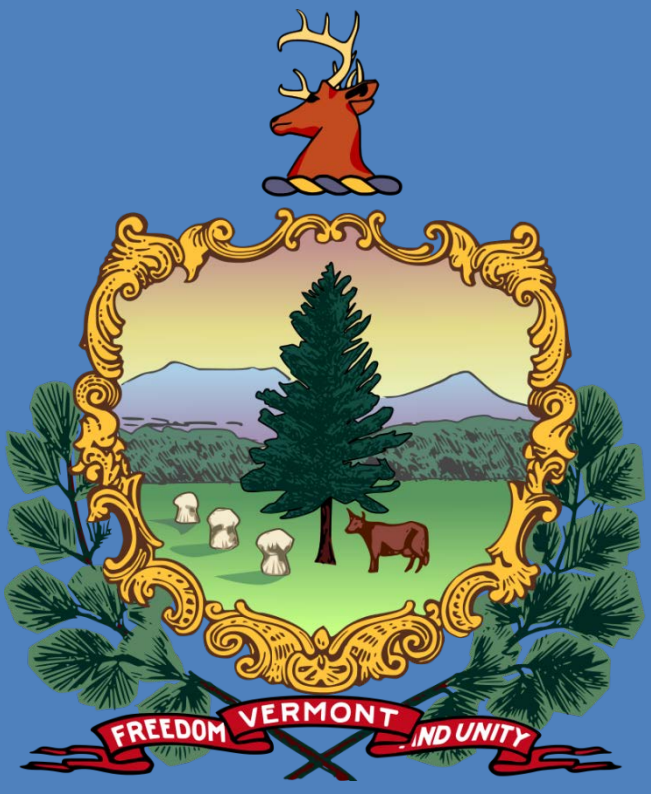
# VERMONT SECURITY BREACH NOTICE ACT **GUIDANCE**




PREPARED BY THE VERMONT OFFICE OF THE ATTORNEY GENERAL
UPDATED JUNE 2020

**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.**

## INTRODUCTION

This Guidance was last materially updated in September 2014. Since then, the number of breaches reported each year has increased significantly. We have also seen a growth in sophistication amongst the business, legal, and enforcement communities in understanding how to protect against, detect, investigate, and respond to security breaches. That greater depth of understanding is reflected in this Guidance.

The Vermont Attorney General believes in fostering a culture of compliance within the business community, of assisting businesses to understand the law rather than solely relying on enforcement actions to encourage compliance. During the past several years we have had many opportunities to work with counsel who represent businesses experiencing breaches, and to the extent that we see repeated requests for clarity or points of misunderstanding, we have addressed these issues in the section "Common questions and misunderstandings," below.

In addition, on July 1, 2020, Act 89 (Bill S.110) of the 2019/20 Legislative Session went into effect. Act 89 introduced substantive amendments to Vermont's Security Breach Notice Act, 9 V.S.A. §§ 2430 & 2435, which are explained in this Guidance. Section 5 ("Recent amendments to the Act"), offers a roadmap to the sections that specifically address those changes. Furthermore, Act 171 of the 2017/18 Legislative Session created a distinct type of Security Breach called a Data Broker Security Breach, which is addressed in Section 36 ("Data Broker Security Breaches").

Finally, we appreciate that businesses must comply with Security Breach Notice Acts that exist in fifty states, three territories and the District of Columbia. This office does not speak for any other Attorney General, but we do frequently engage with our counterparts in other offices, often collaborating on investigations and enforcement actions. This Guidance does not purport to describe how any other Attorney General would interpret similar language in another jurisdiction's Act, but also strives to interpret our language in a manner that does not conflict with our understanding of those interpretations. *See also* Section 38 ("Variation relative to other State Notice Acts").

## OVERVIEW

### 1. WHAT IS THE PURPOSE OF THIS GUIDANCE?

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

Nothing in this guidance constitutes legal advice. Every person, business, and situation relating to data breach is highly fact specific. Depending on specific circumstances you may wish to seek legal counsel in order to both interpret this guidance, and to respond to a known or suspected data breach.

## 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."[i] It is possible for more than one entity to be considered the Data Collector for a specific Security Breach. *See* Section 43 ("Breaches involving multiple parties").

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* Section 35 ("Financial institutions")

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

## 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** or **login credentials** maintained by a data collector.[iii]

*See also* Sections 7 ("What if I'm not sure whether I've had a Security Breach?"), 42 ("Disputes over whether a breach occurred")

## 4. WHAT IS PERSONALLY IDENTIFIABLE INFORMATION (OR "PII")?

PII means a consumer's first name or first initial and last name in combination with one or more of the following digital data elements, when the data elements are not encrypted, redacted, or protected by another method that renders them unreadable or unusable by unauthorized persons:

- a Social Security number;
- a driver license or nondriver State identification card number, individual taxpayer identification number, passport number, military identification card number, or other identification number that originates from a government identification document that is commonly used to verify identity for a commercial transaction;
- a financial account number or credit or debit card number, if the number could be used without additional identifying information, access codes, or passwords;
- a password, personal identification number, or other access code for a financial account;
- unique biometric data generated from measurements or technical analysis of human body characteristics used by the owner or licensee of the data to identify or authenticate the consumer, such as a fingerprint, retina or iris image, or other unique physical representation or digital representation of biometric data;
- genetic information; or
- health records or records of a wellness program or similar program of health promotion or disease prevention; a health care professional's medical diagnosis or treatment of the consumer; or a health insurance policy number.

The Office considers the front of a check, which contains name, account number, routing number, and potentially address and signature, to be PII. A credit card number and name is also PII, regardless of whether the Expiration Date or Security Code (CVV) is included.

PII does not mean publicly available information that is lawfully made available to the general public from federal, state, or local government records.[iv]

## 5. RECENT AMENDMENTS TO THE ACT

The 2020 Amendments go into effect on **July 1, 2020**. The Amendments only apply to security breaches that were discovered or for which the data collector was notified on or after July 1, 2020.

The following substantive changes were introduced by the 2020 Amendments:

- The definition of Personally Identifiable Information was expanded to include:
    - more types of government identification numbers;[v]
    - biometric information;
    - genetic information; and
    - health information.

  *See also* Sections 4 ("What is Personally Identifiable Information (or 'PII')?") and 16 ("Types of 'Personally Identifiable Information'").
- A notice requirement was added for breaches involving **login credentials**, with a different means of notice.

  *See also* Sections 17 ("'Login Credentials'") and 31 ("Notice requirements for a login credential breach").
- The conditions under which **substitute notice** is permitted were narrowed to where the lowest cost of providing Direct Notice via writing, email, or telephone would exceed $10,000, or the data collector does not have sufficient contact information. Substitute notice is no longer permitted based on the number of consumers affected.[vi]

  *See also* Section 29 ("Methods of delivering Consumer Notice").

In addition, Act 171 of 2018 introduced the "Data Broker Security Breach," which does not change the Security Breach Notice Act, but which requires annual reporting and/or disclosure of the number of data broker security breaches experienced in the prior year. *See* Section 36 ("Data Broker Security Breaches").

## 6. 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.

### 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* Section 22 ("Securing your data post-breach")

### INVOLVE LAW ENFORCEMENT **IMMEDIATELY**

*See* Section 23 ("Contacting Law Enforcement").

### IF YOU ARE STORING SOMEONE ELSE'S DATA, CONTACT THE OWNER OF THE DATA **IMMEDIATELY**.

*See* Sections 12 ("'Maintains or possesses'"), 18 ("Who must be notified in the event of a security breach?").

### PROVIDE CONFIDENTIAL PRELIMINARY NOTICE TO THE ATTORNEY GENERAL OR DFR ABOUT THE BREACH **WITHIN 14 DAYS**.[vii]

*See* Section 25 ("14-day Preliminary Notice").

### NOTIFY CONSUMERS ABOUT THE BREACH **IN THE MOST EXPEDIENT TIME POSSIBLE AND NOT LATER THAN 45 DAYS** AFTER DISCOVERY OR NOTIFICATION.[viii]

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

*See* Section 27 ("Consumer Notice").

### NOTIFY THE THREE MAJOR CREDIT REPORTING AGENCIES IF YOU ARE GOING TO SEND A NOTICE OF SECURITY BREACH TO MORE THAN 1,000 CONSUMERS.[ix]

*See* Section 34 ("Contacting the credit reporting agencies").

## DETAILED EXPLANATIONS

### 7. WHAT IF I'M NOT SURE WHETHER I'VE HAD A SECURITY BREACH?

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.

"Security breach" does not include good faith but unauthorized acquisition of personally identifiable information or login credentials by an employee or agent of the business or agency as long as the data 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.[x]

Note that this is a non-exclusive list of factors. A data collector can have a reasonable belief of an unauthorized acquisition of data in the absence of any of these factors. For example, the existence of malware on a computer

network that is of the type that extracts data may be enough to establish a reasonable belief, depending on the circumstances.

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;
- An employee loses a laptop, external hard drive, or thumb drive containing PII in a public place like the back of a taxi;
- 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;
- A server is misconfigured, exposing data on the internet;
- Hackers attempt to sell or barter PII or login credentials maintained by a data collector on the dark web;
- A data collector experiences a ransomware attack, where the ransomware is of the type that has been known to exfiltrate data;
- Scammers acquire login credentials and compromise a business's email system, where email accounts include sent or received PII; or
- A customer's PII is accidentally sent to the wrong customer.

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 an 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* Section 32 ("Security breach where data collector establishes misuse 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. Whereas our role is not to provide legal advice, in the area of data breach we try to provide guidance where feasible.

## 8. WHAT ARE MY LEGAL OBLIGATIONS TO INVESTIGATE A POTENTIAL BREACH?

While the Act does not expressly impose a duty to investigate potential breaches, the deadlines to notify consumers presumes an expedient investigation. **Whether a data collector has acted in the most expedient manner possible and without undue delay is measured from the moment the data collector first discovers or is first notified of information that could lead to confirmation of a security breach.**

Failure to investigate a potential breach which turns out to have been a breach would be considered a violation of the Act. Failure to conduct an investigation expediently, or to cooperate fully with third party investigators such as

Payment Card Institute (PCI) Forensic Investigators (PFIs) such that the investigation takes an unreasonable amount of time, is also considered a violation of the Act.

Furthermore, failure to appropriately investigate a potential breach may also be an unfair or deceptive act in violation of Vermont's Consumer Protection Act, 9 V.S.A. § 2453.

## 9. WHAT ARE MY LEGAL OBLIGATIONS TO REMEDIATE A BREACH?

Upon discovering a security breach, a data collector must take immediate steps to stop the breach from continuing or reoccurring, which could include taking systems offline, removing malware, changing passwords or deleting accounts, installing patches, or other methods. Failure to do so is considered an unfair or deceptive act in violation of Vermont's Consumer Protection Act, 9 V.S.A. § 2453.

## 10. UNDER WHAT CIRCUMSTANCES ARE NOTICE OBLIGATIONS TRIGGERED?

- When a data collector that owns or licenses electronic PII discovers or is notified of a security breach;[xi] *See* Sections 11 ("'Owns or licenses'"), 13 ("'Electronic,' 'computerized,' and 'digital'").
- When a data collector that maintains or possesses electronic PII that it does not own or license discovers a security breach;[xii] *See* Section 12 ("'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;[xiii] *See* Section 15 ("'Discovers or is notified'").
- However, notice 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.[xiv] *See* Sections 32 ("Security breach where data collector establishes misuse is not reasonably possible").

## 11. "OWNS OR LICENSES"

"Owns or licenses" as used in the Act[xv] 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.

## 12. "MAINTAINS OR POSSESSES"

Some data collectors merely maintain or possess[xvi] 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 notice obligation from those that own or license PII. *See* Section 18 ("Who must be notified in the event of a security breach?").

## 13. "ELECTRONIC," "COMPUTERIZED," AND "DIGITAL."

Notice to consumers is only required where a security breach involves electronic,[xvii] otherwise known as computerized or digital, PII. The Act uses these terms interchangeably. This guidance uses the term "electronic." Where information is described as electronic, it 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, which is to say the PII is not all processed electronically. A data collector that conducts business in Vermont and maintains or possesses PII must notify the owners or licensors of the PII even if it is not electronic.

"Electronic" communications means communication via email, instant message, or text message (SMS). Electronic notice means notice via email. Although in some circumstances notice via instant message or text message might be conceivable, generally speaking the amount of information that must be included in the notice makes those methods unwieldy.

## 14. "ACQUISITION"

In 2012, the Act was amended to change the word "access" to "acquisition." It was argued that access was overly broad in that it could include situations where someone glances at a computer screen. However, in practice there appears to be significant overlap between breaches that involve "access" and those that involve "acquisition." For example, if data is made available online due to a misconfigured server or failure to request authentication, this would be considered unauthorized acquisition (as was the case in the *In re SAManage* security breach). If an unauthorized user infiltrates a system and is able to view screens that display PII, this would be considered acquisition. Furthermore, even in situations where exfiltration of data may not be demonstrable (that is, evidence of data being transmitted or downloaded from a system), a breach may still involve unauthorized acquisition (as was the case in the *In re Hilton* security breach). If hardware containing PII (such as a laptop or thumb drive) is lost, acquisition should be presumed.

Often, even where access to a system is clear, it may be difficult to prove that acquisition took place due to the absence of log files. In a circumstance where a data provider is unable to determine whether or not data was actually acquired due to its own failure to preserve the logs that would have provided such evidence, and absent affirmative evidence to the contrary, acquisition should be presumed.

If a situation arises where a data provider believes that access to data took place, but the likelihood of acquisition is extremely low, or the access was fleeting, this may fall within the circumstance described in Section 32 ("Security breach where data collector establishes misuse is not reasonably possible"). If you are uncertain whether acquisition has occurred such that notice requirements are triggered, please contact our Office.

## 15. "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. 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.

Typical scenarios in which a data collector is considered to have "discovered" a potential breach include:

- Finding malware on a computer system of the type that exfiltrates data or surveils systems prior to deploying exfiltration malware;
- Learning of a potential security breach through intrusion detection software or services;
- Learning that an employee has lost hardware containing unencrypted PII or that there has been a theft of hardware; or
- Observing unauthorized access to databases or other systems containing PII, unauthorized changes in access rights in existing user accounts, or the unauthorized creation of new user accounts.

Typical scenarios in which a data collector is considered to have received notice of a potential breach include:

- Receipt of a Common Point of Purchaser notification from a credit card processor, bank or other financial institution;
- Complaints from customers that fraudulent charges were placed on a credit card recently used at the business;
- Notification by law enforcement that criminals are trying to sell data that is claimed to have been stolen from the data collector;
- Notification from third parties that fraudulent emails are being sent from an employee's email account;
- Notification by a computer scientist, forensics firm, or "white hat hacker" that a data collector's data has been exposed;
- Notification by a contractor or other third-party that maintains the data collector's data, that a data breach may have occurred; or
- News or security blog reports of a potential breach.

The discovery date is not the date that an investigation is completed, it is the earliest date that an entity became aware of, or had a reasonable belief of, unauthorized activity.

## 16. TYPES OF "PERSONALLY IDENTIFIABLE INFORMATION"

### SOCIAL SECURITY NUMBER

Only the full Social Security Number (SSN) combined with a name or initial is considered PII. A redacted (last 4 digits) SSN is not PII. A Social Security Number without a name is not PII, however if you do fail to protect SSNs and they are stored in a manner that a bad actor could reidentify the SSN with an individual, this could be considered a violation of

Vermont's Consumer Protection Act. Use of SSNs must also comply with Vermont's Social Security Number Protection Act, 9 V.S.A. § 2340.

## GOVERNMENT IDENTIFICATION NUMBERS

This element includes "a driver license or nondriver State identification card number, individual taxpayer identification number, passport number, military identification card number, or other identification number that originates from a government identification document that is commonly used to verify identity for a commercial transaction."[xviii] If you are uncertain whether a government identification number not expressly listed is considered PII, please contact our Office.

## FINANCIAL ACCOUNT NUMBERS

A credit card number and name is considered PII even in the absence of an Expiration Date or Security Code (CVV). A bank account number and name are considered PII where the acquirer could reasonably determine the bank. A bank account number, name and routing number are also considered PII.

## FINANCIAL ACCOUNT PASSWORDS OR OTHER ACCESS CODES

While login credential breaches have different notice requirements than PII breaches, the loss of login credentials of a financial account triggers the traditional notice requirements for PII breaches.

## BIOMETRIC IDENTIFIERS

This element includes "unique biometric data generated from measurements or technical analysis of human body characteristics used by the owner or licensee of the data to identify or authenticate the consumer, such as a fingerprint, retina or iris image, or other unique physical representation or digital representation of biometric data."[xix] This language was adapted from Oregon's breach act. This was intended to be a broad definition of biometrics, and includes biometric identifiers based on behavior (such as gait, typing patterns or navigation patterns) as well as physical characteristics such as facial and voice recognition.

An individual's signature may be considered a biometric identifier depending on the context. Photographs or videos which have been stored without any form of facial recognition or other computerized or biometric analysis would not be considered biometric data. Note that the science of biometrics is rapidly advancing, and this topic may be revisited as technology changes.

## GENETIC INFORMATION

The term "genetic information" does not include any further elaboration. In determining whether a data element is considered genetic information, you might look to definitions found in other laws for guidance, those definitions are not considered binding. Some laws that define genetic information include:

- Vermont's Genetic Testing Law, 18 V.S.A. § 9331(6).
- Federal Genetic Information Nondiscrimination Act (GINA), 29 USC § 1191b(d)(6) and 29 C.F.R. Part 1635.3(c)
- "DNA Record" as defined in 20 V.S.A. § 1932 would be considered genetic information.

If you are uncertain whether a data falls within this element, please contact our Office.

### HEALTH INFORMATION

This element includes "(I) health records or records of a wellness program or similar program of health promotion or disease prevention; (II) a health care professional's medical diagnosis or treatment of the consumer; or (III) a health insurance policy number."

This definition was the result of significant discussion and debate, during which definitions from Oregon and Delaware were considered. The first part is intentionally broad. It includes two distinct categories of data: "Health records" and "records of a wellness program or similar program of health promotion or disease prevention." Health records are not necessarily limited to records maintained by a health provider or other HIPAA-covered entity. They could include, for example, information about an individual's health maintained by a business or a data broker, whether derived from a diagnosis, predictive analytics, or other methods.

The Act contains an exemption from notice requirements involving health information if:

1. the security breach only involves health information;
2. the data collector is subject to the privacy, security, and breach notification rules adopted in 45 C.F.R. Part 164 pursuant to the federal Health Insurance Portability and Accountability Act, P.L. 104-191 (1996) (HIPAA); and
3. notice is provided to affected consumers pursuant to the requirements of the breach notification rule in 45 C.F.R. Part 164, Subpart D.[xx]

## 17. "LOGIN CREDENTIALS"

**Login credentials** means a consumer's username or email address, in combination with a password or an answer to a security question, that together permit access to an online account.[xxi]

A login credential breach has different notice requirements from a PII breach, as explained in Section 31 ("Notice requirements for a login credential breach").

## 18. 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 to the Attorney General of the security breach, unless they are regulated by DFR, in which case they must notify DFR.[xxii] Even Financial Institutions described above that are otherwise exempt from notifying consumers must notify DFR.[xxiii] The Preliminary Notice is kept confidential and is not subject to public records requests.

  *See* Section 25 ("14-day Preliminary Notice").

- Consumers: All Data Collectors that "own or license" data containing PII, other than financial institutions described in Section 35, must provide Consumer Notice to consumers whose electronic data has been compromised by a security breach.[xxiv]

- 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 immediately 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.[xxv]

  *See* Sections 11 ("Owns or licenses"), 12 ("Maintains or possesses").

## 19. 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 of the Attorney General at:

  Ryan Kriger, Assistant Attorney General
  ago.securitybreach@vermont.gov
  phone: 802-828-5479; fax: 802-828-5479

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

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

## 20. DEADLINES

Deadlines run from discovery or notification of the breach.[xxvi] The 45-day outer limit incorporates the time it will take to conduct an investigation – it does not begin after the investigation is completed. Where an investigation necessarily takes longer than 45 days – for example where identification of affected consumers is very complicated – the Office expects the data provider to prepare to issue notice to the extent possible prior to the completion of the investigation and to issue notice with the utmost expediency once the investigation concludes.

Sometimes the date of discovery or notification is in dispute. The best way to avoid scrutiny is to be able to demonstrate that you acted with diligence and requisite expediency when investigating and issuing notice of a breach. *See* Section 15 ("'Discovers or is notified'").

- Immediately: Notice to the data provider who owns or licenses the data, where the breach is discovered by a data provider that maintains or possesses data that it does not own or license (*See* Section 12 ("'Maintains or possesses'").

- Within 14 business days of discovery of the breach: Preliminary Notice to the Attorney General or DFR.[xxvii] 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.[xxviii] This notice may be delayed upon request of a law enforcement agency.[xxix] 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.[xxx] 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.[xxxi]

## 21. "MOST EXPEDIENT TIME POSSIBLE AND WITHOUT UNREASONABLE DELAY" [xxxii]

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 less than 45 days, if the notice could have been sent significantly more quickly.

For example: *an employee copies an unencrypted spreadsheet containing customers' names, addresses, social security numbers, and other information to a thumb drive. The employee proceeds to lose the thumb drive later that evening. After conducting a thorough search and concluding that the drive is truly lost, they report the event to their superior the following morning. A copy of the spreadsheet still resides on the company's file server.* The company in this scenario knows that a breach has occurred, knows exactly who was affected, and knows the addresses of all the affected consumers. Under this scenario, notice should be issued immediately. Waiting 45 days would be unreasonable.

The Office understands that for some security breaches, a Data Collector may require time to ascertain whether a breach has in fact taken place, whether PII may have been acquired by an unauthorized person, or whether Vermonter's data was involved. Some reasonable delay is appropriate where the goal is to legitimately avoid sending unnecessary notice. The Office also understands that in certain limited circumstances, an investigation may extend beyond 45 days. 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, and to make the Attorney General aware if a breach might take longer to investigate than usual.

## 22. SECURING YOUR DATA POST-BREACH

- 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 offline or isolating the data, such as by removing hard drives from computers.
- Be careful that improperly securing the data could inhibit future investigations. Be sure to inform law enforcement as soon as possible and work with them while securing your data. *See* Section 23 (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 Before and During a Breach.

## 23. 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 notice for purposes of an investigation, the request must be made in writing or you must document the request contemporaneously, noting the date the request was made, the name of the law enforcement officer making the request and the name of the officer's agency.[xxxiii]

- If law enforcement requests a delay in notice 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* Section 27 ("Consumer Notice").

- If law enforcement requests a delay, you must still provide 14-day Preliminary Notice to the Attorney General or DFR. *See* Section 25 ("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* Section 50 ("Reporting a Security Breach to law enforcement").

## 24. HOW DO NOTICE REQUIREMENTS DIFFER BETWEEN A PII BREACH AND A LOGIN CREDENTIAL BREACH?

A security breach that involves both PII and login credentials should be treated as a PII breach. Requirements for PII Breach notice are described in Sections 25 to 30 below.

A security breach that only involves login credentials has different requirements for method of notice to consumers and content of the notice, and in some cases does not require notice to the Attorney General or DFR. These requirements are described in Section 31 ("Notice requirements for a login credential breach").

## 25. 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.

Preliminary notice may be provided electronically or via telephone. If you wish to discuss the breach by telephone, document your call to the Attorney General in your follow-up notice that is sent to the AG along with notice to consumers.

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.

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

  Ryan Kriger, Assistant Attorney General
  ago.securitybreach@vermont.gov
  phone: 802-828-5479; fax: 802-828-5479

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

  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 notice. We understand that more complete information is often not available until just before Consumer Notice is issued later in the process. If a discussion with the Office is not necessary, please send preliminary notice via email. Include the following in the subject or at the top of the email: **"Preliminary Notice of Breach, Confidential & Exempt from Public Records Act."**

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* Section 26 ("Exception to 14-Day Preliminary Notice requirement").

## 26. 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.[xxxiv]

## 27. 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. If you did not previously disclose the information in a preliminary notice, you must also include the date of the security breach, the date of discovery of the breach, and a description of the breach. The consumer notice will be posted on the Attorney General's website, any cover letter will

not. 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.[xxxv]

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.[xxxvi]

*See* Sections 28 ("Content of the Consumer Notice") and 29 ("Methods of delivering Consumer Notice").

## 28. CONTENT OF 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 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. If this is a range of dates, include the earliest date you know of during which the breach was occurring and the date that the breach ended or was remediated.[xxxvii]

A model notice 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.

## 29. METHODS OF DELIVERING CONSUMER NOTICE

Notice must be sent **directly** or via **substitute notice** if certain conditions are met. Either method must include all of the elements listed in Section 28 ("Content of the Consumer Notice").

### DIRECT NOTICE

Direct Notice is accomplished through:[xxxviii]

- 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* Section 30 ("Circumstances permitting Consumer Notice by email")

### SUBSTITUTE NOTICE

Substitute Notice is allowed if you can show one of the following:[xxxix]

- The lowest cost of providing direct notice to affected consumers, among written, email, or telephonic notice would exceed $10,000; or
- You do not have sufficient contact information to direct notice.

This means that if a business is capable of providing direct notice via mail, email, or telephone for less than $10,000, it must issue direct notice. Note that the 2020 Amendments eliminated a 5,000 person national numerical threshold above which substitute notice was permitted.

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.

## 30. CIRCUMSTANCES PERMITTING CONSUMER NOTICE 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.[xl]

## 31. NOTICE REQUIREMENTS FOR A LOGIN CREDENTIAL BREACH

These requirements apply to a security breach that only involves login credentials. Security breaches involving both PII and login credentials should be treated as a PII breach. Security breaches involving credentials have different notice content requirements and different notice delivery requirements. These requirements were designed to mirror the notice requirements of the State of California, Cal. Civ. Code §§ 1798.82(j)(4)-(5).

## CONSUMER NOTICE CONTENT

Notice of a credential breach should include:

- A statement that the breach took place
- Advice to take steps necessary to protect the online account, including to change his or her login credentials for the account and for any other account for which the consumer uses the same login credentials

## CONSUMER NOTICE DELIVERY

Notice for breaches involving login credentials for an **email account** have special requirements.

- **Non-email** credential breaches may be delivered electronically or in any manner that a traditional breach notice can be delivered. *See* Section 29 ("Methods of delivering Consumer Notice").
- **Email account** credential breaches may not deliver notice through the email account whose credentials were involved in the breach. Instead, notice may be delivered:
    - In any manner that a traditional breach notice can be delivered; or
    - by clear and conspicuous notice delivered to the consumer online when the consumer is connected to the online account from an Internet protocol address or online location from which the data collector knows the consumer customarily accesses the account.[xli]

## NOTICE TO ATTORNEY GENERAL OR DEPARTMENT OF FINANCIAL REGULATION

The content of this notice is the same as for a traditional breach: number of consumers effected, date of breach, date of discovery and a description of the breach. The 14-day preliminary notice is also required.

However, notice to the Attorney General or DFR is only required for breaches where the login credentials at issue were maintained or collected by the data collector (for example, this could be due to theft, negligence on the part of the data collector, or interception of the credentials due to the manipulation of a data collectors' login page).

The following situations would not require notice to the Attorney General or DFR:

- A hacker steals login credentials from a party unrelated to the data collector, and uses them to log in to a consumer's account maintained by the data collector;[xlii]
- A hacker uses brute force to determine a consumer's login credentials by repeatedly attempting to log in to an account maintained by the data collector; or
- A hacker creates a fraudulent website that looks like the data collector's website in order to collect login credentials as part of a phishing scheme.

Data collectors are strongly encouraged to implement dual-factor authentication where appropriate in order to protect consumers from these situations.

*See also* Section 25 ("14-day Preliminary Notice").

## 32. SECURITY BREACH WHERE DATA COLLECTOR ESTABLISHES MISUSE IS NOT REASONABLY POSSIBLE

This provision is sometimes referred to as the "risk of harm analysis." 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.[xliii] The Attorney General or DFR will inform you whether they agree with your determination.

The typical scenario where this arises is where an email containing PII is misrouted to the wrong recipient, and that recipient deletes the email and certifies that it was destroyed.

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).[xliv]

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.[xlv]

## 33. 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.[xlvi] *See* Section 25 ("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* Section 27 ("Consumer Notice").

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

## 34. CONTACTING 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 notice 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

## 35. 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.[xlvii]

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

*See* Section 19 ("Notice to the Attorney General or Department of Financial Regulation").

## 36. DATA BROKER SECURITY BREACHES

The definition of "Data Collector" is very broad and includes data brokers.[xlviii] *See* Section 2 ("Does this Guidance apply to me?"). Thus, if a data broker experiences a security breach involving PII or Login Credentials, it must comply with the Act.

In addition, the General Assembly has recognized that data brokers might collect a broad array of data that does not constitute PII, but is sensitive in the context of the large caches of data that data brokers compile about consumers. Thus, data brokers are also required to track "Data Broker Security Breaches," which are defined that same way as security breach except:

1. They involve data brokers[xlix] instead of data collectors; and

2. They involve "brokered personal information"[l] instead of PII or login credentials. The definition of "brokered personal information" is very broad and includes "information that, alone or in combination with the other information sold or licensed, would allow a reasonable person to identify the consumer with reasonable certainty" among other elements.

Data brokers are required to report the number of data broker security breaches they experienced in the previous year when they submit their annual data broker registration required by 9 V.S.A. § 2446. They do not have consumer or AG notice obligations beyond this requirement. However, this obligation does not exempt data brokers from the Act.

More information about the data broker registry can be found in the Office's Data Broker Regulation Guidance.[li]

## 37. VIOLATIONS OF THE ACT

The Act is enforced by the Attorney General and States' Attorneys under the same authority as the Consumer Protection Act.[lii] 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.

For minor deviations from the Act or where the notice is unclear or missing an element, we will often follow up with a call or email to seek clarity or ask you to rectify the issue. Assuming these issues are quickly resolved, it is unlikely exchanges like this will lead to an investigation.

Typically, if the Attorney General investigates a violation of the Security Breach Notice Act, we will also inquire as to whether the business had implemented adequate data security. Failure to do so is a violation of the Consumer Protection Act.

## 38. VARIATION RELATIVE TO OTHER STATE NOTICE ACTS

Security breach notice acts vary from state to state. Vermont's breach act contains the following variations:

- Definition of PII is broader than many states and includes biometric information, genetic information, and health information. *See* Sections 4 ("What is Personally Identifiable Information (or 'PII')?") and 16 ("Types of 'Personally Identifiable Information'").
- Login credential breaches require notice. *See* Sections 17 ("'Login Credentials'") and 31 ("Notice requirements for a login credential breach").
- Notification is triggered by acquisition or reasonable belief of acquisition, not access. *See* Section 14 ("'Acquisition'").
- A risk of harm analysis is permitted, but the results of that analysis must be shared with the AG if a data collector believes notice is not required due to no risk of harm. *See* Section 32 ("Security breach where data collector establishes misuse is not reasonably possible").
- 14-day Preliminary Notice to the AG is required. *See* Section 25 ("14-day Preliminary Notice").
- Consumer Notice must be provided to AG, as well as the number of Vermont consumers affected and the date of discovery. *See* Sections 25 ("14-day Preliminary Notice"), 27 ("Consumer Notice").
- Vermont Department of Financial Regulation must be notified for certain breaches. *See* Section 19 ("Notice to the Attorney General or Department of Financial Regulation").
- Substitute notice requires notification to Vermont media and is only available in limited circumstances. *See* Section 29 ("Methods of delivering Consumer Notice"), Appendix C.
- There is a 45-day outer limit on the notice deadline. *See* Sections 20 ("Deadlines"), 21 ("'Most expedient time possible and without unreasonable delay'").

- There is an encryption safe harbor. *See* Section 4 ("What is Personally Identifiable Information (or 'PII')?").
- The law only applies to electronic records, except in the case of PII maintained or possessed by a data collector who does business in Vermont. *See* Section 18 ("Who must be notified in the event of a security breach?").
- The Act does not contain a private right of action. *See* Section 37 ("Violations of the Act").

### 39. MULTISTATE BREACHES

Sometimes a breach will be significant enough that it is likely that many states will be interested in following up with further questions. In such circumstances, the States have a procedure for streamlining this process. If you believe it might be appropriate to have a discussion with all of the States at once, you can contact **AAG Matthew Van Hise, Privacy Unit Chief of the Illinois Attorney General's Office**, at **MVanHise@atg.state.il.us** or **(217) 782-4436**.

Engaging in a multistate process is often to the benefit of both businesses and the enforcement community, but it is not required of any business. Similarly, no State is required to cooperate in any given multistate process.

**Engaging with multistate stakeholders does not excuse you from your breach notice act obligations in Vermont or any other state, nor does it permit you to disregard correspondence or subpoenas issued by Vermont or any State.**

## COMMON QUESTIONS AND MISUNDERSTANDINGS

### 40. 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.

### 41. DISPUTES OVER "DISCOVERY DATE"

Probably the largest point of contention tends to be over the "discovery date" of a breach. This point comes up in two contexts. First, when the Office receives the AG notice required by 9 V.S.A. § 2435(b)(3), which requires disclosure of the discovery date. Second is in the determination as to whether a business has violated the Act by delaying the provision of Preliminary or Consumer notice.

As explained in Sections 8 ("What are my legal obligations to investigate a potential breach?") and 20 ("Deadlines"), our office begins counting deadlines from the first discovery or notification of the breach, which is the point at which a data collector has reason to begin investigating a breach. The data collector is expected to expediently investigate the breach, and then issue notice if necessary. We understand that there are some cases where this will necessarily take longer and are open to discussing reasonable delays.

The following dates are not considered appropriate "discovery dates:"

- The date that a forensic examiner completes its investigation and confirms the existence of a breach;
- The date that an investigation confirms that exfiltration of data occurred;
- Where hardware has been lost or stolen, the date that the data provider confirms that the hardware is not recoverable;
- Where a data provider is aware that a breach has occurred, the date that it confirms the identities of affected consumers; or

- Where a data provider is aware that a breach has occurred, the date that it confirms that a Vermonter was affected.

If you are not certain what the exact discovery date of a breach is, provide a timeline of events with all major developments and decision points. If the discovery date is left out of a letter or is overly vague, we will follow up and request this timeline.

## 42. DISPUTES OVER WHETHER A BREACH OCCURRED

A security breach has occurred when the data collector has a reasonable belief of unauthorized acquisition of data. This does not mean a belief to an existential certainty. Where log files or other evidence would be necessary to confirm that a breach happened are missing due to a business's failure to maintain the logs, businesses should err on the side of assuming a breach took place. Forensic examiners are often hesitant to state in definitive terms that a breach has occurred – the lack of such definitive terms is not evidence that a breach did not occur.

The risk a business undertakes when it chooses to err on the side of not reporting a breach is that evidence of the breach will later surface. The Office takes situations where a business fails to report a breach very seriously.

Businesses should be aware that the Office receives information relating to breaches that are not reported from numerous sources, including law enforcement, financial institutions, independent contractors, independent forensics firms, vendors, bloggers, and whistleblowers.

Finally, if there is a genuine concern as to whether or not a breach has occurred or who was affected, if the following is in fact accurate, it is acceptable to issue notice with language to the effect of: **"We are unable to confirm that a security breach took place or that you were affected, but we are sending this notice to you in an abundance of caution."**

*See also* Section 7 ("What if I'm not sure whether I've had a Security Breach?").

## 43. BREACHES INVOLVING MULTIPLE PARTIES

It is sometimes the case where multiple parties have responsibility for the PII involved in a security breach. It could be a retailer who outsources its point of sale (POS) system, a hotel that outsources its reservation system, a business that contracts with a payroll firm, or any number of combinations. Occasionally we see a situation where a vendor experiences a breach and, claiming that they do not "own or license" the data, argues that they have no responsibility to notify consumers.

Where parties point fingers at each other and deny responsibility to provide notice, consumers suffer. Where a vendor suffers a breach and requires dozens of customers to issue multiple notices to the same consumers for the same breach, consumers suffer.

The Office's position is that the definition of "maintains or possesses" is very narrow. *See* Section 12 ("'Maintains or possesses'"). Most businesses that experience a breach will have a first-party obligation to notify consumers. However, where there is a breach in which multiple parties have in any way owned, licensed, controlled, processed, or otherwise interacted with the data that was subject to the breach, all parties have an obligation to ensure that consumers are notified. That does not mean all parties must issue the notice, only that notice should be issued by someone, and if no notice is issued, all parties involved may be held responsible.

We recommend that the parties address this issue by specifying through contract the roles and responsibilities each party has in the event of a breach, regardless of whose system the breach takes place on. It may be that the party with the direct relationship with consumers wants to issue the notice, but the logistics and financing of the notice will be paid by a different party. So long as consumers are notified by one of the parties, the Act is satisfied.

Note also that any contractual waiver of responsibilities required by the Act, "is contrary to public policy and is void and unenforceable."[liii]

Finally, where multiple parties are involved in a breach, we expect that all parties will provide full cooperation in responding to the breach, particularly where information required to issue notice (like customer or address lists) is in the possession of different parties. Failure to do so could be considered a violation of the Act and/or the Consumer Protection Act.

## 44. WHERE THE IDENTITY OR STATE OF RESIDENCE OF THE CONSUMERS IS UNCLEAR

Sometimes a breach will occur where the business has no way of identifying affected consumers, knowing whether a Vermont resident is involved or identifying consumers and/or their residency of the affected consumers would unduly delay notice.

Businesses should use common sense in determining which states to notify. A restaurant located in West Lebanon, NH (on the Vermont border) that has a credit card breach probably had Vermont customers. If those customers are unidentifiable, substitute notice should be issued. At the very least, 14-day preliminary notice should be provided to our Office so we can discuss the best way to go about notifying consumers.

If a business wants to issue direct notice and the delay is based on identifying consumers, notice should be ready to go out as soon as customers are identified, and reasonable efforts should be made to expediently identify consumers. Again, 14-day preliminary notice can help ensure that the business is in compliance with the law, if there is a likelihood Vermonters were affected.

If a business knows that the residency of affected consumers will create undue delay, we recommend the business strongly consider notifying the AG's office in their state of residence, and consider issuing substitute notice at least in that state, in accordance with that state's laws. This will at least demonstrate that the business was attempting to act diligently to provide notice in a timely manner.

## 45. DELAY IN PROVIDING NOTICE

Where a business has experienced delay in providing notice due to difficulty in identifying the breach, in determining whether or what PII was involved, or identifying affected consumers, it is expected that once these issues are resolved, it will immediately issue notice. A business that takes three months to investigate a breach might be able to argue the delay was justified. A business that takes three months to investigate and identify consumers and then takes another month to issue notice, has violated the Act.

Often, the decision whether or not to investigate a potential violation comes down to how diligent the business appears to be in complying with the Act. One way a company can demonstrate diligence is by complying with the 14-day notice requirement and cooperating with any initial requests for clarification.

## 46. BREACHES INVOLVING UNSTRUCTURED DATA

Breaches involving unstructured data (often various file types on a file server, or email accounts), can take longer to investigate because it may be unclear whether PII was involved, if any, and who was affected, if anyone. In the event of such a breach, the data collector still has an obligation to expediently investigate the breach, and should deploy any technologies available to assist in searching for PII, within reason relative to the size and sophistication of the business, and the nature of the data involved. Where a business takes a long time to report an unstructured data breach because they did not to take advantage of available technology, it may have violated the Act.

Given the nature of data security, businesses might consider implementing policies prohibiting the collection, storage, and transfer of PII, particularly social security numbers, financial account numbers, and passwords, in unencrypted files or via email.

## 47. BREACHES INVOLVING RANSOMWARE

By their nature, it can be difficult to determine whether data has been exfiltrated in a ransomware attack. Not all ransomware attacks result in a security breach. The key question is what type of ransomware is involved. If it is of the type that solely encrypts your hard drives, then would probably not be considered a security breach, absent additional indicia that data was acquired. If the ransomware is of the type that is known to move, exfiltrate, or otherwise acquire the data, or that permits bad actors further access to your systems, then you should presume a breach has occurred absent strong positive evidence to the contrary. If you determine that a breach has not occurred, you should thoroughly document the decision in the event that your determination is later called into question.

# APPENDIX 1: PROCEDURES BEFORE AND DURING A BREACH

## 48. BEFORE: AVOIDING AND PREPARING FOR A BREACH

- Resources for implementing data security and responding data breaches can be found on the FTC Website and elsewhere at
    - https://www.ftc.gov/tips-advice/business-center/small-businesses/cybersecurity and
    - https://www.ftc.gov/tips-advice/business-center/privacy-and-security/data-security.
    - https://www.ftc.gov/system/files/documents/plain-language/pdf-0154_data-breach-response-guide-for-business-042519-508.pdf.
    - https://www.us-cert.gov/sites/default/files/recommended_practices/NCCIC_ICS-CERT_Defense_in_Depth_2016_S508C.pdf
- The common wisdom is that security breaches are not a question of "if" but of "when" – you should have a data security response plan in place which should include, at minimum:
    - A designated single point person who will oversee the incident response;
    - The employees who will be involved in the incident response team;
    - Any third parties, contractors, and outside vendors who will be involved in breach response (including contact information), such as:
        - Your legal counsel;
        - Your cyber insurance provider;
        - A forensic investigation firm;
        - A breach notice vendor; and
        - Possibly, a public relations firm;
    - A list of law enforcement (state and federal) and regulatory agencies that may require notification in the event of a breach;
    - A list of other parties that you may be contractually obligated to notify in the event of a breach;
    - Clearly delineated roles, responsibilities, and required actions that each individual is required to take in the event of a breach.

  The breach response plan should be available in hard copy. You might consider conducting a "tabletop exercise" to game out how a security breach would be handled.
- Take a data inventory. Know what data you collect and where it is stored. This will help you determine whether PII has been acquired in the event of a breach.
- You can't lose what you don't have. Consider whether it is necessary that you collect different kinds of PII and avoid collecting it if you don't have to. Implement retention policies whereby you delete PII after a specified period of time. Data minimization is one of the best things you can do to avoid a breach.
- Invest in intrusion detection systems. Even if you experience a breach, if you catch it early enough you might be able to minimize the fallout.

- Consider investing in a log aggregator and/or security information and event management (SIEM) tool.
- Conduct periodic proactive security audits and vulnerability assessments. These can not only help prevent breaches, they can help discover breaches as well.
- Place a login banner to ensure that unauthorized users are warned that they may be subject to monitoring.
- Consider installing caller identification.
- Business Email Compromises are often very difficult to investigate because they involve unstructured data. Email systems are frequently targeted and often vulnerable. Implement policies that your employees not transmit PII via business email. Email systems with end-to-end encryption are more secure but will still be vulnerable if credentials are acquired.
- Security breaches can be expensive, and you may not want to reinvent the wheel in the event of a breach. You should strongly consider obtaining cyber insurance.

## 49. AFTER: UPON DISCOVERING A BREACH

- Contact:
    - law enforcement. *See* Sections 23 ("Contacting law enforcement"), 50 ("Reporting a Security Breach to law enforcement").
    - your cyber insurance provider if you have one
    - breach counsel if you have one
- Turn audit trails on.
- Secure log files
- Consider keystroke level monitoring if adequate banner is displayed.
- Request trap and tracing from your local telephone company.
- 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.

## 50. 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, email address, and phone number(s) of the reporting person.
- Name, address, email address, and phone number(s) of the Information Security Officer (ISO).
- Name, address, email 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).

## 51. INCIDENT RESPONSE DOS AND DON'TS

### DO:

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 email traffic.
3. Immediately notify appropriate law enforcement agencies.
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'T:

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.

   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.

2. 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.

3. 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 |

4. 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).

5. 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://ago.vermont.gov/. Another helpful source is the Federal Trade Commission website, available at https://www.consumer.ftc.gov/features/feature-0014-identity-theft.

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* Section 29 ("Methods of delivering Consumer 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

## APPENDIX 4 – TEXT OF THE SECURITY BREACH NOTICE ACT, 9 V.S.A. §§ 2430, 2435

### SECTION 2430. DEFINITIONS

(9) “Login credentials” means a consumer’s user name or e-mail address, in combination with a password or an answer to a security question, that together permit access to an online account.

(10)(A) "Personally identifiable information" means a consumer's first name or first initial and last name in combination with one or more of the following digital data elements, when either the name or the data elements are not encrypted, redacted or protected by another method that renders them unreadable or unusable by unauthorized persons:

(i) Social Security number;

(ii) a driver license or nondriver State identification card number, individual taxpayer identification number, passport number, military identification card number, or other identification number that originates from a government identification document that is commonly used to verify identity for a commercial transaction;

(iii) financial account number or credit or debit card number, if the number could be used without additional identifying information, access codes, or passwords;

(iv) a password, personal identification number, or other access code for a financial account.

(v) unique biometric data generated from measurements or technical analysis of human body characteristics used by the owner or licensee of the data to identify or authenticate the consumer, such as a fingerprint, retina or iris image, or other unique physical representation or digital representation of biometric data;

(vi) genetic information; and

(vii)(I) health records or records of a wellness program or similar program of health promotion or disease prevention;

(II) a health care professional’s medical diagnosis or treatment of the consumer; or

(III) a health insurance policy number.

(B) "Personally identifiable information" does not mean publicly available information that is lawfully made available to the general public from federal, State, or local government records.

(13)(A) "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 or login credentials maintained by a data collector.

(B) "Security breach" does not include good faith but unauthorized acquisition of personally identifiable information or login credentials by an employee or agent of the data collector for a legitimate purpose of the data collector, provided that the personally identifiable information or login credentials are not used for a purpose unrelated to the data collector's business or subject to further unauthorized disclosure.

(C) In determining whether personally identifiable information or login credentials have been acquired or is reasonably believed to have been acquired by a person without valid authorization, a data collector may consider the following factors, among others:

(i) 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;

(ii) indications that the information has been downloaded or copied;

(iii) indications that the information was used by an unauthorized person, such as fraudulent accounts opened, or instances of identity theft reported; or

(iv) that the information has been made public.

## SECTION 2435. NOTICE OF SECURITY BREACHES

(a) This section shall be known as the Security Breach Notice Act.

(b) Notice of breach.

(1) Except as otherwise provided in subsection (d) of this section, any data collector that owns or licenses computerized personally identifiable information or login credentials shall notify the consumer that there has been a security breach following discovery or notification to the data collector of the breach. Notice of the security breach shall be made in the most expedient time possible and without unreasonable delay, but not later than 45 days after the discovery or notification, consistent with the legitimate needs of the law enforcement agency, as provided in subdivisions (3) and (4) of this subsection (b), or with any measures necessary to determine the scope of the security breach and restore the reasonable integrity, security, and confidentiality of the data system.

(2) Any data collector that maintains or possesses computerized data containing personally identifiable information or login credentials that the data collector does not own or license or any data collector that acts or conducts business in Vermont that maintains or possesses records or data containing personally identifiable information or login credentials that the data collector does not own or license shall notify the owner or licensee of the information of any security breach immediately following discovery of the breach, consistent with the legitimate needs of law enforcement as provided in subdivisions (3) and (4) of this subsection (b).

(3) A data collector or other entity subject to this subchapter shall provide notice of a breach to the Attorney General or to the Department of Financial Regulation, as applicable, as follows:

(A) A data collector or other entity regulated by the Department of Financial Regulation under Title 8 or this title shall provide notice of a breach to the Department. All other data collectors or other entities subject to this subchapter shall provide notice of a breach to the Attorney General.

(B)(i) The data collector shall notify the Attorney General or the Department, as applicable, of the date of the security breach and the date of discovery of the breach and shall provide a preliminary description of the breach within 14 business days, consistent with the legitimate needs of the law enforcement agency as provided in this subdivision (3) and subdivision (4) of this subsection (b), of the data collector's discovery of the security breach or when the data collector provides notice to consumers pursuant to this section, whichever is sooner.

(ii) Notwithstanding subdivision (B)(i) of this subdivision (b)(3), a data collector who, prior to the date of the breach, on a form and in a manner prescribed by the Attorney General, had sworn in writing to the Attorney General that it maintains written policies and procedures to maintain the security of personally identifiable information or login credentials and respond to a breach in a manner consistent with Vermont

law shall notify the Attorney General of the date of the security breach and the date of discovery of the breach and shall provide a description of the breach prior to providing notice of the breach to consumers pursuant to subdivision (1) of this subsection (b).

(iii) If the date of the breach is unknown at the time notice is sent to the Attorney General or to the Department, the data collector shall send the Attorney General or the Department the date of the breach as soon as it is known.

(iv) Unless otherwise ordered by a court of this State for good cause shown, a notice provided under this subdivision (3)(B) shall not be disclosed to any person other than the Department, the authorized agent or representative of the Attorney General, a State's Attorney, or another law enforcement officer engaged in legitimate law enforcement activities without the consent of the data collector.

(C)(i) When the data collector provides notice of the breach pursuant to subdivision (1) of this subsection (b), the data collector shall notify the Attorney General or the Department, as applicable, of the number of Vermont consumers affected, if known to the data collector, and shall provide a copy of the notice provided to consumers under subdivision (1) of this subsection (b).

(ii) The data collector may send to the Attorney General or the Department, as applicable, a second copy of the consumer notice, from which is redacted the type of personally identifiable information or login credentials that was subject to the breach, and which the Attorney General or the Department shall use for any public disclosure of the breach.

(D) If a security breach is limited to an unauthorized acquisition of login credentials, a data collector is only required to provide notice of the security breach to the Attorney General or Department of Financial Regulation, as applicable, if the login credentials were acquired directly from the data collector or its agent.

(4)(A) The notice to a consumer required by this subsection shall be delayed upon request of a law enforcement agency. A law enforcement agency may request the delay if it believes that notification may impede a law enforcement investigation, or a national or Homeland Security investigation or jeopardize public safety or national or Homeland Security interests. In the event law enforcement makes the request for a delay in a manner other than in writing, the data collector shall document such request contemporaneously in writing, including the name of the law enforcement officer making the request and the officer's law enforcement agency engaged in the investigation. A law enforcement agency shall promptly notify the data collector in writing when the law enforcement agency no longer believes that notification may impede a law enforcement investigation, or a national or Homeland Security investigation or jeopardize public safety or national or Homeland Security interests. The data collector shall provide notice required by this section without unreasonable delay upon receipt of a written communication, which includes facsimile or electronic communication, from the law enforcement agency withdrawing its request for delay.

(B) A Vermont law enforcement agency with a reasonable belief that a security breach has or may have occurred at a specific business shall notify the business in writing of its belief. The agency shall also notify the business that additional information on the security breach may need to be furnished to the Office of the Attorney General or the Department of Financial Regulation and shall include the website and telephone number for the Office and the Department in the notice required by this subdivision. Nothing in this subdivision shall alter the responsibilities of a data collector under this section or provide a cause of action against a law enforcement agency that fails, without bad faith, to provide the notice required by this subdivision.

(5) The notice to a consumer required in subdivision (1) of this subsection (b) shall be clear and conspicuous. A notice to a consumer of a security breach involving personally identifiable information shall include a description of each of the following, if known to the data collector:

(A) the incident in general terms;

(B) the type of personally identifiable information that was subject to the security breach;

(C) the general acts of the data collector to protect the personally identifiable information from further security breach;

(D) a telephone number, toll-free if available, that the consumer may call for further information and assistance;

(E) advice that directs the consumer to remain vigilant by reviewing account statements and monitoring free credit reports; and

(F) the approximate date of the security breach.

(6) A data collector may provide notice of a security breach involving personally identifiable information to a consumer by one or more of the following methods:

(A) Direct notice, which may be by one of the following methods:

(i) written notice mailed to the consumer's residence;

(ii) electronic notice, for those consumers for whom the data collector has a valid e-mail address if:

(I) the data collector's primary method of communication with the consumer is by electronic means, the electronic notice does not request or contain a hypertext link to a request that the consumer provide personal information, and the electronic notice conspicuously warns consumers not to provide personal information in response to electronic communications regarding security breaches; or

(II) the notice is consistent with the provisions regarding electronic records and signatures for notices in 15 U.S.C. § 7001; or

(iii) telephonic notice, provided that telephonic contact is made directly with each affected consumer and not through a prerecorded message.

(B)(i) Substitute notice, if:

(I) the data collector demonstrates that the lowest cost of providing notice to affected consumers pursuant to subdivision (6)(A) of this subsection among written, e-mail, or telephonic notice would exceed $10,000.00; or

(II) the data collector does not have sufficient contact information.

(ii) A data collector shall provide substitute notice by:

(I) conspicuously posting the notice on the data collector's website if the data collector maintains one; and

(II) notifying major statewide and regional media.

(c) In the event a data collector provides notice to more than 1,000 consumers at one time pursuant to this section, the data collector shall notify, without unreasonable delay, all consumer reporting agencies that compile and maintain files on consumers on a nationwide basis, as defined in 15 U.S.C. § 1681a(p), of the timing, distribution, and content of the notice. This subsection shall not apply to a person who is licensed or registered under Title 8 by the Department of Financial Regulation.

(d)(1) Notice of a security breach pursuant to subsection (b) of this section is not required if the data collector establishes that misuse of personally identifiable information or login credentials is not reasonably possible and the data collector provides notice of the determination that the misuse of the personally identifiable information or login credentials is not reasonably possible pursuant to the requirements of this subsection (d). If the data collector establishes that misuse of the personally identifiable information or login credentials is not reasonably possible, the data collector shall provide notice of its determination that misuse of the personally identifiable information or login credentials is not reasonably possible and a detailed explanation for said determination to the Vermont Attorney General or to the Department of Financial Regulation in the event that the data collector is a person or entity licensed or registered with the Department under Title 8 or this title. The data collector may designate its notice and detailed explanation to the Vermont Attorney General or the Department of Financial Regulation as "trade secret" if the notice and detailed explanation meet the definition of trade secret contained in 1 V.S.A. § 317(c)(9).

(2) If a data collector established that misuse of personally identifiable information or login credentials was not reasonably possible under subdivision (1) of this subsection (d), and subsequently obtains facts indicating that misuse of the personally identifiable information or login credentials has occurred or is occurring, the data collector shall provide notice of the security breach pursuant to subsection (b) of this section.

(3) If a security breach is limited to an unauthorized acquisition of login credentials for an online account other than an e-mail account the data collector shall provide notice of the security breach to the consumer electronically or through one or more of the methods specified in subdivision (b)(6) of this section and shall advise the consumer to take steps necessary to protect the online account, including to change his or her login credentials for the account and for any other account for which the consumer uses the same login credentials.

(4) If a security breach is limited to an unauthorized acquisition of login credentials for an email account:

(A) the data collector shall not provide notice of the security breach through the email account; and

(B) the data collector shall provide notice of the security breach through one or more of the methods specified in subdivision (b)(6) of this section or by clear and conspicuous notice delivered to the consumer online when the consumer is connected to the online account from an Internet protocol address or online location from which the data collector knows the consumer customarily accesses the account.

(e) A data collector that is subject to the privacy, security, and breach notification rules adopted in 45 C.F.R. Part 164 pursuant to the federal Health Insurance Portability and Accountability Act, P.L. 104-191 (1996) is deemed to be in compliance with this subchapter if:

(1) the data collector experiences a security breach that is limited to personally identifiable information specified in 2430(10)(A)(vii); and

(2) the data collector provides notice to affected consumers pursuant to the requirements of the breach notification rule in 45 C.F.R. Part 164, Subpart D.

(f) Any waiver of the provisions of this subchapter is contrary to public policy and is void and unenforceable.

(g) Except as provided in subdivision (3) of this subsection (f), 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 (f) 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.

(g) Enforcement.

(1) With respect to all data collectors and other entities subject to this subchapter, other than a person or entity licensed or registered with the Department of Financial Regulation under Title 8 or this title, the Attorney General and State's Attorney shall have sole and full authority to investigate potential violations of this subchapter and to enforce, prosecute, obtain, and impose remedies for a violation of this subchapter or any rules or regulations made pursuant to this chapter as the Attorney General and State's Attorney have under chapter 63 of this title. The Attorney General may refer the matter to the State's Attorney in an appropriate case. The Superior Courts shall have jurisdiction over any enforcement matter brought by the Attorney General or a State's Attorney under this subsection.

(2) With respect to a data collector that is a person or entity licensed or registered with the Department of Financial Regulation under Title 8 or this title, the Department of Financial Regulation shall have the full authority to investigate potential violations of this subchapter and to prosecute, obtain, and impose remedies for a violation of this subchapter or any rules or regulations adopted pursuant to this subchapter, as the Department has under Title 8 or this title or any other applicable law or regulation.

---

[i] 9 V.S.A. § 2430(6)

[ii] 9 V.S.A. § 2435(b)(1)

[iii] 9 V.S.A. § 2430(13)

[iv] 9 V.S.A. §§ 2430(10) and 2430(13)

[v] Prior to these amendments, the only government identification numbers included in PII were Social Security Number and motor vehicle operator's license number or nondriver identification card number.

[vi] Prior to these amendments, substitute notice was permitted where the cost of Direct Notice via writing or telephone would exceed $5,000, more than 5,000 consumers would be receiving notice, or the data collector does not have sufficient contact information.

[vii] 9 V.S.A. § 2435(b)(3)

[viii] 9 V.S.A. § 2435(b)(1)

[ix] 9 V.S.A. § 2435(c)

[x] 9 V.S.A. § 2430(13)

[xi] 9 V.S.A. § 2435(b)(1)

[xii] 9 V.S.A. § 2435(b)(2)

[xiii] *Id.*

[xiv] 9 V.S.A. § 2435(d)(1)

[xv] 9 V.S.A. § 2435(b)(1)

[xvi] 9 V.S.A. § 2435(b)(2)

[xvii] 9 V.S.A. § 2435(b)(1)

[xviii] 9 V.S.A. § 2430(10)(A)(ii)

[xix] 9 V.S.A. § 2430(10)(A)(v)

[xx] 9 V.S.A. § 2435(e)

[xxi] 9 V.S.A. § 2430(9)

[xxii] 9 V.S.A. § 2435(b)(3)

[xxiii] 9 V.S.A. § 2435(g)(3)

[xxiv] 9 V.S.A. § 2435(b)(1)

[xxv] 9 V.S.A. § 2435(b)(2)

[xxvi] 9 V.S.A. § 2435(b)

[xxvii] 9 V.S.A. § 2435(b)(3)(B)

[xxviii] 9 V.S.A. § 2435(b)(1)

[xxix] 9 V.S.A. § 2435(b)(4)

[xxx] 9 V.S.A. § 2435(b)(3)(C)(ii)

[xxxi] 9 V.S.A. § 2435(b)(3)(C)

[xxxii] 9 V.S.A. § 2435(b)(1)

[xxxiii] 9 V.S.A. § 2435(4)

[xxxiv] 9 V.S.A. § 2435 (b)(3)(B)(ii)

[xxxv] 9 V.S.A. § 2435(b)(3)(C)(ii)

[xxxvi] 9 V.S.A. § 2435(d)(1)

[xxxvii] 9 V.S.A. § 2435(b)(5)

[xxxviii] 9 V.S.A. § 2435(b)(6)(A)

[xxxix] 9 V.S.A. § 2435(b)(6)(B)

[xl] 9 V.S.A. § 2435(b)(6)(A)(ii)

[xli] 9 V.S.A. § 2435(d)(4)

[xlii] 9 V.S.A. § 2435(b)(3)(D)

[xliii] 9 V.S.A. § 2435(d)(1)

[xliv] *Id.*

[xlv] 9 V.S.A. § 2435(d)(2)

[xlvi] 9 V.S.A. § 2435(b)(3)(B)(iv)

[xlvii] 9 V.S.A. § 2435(g)

[xlviii] 9 V.S.A. § 2430(6)

[xlix] 9 V.S.A. § 2430(4)

[l] 9 V.S.A. § 2430(1)

[li] https://ago.vermont.gov/wp-content/uploads/2018/12/2018-12-11-VT-Data-Broker-Regulation-Guidance.pdf

[lii] 9 V.S.A. § 2435(h)

[liii] 9 V.S.A. § 2435(f)