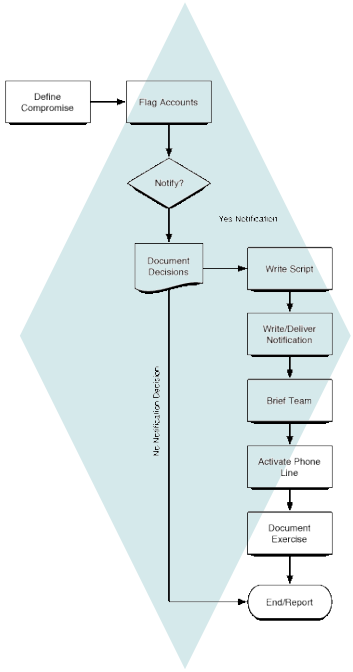
Introduction

CONTACT INFO: www.appliedintent.com

WELCOME to the Applied Intent Customer Notification Process. This guide provides instructions and templates for notifying customers in response to unauthorized access to confidential customer data. This process is designed for small-to-medium financial institutions and is a key component of the larger and more in-depth Applied Intent Incident Response Program©.



Why do I need a Notification Process?

Most banks are not prepared for a compromise of customer data. Many wait until an actual incident occurs and then struggle to fight the fires. Perhaps this is because they tend to think of Incident Response as a "computer" or "technology" issue. It is not. Incident Response is fundamentally a risk management and business resumption activity that should employ both business and technology personnel in a pre-planned and well-orchestrated response.

The banking regulatory agencies (Office of the Comptroller of the Currency, Federal Reserve Board, Federal Deposit Insurance Corporation and Office of Thrift Supervision) have issued an important interpretation of the mandatory information security standards contained within the Gramm-Leach-Bliley Act (GLBA). This guidance, titled "Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice", serves to "clarify the responsibilities of financial institutions under applicable Federal law." While financial institutions are given some discretion in how to implement this Interagency Guidance, overall compliance with this new regulation is mandatory.

What's included in the Process?

- Policy
- Procedures [Workflow]
- Reporting Requirements
- Sample Notification Letter
- Sample Incident Response Form

The Interagency Guidance is essentially composed of three requirements for financial institutions:

1) To establish an operational incident response capability;
2) To perform a "prompt" and "reasonable" investigation when the financial institution becomes aware of an incident of unauthorized access to sensitive customer information in order to determine the likelihood that the information has been or will be misused.
3) Notification of customers if the investigation determines that misuse of its information about a customer has occurred or is reasonably possible.

What is an information security incident?

An information security incident is an event that appears to be a breach of information security safeguards. An incident regarding a compromise of customer data can occur in countless ways.

a) Stolen or Lost Laptop

b) Confidential Reports that were not shredded before going in a dumpster

c) Confidential information attached to email (without utilizing some form of encryption)

d) Employees giving confidential information to the wrong person(s)

e) And many more

Each financial institution should have a well planned and organized Incident Response Program that includes policy, procedure, identification of the staff that will be involved, call lists, forensics tools, etc. When an incident occurs, the response is triggered. People quickly come together, perform triage, and start making repairs and recovering normal operations. One of the final pieces of a complete Incident Response Program is the Customer Notification Process.

This is because some information security incidents will lead to the possible misuse of confidential customer information and, therefore, fall under the Interagency Guidance that requires customer notice.

This Customer Notification Process provides a structured method for determining whether customer notice is appropriate, and then proceeding to develop and execute that notice. This process typically begins after an incident has been reported to your designated Incident Response Team and they have determined that confidential customer data was compromised.

CUSTOMER NOTIFICATION PROCESS

Trigger

A Compromise of confidential customer data has been confirmed

Input

Information and documentation about the reported incident.

Output

A good and documented decision about notifying customers
A completed customer notification exercise
A completed report for regulating agency

Process Steps

Step	Description	Role
1	**Define Circumstances of This Compromise** Specifically identify the volume and type of information that has been lost, the list of customers that was probably included in the compromised data, and the likelihood that the information has been or will be misused.	**Incident Response Team (IRT)**
2	**Flag Accounts that May Have Been Compromised** Make certain all customer information systems are flagged [in the event you have more than one]	**Customer Service Staff**
3	**Determine Whether to Notify Customers** Review company policy, the laws or your State, and regulatory guidance, then decide whether the circumstances of this compromise of information warrant the notification of customers. If you will notify customers, skip to step 5, Write Customer Service Script. If you will *not* notify customers, continue with step 4, Document the Decision.	**Customer Notice Managers (see details below)**

CUSTOMER NOTIFICATION PROCESS

Step	Description	Role
4	**Document the Decision and Report to Regulators** Capture the specific circumstances of this compromise and the decision to notify customers (including details and reasons that led to the decision) and store this information in the company Incident Response File. This concludes the process.	**IRT and Customer Notice Managers**
5	**Write Customer Service Script** Make any modifications necessary to the "Sample Script" for the telephone personnel to use when they receive a customer call about this compromise.	**Customer Notice Managers**
6	**Write and Deliver Customer Notification** Make any modifications necessary to the "Sample Customer Notification Letter" and mail to all customer identified in step 1.	**Customer Notice Managers**
7	**Brief the Customer Service Team** Call together the personnel who will be accepting customer telephone calls related to the customer notification and this incident. Brief them on the circumstances of this loss of data, what the company is doing to protect the customers involved, what customers can do to protect themselves. Walk through the script and instruct the team on any "out of bounds" issues and escalation path. Remember to include the escalation managers in the briefing.	**Customer Notice Managers**
8	**Activate the "Customer Compromise Line"** Turn on the phone number, schedule staff to accept calls, etc.	**Customer Notice Managers**

Step	Description	Role
9	**Document the Customer Notification Exercise** Capture the specific circumstances of this compromise and the decision to notify customers (including details and reasons that led to the decision). Also collect information about the number of customers who called in for additional information and what their primary questions were about (this can be used to improve future scripts and notification letters). NOTE: Regulations require that you provide your report before you have collected all the customer feedback from the call center. This is ok. Regulators will be more concerned with documentation that your decisions and notifications were appropriate and well timed. This concludes the process.	**Customer Notice Managers**

Customer Notice Managers

Because there are significant liabilities involved, it is very important to have the correct people making decisions about whether to notify customers, and what to say. The Executives and/or Managers who are authorized to accept this sort of liability on behalf of your company must be involved. Here is a suggested list of participants in the group of "Customer Notice Managers".

- CEO or designee – Lost customer information can impact both the bottom line of the company and the ongoing reputation of the company. In small institutions, the CEO will likely want to be involved in these decisions. In larger institutions, the CEO may designate a lower executive for this role.
- Director of the impacted Line of Business – Often the lost data will belong to one line of business (e.g., retail banking, mortgage, commercial loans, etc.). The Director of that line of business should be involved in these decisions because it is their customers who are impacted and their managers who will serve in the escalation path for calls.
- Legal Counsel – Notifying larger numbers of customers of lost information could possibly lead to legal action against your financial institution. Include your counsel in discussions of what to include in the Notification Letters and the call center script.
- Information Security Officer – Naturally, your Information Security Officer (if you have one) should be included in this process to advise the CEO and other managers on regulations, relevant laws, and to provide directly relevant experience.
- Compliance Director – Your compliance person should be apprised of all matters that impact the institution's compliance with laws and regulations.

SAMPLE CUSTOMER NOTIFICATION POLICY

PURPOSE

This policy governs decisions and actions associated with notifying customers in response to an information security incident.

POLICY

The [Job Title Here] is responsible for ensuring that [Company Name Here] performs a prompt and investigation of circumstances surrounding potential unauthorized access to sensitive customer information in order to determine the likelihood that the information has been or will be misused.

The [Job Title Here] is responsible for ensuring that notification of customers is carried out IF the investigation determines that misuse of its information about a customer has occurred or is reasonably possible.

Any disclosure of information security incidents at [Company Name Here], including reports to regulators and notifications to customers, must be approved in advance by the CEO or designee.

The [Job Title Here] shall maintain a procedure for customer notifications of information security incidents, including templates for customer letters and call center scripts. Management and legal counsel must approve the procedure and templates, and any periodic changes to them.

Staff is required to use the approved procedure and templates, with reasonable modification for the immediate incident circumstances, for all customer notification scenarios.

REMEMBER:
A Policy is a "personal" thing. It must be built and tailored for your company's culture and characteristics. The Applied Intent, LLC Incident Response Program provides tools for how to build an effective policy tailored just for you!

SAMPLE CALL STAFF INSTRUCTIONS AND TELEPHONE SCRIPT

Instructions

You will be representing [Corporate Name] during our response to the recent incident. It is imperative that when talking to customers you remain calm and assist the customer in understanding the impact on them and any actions they may need to take.

Description of the Incident

Describe in some detail what has happened that triggered the customer notification. Provide enough information to assist the Call Center Representative in answering telephone requests. But don't include too much technological detail, as that will only confuse the average customer. You may wish to include:

- What information was lost
- How the information was lost
- What your institution is doing in response
- Suggestions for how the customer can take action to protect themselves

Escalation Path

Some customers will be upset and/or may not be satisfied with the information your call center has been authorized to provide. ***Before*** this comes up, you should designate your managers for escalation of these calls. Engage the line of business where the incident occurred, their managers, and top-level executives to build and appropriate escalation path for your Call Center Representatives. Here is a suggested escalation table.

Escalation Level	Staff Instruction	Person receiving the escalated call
Level One	Call Center Staff may transfer the call to the designated Manager	Manager from the line of business where the incident occurred. If you are receiving a high volume of calls, you may wish to have this person live in the call center.
Level Two	The Level One Manager should take Customer's contact info and promise prompt call back.	Director from the line of business where the incident occurred.

	Notify the designated manager IMMEDIATELY.	
Level Three	The Level Two Manager should take Customer's contact info and promise prompt call back. Notify the designated manager IMMEDIATELY.	Executive such as President or CEO

Provide all Call Center Representatives with a copy of the letter that was sent to the customer.

Script

Thank you for calling [Corporate Name]. My name is [Name] and I can help you.

CALLER: ASKS FOR DETAILS OF THE INCIDENT

AGENT: *Instructions: Provide the Description of Incident [above]. Do not offer any additional information and DO NOT guess or estimate details not provided to you.*

CALLER: "WHAT IS IDENTITY THEFT?"

AGENT: "Identity theft is the fraudulent user of another person's identification information for the purpose of obtaining credit. If a thief has your credit card they can only buy things with that card. But if a thief has your name and social security number, they may pose as you and try to open a new credit card account that you would not know about until it is too late."

CALLER: "HAS MY IDENTITY BEEN STOLEN?"

AGENT: "We don't know that it has. We only know that your information was accidentally allowed outside our security protections, and it is possible that somebody other than our employees could find it."

CALLER: "IS THERE ANY WAY I CAN KNOW IF I'M A VICTIM OF IDENTIFY THEFT?"

AGENT: "Subscription services are available to watch your credit record for new accounts and inquiries. These services can notify you when there is activity. You would know if that activity was generated by you, or somebody else, and you could respond accordingly. The credit bureaus and other companies offer this service."

CUSTOMER NOTIFICATION PROCESS

CALLER: "WHAT ARE YOU DOING TO GET MY INFORMATION BACK?"

AGENT: *<u>Instructions:</u> Provide the relevant portions of the Description of Incident [above]. Do not offer any additional information and DO NOT guess or estimate details not provided to you.*

CALLER: "WHAT SHOULD I DO NOW?"

AGENT: "We recommend that you carefully examine all credit card billings and other such statements to verify charges. If anything looks suspicious, promptly report the information to _____ as suspected identity theft."

"Also, the Federal Trade Commission offers information on their web site and toll-free number that you may find useful. I can provide you with that contact information if you wish."

CALLER: "I AM ALREADY A VICTIM OF IDENTITY THEFT AND I RECEIVED THE LETTER. IS YOUR INSTITUTION THE CAUSE?"

AGENT: "At this time, we cannot know that. However, you may have information that will be an important lead. Please hold, I am going to transfer you to a manager."

CALLER: "I WANT TO TALK TO A MANAGER"

AGENT: "Please hold, I will transfer you immediately." *Transfer to the escalation level 1 manager and take the Customer Call Record Form to that manager.*

UPON COMPLETION OF THE CALL:

1. Complete the Customer Call Record Form
2. Send the completed form to the escalation level 1 manager for review.

SAMPLE CUSTOMER CALL RECORD/FORM

Date of Call:			
Caller Name:			
Caller Address:			
Caller Phone:			
Did the Caller ask to be Escalated?	☐ Yes ☐ No	Escalation Level	☐ Level 1 ☐ Level 2 ☐ Level 3
Caller Concerns:			
Was Caller Satisfied with Explanations?			
Is Follow-Up Needed?	(if yes, explain)		
Assign Follow-Up:			
Follow-Up Date:			

SUGGESTED COMMUNICATION TO REGULATORS

From: [Corporate Name]

Subject: Recent Incident Name

Incident #: IR1234

General Incident Information

Describe the incident in some detail explaining the incident type, severity, whether there was a loss of availability of services, notification status, etc. If the incident resulted in a customer notification effort also include the letter and number of customers impacted.

What we're doing to protect the organization and our customers

1. Coordination efforts
2. Containment efforts
3. Communication efforts
4. Final Resolution

Security Policies in Place

List any relevant security policies and procedures utilized during this incident [such as patch management, virus detection, notification processes, etc.]

Incident Management Team

Provide a list of names and titles for the incident management team that authorized and made decisions regarding the incident and resolution. Also include one central contact if the regulatory agency has additional questions.

SAMPLE CUSTOMER NOTIFICATION LETTER

Dear _____,

[Corporate Name] believes in acting quickly in our customers' best interest. We recently became aware of an incident involving unauthorized access to certain customers' confidential information. (describe here the incident in general terms)

This incident may have increased the probability of your information being used for fraudulent purposes. It is impossible to know with certainty whether you will experience trouble, but there are steps you can take to protect yourself, should you wish to do so. Here are some possibilities:

- Carefully examine all credit card billings and other such statements to verify charges. If anything looks suspicious, promptly report the incident as suspected identity theft.
- You may wish to visit the Federal Trade Commission's (FTC) web site or call their toll-free number to obtain identity theft guidance and to report suspected incidents of identity theft (see contact information provided below)
- Subscription services are available that can provide notification to you anytime there are changes or inquiries in your credit record.
- The Fair Credit Reporting Act allows you, under certain circumstances, to place a fraud alert in your consumer credit report
- You may also use this letter to obtain a free credit report from the reporting agencies (contact information included below)

Please do not hesitate to contact [Corporate Name] at xxx-xxx-xxxx, our response hotline, for assistance and information related to this incident.

Sincerely,

Board of Directors
[Corporate Name]

Enclosure: Reference Contacts

Reference Contacts

CUSTOMER NOTIFICATION PROCESS

Here are some of the bureaus or agencies you may want to contact if you are a victim of identity theft:

Equifax
11601 Roosevelt Blvd.
St. Petersburg, FL 33716-2202
To Report Fraud: (800) 525-6285
To Order a Credit Report: (800) 685-1111
Website: www.equifax.com

Experian
P.O. Box 1017
Allen, TX 75013
To Report Fraud: (888) 397-3742
To Order a Credit Report: (888) 397-3742
Website: www.experian.com

Trans Union
P.O. Box 390
Springfield, PA 19604
To Report Fraud: (800) 680-7289
To Order a Credit Report: (800)916-8800
Website: www.tuc.com

U.S. Federal Trade Commission
Toll free: (877) 438-4338 or www.consumer.gov/idtheft
Also a free brochure on Identity Theft:
http://www.ftc.gov/bcp/conline/pubs/credit/idtheft.htm