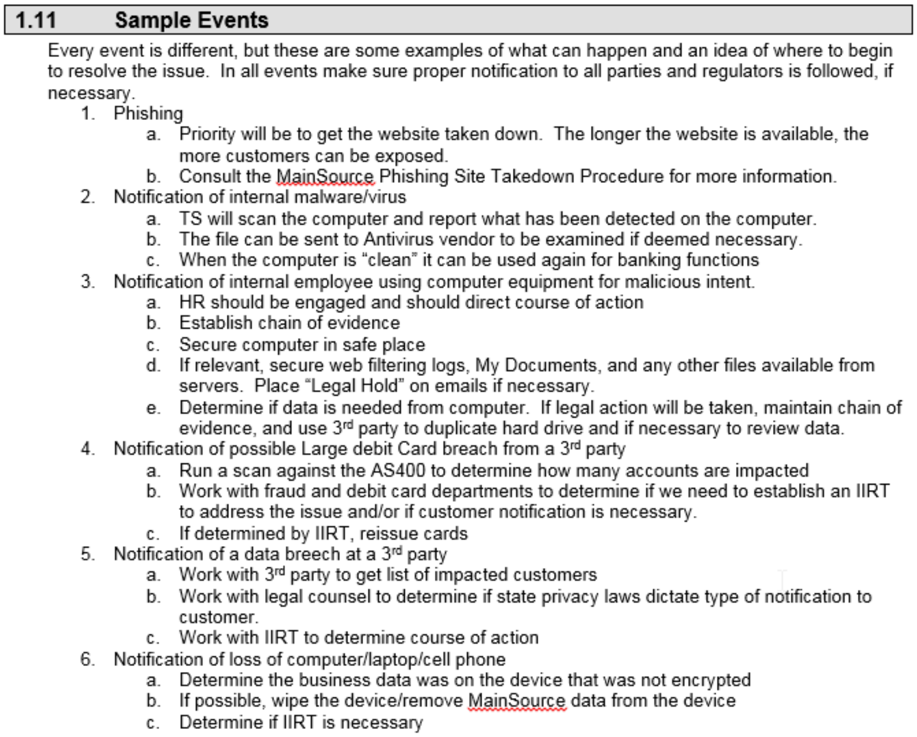
  Information that standing alone is **not generally considered personally identifiable**, because many people share the same trait, includes:

  - First or last name, if common (For example: Ken, Bill, Smith or Brown)
  - Country, state, or city of residence
  - Age, especially if non-specific (such as age in years, without birthdates)
  - Gender or race
  - Workplace or school
  - Grades, salary, or job position

  Sometimes multiple pieces of information, none of which alone may be considered personally identifiable, may uniquely identify a person when brought together. An example might be name, age and address.

- **Rootkits/backdoors;** A rootkit is software that enables privileged access to a computer while actively hiding its presence from administrators by subverting standard operating system functionality or other applications. The backdoor can be another word to describe this functionality, essentially providing a back door way to access a computer or system getting around standard operating system security.

- **Sensitive Customer Information**: This includes a customer's name, address or telephone number in conjunction with the customer's Social Security number, driver's license number, account number, credit or debit card number, or a personal identification number or password that would permit access to the customer's account. It also includes any combination of components of customer information that would allow someone to log on to or access the customer's account, such as a user name and password or password and account number.
- **Sniffer:** A sniffer can also be called a packet analyzer (aka network analyzer, protocol analyzer or sniffer). This is computer software or hardware that can intercept and log traffic passing over a digital network
- **Waerz** refers primarily to copyrighted works distributed without fees or royalties, and may be traded, in general violation of copyright law. The term generally refers to unauthorized releases by organized groups, as opposed to file sharing between friends or large groups of people with similar interest.



1.11 Sample Events

Every event is different, but these are some examples of what can happen and an idea of where to begin to resolve the issue. In all events make sure proper notification to all parties and regulators is followed, if necessary.

1. Phishing
   a. Priority will be to get the website taken down. The longer the website is available, the more customers can be exposed.
   b. Consult the MainSource Phishing Site Takedown Procedure for more information.
2. Notification of internal malware/virus
   a. TS will scan the computer and report what has been detected on the computer.
   b. The file can be sent to Antivirus vendor to be examined if deemed necessary.
   c. When the computer is "clean" it can be used again for banking functions
3. Notification of internal employee using computer equipment for malicious intent.
   a. HR should be engaged and should direct course of action
   b. Establish chain of evidence
   c. Secure computer in safe place
   d. If relevant, secure web filtering logs, My Documents, and any other files available from servers. Place "Legal Hold" on emails if necessary.
   e. Determine if data is needed from computer. If legal action will be taken, maintain chain of evidence, and use 3rd party to duplicate hard drive and if necessary to review data.
4. Notification of possible Large debit Card breach from a 3rd party
   a. Run a scan against the AS400 to determine how many accounts are impacted
   b. Work with fraud and debit card departments to determine if we need to establish an IIRT to address the issue and/or if customer notification is necessary.
   c. If determined by IIRT, reissue cards
5. Notification of a data breech at a 3rd party
   a. Work with 3rd party to get list of impacted customers
   b. Work with legal counsel to determine if state privacy laws dictate type of notification to customer.
   c. Work with IIRT to determine course of action
6. Notification of loss of computer/laptop/cell phone
   a. Determine the business data was on the device that was not encrypted
   b. If possible, wipe the device/remove MainSource data from the device
   c. Determine if IIRT is necessary