DATA BREACH INCIDENT RESPONSE PLAN TOOLKIT

RISK MANAGEMENT PRACTICE GUIDE OF LAWYERS MUTUAL

LAWYERS MUTUAL | LIABILITY INSURANCE COMPANY OF NORTH CAROLINA

www.lawyersmutualnc.com

DATA BREACH/DATA LOSS

INCIDENT REPONSE PLAN

Policies & Procedures For Incident Response

Organization: _____

Serial Number: _____

Date: _____

IDENTITY FRAUD INC.

Prevent | Prepare | Respond

SAMPLE INCIDENT RESPONSE PLAN

TABLE OF CONTENTS

ABOUT THE AUTHOR

Tom Widman, founder, president and CEO of Identity Fraud, Inc., helped pioneer identity and data theft insurance and risk management products. Tom is credited with designing the nation's first Business Identity Fraud insurance product, which has been integrated into IFI's comprehensive small business "SB" data theft risk management offerings. Over the past 25 years, Tom has worked at leading US insurance brokerages and earned the CPCU and AMIM insurance designations while working in the Lloyd's insurance market in London, England. He holds his BA in Economics from the University of California at Berkeley. Contact Tom at twidman@identityfraud.com or 925.296.2601.

APPROVAL SIGNATURE

I have approved this Incident Response Plan as reasonably designed to enable our Company to meet its compliance requirements as well as our continuing service commitments to our members in an incident.

Signed: _____

Title: (Chairman, President, etc.…)

Date: _____

INTRODUCTION

Our incident response plan has been developed to reduce the exposures to our organization, our customers/employees, and our partners that arise out of a data theft or data loss incident. We have an affirmative duty to protect our customer information and to properly respond to an incident that is both part of our Security Plan and that is required by law. (Your State Law)

In order to comply with (Your State Law) and following our Security Plan, our incident response plan specifically includes policies and procedures to:

- Assess the nature and scope of an incident, and identify what customer information systems and types of customer/employee information have been accessed or misused
- Contain and control the incident to prevent further unauthorized access to, or misuse of, customer information, while preserving records and other evidence
- Notify appropriate law enforcement agency
- Maintain or Restore Business Continuity
- Notify customers/employees when warranted

This plan further outlines procedures that we will implement and/or consider in the event an incident occurs. All staff is required to be familiar with this plan and supervisors have been instructed to share this plan with their staff.

It is important to note that our obligations under this plan extend to the information shared with and/or managed by our vendors. Therefore, it is our policy to monitor and review what third party vendors have our information and how we and/or they will respond to an incident occurring in their operations.

INCIDENT RESPONSE TEAM

Considering the size of our Company, we have set forth the following procedures in our Security Plan and at the direction of management responsible for overseeing its development, we have created an incident response team or have appointed a Company individual that is assigned with the duties to implement, review, test, and modify the incident response plan, as appropriate.

While developing our team, we have considered the size of our organization, available staff, staff expertise, budget resources and exposures to incidents. Where we have determined that we lack any specific expertise or other internal resources that are needed to carry out team assignments, we have considered the value of and made preparations for using third party experts. It is our policy and goal to be prepared for and competently respond to an incident.

The team's roles and responsibilities are communicated to all Company staff. Similar communication is provided if, and when, there are changes to the team, or its roles and responsibilities.

In order to measure the effectiveness of the team, it is our policy to evaluate the team's performance and preparedness, at least annually. While our evaluation may be conducted by management, staff, outside experts, and/or by the team's self assessment, the evaluation will consider the following:

- Benchmarking or comparing to other Incident Response Teams
- General discussions with management, team members and staff
- Surveys dispersed to management, team members and staff
- An audit by a third party knowledgeable in incident response plans, policies and procedures and actual incidents

Additional information that may be made available during the evaluation process may include:

- Number of reported incidents
- Response time
- Number of incidents successfully resolved
- Information or updates that have been supplied to the organization
- Whether or not security issues remain within the organization and what they are
- Preventive measures or practices in place, are being implemented, or pending further review

In an effort to maintain awareness of the incident response plan and its team, it is our policy to distribute the following team member contact sheet to all staff and to post the contact sheet in a convenient and conspicuous location.

INCIDENT RESPONSE CONTACT SHEET

DATE:

Incident Response Manager: (name) _____

(telephone) _____

(mobile) _____

(email) _____

Responsibility: _____

_____

Incident Response Manager: (name) _____

(telephone) _____

(mobile) _____

(email) _____

Responsibility: _____

_____

Incident Response Manager: (name) _____

(telephone) _____

(mobile) _____

(email) _____

Responsibility: _____

_____

Incident Response Manager: (name) _____

(telephone) _____

(mobile) _____

(email) _____

Responsibility: _____

_____

SUSPECTING OR DETECTING AN INCIDENT

In the event an incident is suspected, is actually occurring, or has actually occurred, it is our policy to have the staff member that becomes aware of the circumstance to report the event as an incident to their immediate supervisor. In the event a staff member is unable to communicate with their supervisor, contact is to be escalated to any one of the Incident Response Team Members, as identified in the Incident Response Contact Sheet.

The following definitions are adopted to interpret what constitutes an incident:

Incident

Any perceived, actual, or successful attempt to gain unauthorized access to or use of customer/employee information that could result in substantial harm or serious inconvenience to a customer.

(Incidents may arise out of or include breach of data confidentiality, stolen computer, laptop, PDA, or storage device, data modification / destruction, unauthorized use of data, computers or changes to computers and any attempts of the above, a computer virus, computer spyware, burglary, pre-text calls, and more. Incidents may also be detected based on anomalies in information, unusual behavior by customers or staff, and notification by a customer, vendor, or law enforcement, etc.)

Customer/Employee Information:

Any record containing nonpublic personal information about a customer/employee, whether in paper, electronic, or other form, maintained by or on behalf of the Company.

Employee/customer information that is considered sensitive in nature is as follows:

Name, address, or telephone number, social security number, financial institution account numbers, a personal identification number or password that would permit access to the customer's or employee's account. Sensitive customer's and employee's information also includes any combination of components of customer's and employee's information that would allow someone to log onto or access the customer's and employee's account, such as a user name and password or password and account number.

Following the detection of an actual or perceived incident, staff is instructed to complete the following Incident Response Discovery Form and forward it to their supervisor or an incident response team member, as appropriate.

INCIDENT RESPONSE DISCOVERY FORM

Date: _____

Time: _____

Your Name:_____

Dept: _____

Phone:_____

Location Where Occurred: _____

Date Discovered: _____

Time Discovered: _____

Who Discovered: _____

Please Provide A Description Of The Incident Below:

_____

_____

_____

_____

_____

_____

Name of Supervisor Contacted: _____

Contact Number of Supervisor:_____

Incident Response Manager Contacted:_____

Contact Number of Incident Manager: _____

INCIDENT ASSESSMENT AND ANALYSIS

The internal and external environment of our Company is subject to constant change. Therefore, it is our policy to assess each incident based on its own unique merits and characteristics.

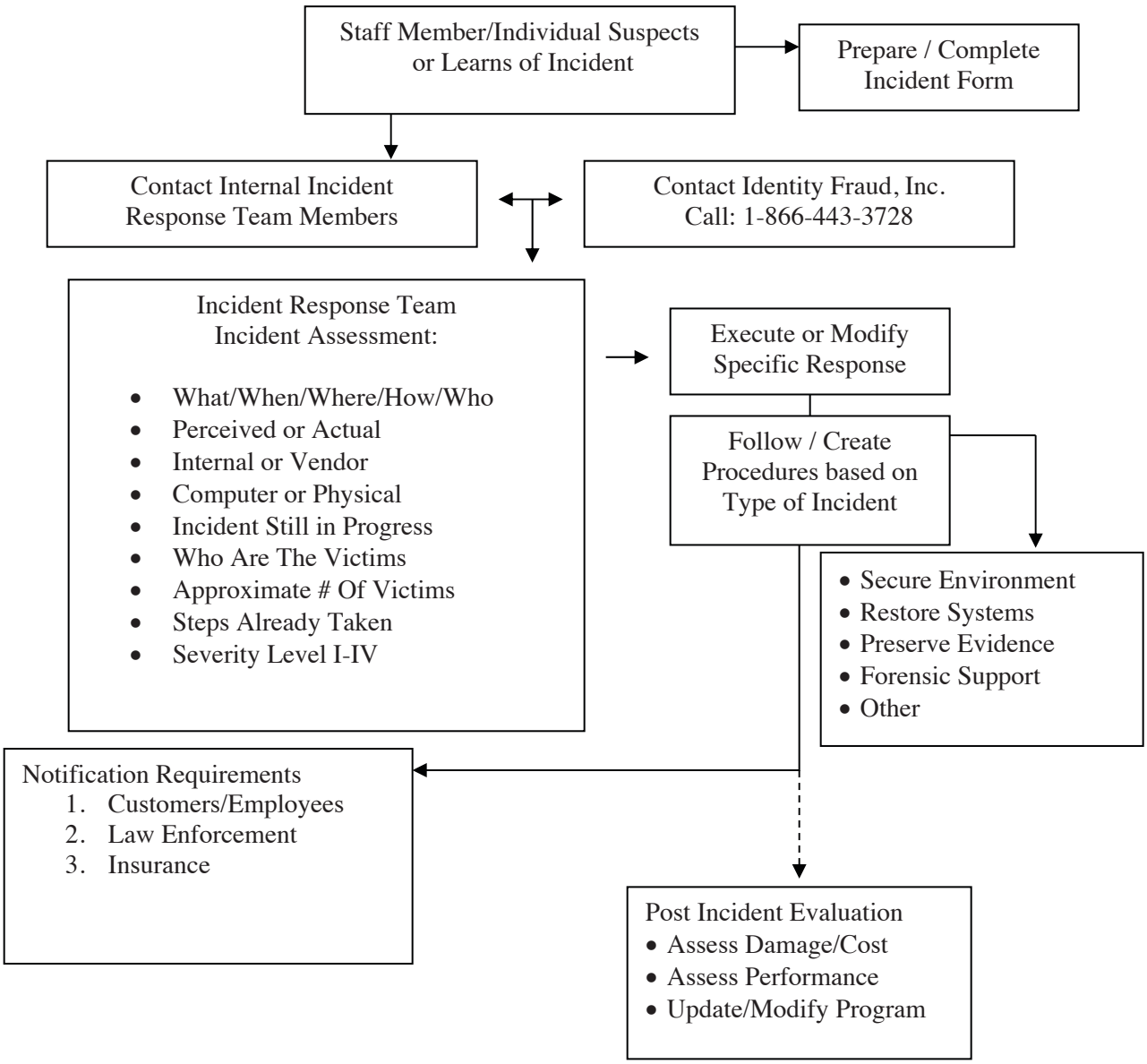
Upon assessing the incident, we shall consider the following:

1. Is the incident perceived or real?
2. Is the incident arising internally? Or, externally at a vendor?
3. Is the incident "live" and still in progress?
4. What is the threat targeting?
5. What type of incident is it?
6. Is the incident singular or part of a multi-faceted attack?
7. What evidence exists?
8. Will evidence be preserved?
9. What steps have already been taken to remedy the incident?
10. What is the estimated severity?
    a. Level 1 – Life Threatening?
    b. Level 2 – Threat to Customer/Employee (Sensitive) Data?
    c. Level 3 – Threat to Operating or Computer Systems?
    d. Level 4 – Will Services be Disrupted?
11. Can the incident be contained?
12. Will containment efforts alert the attacker?
13. How might the incident evolve?
14. Can the incident reoccur?
15. What are worst-case & reasonable scenarios?
16. Is the incident an emergency?
17. Is outside assistance to assess or remedy the incident justified?
18. How will normal operations resume?
19. What additional assessment criteria are needed?

Following the incident assessment, team members will create an incident response strategy and will carry out duties to execute the incident response strategy according to established and/or new policies and procedures. For illustration and reference purposes only, the following flow chart is provided.

DATA BREACH INCIDENT RESPONSE FLOW CHART

Sample Only



NOTIFICATION

As a business subject to regulations and laws, and as a business that emphasizes the value of customer/employee trust and loyalty, it is our policy to notify the following parties in the event of an incident.

1. Our President, CEO, Board of Directors and our Security Division
2. Appropriate law enforcement authorities
3. Customers and employees, when warranted

We are given a reasonable time to investigate. A determination will need to be made regarding the likelihood that information has been or will be misused or is reasonably possible to be misused. While notice to customers/employees may also be delayed if law enforcement is involved in an investigation and if such notice will interfere with the investigation, it is our policy to provide notice to customers/employees as soon as notification will no longer interfere with such investigation.

During our investigation of an incident, we will need to determine which customer/employee information has been improperly accessed, if any. In the event we are able to determine that a group of files has been improperly accessed, but are unable to identify which specific customer/employee information has been accessed, notification will be made to all customers/employees in the group if we determine that misuse of the information is reasonably possible.

CUSTOMER/EMPLOYEE NOTICE CONTENT

The content of the customer/employee notification will be given in a clear and conspicuous manner that provides a description of the incident, including the type of customer/employee information that is the subject of unauthorized access or use. Other content that we will consider includes:

- What the Company has done to protect the information from further unauthorized access or use
- A telephone number the customers/employees may call for further information and assistance
- A reminder that customers/employees should remain vigilant over the next twelve to twenty-four months and to promptly report incidents of suspected identity theft to their financial institution(s) and law enforcement
- Recommendations that the customer/employee review account statements and report suspicious activity
- A description of credit bureau fraud alerts and how they may be obtained
- Recommendations that the customer/employee periodically obtain credit reports and have information relating to fraudulent transactions deleted from their records
- An explanation of how to obtain credit reports free of charge
- Information about the Federal Trade Commission's website, phone number, and online identity theft resources and guidance on preventing identity theft
- Other customer/employee remedies provided by the (Company) at no cost to the member

Customer/employee notice will be delivered in a manner designed to ensure that a customer/employee can reasonably be expected to receive it, either by phone, letter, email, or similar communication.

CUSTOMER/EMPLOYEE NOTIFICATION LETTER

Sample Only

The following notification letter illustrates content that we may include in a response.

Date

First Name Last Name
Address
City, State, Zip Code

RE: Incident Subject / Your Personal Information

Dear First Name Last Name:

We are writing to let you know that as a result of the recent data breach and attempt to misappropriate your personal information, (Company's Name) is taking steps to help protect your identity.

The personal data that was potentially exposed includes your name, address, telephone number, account number, social security number …….

Although we have no indication that your personal information has been abused, we take the protection of your account information and your identity very seriously. Therefore, we are implementing the following precautionary measures to protect you.

- We have placed a warning flag on your customer/employee file.
- We will take additional steps to confirm your identity as the customer/employee of the file whenever you contact us.
- We have established a dedicated phone number at (Company's Name), (123) 456-7890 **or toll-free** (800) 456-7890, to answer your questions and provide additional information. This number will be available Monday through Friday from 8:00 am to 6:00 pm and Saturday from 9:00 am to 5:00 pm.
- (Company's Name) will pay the cost of enrollment for a one-year membership in the Identity Fraud, Inc. *Identity Protection Plan*, customized especially for our members. This service, at no cost to you, starts today and provides:
  - Access to VRS Elite™ fraud resolution counselors (24/7) to answer questions you have and to help resolve any circumstances relating to identity theft, whether simple or complex. Simply call IFI toll-free at **1-866-4-IDFRAUD** (1-866-443-3728).

- $25,000 of identity insurance ($0 deductible) to cover certain expenses you may incur as a result of identity theft.
- Credit Report Monitoring, which will monitor your Experian credit file and send an email to you of any unusual activity on your credit file. (Your enrollment is required)
- One free copy of your credit report
- Access to the IFI Members Section for additional benefits, including educational materials, newsletters, discounts on additional products, and more

To enroll in the Credit Monitoring program, please call Identity Fraud, Inc. at 1-866-443-3728 between the hours of 8:00 am to 5:00 pm, Monday through Friday, Pacific Standard Time.

As an additional precaution, you may want to consider taking the following step:

- You may want to place a FREE 90-day initial Security Alert on your credit bureau file.The Security Alert, which can be requested only by you, provides another significant layer of protection by flagging your credit file for additional scrutiny by potential lenders. If you choose to activate a Security Alert, you need to successfully activate the alert with only ONE of the three main credit reporting agencies listed below. The agency you report to will automatically notify the other two agencies, as required by law. Their contact information is:

Equifax	Experian	TransUnion
1-888-766-0008	1-888-397-3742	1-800-680-7289

(Company's Name) is committed to protecting the confidentiality of our customer/employee personal information. While we regret any concern or inconvenience the recent incident may cause you, both Identity Fraud, Inc. and (Company's Name) believe the above items will help protect you from potential identity theft, no matter what type or how it may occur.

Please do not hesitate to contact us if we can assist you in any way.

Sincerely,
First Name Last Name
President and CEO

ADDITIONAL POLICIES AND PROCEDURES

Documentation

Documentation of an actual or perceived incident will include but not be limited to information relating to the person(s) that discovered the incident, suspect(s), incident assessment, strategic response, hard copy evidence, electronic evidence (computer logs, emails, telephone recordings, etc.) meeting notes, damage, and costs.

Damage / Cost Assessment

Prior to an incident occurring and during and after an incident occurs, attempts will be made to quantify the potential damage to the Company and the associated costs to contain and remedy the incident.

Insurance

Insurance coverage may or may not apply to incidents. Therefore, we will conduct a review to better determine when insurance may or may not apply to various incidents and whether or not insurance applies to any specific incident that is occurring. We will consult our professional insurance advisor/broker and/or company, as necessary.

Review and Adjust

Following an incident, Company and incident response team will review its performance and take appropriate steps to improve its prevention and response efforts and to improve its policies and procedures to better avoid the recurrence of incidents.

Board of Directors Management and Reporting

It is our policy to provide a report, at least annually, to management and/or the Board of Directors regarding the status and condition of our incident response plan and team. Furthermore, following an actual incident or testing of an incident, a report will be prepared and distributed to the appropriate parties.

End of Document