

Attorney General Security Breach Notification Guidance

This Guidance describes the steps a business or state agency should take in the event the business or state agency suspects that its computerized data or systems containing “personal information,” as defined in the statute, has been subject to a security breach.

The Security Breach Notice Act, [9 V.S.A. § 2430](#) and [§ 2435](#), became effective on January 1, 2007. This law requires businesses and state agencies to notify consumers in the event a business or state agency suffers a “security breach,” defined as the **“unauthorized acquisition or access of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by the [state agency or business].”** 9 V.S.A. § 2430(8). The law provides that businesses and state agencies do not need to give notice where they determine that misuse of personal information is not reasonably possible, and they provide a detailed explanation of that determination to the Vermont Attorney General’s Office.

“Personal information” that is subject to the law is defined as:

an individual’s 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 the data elements are not encrypted or redacted or protected by another method that renders them unreadable or unusable by unauthorized persons:

- i. Social Security number;
- ii. Motor vehicle operator’s license number or non-driver identification card number;
- iii. Financial account number or credit or debit card number, if circumstances exist in which the number could be used without additional identifying information, access codes, or passwords;
- iv. Account passwords or personal identification numbers or other access codes for a financial account.

9 V.S.A. § 2430(5). The statute further requires that notice be sent to affected consumers following discovery of or notification about the breach “in the most expedient time possible and without unreasonable delay,” consistent with the needs of law enforcement. 9 V.S.A. § 2435(b).

You, as a business or state agency, should take the following steps if you suffer from a security breach. Review all steps immediately, and take as many of the detailed steps as possible, as quickly as possible.

1. Secure the data immediately.

- a. Call your head of computer operations or information technology to find out what steps must be taken to secure the data. Take all appropriate measures to secure the data, including possibly taking the computer server off line or isolating the data.

- b. Do NOT attempt to determine whether the data has been compromised until law enforcement has approved the steps you plan to take.
- c. See Appendix 1 for a description of some of the steps that should be taken to secure the data in the event of a security breach.

2. Involve Law Enforcement immediately.

- a. Call the state police or FBI to report the incident and determine the next steps to take. If you are a Vermont-based business or state agency, or the data at issue is housed in Vermont, call:

FBI: During normal business hours, call the Burlington FBI office at: 802-863-6316
After normal business hours, call the Albany FBI office at: 518-465-7551

State Police: Bureau of Criminal Investigation: 802-244-8781

If your business or agency is located out of state and the data at issue is housed out of state, call the FBI, state police or other appropriate law enforcement agency in your area.

- b. Inform the FBI or state police of your obligation to notify consumers of the breach **within 10 business days**. If either the FBI or state police requests a delay in notification for purposes of a law enforcement investigation, the request must be made in writing or you must document the request contemporaneously, noting the name of the law enforcement officer making the request and the name of the officer's agency.
- c. If either the FBI or state police requests a delay in notification for purposes of a law enforcement investigation, prepare your notification to consumers so that you can send it immediately upon hearing that the delay is no longer needed. (See Step 5 below.)
- d. The law enforcement agency making a request for delay is responsible for promptly notifying you when the law enforcement agency believes that notifying consumers will no longer impede the law enforcement investigation. Until you are notified that the delay is no longer needed, you should contact the responsible law enforcement officer every 15 days to determine that the delay is still required.
- e. After the law enforcement agency notifies you that the delay is no longer needed, **immediately** send your notice to consumers.
- f. It should not be necessary for law enforcement to complete its investigation before notice to affected consumers can be sent.

- 3. Contact any entities from which you may have obtained the data immediately.**
 - a. If you received the data from other entities, such as banks or other states, contact these entities as they may have their own obligations to notify consumers about the security breach.

- 4. Notify the Vermont Attorney General's Office about the breach.**
 - a. Call, fax, or email the Vermont Attorney General's Office to inform the Attorney General of the breach by contacting:

Ryan Kriger, Assistant Attorney General
AJ Van Tassel Sweet, Investigator
phone: 802-828-5479 fax: 802-828-2154
email: data.security@atg.state.vt.us

- 5. Notify consumers about the breach WITHIN 10 BUSINESS DAYS OF DISCOVERY.**
 - a. If law enforcement does not request a delay in notification to consumers, you should notify consumers about the breach **within 10 business days of discovery of the breach.**

 - b. The notice must contain the following information:
 - A general description of the unauthorized access or acquisition.
 - The type of personal information affected.
 - A general description of the steps you will take to protect the information from further unauthorized access or acquisition.
 - Your toll-free telephone number that consumers may call for further information and assistance.
 - Advice that directs the consumer to remain vigilant by reviewing account statements and obtaining free credit reports from each credit reporting agency to determine if there is suspicious activity such as new accounts being opened in the consumer's name. Consumers in Vermont are entitled to two free credit reports each year from each credit reporting agency. Information on how to obtain a free credit report is available [here](#).

 - c. A model notification letter is provided in Appendix 2. The model letter is designed to be used when you do not know whether the consumer's information has been misused. If you are aware that the consumer's information has been misused, then a more specific letter should be sent, outlining how the information has been misused and

recommending that the consumer take immediate action to guard against identity theft.

- d. Consider whether you will offer credit monitoring services to consumers. These are services offered by credit reporting agencies to determine if there is suspicious activity such as new accounts being opened in the consumer's name. While not required by law, many companies and agencies that experience breaches provide credit monitoring services to consumers.
- e. Send the notice in one of the following ways.
 - 1. Direct notice to consumers through:
 - i. A mailing to the consumer's residence; or
 - ii. Telephone, provided telephone contact is made directly with each consumer, and not through a pre-recorded message; or
 - iii. Electronic notice via email. (Note: it is difficult to qualify to use email notice under the law. See 9 V.S.A. § 2435(b)(5)(A)(ii).)
 - 2. Substitute notice is allowed if you can show one of the following:
 - i. Providing direct notice through the mail or telephone would cost more than \$5,000;
 - ii. The group of consumers affected by the security breach exceeds 5,000; or
 - iii. The data collector does not have sufficient contact information to provide notice via the mail or telephone.

If you satisfy one of the three criteria for substitute notice, then you may provide notice to affected consumers by doing **both** of the following:

- A. Prominently placing the notice on your website; **and**
 - B. Sending a press release with all the information to be contained in the notice to major statewide and regional media.
- f. Whichever form of distribution you use, the notice must contain all of all the elements outlined in 5.b above.

6. Notify the three major credit reporting agencies if you are going to send a notice of security breach to more than 1,000 consumers. This notice to credit reporting agencies shall be sent no later than the same day as the notices are sent to consumers.

a. The notification to the credit reporting agencies should be sent to the following addresses:

- **Equifax**

U.S. Consumer Services
Equifax Information Services, LLC
Phone: 678-795-7971
Email: businessrecordsecurity@equifax.com

- **Experian**

Experian Security Assistance
P.O. Box 72 Allen, TX 75013
Email: BusinessRecordsVictimAssistance@experian.com

- **TransUnion**

Phone: 1-800-372-8391
Email: fvad@transunion.com

7. Notice of a security breach is not required if you determine that misuse of personal information is not reasonably possible, and you so inform the Vermont Attorney General's Office without unreasonable delay.

a. If you establish that misuse of the data is not reasonably possible, then you may forgo notifying affected consumers about the breach *as long as* you provide a detailed explanation of your determination to the Attorney General's Office. The explanation should be provided to the following:

Consumer Protection Unit
Vermont Attorney General's Office
109 State Street
Montpelier, Vermont 05609-1001

b. You may designate your explanation as "trade secret" if it meets the definition of trade secret under 1 V.S.A. § 317(c)(9).

c. If you learn, after notifying the Attorney General's Office, that misuse of the personal information has occurred or is occurring, then you must provide notice of the security breach to affected consumers without unreasonable delay after receiving such information consistent with section 5 of this Guidance above.

8. This Guidance does not apply to certain financial institutions and certain other businesses subject to regulation by the Department of Banking, Insurance, Securities and Health Care Administration (BISHCA).

The Guidance does not apply to: (1) a person or entity licensed or registered with BISHCA under Titles 8 or 9 of the Vermont Statutes Annotated, however, such person or entity is subject to guidance, bulletins, and regulations issued by BISHCA; or (2) a financial institution, bank, or credit union that is subject to either: (A) The Federal Interagency Guidance Response Programs for Unauthorized Access to Consumer Information and Customer Notice, issued on March 7, 2005, by the Board of Governors of the Federal Reserve System, the Federal Deposit Insurance Corporation, the Office of the Comptroller of the Currency, and the Office of Thrift Supervision, as such federal guidance may be revised from time to time; or (B) The Final Guidance on Response Programs for Unauthorized Access to Member Information and Member Notice, issued on April 14, 2005, by the National Credit Union Administration, as such federal guidance may be revised from time to time.

APPENDIX 1

Procedures Computer Users Should Institute Both Prior to Becoming a Computer Crime Victim and After a Violation Has Occurred

Guidance from the FBI National Computer Crime Squad

www.emergency.com/fbi-nccs.htm

- Place a login banner to ensure that unauthorized users are warned that they may be subject to monitoring.
- Turn audit trails on.
- Consider keystroke level monitoring if adequate banner is displayed.
- Request trap and tracing from your local telephone company.
- Consider installing caller identification.
- Make backups of damaged or altered files.
- Maintain old backups to show the status of the original.
- Designate one person to secure potential evidence.
- Evidence can consist of tape backups and printouts. These should be initialed by the person obtaining the evidence and should be retained in a locked cabinet with access limited to one person.
- Keep a record of resources used to reestablish the system and locate the perpetrator.

Reporting a Computer Crime to Law Enforcement

When reporting a computer crime, be prepared to provide the following information:

- Name and address of the reporting agency.
- Name, address, e-mail address, and phone number(s) of the reporting person.
- Name, address, e-mail address, and phone number(s) of the Information Security Officer (ISO).
- Name, address, e-mail address, and phone number(s) of the alternate contact (e.g., alternate ISO, system administrator, etc.).
- Description of the incident.
- Date and time the incident occurred.
- Date and time the incident was discovered.
- Make/model of the affected computer(s).
- IP address of the affected computer(s).
- Assigned name of the affected computer(s).
- Operating System of the affected computer(s).
- Location of the affected computer(s).

Incident Response DOs and DON'Ts

DOs

1. Immediately isolate the affected system to prevent further intrusion, release of data, damage, etc.
2. Use the telephone to communicate. Attackers may be capable of monitoring E-mail traffic.
3. Immediately notify an appropriate law enforcement agency.
4. Activate all auditing software, if not already activated.
5. Preserve all pertinent system logs, e.g., firewall, router, and intrusion detection system.
6. Make backup copies of damaged or altered files, and keep these backups in a secure location.
7. Identify where the affected system resides within the network topology.
8. Identify all systems and agencies that connect to the affected system.
9. Identify the programs and processes that operate on the affected system(s), the impact of the disruption, and the maximum allowable outage time.
10. In the event the affected system is collected as evidence, make arrangements to provide for the continuity of services, i.e., prepare redundant system and obtain data back-ups. To assist with your operational recovery of the affected system(s), pre-identify the associated IP address, MAC address, Switch Port location, ports and services required, physical location of system(s), the OS, OS version, patch history, safe shut down process, and system administrator or backup.

DON'Ts

1. Delete, move, or alter files on the affected systems.
2. Contact the suspected perpetrator.
3. Conduct a forensic analysis.

APPENDIX 2

SAMPLE LETTER

To Be Used When The Breached Entity Does Not Know Whether the Consumer's Information Has Been Misused

Dear :

We are writing to you because of a recent security incident at *[name of organization]*. *[Describe what happened in general terms, what kind of personal information was involved, and what you are doing in response.]*

Below is a check list of suggestions of how you can best protect yourself.

1. **Review your bank, credit card and debit card account statements** over the next twelve to twenty-four months and immediately report any suspicious activity to your bank or credit union.
2. **Monitor your credit reports** with the major credit reporting agencies.

Equifax
1-800-685-1111
P.O. Box 740241
Atlanta, GA 30374-0241
www.equifax.com

Experian
1-888-397-3742
P.O. Box 2104
Allen, TX 75013
www.experian.com

TransUnion
1-800-916-8800
P.O. Box 2000
Chester, PA 19022
www.transunion.com

Under Vermont law, you are entitled to a free copy of your credit report from those agencies every twelve months. *[If you are offering consumers credit monitoring services, insert description of the services and instructions on how to access them.]*

Call the credit reporting agency at the telephone number on the report if you find:

- Accounts you did not open.
 - Inquiries from creditors that you did not initiate.
 - Inaccurate personal information, such as home address and Social Security number.
3. If you do find suspicious activity on your credit reports or other account statements, call your local police or sheriff's office and **file a report of identity theft**. *[Or, if appropriate, give contact number for law enforcement agency investigating the incident for you.]* Get a copy of the police report. You may need to give copies of the police report to creditors to clear up your records, and also to access some services that are free to identity theft victims.
 4. If you find suspicious activity on your credit reports or on your other account statements, **consider placing a fraud alert** on your credit files so creditors will contact you before opening new accounts. Call any one of the three credit reporting agencies at the number below to place fraud alerts with all of the agencies.

Equifax
800-525-6285

Experian
888-397-3742

TransUnion
800-680-7289

5. If you find suspicious activity on your credit reports or on your other account statements, **consider placing a security freeze** on your credit report so that the credit reporting agencies will not release information about your credit without your express authorization. A security freeze may cause delay should you wish to obtain credit and may cost some money to get or remove, but it does provide extra protection against an identity thief obtaining credit in your name without your knowledge. If you have Internet access and would like to learn more about how to place a security freeze on your credit report, please visit the Vermont Attorney General's website at: <http://www.atg.state.vt.us/issues/consumer-protection/identity-theft.php>.

You may also get information about security freezes by contact the credit bureaus at the following addresses:

Equifax:

https://www.freeze.equifax.com/Freeze/jsp/SFF_PersonalIDInfo.jsp

Experian:

http://www.experian.com/consumer/security_freeze.html

TransUnion:

<http://www.transunion.com/corporate/personal/fraudIdentityTheft/fraudPrevention/securityFreeze.page>

If you do not have Internet access but would like to learn more about how to place a security freeze on your credit report, contact the Vermont Attorney General's Office at 802-656-3183 (800-649-2424 toll free in Vermont only).

6. Even if you do not find suspicious activity on your credit report or your other account statements, it is important that you **check your credit report** for the next two years. Just call one of the numbers in paragraph 2 above to order your reports or to keep a fraud alert in place.

Helpful information about fighting identity theft, placing a security freeze, and obtaining a free copy of your credit report is available on the Vermont Attorney General's website at <http://www.atg.state.vt.us>. Another helpful source is the Federal Trade Commission website, available at <http://www.ftc.gov/bcp/edu/microsites/idtheft/>.

If there is anything *[name of your organization]* can do to assist you, please call *[toll-free phone number]*.

[Closing]