Vermont Attorney General Security Breach Notification Guidance
Updated September 2014

If you have a Security Breach, you must provide Preliminary Notice to the Vermont Office of the Attorney General (the "Office") within 14 business days of discovery or notification of the breach, and provide Consumer Notice in the most expedient time possible in the most expedient time possible and not later than 45 days after discovery or notification of the breach. Preliminary Notice is kept confidential.

If you have any questions or are uncertain about anything in the guidance, please contact the Office at ago.securitybreach@vermont.gov or 802-828-5479.

Overview

1. What is the purpose of this Guidance?

This Guidance describes how the Vermont Office of the Attorney General (the "Office") interprets the Data Breach Notification Act, 9 V.S.A. § 2430 and § 2435 (the "Act"). This Guidance is not directed towards entities regulated by the Department of Financial Regulation ("DFR"). This Guidance also does not address security issues raised by federal law like HIPAA and the Gramm-Leach-Bliley Act.

2. Does this Guidance apply to me?

Yes, if you are a Data Collector that has experienced a Security Breach. "Data Collector" is a very broad term, and includes any entity that "for any purpose, whether by automated collection or otherwise, handles, collects, disseminates, or otherwise deals with nonpublic personal information."[1]

In addition to most businesses, the state, state agencies, municipalities, public and private universities, and both for-profit and non-profit entities are subject to the Act. Certain financial institutions, however, are exempt from *most* provisions of the Act. *See* Question 28 (How does the Act apply to financial institutions?)

The location of the Data Collector in is not relevant. As long as one Vermont resident has been affected by a Security Breach, the Act applies to the Data Collector.[2]

3. What is a Security Breach?

"Security breach" means unauthorized acquisition of electronic data or a reasonable belief of an unauthorized acquisition of electronic data that compromises the security, confidentiality, or integrity of a consumer's personally identifiable information maintained by the Data Collector.

See also Question 6 (What if I'm not sure whether I've had a Security Breach?)

4. What is Personally Identifiable Information (or "PII")?

PII means an individual's first name or 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:

- Social Security number;
- Motor vehicle operator's license number or non-driver identification card number;
- 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; or
- Account passwords or personal identification numbers or other access codes for a financial account.

The Office considers the front of a check, which contains name, account number, routing number, and potentially address and signature, to be PII.

PII does not include information from federal, state, or local governments that is lawfully made available to the general public.[3]

5. I think I've suffered a Security Breach, what should I do?

You, as a business or state agency, should take the following steps if you think you may have suffered a security breach. Review all steps immediately, and take as many of the steps as possible, as quickly as possible. Each step is described more fully below in Detailed Explanations.

a. Secure the data immediately

Take reasonable steps to stop ongoing data theft, ideally without destroying evidence that could be used in a future investigation. For example, you can secure the data by disconnecting affected computers from networks or removing affected hard drives.

See also Question 17 (How do I secure my data?)

b. Involve Law Enforcement immediately

See Question 18 (Contacting Law Enforcement).

c. If you are storing someone else's data, contact the owner of the data.

See Questions 9 (Explain "maintains or possesses"), 12 (Who must be notified in the event of a security breach?).

d. Provide confidential Preliminary Notice to the Attorney General or DFR about the breach within 14 days.[4]

   See Question 19 (Explain the 14-day Preliminary Notice).

e. Notify consumers about the breach in the most expedient time possible and not later than 45 days after discovery or notification.[5]

   The most expedient time possible will often be much quicker than 45 days.

   See Question 21 (Explain the Consumer Notice).

f. Notify the three major credit reporting agencies if you are going to send a notice of security breach to more than 1,000 consumers.[6]

   See Question 27 (How do I notify the credit reporting agencies?)

Detailed Explanations

6. What if I'm not sure whether I've had a Security Breach?

"Security breach" does not include good faith but unauthorized acquisition of personally identifiable information by an employee or agent of the business or agency as long as it is not disclosed further and is not used for a purpose unrelated to the activities of the business or agency.

In determining whether information has been acquired or is reasonably believed to have been acquired, the following factors may be considered, among others:

- indications that the information:
    - is in the physical possession and control of a person without valid authorization, such as a lost or stolen computer or other device containing information;
    - has been downloaded or copied;
    - was used by an unauthorized person, such as fraudulent accounts opened or instances of identity theft reported; or
- the information has been made public, such as posting on a website.[7]

The following are a few examples of incidents that qualify as security breaches:

- Hackers infiltrate a computer network, using either malware or by obtaining an employee's login credentials, and steal PII (See Question 4);
- An employee leaves a laptop, external hard drive, or thumb drive containing PII in a public place;

- An ex-employee refuses to return a laptop that contains PII;

- A backup tape containing PII is accidentally thrown out or gets lost in transit; and

- A customer's PII is accidentally sent to the wrong the wrong customer.

We understand that it can take time to determine who must be notified, or even whether a Vermont resident has been affected. We recommend that if you have a reasonable suspicion that a Vermont resident may have been affected, you notify the Attorney General as soon as possible. The Preliminary Notice is confidential, and there is no penalty if it turns out that no Vermonter was affected by the breach or if some of the initial information was incorrect.

When the Office sees that the date of discovery or notification is significantly later than the date of the breach, the Office may inquire as to why the data collector took as long as it did to discover the breach, what breach alert systems it had in place, and what steps it is planning to take to be more alert in the future.

Depending on the amount of time that a data collector has had to investigate a breach, a discovery that Vermont consumers have been affected that is significantly later than the date of discovery of the breach may imply in improper investigation. Where a data collector has known of a breach for a significant amount of time, the Attorney General expects to be notified, and for Consumer Notice to be sent quickly after Vermont consumers are determined to have been affected.

See also Question 25 (I had a security breach, but I think that misuse of the PII is not reasonably possible).

If you are still unsure whether a breach has occurred, contact the Office of the Attorney General at ago.securitybreach@vermont.gov or 802-828-5479.

7. Under what circumstances is notification triggered?

- When a data collector that owns or licenses electronic PII discovers or is notified of a security breach;[8] *See* Questions 8 (Explain "owns or licenses"), 10 (Explain "electronic" or "computerized").

- When a data collector that maintains or possesses electronic PII that it does not own or license discovers a security breach;[9] *See* Question 9 (Explain "maintains or possesses").

- When a Data Collector that conducts business in Vermont and maintains or possesses any PII (not just electronic PII) that it does not own or license, discovers or is notified of a security breach;**[10]** *See* Questions 12 (Explain "discovers or is notified").

- However, notification is not required if the data collector establishes that misuse of the PII is not reasonably possible and the data collector provides notice of this determination to the Attorney General.[11] *See* Question 25 (I had a security breach, but I think that misuse of the PII is not reasonably possible).

8. Explain "owns or licenses"

"Owns or licenses" as used in the Act[12] is interpreted broadly. A data collector owns or licenses PII if it receives, stores, maintains, processes, or otherwise has access to PII in connection with the provision of goods or services or in connection with employment. For example:

- A business that permits payment by credit card owns or licenses the credit card data when it processes the payment.
- A business that processes transactions for client businesses also owns or licenses the credit card data of its clients.
- A business that collects social security numbers of either customers or employees owns or licenses the SSNs for purposes of reporting a breach.

9. Explain "maintains or possesses"

Some data collectors merely maintain or possess[13] PII, but do not own or license it. This is a narrow category in which a business does not use the PII in connection with any transaction or employment. It is, essentially, just storing the PII. For example:

- A business that provides physical or electronic storage for client businesses, but does not use the stored information for any business purpose, maintains or possesses any PII being stored.
- A server farm that leases out processing capacity to businesses maintains or possesses any PII that may be stored on its servers.
- A cloud email provider maintains or possesses any PII that might have been transmitted via its email services.

Entities that maintain or possess PII have a different notification obligation from those that own or license PII. *See* Question 12 (Who must be notified in the event of a security breach?)

10. Explain "electronic" or "computerized"

Notice to consumers is only required where a security breach involved electronic,[14] otherwise known as computerized, PII. The Act uses both terms. This guidance uses the term "electronic." Electronic information is in contrast with hard-copy or paper information. However, often information exists in both paper and electronic forms (*i.e.* print-outs from a database). Because it can be difficult to determine whether a security breach resulted from the loss of the electronic data or the print-out, Consumer Notice is required unless the information involved exists only in paper form.

11. Explain "discovers or is notified"

Discovery includes a reasonable belief that unauthorized acquisition of PII has occurred; 100% certainty that a breach has taken place is not required for the clock to start running.

Notification also often does not provide complete certainty that a breach has occurred. For example, law enforcement might notify a business that criminals are trying to sell data that is suspected to come from the business. Banks and credit unions may determine that a business is the likely common point of purchase from which multiple instances of credit card fraud are occurring. If a retailer or other Data Collector receives notification that it might have had a data breach, it has a duty under the Consumer Protection Act to expediently determine whether or not a breach has likely taken place.

12. Who must be notified in the event of a security breach?

- The Office of the Attorney General or Department of Financial Regulation ("DFR"): All Data Collectors must provide Preliminary Notice Attorney General of the security breach, unless they are regulated by DFR, in which case they must notify DFR.[15] Even Financial Institutions described above that are otherwise exempt from notifying consumers must now notify DFR.[16] The Preliminary Notice is kept confidential and is not subject to public records requests.

  See Question 19 (Explain the 14-day Preliminary Notice).

- Consumers: All Data Collectors that "own or license" data containing PII, other than financial institutions described in Question 28, must provide Consumer Notice to consumers whose electronic data has been compromised by a security breach.[17]

- Data Owners or Licensors: Where a data collector "maintains or possesses" data containing PII, but is not the owner or licensor of the PII, the data collector must notify the owner or licensor of the data. If the data collector conducts business in Vermont, this applies to any data containing PII, otherwise it only applies to electronic data containing PII.[18]

  See Questions 8 (Explain "owns or licenses"), 9 (Explain "maintains or possesses")

13. Should I send notice to the Attorney General or Department of Financial Regulation?

- All data collectors not regulated by the Department of Financial Regulation must send Preliminary Notice to the Office at:

  Ryan Kriger, Assistant Attorney General
  AJ Van Tassel, Investigator
  ago.securitybreach@vermont.gov
  phone: 802-828-5479 fax: 802-828-5479

- Data Collectors regulated by DFR should send Preliminary Notice to:

  Dave Cassetty, General Counsel
  Department of Financial Regulation
  89 Main St., Montpelier VT 05620-3101
  phone: 802-828-3301 fax: 802-828-1919

14. What deadlines apply?

- Within 14 business days of discovery of the breach: Preliminary Notice to the Attorney General or DFR.[19] This notice is confidential, and may not be delayed by request of a law enforcement agency.

- In the most expedient time possible and without unreasonable delay, but not later than 45 calendar days after the discovery or notification of the breach: Consumer Notice. Often, the most expedient time possible will be significantly less than 45 days.[20] This notice may be delayed upon request of a law enforcement agency.[21] This notice will be posted on the AGO website. If you wish, you may provide an alternate copy for public posting that redacts the type of PII that was subject to the breach.[22] If you provide a draft of this notice before sending it to consumers, the Office of the Attorney General will attempt to review the notice and inform you if it contains any deficiencies.

- When notice to consumers is sent: a copy of the Consumer Notice and the number of Vermont consumers affected (if known), to the Attorney General or DFR.[23]

15. Explain "most expedient time possible and without unreasonable delay"[24]

Data thieves are able to commit fraud using stolen data within days, or even hours, of committing a theft. It is therefore critical to send the Consumer Notice as soon as possible. Though the statute sets an outer limit of 45 days on the Consumer Notice requirement, often it will be possible to issue Consumer Notice much earlier. A data collector violates the Act by delaying the sending of Consumer Notice even if the delay is not more than 45 days if the notice could have been sent more quickly.

However, the Attorney General understands that in the time immediately after a security breach, a Data Collector may be uncertain whether a breach has taken place, and whether PII was in fact acquired by an unauthorized person. Some reasonable delay is appropriate where the goal is to legitimately avoid sending unnecessary notice. One reason the statute provides for confidential Preliminary Notice is so businesses can get assistance from the Office or DFR in determining whether a breach has occurred.

16. When do deadlines run from?

Deadlines run from discovery or notification of the breach.[25]

See Question 11 (Explain "discovers or is notified").

17. How do I secure my data?

- 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, such as by removing hard drives from computers.

- Be careful that securing the data improperly could harm a future investigation. Be sure to inform law enforcement as soon as possible and work with them while securing your data. *See* Question 18 (Contacting law enforcement).

- The following steps can assist in a future investigation:

    - 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 dated and 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 efforts to reestablish the system and locate the perpetrator, including the date of the action, person communicated with, and contact information for that person.

See also Appendix 1 – Procedures Businesses Should Institute Both to Avoid Security Breaches and After a Breach Has Occurred.

18. Contacting law enforcement.

- Call the FBI or state or local police 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: 802-863-6316

    After normal business hours, call the Albany FBI office: 518-465-7551

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

    Your Local Police Department

    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.

- Inform law enforcement of your obligation to notify consumers of the breach in the most expedient time possible and without unreasonable delay. If law enforcement requests that you delay notification for purposes of an 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.[26]

- If law enforcement requests a delay in notification for purposes of an investigation, prepare your Consumer Notice so that you can send it immediately upon hearing that the delay is no longer needed. *See* Question 21 (Explain the Consumer Notice).

- If law enforcement requests a delay, you must still provide 14-day Preliminary Notice to the Attorney General or DFR. *See* Question 19 (Explain the 14-day Preliminary Notice).

- The law enforcement agency making a request for delay is responsible for promptly notifying you when the agency believes that notifying consumers will no longer impede its investigation.

- It may not be necessary for law enforcement to complete its investigation before the Consumer Notice can be sent. Consequently, 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.

- After law enforcement notifies you that the delay is no longer needed, immediately send your Consumer Notice.

See also Appendix 1 – Procedures Businesses Should Institute Both to Avoid Security Breaches and After a Breach Has Occurred.

19. Explain the 14-day Preliminary Notice.

The Act requires you to notify the Attorney General of a breach within 14 days of discovery of a breach. This notice may not be made public by the Attorney General, and should contain any information known to you at the time it is submitted, including of the date of the security breach, the date of discovery, and a description of the breach.

If the date of the breach is not known within the 14 day period, send the Attorney General the date of the breach as soon as it is known.

If you plan to issue the Consumer Notice within 14 days, you can provide this information and the information required below in a single communication.

- Notice to the Attorney General should be sent to Office at:

  Ryan Kriger, Assistant Attorney General
  AJ Van Tassel, Investigator
  ago.securitybreach@vermont.gov
  phone: 802-828-5479 fax: 802-828-5479

- Data Collectors regulated by DFR should send Preliminary Notice to:

  Dave Cassetty, General Counsel
  Department of Financial Regulation
  89 Main St., Montpelier VT 05620-3101
  phone: 802-828-3301 fax: 802-828-1919

If any information provided in the Preliminary Notice is inaccurate, our policy is not to penalize the company. The purpose of this notice is so that the Attorney General can be aware that a breach may have occurred and assist you in determining whether a breach has occurred and appropriate consumer notification. We understand that more complete information is often not available until just before Consumer Notice is issued later in the process.

Sometimes law enforcement will instruct you not to issue Consumer Notice as doing so may interfere with their investigation. Delaying Consumer Notice at the request of law enforcement is permitted by the Act. Unlike Consumer Notice, Preliminary Notice may not be delayed by law enforcement.

See also Question 20 (Exception to 14-Day Preliminary Notice requirement).

20. Exception to 14-Day Preliminary Notice requirement:

The 14-day preliminary notice need not be submitted if, prior to the date of the breach, you have sworn in the form provided on the Attorney General's website that you maintain written policies and procedures to maintain the security of personally identifiable information and to respond to a breach in a manner consistent with Vermont law.[27]

21. Explain the Consumer Notice.

When you provide notice to consumers, you must provide a copy of the Consumer Notice, along with the number of Vermont consumers who were affected, to the Attorney General. That notice will be posted on the Attorney General's website. If you prefer, the Attorney General will post a second version of the notice in which you have redacted the type of personally identifiable information that was subject to the breach.[28]

Prior to notifying consumers, you may provide a draft of your Consumer Notice to the Attorney General, and we will assist in determining that the notice complies with our statute so that you can avoid resending the notice.

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 Attorney General without unreasonable delay.[29]

See Questions 22 (What must be included in the Consumer Notice), 23 (How must Consumer Notice be sent?).

22. What must be included in the Consumer Notice?

The Consumer Notice must contain the following:

- A general description of the unauthorized acquisition of the data.
- The type of personally identifiable information acquired.
- A general description of the steps you will take to protect the information from further unauthorized acquisition.
- A telephone number, toll-free if available, 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 one free credit report each year from each credit reporting agency. Information on how to obtain a free credit report is available here.
- The approximate date of the security breach.[30]

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.

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 free credit monitoring services to consumers for a specific period of time, typically one year.

23. How must Consumer Notice be sent?

Notice must be sent directly or via substitute notice if certain conditions are met. Either method must include all of the elements listed in Question 22.

a. Direct notice is accomplished through:[31]

- A mailing to the consumer's residence; or
- Telephone, provided telephone contact is made directly with each consumer, and not through a pre-recorded message; or

- Email. *See* Question 24 (Under what circumstances may Consumer Notice be sent by email?)

b. Substitute notice is allowed if you can show one of the following:[32]

- Providing direct notice through the mail or telephone would cost more than $5,000; or
- The number of consumers affected by the security breach exceeds 5,000 nationally; or
- You do not have sufficient contact information to provide notice via the mail or telephone.

Substitute notice requires both of the following:

- Prominently placing the notice on your primary consumer-facing website, if you have one; and
- Sending a press release with all the information to be contained in the notice to major statewide and regional media. A list of media is available in Appendix 3. Coordinate with the Attorney General to confirm that you have notified the appropriate media contacts for your business.

24. Under what circumstance may Consumer Notice be sent by email?

Email notice is only permitted if:

- the data collector does not have contact information necessary to notify via direct mail or telephone; and
- the data collector's primary method of communication with the consumer is by electronic means.

If email notice is used:

- the email notice may not request or contain a hypertext link to a request that the consumer provide personal information;
- the email notice must conspicuously warn consumers not to provide personal information in response to electronic communications regarding security breaches; and
- the email notice must comply with the provisions regarding electronic records and signatures for notices as set forth in 15 U.S.C. § 7001.[33]

25. I had a security breach, but I think that misuse of the PII is not reasonably possible.

If you establish that misuse of the personal information is not reasonably possible, and you provide notice of this determination to the Attorney General or DFR, notice to consumers may not be

necessary.[34] The Attorney General or DFR will inform you whether they agree with your determination.

We recommend that you provide the notice of your determination in writing, via letter or email, to document the exchange. If you inform the Attorney General or DFR via telephone, we recommend you document the conversation with a follow-up letter or email.

You may designate your explanation as "trade secret" if it meets the definition of trade secret under 1 V.S.A. § 317(c)(9).[35]

If you learn, after notifying the Attorney General, that misuse of the personal information has occurred or is occurring, you must provide notice of the security breach to affected consumers without unreasonable delay after receiving such information.[36]

26. What information does the Attorney General hold confidential?

The Preliminary Notice of a security breach, which a data collector is required to provide within 14-days of discovery of the breach, may not be made public.[37] *See* Question 19 (Explain the 14-day Preliminary Notice).

The Consumer Notice, which a data collector is required to provide to the Attorney General, is posted to the Attorney General's website, here. We post these notices so that consumers can confirm that notices they receive are legitimate. A data collector is allowed to provide an alternate notice to consumers for posting in which the type of PII is redacted. *See* Question 21 (Explain the Consumer Notice).

The Attorney General is permitted to communicate about data breaches with other law enforcement entities.

27. Should I contact the credit reporting agencies?

Notify the three major credit reporting agencies if you are going to send a notice of security breach to more than 1,000 consumers.

Notice to credit reporting agencies shall include the timing, distribution, and content of the Consumer Notice and must be sent without unreasonable delay. The Attorney General considers notice sent no later than the same day as Consumer Notice is sent to meet this requirement.

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
  Fraud Victim Assistance Dept
  P.O. Box 6790, Fullerton, CA 92834
  Phone: 1-800-372-8391 (1-800-FRAUD911)
  Email: fvad@transunion.com

28. How does the Act apply to financial institutions?

The Act states:

> Except as provided in subdivision (3) of this subsection, a financial institution that is subject to the following guidances, and any revisions, additions, or substitutions relating to an interagency guidance shall be exempt from this section:
>
> (1) 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.
>
> (2) 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.
>
> (3) A financial institution regulated by the Department of Financial Regulation that is subject to subdivision (1) or (2) of this subsection shall notify the Department as soon as possible after it becomes aware of an incident involving unauthorized access to or use of personally identifiable information.[38]

All financial institutions must still provide Preliminary Notice to the Department of Financial Regulation. Financial institutions not exempted by this section must provide Consumer Notice.

See Question 13 (Should I send notice to the Attorney General or Department of Financial Regulation?)

29. If I report the breach to you, are you going to investigate me?

As a general rule, if security breach notices are sent within the appropriate deadlines and the nature of the breach does not indicate a lack of appropriate data security, our office is unlikely to investigate the security breach.

We understand that even a business taking reasonable steps to protect sensitive data may suffer a security breach. Our goal is not to penalize businesses that have acted responsibly, it is to protect consumers.

30. What happens if I violate the Act?

The Act is enforced under the same authority as the Consumer Protection Act.[39] The Attorney General may investigate by issuing a Civil Investigative Demand (civil subpoena), and may seek injunctive relief and civil penalties of up to $10,000 per violation. Each day past the statutory deadlines that each consumer, or the Attorney General, is not informed is considered a separate violation.

---

[1] 9 V.S.A. § 2430(3)
[2] 9 V.S.A. § 2435(b)(1)
[3] 9 V.S.A. § 2430(5)
[4] 9 V.S.A. § 2435(b)(3)
[5] 9 V.S.A. § 2435(b)(1)
[6] 9 V.S.A. § 2435(c)
[7] 9 V.S.A. § 2430(8)
[8] 9 V.S.A. § 2435(b)(1)
[9] 9 V.S.A. § 2435(b)(2)
[10] *Id.*
[11] 9 V.S.A. § 2435(d)(1)
[12] 9 V.S.A. § 2435(b)(1)
[13] 9 V.S.A. § 2435(b)(2)
[14] 9 V.S.A. § 2435(b)(1)
[15] 9 V.S.A. § 2435(b)(3)
[16] 9 V.S.A. § 2435(f)(3)
[17] 9 V.S.A. § 2435(b)(1)
[18] 9 V.S.A. § 2435(b)(2)
[19] 9 V.S.A. § 2435(b)(3)(B)
[20] 9 V.S.A. § 2435(b)(1)
[21] 9 V.S.A. § 2435(b)(4)
[22] 9 V.S.A. § 2435(b)(3)(C)(ii)
[23] 9 V.S.A. § 2435(b)(3)(C)
[24] 9 V.S.A. § 2435(b)(1)
[25] 9 V.S.A. § 2435(b)
[26] 9 V.S.A. § 2435(4)
[27] 9 V.S.A. § 2435 (b)(3)(B)(ii)
[28] 9 V.S.A. § 2435(b)(3)(C)
[29] 9 V.S.A. § 2435(d)(1)
[30] 9 V.S.A. § 2435(b)(5)
[31] 9 V.S.A. § 2435(b)(6)(A)
[32] 9 V.S.A. § 2435(b)(6)(B)
[33] 9 V.S.A. § 2435(b)(6)(A)(ii)
[34] 9 V.S.A. § 2435(d)(1)
[35] *Id.*
[36] 9 V.S.A. § 2435(d)(2)
[37] 9 V.S.A. § 2435(b)(3)(B)(iv)
[38] 9 V.S.A. § 2435(f)
[39] 9 V.S.A. § 2435(g)

APPENDIX 1

Procedures Businesses Should Institute Both to Avoid Security Breaches and After a Breach Has Occurred

- 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 Security Breach 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 before consulting a forensic expert or law enforcement.
2. Contact the suspected perpetrator.
3. Delay Preliminary Notice to the Attorney General.

APPENDIX 2 – MODEL LETTER

This model letter is to be used when the breached entity does 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.

Examples of past security breach notice letters may be found here.

Dear _____:

We are writing to you because of a recent security incident at [name of organization]. [Describe what happened in general terms the type of personal information that was involved (e.g., social security number, financial account number, account password, driver's license number)] [Describe in general terms, what you are doing to protect personal information from further unauthorized access or acquisition.]

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	Experian	TransUnion
1-800-685-1111	1-888-397-3742	1-800-916-8800
P.O. Box 740241	P.O. Box 2104	P.O. Box 2000
Atlanta, GA 30374-0241	Allen, TX 75013	Chester, PA 19022
www.equifax.com	www.experian.com	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	Experian	TransUnion
888-766-0008	888-397-3742	800-680-7289

5. You may also get information about **security freezes** by contacting 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.ago.vermont.gov. 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 [phone number, toll-free if available].

[Closing]

APPENDIX 3 – MEDIA FOR SUBSTITUTE NOTICE

Substitute notice requires that the data provider issue a press release containing all information found in the Consumer Notice to the following media outlets. *See* Question 23.b (Substitute notice). There is no obligation to ensure (such as through paid advertising) that the media outlet does anything with the information.

Newspapers

- Bennington Banner – news@benningtonbanner.com
- Brattleboro Reformer – news@reformer.com
- Burlington Free Press – metro@burlingtonfreepress.com
- Caledonian Record – news@caledonian-record.com
- Newport Daily Express – kwells@newportvermontdailyexpress.com
- Rutland Herald – pressreleases@rutlandherald.com
- Seven Days – pamela@sevendaysvt.com
- St. Albans Messenger – news@samessenger.com
- Times-Argus – news@timesargus.com
- Valley News – newseditor@vnews.com
- Vermont Digger – vtdigger@gmail.com

Television Stations

- WCAX – news@wcax.com
- WETK – viewerservices@vermontpbs.org
- WNNE – lhayes@hearst.com
- WPTZ – lhayes@hearst.com

Radio

- Barre WORK – ltrask@greateasternradio.com
- Berlin WWFY – ltrask@greateasternradio.com
- Burlington WBTZ – mailbag@999thebuzz.com
- Burlington WEZF – jamiedennis@star929.com (also The Planet 96.7)
- Burlington WOKO – woko@woko.com
- Champlain Valley WCPV – jamiedennis@star929.com
- Lyndon WGMT – magic9777@gmail.com
- Manchester WEQX – eqx@weqx.com
- Randolph WCVR – ray@listenvermont.com
- Rutland WJJR – wjjr@catamountradio.com
- Rutland WZRT – tjaye@catamountradio.com
- St. Johnsbury WKXH – kix105@kix1055.com
- Waterbury WDEV – wdev@radiovermont.com
- VPR – news@vpr.net