DRM Downs Rachlin Martin PLLC
Business Sense · Legal Ingenuity

Road Map to the Vermont Security Breach Notice Act (9 V.S.A § 2435)

Part 1 – Does the Act Apply?

STEP 1
Are you a data collector?

If yes, continue to Step 2
If no, the Act does not apply

You are a data collector if, for any purpose and by any means, you:

- Handle
- Collect
- Disseminate, or
- Otherwise deal with…

…Consumers' (Vermont residents) **"personally identifiable information" ("PII")** that is (a) not publicly available and (b) not encrypted, redacted or otherwise protected from unauthorized view or use.

PII includes a person's first name (or initial) and last name **in combination with** any of these:

- Social Security number
- Driver's license number
- Non-driver ID card number
- Financial account number
- Credit or debit card number
- Financial account access code (e.g., PIN)

STEP 2
Do you own or license computerized data containing PII? Do you maintain or possess any records or computerized data containing PII that you don't own or license?

If yes to any, continue to Step 3
If no, the Act does not apply

STEP 3 Have you had a "security breach"?

If yes, continue to Step 4
If no, the Act does not apply

A security breach is defined as:

An 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 PII.

To determine if you've had a security breach, you may consider factors such as:

- Whether the data is in the physical possession and control of an unauthorized person (e.g. lost/stolen computer or device)
- Whether the data has been downloaded or copied
- Whether the data was used by an unauthorized person (e.g., instances of identity theft have been reported)
- Whether the data has been made public.

NOTE: A "security breach" does not include an unauthorized acquisition of PII by your employee or someone acting on your behalf, as long as:

- The acquisition was in good faith
- The acquisition was for a legitimate purpose of yours
- The PII is not used for a purpose unrelated to your business, and
- The PII is not subject to further unauthorized disclosure.

DRM Downs Rachlin Martin PLLC
Business Sense · Legal Ingenuity

Road Map to the Vermont Security Breach Notice Act (9 V.S.A § 2435)

Part 2 – What Notice Requirements Apply?

STEP 4
Is there a reasonable possibility of misuse of any PII acquired in the security breach?

If no

If yes, continue to Step 5

You don't need to provide notices required by Section 2435(b),

But:

- If you are licensed or registered with the Department of Financial Regulation under Titles 8 or 9 of the VT Statutes, you must inform the Department that you have had a security breach but have determined that misuse of PII is not reasonably possible, and must provide a detailed explanation for your determination. Otherwise, you must provide this information to the VT Attorney General.
- If you later learn that misuse of PII has occurred or is occurring, you must provide the notices required by Section 2435(b).

STEP 5
You must provide the notices required by the Act.

If you own or license computerized data containing PII:

Notify affected **consumers** as quickly as possible, **but no later than 45 days** after you discover or are notified of the breach.

NOTE: You may delay the required notice if you are requested to do so by a law enforcement agency.

The notice to consumers may be made directly via written, telephonic (but not prerecorded) or electronic means. If you can demonstrate that the cost of providing notice would exceed $5,000 or the number of affected consumers exceeds 5,000, or if you don't have sufficient contact information, you may provide "substitute" notice through a conspicuous posting on your website **and** notification to major media.

The notice to consumers must be **clear and conspicuous**, and must include the following, if known:

- A description of the breach including the approximate date and the type of PII that was subject to the breach;
- A description of your general actions to protect the PII from further breaches;
- A telephone number consumers may call for further information and assistance; and
- Advice directing consumers to remain vigilant by reviewing account statements and monitoring free credit reports.

If you maintain or possess any records or computerized data containing PII that you don't own or license:

Notify the **owner or licensee** of the PII **immediately** after you discover or are notified of the security breach. (The owner or licensee must provide the notice described earlier.)

Other required notices

Preliminary notice to Vermont agencies:

- If you are licensed or registered with the Department of Financial Regulation under Titles 8 or 9 of the VT Statutes, notify the Department of the breach. Otherwise, notify the VT Attorney General.
- The notice must include date of the breach, date of discovery of the breach, description of the breach (including number of Vermont consumers affected, if known), and a copy of the notice provided to consumers. If you don't yet know the date of the breach, you must provide that to the Department or Attorney General as soon as it is known.
- Make the notice to the Department or Attorney General **within 14 business days** after you discover the breach, or at the same time notice of the breach is provided to consumers, **whichever is sooner.** (EXCEPTION: In one circumstance you must notify the Attorney General before notifying consumers.)

Notice to credit reporting agencies:

- If you need to provide notice to more than 1,000 consumers for a breach, you must also promptly notify all national consumer credit reporting agencies (Equifax, Experian, and TransUnion) of the timing, distribution and content of the consumer notice.