[Credit Union]

Incident Response Plan

Board Approval Date:

Incident Response Plan

TABLE OF CONTENTS

Page

[1. OVERVIEW 3](#_Toc410895623)

[2. INCIDENT RESPONSE ORGANIZATIONAL STRUCTURE 3](#_Toc410895624)

[2.1 Incident Response Organizational Structure 4](#_Toc410895625)

[2.2 Roles and Responsibilities 5](#_Toc410895626)

[2.2.1 Board of Directors 5](#_Toc410895627)

[2.2.2 Executive Management Team 5](#_Toc410895628)

[2.2.3 Incident Response Team (IRT) 5](#_Toc410895631)

[2.2.4 Incident Response Support Team (IRST) 7](#_Toc410895633)

[3. SECURITY INCIDENTS 8](#_Toc410895636)

[3.1 Incident Levels 9](#_Toc410895637)

[3.2 Level Notification Guidelines 9](#_Toc410895638)

[4. DISCOVERY AND REPORTING 10](#_Toc410895639)

[4.1 Discovery and Initial Reporting 10](#_Toc410895640)

[4.1.1 DDoS Discovery and Initial Reporting 10](#_Toc410895641)

[4.1.2 DDoS Reporting Escalation 11](#_Toc410895642)

[4.2 Reporting Incidents to Incident Response Team 11](#_Toc410895643)

[4.2.1 Security Incident Reporting Procedures 11](#_Toc410895644)

[4.2.2 DDoS Reporting Procedures 11](#_Toc410895645)

[4.2.3 Team Conference Calls 12](#_Toc410895646)

[4.2.4 Reporting Lost and Stolen Equipment 12](#_Toc410895647)

[4.3 Responding to the Incident: 12](#_Toc410895648)

[4.3.1 Investigations of Security Incidents 12](#_Toc410895649)

[4.3.2 Forensic Analysis 13](#_Toc410895650)

[4.3.3 Investigations of Incidents Involving Unauthorized Access (“Intrusions”) 13](#_Toc410895651)

[4.3.4 Data Preservation in Connection with Malicious Events 13](#_Toc410895652)

[4.4 Incident Containment 13](#_Toc410895653)

[4.4.1 Containment Actions for Incidents Generally 13](#_Toc410895654)

[4.4.2 DDoS Containment Actions 14](#_Toc410895655)

[4.4.3 Lost Device Containment Actions 14](#_Toc410895656)

[4.5 Corporate Communications Procedures 14](#_Toc410895657)

[4.5.1 Corporate Incident Response Group 14](#_Toc410895658)

[4.5.2 Corporate Respose Escalation Process 15](#_Toc410895659)

[5. NOTIFICATIONS 16](#_Toc410895660)

[6. CREDIT MONITORING 16](#_Toc410895661)

[7. SUSPICIOUS ACTIVITY REPORTS 16](#_Toc410895662)

[8. CLAIMS FOR REIMBURSEMENT 17](#_Toc410895663)

[8.1 Request received from affected Constituent 17](#_Toc410895664)

[8.2 Credit Union reimbursement or other Requests 17](#_Toc410895665)

[9. POST INCIDENT REVIEW 17](#_Toc410895666)

[APPENDIX I FORENSIC FIRMS 18](#_Toc410895667)

[APPENDIX II THIRD PARTY LEGAL COUNSEL 19](#_Toc410895668)

[APPENDIX III SAR COMPLETION GUIDELINES 20](#_Toc410895669)

# OVERVIEW

[Credit Union] relies upon Confidential Information. “Confidential Information,” as that term is used in this Plan, includes a member’s, employee’s, or another individual’s name, in conjunction with the individual’s Social Security number, driver's license number, account number, or credit or debit card number. Our members provide Confidential Information that we store and process on our systems and that we, in turn, provide to third parties, such as payment card payment processing companies, on-line banking system operators, and others. “Confidential Information” also includes any combination of information that would allow someone to log onto or access the individual’s account, such as user name and password or account number and password.

This Incident Response Plan describes actions [Credit Union] should consider to respond to Security Incidents. (“Security Incident” is defined in section 3 below.) To promptly respond to such incidents, employees who become aware of suspected or actual Security Incidents should immediately notify their supervisors and the Chief Information Security Officer (“CISO”). The CISO leads the Incident Response Team (“IRT”).

# INCIDENT RESPONSE ORGANIZATIONAL STRUCTURE

The IRT consists of representatives from the Information Technology, Security, Retail, Communications, and Administration departments. [Credit Union] management created the IRT to ensure that we respond to Security Incidents in a centralized and coordinated manner. The IRT provides direction and support to affected business units. The IRT also acts as a liaison to the Executive Management Team.

An Incident Response Support Team (“IRST”) has also been established to assist the IRT, as needed. This team can be activated by the IRT to provide additional support. The IRST is comprised of management personnel responsible for key business areas that may be useful to help respond to some incidents.

## Incident Response Organizational Structure

**INCIDENT DETECTED AND REPORTED**

**Board or Directors**

**Executive Management Team**

**INCIDENT RESPONSE TEAM**

## Roles and Responsibilities

### Board of Directors

The Board of Directors (“Board”) supports and oversees the [Credit Union]’s incident response efforts. The Board should ensure that adequate resources are available to respond to the incident. The Board may review and approve the Incident Response Plan, as needed.

### Executive Management Team

The Executive Management Team (“EMT”) monitors and manages the response effort. The EMT may approve actions that exceed pre-approved response activities, as it deems appropriate. The President and CEO, or his or her designate, should approve any public statements regarding a Security Incident.

#### Executive Management Team Members

| EMT Members | Title |
| --- | --- |
| [Insert Name] | President and Chief Executive Officer |
| [Insert Name] | Chief Operating Officer (“COO”) |
| [Insert Name] | Chief Information Officer (“CIO”) |
| [Insert Name] | Chief Administrative Officer (“CAO”) |
|  |  |

#### Executive Management Team Member Responsibilities

* President and CEO: The President and CEO serves as the primary media spokesperson.
* Chief Operating Officer: The COO manages and directs the EMT. The COO may temporarily amend or suspend [Credit Union] policy during crisis situations, as needed.
* Chief Information Officer: The CIO manages the Information Technology Department’s incident response activities, if necessary. The CIO also serves as a member of the Incident Response Team.
* Chief Administrative Officer. The CAO coordinates crisis communications regarding an incident.

### Incident Response Team (IRT)

The IRT coordinates Incident Response activities.

**Incident Response Team Members**

|  |  |
| --- | --- |
| IRT Members | Title |
| [Insert Name] | Chief Information Security Officer (“CISO”) (Team Leader) |
| [Insert Name] | Chief Information Officer (“CIO”) |
| [Insert Name] | Chief Corporate Governance Officer |
| [Insert Name] | Assistant Chief Operating Officer  |
| [Insert Name] | Director of Security |
| [Insert Name] | Chief Administrative Officer (“CAO”) |
|  |  |

#### Incident Response Team Member Responsibilities

* Chief Information Security Officer: The CISO leads the IRT. The CISO develops and implements the Incident Response Plan and coordinates response efforts of the IRT and IRST. The CISO, in consultation with legal counsel, ensures that an appropriate [Credit Union] official notifies (a) relevant insurers, (b) [Credit Union]’s primary Federal and State regulatory agencies, and (c) any other appropriate State agencies, of a Security Incident as soon as possible. The CISO may designate members of his or her staff to take certain actions to respond to Security Incidents but the CISO remains responsible for ensuring that the IRT takes appropriate steps to respond to Security Incidents.
* Chief Information Officer: The CIO manages IT staff as they provide services to help respond to Security Incidents.
* Chief Corporate Governance Officer: The Chief Corporate Governance Officer reviews and approves any communications related to Security Incidents sent outside [Credit Union].
* Assistant Chief Operating Officer: The Assistant COO manages administrative response activities and works with Corporate Communications and Information Technology staff to draft Frequently Asked Questions (“FAQs”) and other communications related to Security Incidents. The Assistant COO ensures that [external counsel] is engaged, if necessary (1) to determine whether notifications must be sent to members, employees, or others regarding a Security Incident and (2) to advise the IRT of any additional steps [Credit Union] should take to respond to a Security Incident.
* Director of Security: The Director of Security manages the Security Department’s response to Security Incidents, including its investigation of Security Incidents (as needed). In consultation with legal counsel, the Director of Security submits any needed Suspicious Activity Reports (“SARs”), contacts law enforcement agencies, and serves as liaison between [Credit Union] and law enforcement officials. The Director of Security serves as the leader of the IRT if the CISO is unavailable.
* Chief Administrative Officer: The CAO manages the drafting of communications concerning Security Incidents, including FAQs for internal use. The CAO issues public statements if directed to do so by Executive Management. The CAO coordinates contact with the media.

### Incident Response Support Team (IRST)

The Incident Response Support Team (“IRST”) includes members of the [Credit Union] management team who manage certain administrative functions and branch operations within [Credit Union]. The CISO determines whether the Incident Response Support Team should be activated. The IRT may identify other or additional IRST members to help respond to a Security Incident.

#### Incident Response Support Team Members

| IRST Members | Title |
| --- | --- |
| [Insert Name] | Director of Retail Operations |
| [Insert Name] | Compliance, Privacy & Fair Lending Officer |
| [Insert Name] | Director of Retail Banking |
| [Insert Name] | Mortgage Call Center Director |
| [Insert Name] | Website Administrator |
| [Insert Name] | Communications |
|  |  |

#### Incident Response Support Team Member Responsibilities

Director of Retail Operations: The Director of Retail Operations manages and coordinates Card Services and eRisk departments actions related to Security Incidents that involve debit cards or credit cards. If members or employees are notified of a Security Incident and if [Credit Union] employees (rather than contractor call center personnel) will respond to calls related to the Security Incident, the Director of Retail Operations will the ensure employees answering calls receive FAQs and are following scripts to ensure their answers are consistent. The Director of Retail Operations will coordinate the activities of the various departments that help respond to Security Incidents. The Director of Retail Operations will ensure that supervisors of employees whose work involves electronic fund transfers advise the employees of Security Incidents and the supervisors make ensure such employees follow bank procedures that require members to authenticate requests to move funds.

Chief Risk Officer: The Chief Risk Officer ensures [Credit Union] provides necessary resources to respond to Security Incidents.

Compliance, Privacy and Fair Lending Officer: The Compliance, Privacy and Fair Lending Officer ensures [Credit Union] meets its compliance duties related to Security Incidents.

Director of Retail Banking: The Director of Retail Banking manages communications sent to the branches related to Security Incidents. The Director of Retail Banking ensures appropriate managers at each branch are aware of the Security Incident and follows bank procedures regarding authentication of Member requests. The Director of Retail Banking also ensures branch managers receive FAQs and that employees answering questions about Security Incidents follow the FAQs when they answer questions from Members or others who inquire.

Mortgage Call Center Director: The Mortgage Consultation Center (“MCC”) Director briefs MCC personnel about Security Incidents, ensures MCC personnel receive Security Incident FAQs, and ensures they follow the FAQs when they answer Members’ questions.

Website Administrator: The Website Administrator posts website notifications when requested to do so by the CISO or by a member of the IRT.

Communications: The Communications Director drafts public statements concerning Security Incidents, drafts FAQs for internal departmental use, and coordinates contacts with the media.

# SECURITY INCIDENTS

A Security Incident includes (i) any incident that may compromise the integrity, operation, or security of [Credit Union]’s computer systems, including a DDoS attack; and (ii) any actual or attempted unauthorized acquisition of data that compromises the security, confidentiality, or integrity of information maintained by or for [Credit Union].

Examples of Security Incidents include: (a) unauthorized access to or acquisition of unencrypted and unredacted records or data containing Confidential Information; and (b) unauthorized access to or acquisition of encrypted records or data containing Confidential Information together with access to or acquisition of the encryption or decryption key.

For purposes of this Incident Response Plan (“IRP), the occurrence of any of the following situations should be considered a Security Incident:

* Electronic equipment (such as a PDA, tablet, laptop computer, desktop computer, back-up tape, or USB storage device) containing unencrypted Confidential Information is lost or stolen;
* An unauthorized person attempts to access or successfully accesses, by electronic or physical means, a [Credit Union] or third-party computer system that stores or processes unencrypted Confidential Information;
* An individual intentionally or unintentionally gains unauthorized access to [Credit Union] proprietary or Confidential Information owned or licensed by [Credit Union];
* A denial of service attack is mounted against one of [Credit Union]’s web sites;
* An ATM encryption key is compromised;
* Any [Credit Union] equipment is used without authorization to process or store data; and
* The configuration of any [Credit Union] equipment or software is changed without the owner’s knowledge, instruction, or consent.

## Incident Levels

This Plan classifies Security Incidents based on the severity of the incident. Each level requires a different type of response. As soon as possible after the CISO receives notice of a Security Incident, he or she should determine the level of incident. The CISO may consult IRT members to determine the incident level.

**Level A Incident**: Exposes or potentially exposes 500 or more records or sets of data containing Confidential Information or may cause a high level of financial loss or reputational damage to [Credit Union] or to another entity or person

**Level B Incident**: Exposes or potentially exposes fewer than 500 records or sets of data containing Confidential Information or may cause a moderate level of financial loss or reputational damage to [Credit Union] or to another entity or person.

**Level C Incident**: Does not expose or potentially expose records or data containing Confidential Information, but may cause a low level of financial loss or reputational damage to [Credit Union] or to another entity or person.

## Level Notification Guidelines

[Credit Union] management may ultimately determine the members of the IRT, IRST, and others who should be notified of a Security Incident. The CISO should initially ask the following team members to convene to begin responding to each level of incident:

|  |  |
| --- | --- |
| **Incident Level** | **Initial Response Participants** |
| Level A Incidents | Executive Management Team, Incident Response Team |
| Level B Incidents | Incident Response Team, Incident Response Support Team members as deemed appropriate by IRT members |
| Level C Incidents | Members of Incident Response Support Team to be determined by CISO |
|  |  |

# DISCOVERY AND REPORTING

## Discovery and Initial Reporting

Security Incidents may be reported to the CISO in various ways, including as follows:

* Any employee who discovers or suspects a Security Incident has occurred should immediately notify his or her supervisor, who, in turn, should notify the CISO.
* If the Helpdesk receives notification from a user via email, web, or phone that a Security Incident may have occurred, the Helpdesk should immediately notify the CISO.
* If a Network Administrator receives an alert regarding a potential incident via an Intrusion Detection System, Intrusion Prevention System, or Security Event Information Management System, the Administrator should immediately notify the CISO.
* If a Server Administrator determines from reviewing system security logs that a Security Incident may have occurred, the Administrator should immediately notify the CISO.

**INCIDENT DETECTED AND REPORTED**

The CISO may be notified of a Security Incident by phone; however, if the CISO is notified by phone, an e-mail notification should follow. The CISO’s contact information is:

Office Telephone: [Insert Phone No.]

Cellular Telephone: [Insert Phone No.]

E-Mail: [Insert email address]

Employees should be trained regarding how to recognize a potential Security Incident. An employee who reports a potential Security Incident should not discuss the incident with anyone other than his or her supervisor or the CISO unless requested to do so by the employee’s supervisor or by a member of [Credit Union]’s management.

### DDoS Discovery and Initial Reporting

[Include any parts of this paragraph that are appropriate.] [Credit Union] is a subscriber of [Company’s] “[service name]” service. This service monitors the [Credit Union]’s Internet-facing IP address range for increases in incoming bandwidth usage over a pre-determined baseline. Should an increase in traffic be detected, [Company] automatically diverts all traffic in connection with the targeted IP address to its packet scrubbing facilities, where each packet is reviewed for Distributed Denial of Service (“DDoS”) attack signatures. These malicious packets are dropped and non-DDoS traffic is passed through to the destination IP address.

[Include any parts of this paragraph that are appropriate.] [Credit Union] also relies upon [Company] Intrusion Detection and Intrusion Prevention sensors that monitor incoming packets for the purpose of detecting various attack patterns. Identified patterns result in dropping of malicious packets, blocking transmissions from malicious originating IP address, or both. In addition, [Company] Host Intrusion Prevention for Server is utilized and has been installed on all external facing web servers to add an additional layer of protection. This product relies upon behavioral and signature analysis to detect and block attacks. These alerts are monitored by the IT Operations group twenty-four hours a day, seven days a week, with escalation to the appropriate Network Infrastructure team member who, in turn, will escalate to the CISO as appropriate.

### DDoS Reporting Escalation

Upon receiving an automated alert, the Network Infrastructure team will review the alert. If a DDoS attack is suspected, a Network Infrastructure team member should immediately notify the CISO. Further, if the Network Infrastructure team cannot determine within 10 minutes whether or not a DDoS attack is occurring, a Network Infrastructure team member should immediately escalate the issue to the Network Infrastructure Manager. The Infrastructure Manager should attempt to determine whether a DDoS attack is underway. If the Infrastructure Manager determines a DDoS attack is probably occurring, he or she should immediately notify the CISO and should take appropriate corrective action.

## Reporting Incidents to Incident Response Team

### Security Incident Reporting Procedures

When the CISO receives a report of a Security Incident, he or she should prepare (or have prepared) a written Notice of Security Incident. Notices regarding Level A Incidents should be circulated to the EMT and IRT. Notices regarding Level B Incidents should be circulated to the IRT. Notices regarding Level C Incidents should be circulated to IRST members as determined by the CISO. Notices should include the following information:

* Date of the Incident;
* Incident Level;
* Location of the Incident;
* Time and duration (if known) of the Incident;
* General description of the Incident, including the type of information involved (e.g., debit or credit card data, loan data, member or employee Confidential Information, or [Credit Union] proprietary information);
* Contact information of the person who reported the Incident; and
* Any additional important facts known at the time; and
* Probable impacts of the Incident.

### DDoS Reporting Procedures

Upon receipt of notification of suspected DDoS attack, the CISO should immediately contact the CIO and other IT Directors identified below:

| Director Name | Office Phone Number | Cell Phone Number |
| --- | --- | --- |
| [Insert Name] | [Insert Phone No.] | [Insert Phone No.] |
| [Insert Name] | [Insert Phone No.] | [Insert Phone No.] |
| [Insert Name] | [Insert Phone No.] | [Insert Phone No.] |
|  |  |  |

### Team Conference Calls

* For any Level A Incident and for any confirmed DDoS attack, the CISO will establish a conference bridge for the EMT and IRT to discuss the Incident.
* For any Level B Incident, the CISO will establish a conference bridge for the IRT to discuss the Incident.
* If the CISO cannot access the Internet, the conference bridge can be set up from an external device such as a smart phone or a computer outside the [Credit Union] network (i.e. home computer).

### Reporting Lost and Stolen Equipment

Instructions for reporting lost or stolen equipment are included in the Information Technology and Security Policy, which is posted on the [Credit Union] Intranet. [Repeat those instructions here.]

## Responding to the Incident:

### Investigations of Security Incidents

Upon learning of a Security Incident, the IRT should ensure that an investigation is promptly conducted to determine:

* The cause of the Security Incident;
* The nature and scope of the information exposed, including, if individuals’ Confidential Information was exposed, the states where the individuals reside;
* The appropriate Incident Level of the Security Incident;
* Through consultation with legal counsel, the statutes and regulations that apply to the Incident ;
* Whether it is necessary, under applicable laws and regulations, to notify affected individuals or regulators of the Security Incident; and
* The date by which notice should be provided to individuals and regulators and the appropriate method for making such notifications, if they are required.

### Forensic Analysis

The IRT will determine whether a forensic specialist should be engaged to assist in investigating a Security Incident. A list of forensic firms can be found in Appendix I.

### Investigations of Incidents Involving Unauthorized Access (“Intrusions”)

Investigations of Intrusions typically include assistance from a computer forensic investigator. Such investigations may include:

* Analyzing all available information to assess extent of the intrusion and the intruder’s activities;
* Communicating with all parties that need to be aware of an intrusion and participate in handling it, taking into account that an intruder may be able to access and monitor standard means of communication;
* Collecting and preserving information associated with the intrusion;
* Containing the intrusion;
* Eliminating the intruder’s means of access and any related vulnerabilities;
* Returning affected systems to normal operation;
* Determining the magnitude of the Incident by identifying how many hosts or network devices were compromised;
* Assessing the damage by determining the extent to which the systems have been compromised or altered;
* Isolating affected systems if they pose an immediate threat to external entities or critical business functions; and
* Continued monitoring of affected devices and networks to identify the source of the intrusion, the mechanics of the compromise, the goals of the intruder, and to define scope of the intrusion.

### Data Preservation in Connection with Malicious Events

Computers and data storage devices compromised in connection with a Security Incident may be backed-up or imaged before any actions are taken that could affect the integrity of data on the computer or device. This determination will be made by the CISO in consultation with legal counsel.

## Incident Containment

### Containment Actions for Incidents Generally

The IRT will seek to ensure that the Incident is contained by adopting an appropriate strategy tailored to the Incident. The CISO, in conjunction with the CIO and others as deemed necessary, will determine through investigation the appropriate steps to be taken to contain the Incident. In addition, the CISO may ask the appropriate members of management to review the Incident and to take steps to prevent a similar Incident from occurring. Actions identified to contain the incident may take place concurrently with the Incident investigation.

### DDoS Containment Actions

* Contact ISPs to alert of DDoS attack and initiate potential IP address blocks at ISP level.
* Attempt to block specific IP addresses or ranges of IP addresses depending on the volume of source IP addresses conducting the attack.
* Determine necessity of potentially changing default outbound routing (Internet traffic) through another Internet connection.
* Confirm VPN connections are available for remote access into [Credit Union] network.

### Lost Device Containment Actions

* Interview employee involved.
* Determine whether backup data is available to replicate the data on the lost device.
* Determine whether the data on the lost device was encrypted.
* If the data was not encrypted, determine in consultation with legal counsel whether individuals must be notified that their Confidential Information was potentially exposed.

## Corporate Communications Procedures

[Include this section if appropriate.] To address the possibility that [Credit Union] operations may be disrupted by a Level A Incident or by a confirmed DDoS attack, certain [Credit Union] business units should coordinate their response activities. A corporate-level Incident Response email distribution group has been formed for communications to individuals and departments involved in the response process. The e-mail group will be used to notify appropriate departments and individuals that a Security Incident has occurred. The e-mail distribution group is **[Insert Link].**

### Corporate Incident Response Group

The Corporate Incident Response (“CIR”) group consists of managers of the following business units:

* Information Technology
* Retail Banking
* Communications
* Security
* Member Contact Center
* Retail Operations
* Online Banking
* Processing Solutions
* Office of the Chief Risk Officer
* Website Administrator
* Mortgage Consultation Center

### Corporate Response Escalation Process

* The CISO will notify the CIR group of any Level A Incident or confirmed DDoS attack involving [Credit Union]-owned systems.
* Executive Management will determine whether the Board of Directors should be notified.
* The IRT will determine whether internal communications will be sent in other circumstances. If such communications are not initiated, the IRT will continue to monitor the situation to determine whether changed circumstances require initiating communications activities.
* If such additional internal communications are initiated, the CISO will establish a conference bridge for CIR group members to discuss any actions CIR members should take to help respond to the Incident.
* If such additional internal communications are initiated,the Corporate Communications department should send CIR members the current FAQs.
* CIR group members that oversee business units that receive questions from [Credit Union] members should inform their staff of the actions that have been taken to respond to the Security Incident. Such business units include:
* Retail Banking
* Retail Operations
* Member Contact Center
* Online Banking
* Cash Management
* Mortgage Consultation Center
* CIR group members for the above business units should distribute FAQs to the employees in their respective areas to enable the employees to answer members’ questions.
* CIR group members serve as the primary liaisons between their respective departments and the CIR group. Communication may be sent to CIR members by e-mail to the CIR email distribution group and via conference bridge that will be set up by the IT Department. Call-in information will be distributed by the IT Department
* If an employee receives a question from a [Credit Union] member that is not addressed in the FAQs, he or she should promptly bring the question to the attention of the department head. The question should be disseminated to CIR group so that the FAQs can be updated, approved, and re-distributed.
* If an employee receives a question from a [Credit Union] member that is not addressed in the FAQs, the employee should tell the member that he or she will receive a phone call that will include an answer on behalf of [Credit Union]
* The Retail Operations department head should advise departments that process money transfers that, due to the Security Incident, their staff should be especially alert for indications of fraudulent wire transfer requests and fraudulent ACH-related transactions.
* The IRT should periodically provide updates to the CIR group regarding the investigation and containment of the Security Incident, as well as an update when the Incident response has been completed.

# NOTIFICATIONS

Certain Security Incidents will require that potentially affected individuals receive notification of the Incident. Such notifications will be sent when legal counsel advises it is appropriate. The IRT, in conjunction with legal counsel, will determine the method or methods by which such notifications will be sent.

# CREDIT MONITORING

[Credit Union] may, if appropriate, offer individuals potentially affected by a Security Incident the option to enroll in a credit monitoring service for a defined period of time at [Credit Union]’s expense. The determination of whether and for how long to offer this service will depend on the nature and extent of the Security Incident, and the risks posed by the information compromised. Determinations regarding credit monitoring should be made by the IRT, in consultation with the Assistant COO.

# SUSPICIOUS ACTIVITY REPORTS

Credit unions must file suspicious activity reports (“SARs”) as described in Section 748.1(c) of the NCUA’s rules. The IRT, in conjunction with the Assistant COO, Director Security, and legal counsel, if needed, will determine whether a Security Incident requires [Credit Union] to file an SAR. The IRT, in conjunction with the Assistant COO, Director Security, and legal counsel, if needed, will also when law enforcement will be notified, consistent with Section 748.1(c) of the NCUA’s rules. Additional details regarding SAR reporting can be found in Appendix III.

# CLAIMS FOR REIMBURSEMENT

## Request received from affected individuals

Whenever an incident occurs, [Credit Union] may be asked to reimburse an affected individual. [Credit Union] may be required by law, rule, or regulation to reimburse the individual; and will then do so pursuant to the applicable law, rule or regulation. If reimbursement is not required, [Credit Union] may choose to reimburse an affected individual for his or her entire, or portion of the, loss suffered. The determination as to whether such voluntary reimbursement will occur will be made by Executive Management, with the advice of legal counsel.

## Credit Union reimbursement or other Requests

Whenever the effects of a Security Incident requires [Credit Union] to take certain (for example, notifying potentially-affected individuals, issuing new payment cards), the department head of the affected business unit should document the expenses (whether in or outside of his or her department) and report them to the Assistant COO.

The Assistant COO should, in-turn, report the expenses to the Corporate Risk Officer. The Corporate Risk Officer, should review any relevant contracts, and consider, with legal counsel and Executive Management as appropriate, possible courses of action, including making demands for reimbursement and pursuing legal remedies (e.g., bringing a lawsuit, including participating in class action litigation).

The Assistant COO should document his or her consideration of such potential actions. legal counsel may maintain separate records of his or her actions referred to in this section.

# POST-INCIDENT REVIEW

* The CISO should notify the IRT and, if applicable, the CIR group, when the CISO determines Incident response activities have ended.
* The IRT should consider distributing post-Incident talking points to business units that respond to member questions.
* After Incident Response activities have ended, the IRT and, if appropriate, the CIR group, should meet to discuss the events that occurred and to provide oral feedback regarding procedures followed to respond to the Incident. Such feedback should be used to revise the procedures, if necessary.
* Post-incident assessments should be documented in writing only after consulting with legal counsel.

#### APPENDIX I FORENSIC FIRMS

The Incident Response Team is responsible for determining which forensic firm will be used in the event a forensic analysis is needed in connection with a Security Incident. The firm selected will be engaged by the Third Party legal counsel identified in Appendix II. The following is a list of approved forensic investigative firms that could be used in the event of a computer system breach:

Firm Name:

Primary Contact:

Telephone:

eMail:

Firm Name:

Primary Contact:

Telephone:

eMail:

Firm Name:

Primary Contact:

Telephone:

eMail:

#### APPENDIX II THIRD PARTY LEGAL COUNSEL

The following legal counsel will be used to engage the forensic analysis firm identified by the Incident Response Team:

Firm Name:

Primary Contact:

Telephone:

eMail:

#### APPENDIX III SAR COMPLETION GUIDELINES

All credit unions operating in the United States are required to file a SAR following the discovery of:

* Insider abuse involving any amount: Whenever the credit union detects any known or suspected Federal criminal violation, or pattern of criminal violations, committed or attempted against the credit union or involving a transaction or transactions conducted through the credit union, where the credit union believes that it was either an actual or potential victim of a criminal violation, or series of criminal violations, or that the credit union was used to facilitate a criminal transaction, and the credit union has a substantial basis for identifying one of its directors, officers, employees, agents or other institution-affiliated parties as having committed or aided in the commission of a criminal act regardless of the amount involved in the violation.
* Violations aggregating $5,000 or more where a suspect can be identified:Whenever the credit union detects any known or suspected Federal criminal violation, or pattern of criminal violations, committed or attempted against the credit union or involving a transaction or transactions conducted through the credit union and involving or aggregating $5,000 or more in funds or other assets, where the credit union believes that it was either an actual or potential victim of a criminal violation, or series of criminal violations, or that the credit union was used to facilitate a criminal transaction, and the credit union has a substantial basis for identifying a possible suspect or group of suspects. If it is determined prior to filing this report that the identified suspect or group of suspects has used an “alias,” then information regarding the true identity of the suspect or group of suspects, as well as alias identifiers, such as drivers’ licenses or social security numbers, addresses and telephone numbers, must be reported.
* Violations aggregating $25,000 or more regardless of a potential suspect:Whenever the credit union detects any known or suspected Federal criminal violation, or pattern of criminal violations, committed or attempted against the credit union or involving a transaction or transactions conducted through the credit union and involving or aggregating $25,000 or more in funds or other assets, where the credit union believes that it was either an actual or potential victim of a criminal violation, or series of criminal violations, or that the credit union was used to facilitate a criminal transaction, even though there is no substantial basis for identifying a possible suspect or group of suspects.
* Transactions aggregating $5,000 or more that involve potential money laundering or violations of the Bank Secrecy Act:Any transaction (which for purposes of this subsection means a deposit, withdrawal, transfer between accounts, exchange of currency, loan, extension of credit, purchase or sale of any stock, bond, certificate of deposit, or other monetary instrument or investment security, or any other payment, transfer, or delivery by, through, or to a credit union, by whatever means effected) conducted or attempted by, at or through the credit union and involving or aggregating $5,000 or more in funds or other assets, if the credit union knows, suspects, or has reason to suspect that:
* The transaction involves funds derived from illegal activities or is intended or conducted in order to hide or disguise funds or assets derived from illegal activities (including, without limitation, the ownership, nature, source, location, or control of such funds or assets) as part of a plan to violate or evade any law or regulation or to avoid any transaction reporting requirement under Federal law;
* The transaction is designed to evade any regulations promulgated under the Bank Secrecy Act; or
* The transaction has no business or apparent lawful purpose or is not the sort in which the particular Member would normally be expected to engage, and the credit union knows of no reasonable explanation for the transaction after examining the available facts, including the background and possible purpose of the transaction.

The Bank Secrecy Act requires all credit unions to file currency transaction reports (CTRs) in accordance with the Department of the Treasury’s implementing regulations (31 CFR Chapter X). These regulations require a credit union to file a CTR whenever a currency transaction exceeds $10,000. If a currency transaction exceeds $10,000 and is suspicious, the institution must file both a CTR (reporting the currency transaction) and a suspicious activity report (reporting the suspicious or criminal aspects of the transaction). If a currency transaction equals or is below $10,000 and is suspicious, the institution should only file a suspicious activity report.

* Computer Intrusion:For purposes of this report, “computer intrusion” is defined as gaining access to a computer system of a credit union to:
* Remove, steal, procure, or otherwise affect funds of the institution or the institution’s Members;
* Remove, steal, procure or otherwise affect critical information of the institution including Member account information; or
* Damage, disable or otherwise affect critical systems of the institution.

For purposes of this reporting requirement, computer intrusion does not mean attempted intrusions of websites or other non-critical information systems of the institution that provide no access to institution or Member financial or other critical information.

The information set forth in this document is intended as general risk management information. It is made available with the understanding that Beazley does not render legal services or advice. It should not be construed or relied upon as legal advice and is not intended as a substitute for consultation with counsel. Beazley has not examined and/ or had access to any particular circumstances, needs, contracts and/or operations of any party having access to this document. There may be specific issues under applicable law, or related to the particular circumstances of your contracts or operations, for which you may wish the assistance of counsel. Although reasonable care has been taken in preparing the information set forth in this document, Beazley accepts no responsibility for any errors it may contain or for any losses allegedly attributable to this information.