# Data Security Breach Notice Letter

DANA B. ROSENFELD & ALYSA ZELTZER HUTNIK, KELLEY DRYE & WARREN LLP

A letter from a company to individuals (for example, employees or customers) notifying those individuals of a data security breach involving their personal information. This Standard Document has integrated notes with important explanations and drafting tips.

### **DRAFTING NOTE**

# **Read This Before Using Document**

To date, most states, the District of Columbia, Puerto Rico and the US Virgin Islands have enacted data breach notification laws. requiring businesses and other entities to notify affected individuals when a data breach involving their personally-identifiable information (also referred to as PII or personal information) occurs. The requirements of these laws vary and sometimes conflict, creating a significant compliance challenge for companies suffering a data security breach affecting individuals residing in multiple states. There is no single form letter that guarantees compliance with all of these laws. However, a common strategy to respond to this challenge is to:

- Review the breach notifications laws for each relevant state (meaning those states where individuals whose personal information is held by the company reside).
- Draft one template letter that meets the requirements of most of those state laws and one or more additional template letters to address relevant states having conflicting or more restrictive requirements.

This Standard Document provides a general template to assist in preparing data breach notice letters for affected individuals in connection with state data breach notification requirements. It must be tailored to:

- Reflect your company's particular circumstances and to address the specific state law requirements.
- Account for industry-specific federal or state legal requirements.

The contact information provided in the sample letter for federal and state agencies as well as the national consumer reporting agencies should always be checked to ensure that it is up to date.

This Standard Document is not intended for use by companies subject to breach notification requirements under the federal Gramm-Leach-Bliley Act (GLBA) or Health Insurance Portability and Accountability Act (HIPAA) (for more information on GLBA and HIPAA, see *Practice Note, US Privacy and Data Security Laws: Overview (http://us.practicallaw.com/6-501-4555)*).



For more information on US data breach notification laws, see *Practice Note, Privacy and Data Security: Breach Notification (http://us.practicallaw.com/3-501-1474)*. A list of State Security Breach Notification Laws with links to the text of each law is maintained by the National Conference of State Legislatures.

### **Contents of the Notice**

Most state breach notification laws do not set out specific requirements for the notice's content. However, an assessment of state breach notification statutes that do set out minimum requirements suggests that the notice generally should be in plain English and include:

- The date of the notice.
- The reporting entity's name and contact information so that affected individuals can obtain additional assistance or information.
- A brief description of the data breach incident in general terms. However, this should not be included in notices to residents of Massachusetts (see *Drafting Note*, *Brief Description of Incident and Categories of PII Involved*).
- The date of the breach, or if unknown, the approximate date or date range of the breach.
- The categories of personal information at issue.
- Whether notice was delayed as a result of law enforcement investigation.
- A brief description of the actions taken by the business to contain the breach and protect data from further unauthorized access or use.
- Advice on actions affected individuals should take.
- Contact information for law enforcement and other government authorities, including the Federal Trade Commission (FTC).
- Contact information for national consumer reporting agencies.

#### Other Considerations

State data breach notification laws also include other requirements. For example, when preparing for and responding to a data breach, companies must also consider legal requirements relating to the:

- Timing of notification.
- Method of notification. Some states specify how notice must be made, for example, by mail, telephone and other means, and in some circumstances, may permit substitute notice if individual notices cannot be provided.
- Notification of other entities, for example, the state attorney general and the office of consumer affairs, the FTC and law enforcement authorities and/or consumer credit reporting agencies.

Because significant liability issues could be involved with a data breach and data breach notification letters are often made public and reviewed by regulators, plaintiffs' lawyers and the media, it is critical to ensure that the notice has the appropriate substance. When preparing form notice letter templates, as well as when modifying the templates for use in response to an actual or suspected breach, the form notice letter should be reviewed by the company's:

- Legal counsel.
- Chief information officer (or equivalent officer).
- Public relations and corporate communications teams.

Ideally, even in advance of a breach, these individuals will be part of a formalized breach response team prepared to provide a prompt and legally compliant corporate reaction to the breach.

For guidance on preparing for and responding to a data security breach, see *Practice Note, Privacy and Data Security: Breach Notification (http://us.practicallaw.com/3-501-1474)*.

[COMPANY LETTERHEAD]

[INDIVIDUAL NAME]
[STREET ADDRESS]
[CITY, STATE AND POSTAL CODE]
[CREDIT MONITORING PROMOTION CODE]
[DATE]

Dear [INDIVIDUAL NAME]:

We value your business and respect the privacy of your information, which is why, as a precautionary measure, we are writing to let you know about a data security incident that [may involve/involves] your personal information.

[[Between/On] [IDENTIFY TIME PERIOD OF BREACH], [SUMMARIZE BREACH INCIDENT].] The data accessed [may have included/included] personal information such as [IDENTIFY TYPES OF PII AT ISSUE]. [To our knowledge, the data accessed did not include any [IDENTIFY TYPES OF PII NOT INVOLVED]].

#### **DRAFTING NOTE**

# Brief Description of Incident and Categories of PII Involved

Breach notice letters (with the exception of letters to Massachusetts residents) typically include a brief description in general terms of the incident, including the approximate date of the incident. This is a requirement of several state breach notification laws.

Massachusetts law, on the other hand, requires that the notice:

- **Not** include a description of the nature of the breach.
- Not specify the number of individuals affected.

When preparing a notice for Massachusetts residents, do not include the first bracketed sentence of the second paragraph above.

Several state breach notification laws also require that the notice identify the categories of personal information involved, for example an individual's:

Name or address.

- Birth date.
- Phone number.
- Driver's license number.
- Credit card number.
- Bank account number.
- Social Security number.
- Medical or health insurance information.

California law also requires that the notice describe whether notification was delayed as a result of a law enforcement investigation if is possible to determine that information at the time notice is provided.

The language in this section must be tailored to reflect the actual circumstances of the breach and legal requirements of the relevant states. Legal counsel preparing the notice also should consult with the appropriate law enforcement authorities handling the case on the specific information to include so that providing the notice does not adversely affect any criminal investigation.

[COMPANY NAME] values your privacy and deeply regrets that this incident occurred. [COMPANY NAME] is conducting a thorough review of the potentially affected [records/computer system/IDENTIFY OTHER][, and will notify you if there are any significant developments]. [COMPANY NAME] has implemented additional security measures designed to prevent a recurrence of such an attack, and to protect the privacy of [COMPANY NAME]'s valued [customers/employees/IDENTIFY GROUP OF AFFECTED INDIVIDUALS].

The company also is working closely with [major credit card suppliers and] law enforcement to ensure the incident is properly addressed.

# **DRAFTING NOTE**

# Actions Taken by the Company Following Discovery of the Breach

Some state breach notification laws require that the notice briefly describe the general actions the business has taken to remedy the situation. This is also consistent with Federal Trade Commission (FTC) guidance, and may include, for example:

- Containing the breach.
- Implementing additional internal controls and safeguards.
- Making changes to existing policies.
- Cooperating with the law enforcement investigation.

 Notifying the major credit reporting agencies.

The language in this section must be tailored to reflect the actual actions taken by the company, but any statements should be phrased in general terms. Legal counsel preparing the notice should consult with the business's law enforcement contacts on the specific information to include so that the notice does not adversely affect any criminal investigation or compromise the business's ability to mitigate the initial breach and prevent any further breach.

Please also review the attachment to this letter (Steps You Can Take to Further Protect Your Information) for further information on steps you can take to protect your information[, and how to receive free credit monitoring for one year].

#### **DRAFTING NOTE**

# Recommendations for Affected Individuals

Some states require that the breach notice include information on certain actions affected individuals can take to protect themselves. For example, some states (including Hawaii, Vermont, Michigan, Missouri and North Carolina) require that the notice include advice directing individuals to remain vigilant by:

- Reviewing account statements.
- Monitoring free credit reports.

Consistent with these state law requirements, the FTC recommends that the notice explain the steps affected individuals

can take to protect against misuse or disclosure specific to the type of personal information subject to the breach. For example, if Social Security numbers have been compromised, the FTC recommends that affected individuals contact the three national credit reporting agencies to have fraud alerts placed on their credit reports.

In the standard document, this information has been set out in an Appendix for convenience (see *Steps You Can Take To Further Protect Your Information*) but alternatively can be incorporated here. The last bracketed phrase above can be included if the company is offering free credit monitoring to affected individuals.

For further information and assistance, please contact [NAME OF COMPANY REPRESENTATIVE/COMPANY] at [TELEPHONE NUMBER/TOLL-FREE NUMBER] between [TIME] a.m.- [TIME] p.m. [EST] daily[, or visit [WEBSITE]].

### **DRAFTING NOTE**

# Questions about this Notice

The notice should, and in some states must, include contact information for a company representative who can assist and provide additional information to affected individuals.

One specific state law variation to keep in mind for this section of the letter includes the type of contact information that must

be included. For example, Vermont's and Wyoming's breach notification laws require that a toll-free telephone line be set up to provide further information and assistance. West Virginia law also requires that the company identify a contact for learning what types of PII are maintained and whether the company maintained personal information about an individual.

Sincerely,

[NAME]

[TITLE]

### **DRAFTING NOTE**

# **Signature**

The notice should generally be signed by a senior executive of the company. This may

help signal to affected individuals that the company is proactive and takes the incident seriously.

### STEPS YOU CAN TAKE TO FURTHER PROTECT YOUR INFORMATION

#### **DRAFTING NOTE**

# Steps You Can Take To Further Protect Your Information

The FTC recommends that the notice explain the steps affected individuals can take to protect themselves against identity theft that are appropriate for the type of personal information at issue. Some state notification laws also specifically require that the notice identify protective steps individuals can take. For example, some states require that the

notice advise individuals to remain vigilant by:

- Reviewing their account statements.
- Monitoring free credit reports.
- Contacting law enforcement in the event of actual or suspected identity theft.

Other states, for example, Massachusetts and West Virginia, require that the notice include instructions on how to request a security freeze.

© 2014 Thomson Reuters. All rights reserved.

# Review Your Account Statements and Notify Law Enforcement of Suspicious Activity

As a precautionary measure, we recommend that you remain vigilant by reviewing your account statements and credit reports closely. If you detect any suspicious activity on an account, you should promptly notify the financial institution or company with which the account is maintained. You also should promptly report any fraudulent activity or any suspected incidence of identity theft to proper law enforcement authorities, your state attorney general, and/or the Federal Trade Commission.

To file a complaint with the FTC, go to www.ftc.gov/idtheft or call 1-877-ID-THEFT (877-438-4338). Complaints filed with the FTC will be added to the FTC's Identity Theft Data Clearinghouse, which is a database made available to law enforcement agencies.

### **DRAFTING NOTE**

# Review Account Statements and Contact Law Enforcement about Suspicious Activity

This paragraph advises individuals to review their account statements and alert law enforcement if identity theft is suspected. Some specific state law requirements to keep in mind for this section of the letter include:

 Some states (including Hawaii, Michigan, Missouri, North Carolina and Vermont) require the notice to direct affected individuals to remain vigilant by reviewing account statements and monitoring free credit reports.

- Other states (for example, Oregon and lowa) require the notice to include advice to consumers to report suspected incidents to local law enforcement or the state attorney general's office.
- Massachusetts law also requires that individuals be notified of their right to obtain a police report. For letters to residents of Massachusetts, the following language should be added to the end of the first paragraph above: "You have the right to obtain a police report regarding the breach."

# Copy of Credit Report

You may obtain a free copy of your credit report from each of the three major credit reporting agencies once every 12 months by visiting http://www.annualcreditreport.com, calling toll-free 877-322-8228, or by completing an Annual Credit Report Request Form and mailing it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348. You can print a copy of the request form at https://www.annualcreditreport.com/cra/requestformfinal.pdf. Or you can elect to purchase a copy of your credit report by contacting one of the three national credit reporting agencies. Contact information for the three national credit reporting agencies for the purpose of requesting a copy of your credit report or for general inquiries is provided below:

Equifax	Experian	TransUnion
(800) 685-1111	(888) 397-3742	(800) 916-8800
www.equifax.com	www.experian.com	www.transunion.com
P.O. Box 740241	535 Anton Blvd., Suite 100	P.O. Box 6790
Atlanta, GA 30374	Costa Mesa, CA 92626	Fullerton, CA 92834

#### **DRAFTING NOTE**

# **Copy of Credit Report**

Breach notification letters typically provide information on how individuals can obtain a free copy of their credit reports. Some state laws (for example, Maryland, North Carolina and West Virginia) require that the notice letter include contact information for the three national credit reporting agencies (including their toll-free telephone numbers

and addresses). Some state notification laws require that a company suffering a breach also notify the three national credit reporting agencies in addition to notifying consumers.

A company suffering a breach may offer to provide each affected individual with a free copy of his credit report, in which case this section should be revised to reflect this offer.

### Fraud Alert

[We recommend/You may want to consider] placing a fraud alert on your credit report. An initial fraud alert is free and will stay on your credit file for at least 90 days. The alert informs creditors of possible fraudulent activity within your report and requests that the creditor contact you prior to establishing any accounts in your name. To place a fraud alert on your credit report, contact any of the three credit reporting agencies identified above. Additional information is available at http://www.annualcreditreport.com.

# **DRAFTING NOTE**

### **Fraud Alert**

This section provides information on how to place a fraud alert on credit reports. West Virginia law requires that the notice include

instructions on how to place a fraud alert. The FTC also recommends that when Social Security numbers have been compromised, companies advise affected individuals to have fraud alerts placed on their credit reports.

# [Credit Report Monitoring

In addition, [COMPANY] has arranged with [NAME OF SERVICE PROVIDER] to provide you with credit monitoring for one year, at no cost to you. The [SERVICE] package provides you with the following benefits:

[SUMMARY OF BENEFITS]

To take advantage of this offer, you must enroll [within 90 days] from receipt of this letter.

[INSERT ENROLLMENT INSTRUCTIONS]]

# **DRAFTING NOTE**

# **Credit Report Monitoring**

This optional provision should be included if the company is offering to provide free

credit report monitoring. If included, this paragraph should be revised to provide a brief summary of the benefits as well as instructions for individuals to enroll.

© 2014 Thomson Reuters. All rights reserved.

# [Security Freeze

In some US states, you have the right to put a security freeze on your credit file. This will prevent new credit from being opened in your name without the use of a PIN number that is issued to you when you initiate the freeze. A security freeze is designed to prevent potential creditors from accessing your credit report without your consent. As a result, using a security freeze may interfere with or delay your ability to obtain credit. You must separately place a security freeze on your credit file with each credit reporting agency. [Additionally, if you request a security freeze from a consumer reporting agency there may be a fee up to \$5 to place, lift or remove the security freeze.]] In order to place a security freeze, you may be required to provide the consumer reporting agency with information that identifies you including your full name, Social Security number, date of birth, current and previous addresses, a copy of your state-issued identification card, and a recent utility bill, bank statement or insurance statement.

### **DRAFTING NOTE**

# **Security Freeze**

Massachusetts and West Virginia breach notification laws require that the notice include information instructing affected individuals on how to place a security freeze on their credit files.

Massachusetts law further requires that the notice disclose any fees charged by the consumer reporting agencies. Many states do have laws allowing individuals to place security freezes on their files; however, the fees to place, lift or remove the security freeze may vary by state. The last sentence of this paragraph is in brackets and reflects Massachusetts law allowing consumer reporting agencies to charge up to \$5 to place, temporarily lift or remove the freeze unless the individual is an identity theft victim (or spouse of a victim) and has obtained a valid police report.

### Additional Free Resources on Identity Theft

You may wish to review the tips provided by the Federal Trade Commission on how to avoid identity theft. For more information, please visit http://www.ftc.gov/idtheft or call 1-877-ID-THEFT (877-438-4338). [A copy of Taking Charge: What to Do if Your Identity is Stolen, a comprehensive guide from the FTC to help you guard against and deal with identity theft, [is enclosed/can be found on the FTC's website athttp://www.ftc.gov/bcp/edu/pubs/consumer/idtheft/idt04.shtm.]

[Maryland residents may also wish to review information provided by the Maryland Attorney General on how to avoid identity theft at http://www.oag.state.md.us/idtheft, or by sending an email to idtheft@oag.statemd.us, or calling 410-576-6491.]

[North Carolina residents may wish to review information provided by the North Carolina Attorney General at http://www.ncdoj.gov, by calling 877-566-7226, or writing to 9001 Mail Service Center, Raleigh, NC 27699.]

#### **DRAFTING NOTE**

# Additional Resources on Identity Theft

The first paragraph reflects the FTC's recommendation that the notice include current information about identity theft. The FTC maintains resources and information on its website to help individuals safeguard their privacy and deal with identity theft.

The second and third paragraphs should be included in a notice letter to Maryland

and North Carolina residents, respectively. It reflects the Maryland and North Carolina requirements that the notice include contact information (including toll-free numbers, addresses and websites) for the FTC and state attorneys general and a statement that the individual can find out additional information from these sources about steps he can take to avoid identity theft.

# ABOUT PRACTICAL LAW

Practical Law provides legal know-how that gives lawyers a better starting point. Our expert team of attorney editors creates and maintains thousands of up-to-date, practical resources across all major practice areas. We go beyond primary law and traditional legal research to give you the resources needed to practice more efficiently, improve client service and add more value.

If you are not currently a subscriber, we invite you to take a trial of our online services at **practicallaw.com**. For more information or to schedule training, call **888.529.6397** or e-mail **training.practicallaw@thomsonreuters.com**.

12-14