

INCIDENT RESPONSE GUIDELINES

Table of Contents

| | | |
|------|----------------------------------|------------|
| I. | INTRODUCTION | Page 2 |
| II. | PREPARATION | Page 3 – 4 |
| III. | INVESTIGATION | Page 5 |
| IV. | IMMEDIATE REMEDIAL ACTIONS | Page 6 |
| V. | CUSTOMER NOTIFICATION ACTIVITIES | Page 6 – 7 |

INCIDENT RESPONSE GUIDELINES

Introduction

NOTE: THE NATIONAL CREDIT BUREAUS ARE REQUIRING THAT ALL COMPANIES THAT ACCESS THEIR CREDIT INFORMATION HAVE WRITTEN PROCEDURES IN THE EVENT YOUR COMPANY IS EXPOSED TO A DATA BREACH. THE FOLLOWING “INCIDENT RESPONSE GUIDELINES” IS A SAMPLE OF THE DOCUMENTATION YOU WILL NEED.

ONE SOURCE IS NOT OFFERING LEGAL ADVISE, WE ARE ONLY PROVIDING AN EXAMPLE AND RECOMMEND YOU CONSULT YOUR ATTORNEY TO BE SURE THAT YOU ARE IN COMPLIANCE WITH BOTH THE BUREAUS’ POLICIES AND THE FEDERAL LAWS CONCERNING DATA BREACH.

The procedures outlined in this document are the guidelines to be followed by (insert company name), (Our Company), in the event of a security breach involving personal, sensitive information on applicants applying for a mortgage loan.

The definition of a “breach” generally means compromise of the security, confidentiality, or integrity of data that results in, or there is a reasonable basis to conclude has resulted in, the unauthorized acquisition of and access to personal information. The definition of personal, sensitive information also varies amongst federal and state laws but generally includes: first name, or first initial and last name, in combination with any one or more of the following data elements, when either the name or data elements are not encrypted: 1) Social Security Number, 2) Drivers License Number 3) Account number, credit or debit card number, in combination with any required security code, access code, or password permitting access to an individual’s financial account. These incidents can be caused by rogue or former employees, access ID breaches, access ID violations, theft, or rogue businesses that gained access to credit information due to fraudulent applications or inadequate membership vetting.

As is the requirement of the three bureaus, **Our Company** will immediately notify our Credit Reporting Agency (CRA), and **our CRA will notify the national credit bureau(s) that may be involved; Equifax, Experian and TransUnion at the addresses shown below.** **Our Company** will also notify all affected consumers in a manner that is in accordance with federal and state legislation. Since each investigation is unique and may require additional action from **Our Company and Our Company** will work closely with our CRA, the national bureaus and law enforcement when necessary.

Equifax Regulatory Compliance Investigations Department at: 402-330-1620

Experian Regulatory Compliance Investigations Department at: 800-295-4305

TransUnion Regulatory Compliance Investigations Department at jtilley@tusales.com

INCIDENT RESPONSE GUIDELINES

II. PREPARATION

The following information considers the steps necessary to prepare for a possible incident involving unauthorized access to consumer personal, sensitive information involving **Our Company** consumer's business. This section provides the background of information needed to guide **Our Company** through an investigation and consumer notification.

- 1) **Our Company** Key Personnel will be identified that will be allowed to gather the appropriate information about incidents, manage the consumer notification projects and respond to requests from the bureaus and law enforcement. These Key personnel will have the experience and authority to communicate with the bureaus during the course of the investigation and will respond quickly to any and all questions/requests generated by the bureaus, law enforcement and the consumer.
- 2) **Our Company** Key Personnel will know and understand federal and state law requirements so that we are aware of any specific timelines that are in place; and will understand that the laws are based on the consumer's address, not our business's location.
- 3) **Our Company** Key Personnel will review each data element on the credit reports obtained from the CRA and if consumers sensitive data account numbers are not truncated, will request our CRA to truncate the accounts to reduce exposure. Current laws generally require notifications based on the type and combination of data that was compromised.
- 4) **Our Company** will establish a method to obtain "best" addresses for consumers whom you will be notifying in the event of a breach. Understanding that in many situations the inquiry address is not legitimate. Therefore, if you mail to the address used for the fraudulent or suspicious inquiries, you may be notifying the fraudster, not the consumer you intended to notify.
- 5) **Our Company** will research nationally recognized commercial consumer monitoring services that provide the ability to offer affected consumers one year free credit monitoring services; and several options are available to **Our Company**.
- 6) **Our Company** will draft a consumer notification letter that can be used for most situations. While every incident will require unique information for the letter, all notices will need to include:
 - a) Contact information for each of the national credit reporting agencies.
 - b) Instructions on how the consumers can add initial security alerts.
 - c) The offer of credit monitoring and accompanying instructional information
 - d) Contact information for credit reporting agency to call if they have questions. It will be easier if you have a draft outline or template to use prior to an incident.
- 7) **Our Company** will maintain a stock of business letterhead stationery for the purpose of notifying consumers of the possible breach.
- 8) **Our Company** will research a "letter shop" business that can manage notification to the consumers in the event that the consumer population is too large to handle in-house; several options are available to **Our Company**.

INCIDENT RESPONSE GUIDELINES

- 9) The loan origination mortgage software utilized by **Our company** and/or our credit reporting agency can provide activity logs that can provide detailed information for use in the investigation process to be able to identify the affected consumer population. This information may also have to be submitted to law enforcement under subpoena. The information generally needed during investigations by the bureaus and law enforcement includes, but is not limited to, the following:
- a) At least 2 years of inquiry history
 - b) IP address for each inquiry
 - c) User IDs
 - d) Date/time of each inquiry
 - e) Subscriber code
 - f) User ID information (operator initials, names etc)
 - g) You should review with your counsel what other systems and logs may be required under federal and state law, including the FTC's GLB Safeguards Rule.
- 10) **Our Company** understands it's responsibility to have written procedures in order to be in compliance with the national bureaus' security policies as well as the Gramm-Leech Bliley Act (Safeguard Rule) and the FTC Disposal Rule.

Our Company procedures include

- a) User IDs are NOT shared by our employees.
 - b) A periodic review of Authorized Employee's activities, Authorized Employee's access rights, inactivity reviews, authentication and authorization process review, etc.
 - c) Ability to obtain credit information is restricted to a few key personnel.
 - d) We do not discuss internal subscriber account numbers and passwords by telephone with any unknown caller, even if the caller claims to be an employee of one of the bureaus.
 - e) All terminal devices used to obtain credit information are placed in a secure location within our facility so that unauthorized persons cannot easily access them. All keyboards are locked after 5 minutes of non-use.
 - f) After normal business hours, all devices are turned off and locked or systems used to obtain credit information.
 - g) Hard copies and electronic files of consumer reports within our facility are secured so that unauthorized persons cannot easily access them.
 - h) All employees are made aware that access ID sharing is forbidden.
 - i) All consumer sensitive data will be disposed of in accordance with the FTC Disposal Rule and no consumer
- 11) **Our Company** consults with the consumer regarding inquiries on their credit report to look for suspicious or fraudulent activity.
- 12) **Our Company** maintains PGP encryption software. In the event of an Incident breach and the subsequent investigation process, you will be required to share personal sensitive consumer identification information with the bureaus and ALL such information transmitted must be encrypted.

INCIDENT RESPONSE GUIDELINES

III. INVESTIGATION

What to expect when a breach of consumer information has occurred within **Our Company** environment and what information will likely be asked to provide for investigative analysis to determine cause and scope of the breach.

- 1) If an incident-breach has occurred or been detected, **Our Company** will
 - a) Immediately notify the CRA, who will notify the national credit reporting repositories
 - b) Immediately begin an investigation to
 - i) Determine the cause.
 - ii) Determine the scope.
 - iii) Identify consumers.
 - iv) Be ready to assist law enforcement, if necessary.
- 2) **Our Company** will take an active role in researching, analyzing and sharing information that is uncovered during the investigation of the incident with the CRA, and all other agencies involved in the investigation of the breach.
- 3) **Our Company** will cooperate, communicate and maintain a high sense of urgency in investigating the incident. Some of the information national bureaus will require includes (but is not limited to):
 - a) Membership documentation signed with the credit reporting agency
 - b) List of access User IDs that may have been misused.
 - c) Dates of User ID accessed the credit information.
 - d) Dates of employment for specific User ID employee.
 - e) List of IP addresses used for inquiries under investigation.
 - f) Methods of access
 - g) Names, addresses and contact information for any third parties involved in the data transmission from bureau to **Our Company**, (ISPs, ASPs, etc.).
 - h) Names of suspect rogue employees and dates of employment.
 - i) Activity logs
 - j) Billing data.
- 4) **Our Company** understands that our CRA may be required to suspend our company's access to the national credit bureau(s) information until the bureau(s) is satisfied that data security has been restored.
 - a) National bureaus will require written confirmation that this has been done.

INCIDENT RESPONSE GUIDELINES

IV IMMEDIATE REMEDIAL ACTION

Actions **Our Company** may be asked to take in order to stop unauthorized access prevent re-occurrence and gain information to implement longer term remedial measures.

- 1) **Our Company** understands that in order to stop unauthorized access or to prevent the compromise of the investigation and that of law enforcement, our CRA may be required by the bureau(s) to immediately suspend access to the bureaus' data information.
- 2) **Our Company** understands that other actions that may be required::
 - a) Access Security Requirements certification.
 - b) Review and change internal procedures as needed to prevent the activity from re-occurring.
 - c) Limit access to a select, trusted few.
 - d) Procedures to ensure User IDS are not shared and are kept in a secure location.
 - e) A direct audit by the bureaus(s) of our company's policies, practices and facilities may be warranted, depending on the investigation findings.

V. CONSUMER NOTIFICATION ACTIVITIES

Guidelines and expectations for conducting a consumer notification in the event of unauthorized access to consumer personal, sensitive information including; letter content, credit monitoring and credit reporting agency alert messages.

- 1) Ascertain needs/requirements in order to conduct consumer notification:
 - a) Company letterhead/envelopes.
 - b) Use of a letter shop or internal project.
 - c) Obtain full list of affected consumers for mailing.
 - d) Identify if best consumer addresses are available for mailing. If not:
 - i) Ascertain best way to obtain best addresses including use of pre-established services offered by the national bureau(s) relating to Address Update services.
- 2) The consumer credit monitoring company selected by **Our Company** will be notified and the appropriate information relating to this service will be provided to the consumer in the Notification Letter, including website information and promotional codes.
- 3) **Our Company** contact information and phone number will be included in the consumer notification for consumer calls. If the incident breach is large in scope
 - a) A call center may be required and this information will be provided to the consumer, or
 - b) **Our Company** may discuss the possibility of custom URL web links to national bureau(s). This will make linking to these sites easier for the consumers.
- 4) To prevent embarrassing and costly mistakes, a draft template of the consumer notification letter will be created assuring that all information, links, instructions and phone numbers are correct and up-to-date.
 - a) A copy of this consumer notification letter draft will be provided to the national bureau(s) Investigators ASAP for approval of the final draft prior to the mail drop date.

INCIDENT RESPONSE GUIDELINES

- 5) Request the national bureau(s) to add Alerts to the credit files of the consumers that have been identified and have been affected by a breach.
- 6) Conduct any and all third-party notifications required by federal and state security breach notification laws. (For example, New York A. 4254 & S. 5827 require that you notify the state Attorney General, Consumer Protection Board and Cyber Security Office when any New York State consumers are notified.)
- 7) **Our Company** will prepare for calls from outside parties related to this incident such as state agencies, law enforcement and the media. Staff members will be trained on how to respond to these calls or to whom to transfer these calls.
- 8) **Our Company** will prepare an incoming call activity log that will be maintained for each incident for future reference regarding conversations and follow up with consumers.