

VERMONT

IDENTITY THEFT RANKING BY STATE: Rank 47, 38.1 Complaints Per 100,000
Population, 237 Complaints (2007)
Updated December 30, 2008

Current Laws: Under state law, no person shall obtain, produce, possess, use, sell, give, or transfer personal identifying information belonging or pertaining to another person with intent to use the information to commit a misdemeanor or a felony. In addition, no person shall knowingly or recklessly obtain, produce, possess, use, sell, give, or transfer personal identifying information belonging or pertaining to another person without consent, or knowingly or recklessly facilitate the use of the information by a third person to commit a misdemeanor or a felony. Violators will face up to three years in prison and/or a fine up to \$5000. Second or subsequent violations will result in up to ten years in prison and/or a fine of up to \$10,000.

Personal identifying information includes name, address, birth date, Social Security number, motor vehicle personal identification number, telephone number, financial services account number, savings account number, checking account number, credit card number, debit card number, picture, identification document or false identification document, electronic identification number, educational record, health care record, financial record, credit record, employment record, e-mail address, computer system password, or mother's maiden name, or similar personal number, record, or information.

These provisions do not apply when a person obtains the personal identifying information belonging or pertaining to another person to misrepresent the person's age for the sole purpose of obtaining alcoholic beverages, tobacco, or another privilege denied based on age.

Statute: 13 § 2030:

<http://www.leg.state.vt.us/statutes/fullsection.cfm?Title=13&Chapter=047&Section=02030>

Payment Cards: It is unlawful for a person, with intent to defraud, to obtain or attempt to obtain money, property, services or any other thing of value, by the use of a credit card that he knows, or reasonably shall have known, to have been stolen, forged, revoked, cancelled, unauthorized or invalid for use by him for such purpose.

Violations are punishable by imprisonment of up to six months and/or a fine up to \$500 if the aggregate value of the money, property, services or other things of value obtained is \$50 or less. If the value is over \$50, it is punishable by up to one year in jail and/or a fine up to \$1000.

Possessing a credit card issued to another person, with the intent to use the credit card without the consent of the cardholder, is punishable by up to six months in jail and/or a fine up to \$500. A law enforcement officer who finds a credit card in the possession of a person other than the cardholder must seize the card unless it is affirmatively made to appear that an unauthorized use

of the card is not intended. A card seized under such circumstances must be returned to the card issuer at such time as it may not be needed as material or relevant evidence for prosecution.

Statute: 9 § 4041 – 4045:

<http://www.leg.state.vt.us/statutes/fullchapter.cfm?Title=09&Chapter=105>

State law requires credit card issuers that mail solicitations and receive a completed application with a different address from the solicitation to verify the change of address.

Statute: 9 § 24801:

<http://www.leg.state.vt.us/statutes/fullsection.cfm?Title=09&Chapter=063&Section=02480>

Social Security Numbers: State law provides protections on Social Security numbers (SSN).

Under the law, businesses and state and local governments may not:

- Intentionally communicate or otherwise make available to the general public an individual's Social Security number;
- Intentionally print or imbed a SSN on any card required for the individual to access products or services;
- Require an individual to transmit his/her SSN over the Internet unless the connection is secure or the SSN is encrypted;
- Require an individual to use his/her SSN to access a web site, unless a password or unique personal identification number or other authentication device is also required to access the internet website;
- Print an individual's SSN on any materials that are mailed to the individual, unless state or federal law requires the number to be on the document to be mailed; or
- Sell, lease, lend, trade, rent, or otherwise intentionally disclose an individual's Social Security number to a third party without written consent to the disclosure from the individual, when the party making the disclosure knows or in the exercise of reasonable diligence would have reason to believe that the third party lacks a legitimate purpose for obtaining the individual's Social Security number.

In addition, state and local governments may not collect a SSN from an individual unless authorized or required by law, state or federal regulation or grant agreement to do so, unless the collection is related to the performance of the agency's duties and responsibilities. SSNs must also be redacted before the document is posted on a Web site.

However, if a business or government agency has previously used an individual's SSN in a manner inconsistent with these provisions prior to January 1, 2007, it may continue using the SSN if the following conditions are met:

- The use of the SSN must be continuous. If its use is stopped for any reason, the provisions will apply.
- The individual is provided an annual disclosure that informs him/her that he/she has the right to stop the use of his or her Social Security number in a manner prohibited by the law.
- A written request by an individual to stop the use of his or her Social Security number is implemented within 30 days of the receipt of the request. There may not be a fee or charge for implementing the request.
- The business does not deny services to an individual because the individual makes a written request pursuant to this subsection.

Statute: 9 § 2440:

<http://www.leg.state.vt.us/statutes/fullsection.cfm?Title=09&Chapter=062&Section=02440>

Disposal of Records: To prevent identity theft, state law restricts how businesses can dispose of paper records with personal identifying information about individuals. The law requires businesses to take all reasonable steps to destroy or arrange for the destruction of a customer's records within its custody or control containing personal information which is no longer to be retained by the business by shredding, erasing, or otherwise modifying the personal information in those records to make it unreadable or indecipherable.

The law defines personal identifying information as the following information that identifies, relates to, describes, or is capable of being associated with a particular individual: his/her signature, Social Security number, physical characteristics or description, passport number, driver's license or state identification card number, insurance policy number, bank account number, credit card number, debit card number, or any other financial information.

Statute: 9 § 2445:

<http://www.leg.state.vt.us/statutes/fullsection.cfm?Title=09&Chapter=062&Section=02445>

Victim Assistance:

Mandatory Police Reports: Under state law, a person who has learned or reasonably suspects that his or her personal identifying information has been unlawfully used by another may make a complaint about the unlawful use to the state police or the person's local law enforcement agency. Even if the jurisdiction lies elsewhere for investigation and prosecution, the agency must take the complaint and provide the complainant with a copy of the complaint. The report must contain the name of the officer taking the complaint and an incident or case number assigned to the complaint. If the suspected crime was committed in another jurisdiction, may refer the complaint to a law enforcement agency in a different jurisdiction.

Statute: 9 § 2480k:

<http://www.leg.state.vt.us/statutes/fullsection.cfm?Title=09&Chapter=063&Section=02480k>

Credit Files of Deceased Persons: State law permits an executor, administrator, or other person authorized to act on behalf of an estate of a deceased person to request that a credit reporting agency indicate on the deceased person's credit reporting file that the person is deceased.

Statute: 9 § 2480n:

<http://www.leg.state.vt.us/statutes/fullsection.cfm?Title=09&Chapter=063&Section=02480n>

Security Freeze: State law allows all consumers to place security freezes on their consumer credit reports to prevent identity thieves from opening new accounts in their names. Such a freeze enables the consumer to prevent anyone from looking at his/her credit file for the purpose of granting credit unless the consumer chooses to allow a particular business look at the information. To request a freeze, a consumer must request one in writing by certified mail or by a secure e-mail connection (if provided) to the credit reporting agencies. A credit reporting agency may charge up to \$10 to place the freeze, although there is no charge for victims of identity theft with a valid police report or other complaint. The agencies may charge a \$5 fee for temporarily unlocking the freeze, but again, victims may not be charged.

The reporting agency must place the freeze within five business days after receiving the request, and within ten days of placing the freeze must send a written confirmation of the freeze and provide the consumer with a unique personal identification number or password to be used when providing authorization for the release of credit information for a specific party or period of time. Requests for a temporary unlocking of the freeze must be completed within three business days. Statute: 9 § 2480h:

<http://www.leg.state.vt.us/statutes/fullsection.cfm?Title=09&Chapter=063&Section=02480h>

Office of the Attorney General, “How to Freeze Your Credit Files”

(http://www.atg.state.vt.us/upload/1152194966_How_to_Freeze_your_Credit_Files.pdf)

Security Breach: State law requires state and local government agencies and businesses operating in the state that collect and maintain computerized records containing consumers’ personal information to notify consumers when their personal information is compromised during a security breach, putting them at risk of identity theft. A security breach occurs upon “unauthorized acquisition or access of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by the data collector.”

Personal identifying information is defined as an individual’s first name or first initial and last name in combination with one or more of the following data elements, when either the name or the data elements are not encrypted or redacted or protected by another method that renders them unreadable or unusable by unauthorized persons: Social Security number, motor vehicle operator’s license number, or financial account or credit or debit card number in combination with any required access code. Publicly available information is not included.

Disclosure must occur to any resident of the state whose personal information was, or is reasonably believed to have been, accessed by an authorized person. The disclosure must be made in the most expedient time possible, and without unreasonable delay, consistent with legitimate needs of law enforcement. The notice must include a description of the following: the incident in general terms; the type of personal information that was subject to the unauthorized access or acquisition; the general acts of the business to protect the personal information from further unauthorized access or acquisition; a toll-free telephone number that the consumer may call for further information and assistance; and advice that directs the consumer to remain vigilant by reviewing account statements and monitoring free credit reports.

Notification can be provided to the affected persons by mail, e-mail, or by telephone (not a pre-recorded message). Any electronic notice must not request or contain a hypertext link to a request that the consumer provide personal information, and must also conspicuously warn consumers not to provide personal information in response to electronic communications regarding security breaches. If the cost of providing regular notice would exceed \$5,000, the amount of people to be notified exceeds 5,000, or the entity or business not have sufficient contact information, substitute notice may be provided. When substitute notice is used, it must consist of a conspicuous posting on the entity’s web site and notification to major statewide and regional media. If more than 1,000 consumers at one time are affected, the business or agency must also notify consumer reporting agencies.

Statute: 9 § 2435:

<http://www.leg.state.vt.us/statutes/fullsection.cfm?Title=09&Chapter=062&Section=02435>

Office of the Attorney General, “Security Breach Guidance”

http://www.atg.state.vt.us/upload/1177431104_Security_Breach_Guidance.pdf

State Resources:

Office of the Attorney General, “Identity Theft”

<http://www.atg.state.vt.us/display.php?smod=198>

This web site explains Vermont’s laws on identity theft and some of the programs available to prevent and respond to identity theft crimes. It directs victims of identity theft to: *“File a police report and ask for a copy for your records,”* and *“When working with companies and law enforcement officials to correct your ID theft problems, write down the name of anyone you talk to, what s/he told you, and the date of the conversation.”*

Department of Motor Vehicles, “Information for Compromised Licenses”

<http://www.dmv.state.vt.us/documents/MiscellaneousDocuments/COMPROMISEDLicenseInformation.pdf>

This document provides information to people whose driver’s licenses have been compromised by identity theft or security breaches.

Legislation:

2006:

SB 267 extends the security freeze provisions enacted by HB 327 in 2004 to all Vermont consumers. Previously, only victims of identity theft were permitted to place a security freeze on their credit files.

Under **SB 284**, consumers will receive notice if certain personal information, such as a Social Security number or financial account numbers, has been accessed by an unauthorized person in a security breach. The law is designed to inform consumers when their personal information may be at risk, so they can take steps to ensure they will not become a victim of identity theft. The law requires businesses and state agencies to notify consumers if the agency or business has suffered a security breach. A breach is defined as the unauthorized acquisition or access of computerized data that compromises the security, confidentiality or integrity of certain personal information kept by the agency or business.

2004:

HB 327 makes identify theft a felony and provides consumers with new protections. The bill:

- Creates the crime of identity theft, defined as the possession, use, or transfer of personal identifying information belonging to or pertaining to another person with the intent to use the information to commit a misdemeanor or a felony. It also includes knowingly or recklessly possessing, using, or transferring personal identifying information belonging or pertaining to another person without consent, or knowingly or recklessly facilitating the use of the information by a third person to commit a misdemeanor or felony.
- Imposes a maximum penalty of three years in jail and a \$5,000 fine for a first offense. Subsequent convictions carry a 10-year jail term and a \$10,000 fine.
- Allows victims of identity theft who have filed a police report, investigative report, or complaint, filed with law enforcement about unlawful use of their personal information to place a security freeze on their credit reports, preventing others from opening new accounts in their name.
- Requires state and local police to take police reports for complaints about identity theft. Such a complaint is needed to deal with creditors.
- Requires credit card issuers that mail solicitations and receive a completed application with a different address from the solicitation to verify the change of address.
- Requires all governmental entities to redact Social Security numbers from a document before posting or requiring the posting of that document. The files and records available in the office of a town clerk are excluded from this requirement.
- Permits an executor, administrator, or other person authorized to act on behalf of an estate of a deceased person to request that a credit reporting agency indicate on the deceased person's credit reporting file that the person is deceased.