

DATA BREACH NOTIFICATION LETTER

This is a customizable starting template, not a finished legal document. Replace every **[BRACKETED]** field with your specifics, delete or adapt any clause that does not fit your situation, and have a licensed attorney in the governing jurisdiction review it before you send or rely on it. CyberSygn is not a law firm and this template is not legal advice. This document type carries significant legal and/or financial consequences and varies substantially by jurisdiction. Having a licensed attorney review it before use is strongly recommended.

This Data Breach Notification Letter (this "**Notice**") is issued by **[ORGANIZATION LEGAL NAME]**, a **[STATE]** **[ENTITY TYPE, e.g. limited liability company]** with its principal place of business at **[ORGANIZATION ADDRESS]** (the "**Organization**," "**we**," "**us**," or "**our**"), to **[AFFECTED INDIVIDUAL / CUSTOMER NAME]** (the "**Recipient**" or "**you**"), whose personal information may have been involved in a data security incident described below.

Breach-notification obligations — including who must be notified, what the notice must say, the deadline to send it, and whether regulators or credit bureaus must also be informed — are set by federal, state, and sometimes international law and vary substantially by jurisdiction and by the type of data involved. This template is a drafting aid only; the Organization must confirm the specific legal requirements that apply before sending any notice.

Recitals. The Organization experienced or discovered an incident that may have compromised personal information. The Organization is providing this Notice to inform affected individuals of what happened, what information was involved, what the Organization is doing, and what steps the Recipient can take. Accordingly, the Organization issues the following.

1. Summary of the Incident

1.1 What happened. On or about **[DATE OF INCIDENT]**, the Organization **[DESCRIBE WHAT OCCURRED, e.g. discovered unauthorized access to a system / learned of the loss of a device / identified a phishing compromise]**. The Organization became aware of the incident on **[DATE OF DISCOVERY]**.

1.2 Plain-language explanation. In plain terms, **[BRIEF NEUTRAL DESCRIPTION OF HOW THE INFORMATION MAY HAVE BEEN EXPOSED]**. The Organization is providing this Notice out of an abundance of caution and in keeping with its commitment to protecting your information.

1.3 No confirmed misuse (if applicable). As of the date of this Notice, the Organization **[has / has not]** received reports that your information has been misused as a result of this incident. The Organization is continuing to investigate.

2. Information Involved

2.1 Categories of data. Based on the Organization's investigation to date, the information that may have been involved includes: **[LIST CATEGORIES, e.g. name, address, email, account number, Social Security number, driver's license number, financial account information, health information, or login credentials]**.

2.2 Information not involved (if applicable). To the best of the Organization's knowledge, the following information was not involved: **[LIST, e.g. full payment card numbers, passwords stored in encrypted form]**.

2.3 Ongoing review. This list reflects the Organization's understanding as of the date of this Notice and may be updated as the investigation continues.

3. What the Organization Is Doing

3.1 Investigation and containment. On discovering the incident, the Organization **[took the affected system offline / reset credentials / engaged a forensic firm / notified law enforcement]** and took steps to contain the incident and prevent recurrence.

3.2 Remediation. The Organization is **[DESCRIBE REMEDIAL MEASURES, e.g. enhancing access controls, increasing monitoring, and reviewing its security program]**.

3.3 Regulatory and other notifications. Where required by applicable law, the Organization is notifying **[applicable regulators, attorneys general, credit reporting agencies, and/or other authorities]**. This Notice does not waive any of the Organization's legal rights or defenses.

4. What You Can Do

4.1 Stay alert. The Organization encourages you to review your account statements and to monitor your accounts and credit reports for suspicious activity. Report any suspected fraud promptly to the relevant institution.

4.2 Credit reports and fraud alerts. You may obtain free copies of your credit reports and may place a fraud alert or security freeze on your credit file. Procedures and rights for fraud alerts and freezes vary by jurisdiction; contact the major credit reporting agencies and review the resources referenced in Section 6.

4.3 Identity-protection services (if offered). The Organization **[is / is not]** offering complimentary **[credit monitoring / identity-protection]** services for **[NUMBER]** months. If offered, enrollment instructions and an activation code are provided in **[ATTACHMENT / SECTION]**, and enrollment must be completed by **[DEADLINE]**.

5. Protecting Yourself Going Forward

5.1 Account security. Consider changing passwords and security questions for the affected account and for any other account where you used the same credentials, and enabling multi-factor authentication where available.

5.2 Beware of scams. Be cautious of unsolicited communications referencing this incident. The Organization will not ask you for your full account number, password, or Social Security number by email or phone in connection with this Notice.

5.3 Document concerns. Keep records of any suspicious activity, including dates and descriptions, in case you need to report it to authorities or institutions.

6. For More Information

6.1 Contact us. If you have questions, you may contact **[CONTACT NAME / TEAM]** at **[PHONE]** or **[EMAIL]**, **[HOURS / DAYS]**, or write to **[MAILING ADDRESS]**.

6.2 Government resources. You can learn more about steps to protect against identity theft from your state or national consumer-protection authority and, in the United States, from the Federal Trade Commission's identity-theft resources. Contact details for the major credit reporting agencies are commonly available through those resources.

6.3 Reference number. Please reference incident number **[INCIDENT REFERENCE NUMBER]** in any correspondence so the Organization can assist you efficiently.

7. Important Notices

7.1 **No admission.** This Notice is provided to inform you and to comply with applicable law. Nothing in this Notice is an admission of fault, liability, or wrongdoing by the Organization, and the Organization reserves all rights and defenses.

7.2 **Accuracy and updates.** The information in this Notice reflects the Organization's understanding as of the date below. The Organization may provide updates if material new information becomes available.

7.3 **Jurisdictional variation.** Your legal rights, and the Organization's obligations, depend on the laws applicable to you and to the data involved, which vary by jurisdiction. This Notice does not summarize all of those rights; consult the resources above or a qualified professional.

7.4 **Governing law.** Matters relating to this Notice are governed by applicable law, including the breach-notification laws of **[STATE / RELEVANT JURISDICTIONS]**, without limiting any other applicable law.

ISSUED ON BEHALF OF THE ORGANIZATION as of the date below.

ORGANIZATION REPRESENTATIVE	REVIEWED BY (Counsel / Privacy Officer)
Signature: _____	Signature: _____
Printed name: [NAME]	Printed name: [NAME OR N/A]
Title: [TITLE]	Title: [TITLE OR N/A]
Date: _____	Date: _____

Date of this Notice: **[NOTICE DATE]**

Template provided by CyberSygn. Not legal advice. CyberSygn is not a law firm. Consult a licensed attorney in your jurisdiction before relying on this document.