Attorney General Guidance Concerning the Protection of Social Security Numbers

Introduction

The Social Security number (SSN) has a unique status as an identifier of consumers. If SSNs fall into the wrong hands, they can be misused in a manner that presents consumers with a risk of identity theft. SSNs play a significant role in linking records that contain sensitive information that individuals generally wish to keep confidential.

Created by the federal government in 1936 to track workers' earnings and eligibility for retirement benefits, the SSN is now used in both the public and private sectors for a myriad of purposes unrelated to retirement benefits. The SSN is a unique identifier that does not change through a consumer's lifetime, allowing it to serve many record management purposes.

Today SSNs are widely used as representations of individual identity, as passwords, and as the keys for linking multiple records together. The problem is that these uses are incompatible. The widespread use of the SSN as an individual identifier, resulting in its appearance on mailing labels, ID cards and badges, and various publicly displayed documents, makes it unfit to be a secure password providing access to financial records and personal information.

The need to significantly reduce the risks to individuals of inappropriate disclosure and misuse of SSNs has in recent years led Vermont and other states to take steps to limit the use and display of SSNs. This Guidance describes the recommended steps a business or state agency should take in order to ensure the protection of SSNs as required by Vermont law.

Vermont's Social Security Number Protection Act, 9 V.S.A. § 2440, contains five components:

- § 2430 contains definitions applicable to the rest of the law.
- § 2440(b) & (c) contain provisions applicable to SSN storage, use, and display by businesses.
- § 2440(d) & (e) contain provisions applicable to SSN storage, use, and display by state agencies.
- § 2440(f) allows an individual to have his or her SSN redacted from a town or court internet website.
- § 2440(g) provides for enforcement of the Act by the Attorney General and State's Attorney with respect to businesses and state agencies, and by the Department of Banking, Insurance, Securities, and Health Care Administration with respect to a person or entity regulated by the Department, and further provides for the confidentiality of information provided to the Attorney General or State's Attorney by the Vermont Department of Public Safety and law enforcement agencies.

This Guidance contains the following:

1. The key points of Vermont's SSN law as it pertains to businesses.
2. The key points of Vermont's SSN law as it pertains to state agencies.
3. A summary of an individual's right to request removal of certain personal information from a town or court internet website.
4. A summary of other Vermont laws pertaining to confidentiality of SSNs.

5. Recommended practices with respect to reducing the use and exposure of SSNs.
6. Examples of appropriate SSN usage.

This Guidance is not intended as a substitute for a complete review of Vermont's Protection of Social Security Numbers Act. It is, instead, intended as a guide to key requirements of the law.

If you have any questions about the Guidance or Vermont's Protection of Social Security Numbers law, please contact: data.security@atg.state.vt.us

Vermont law on SSN confidentiality as it pertains to a business

Requirements

Under the provisions of 9 V.S.A. § 2440(b), a business may not do any of the following:

1. Intentionally communicate or otherwise make available to the general public an individual's SSN.
2. Intentionally print or imbed an individual's SSN on any card required for the individual to access products or services provided by the person or entity.
3. Require an individual to transmit his or her SSN over the internet unless the connection is secure or the SSN is encrypted.
4. Require an individual to use his or her SSN to access an internet website, unless a password or unique personal identification number or other authentication device is also required to access the internet website.
5. Print an individual's SSN on any materials that are mailed to the individual, unless state or federal law requires the SSN to be on the document to be mailed.
6. Sell, lease, lend, trade, rent or otherwise intentionally disclose an individual's SSN 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 SSN.

Exceptions

The requirements pertaining to use of an SSN by a business shall not apply:

1. When an SSN is included in an application or in documents related to an enrollment process, or to establish, amend, or terminate an account, contract, or policy, or to confirm the accuracy of the SSN for the purpose of obtaining a credit report. (No part of the SSN may be printed on a postcard or mailer not requiring an envelope, or be visible without the envelope having been opened.)
2. To the collection, use, or release of an SSN reasonably necessary for administrative purposes or internal verification.
3. To the opening of an account or the provision of or payment for a product or service authorized by an individual.
4. To the collection, use, or release of an SSN to investigate or prevent fraud; conduct background checks; conduct social or scientific research; collect a debt; obtain a credit report from or furnish data to a credit reporting agency pursuant to the Fair Credit Reporting Act; undertake a permissible purpose enumerated under Gramm Leach Bliley;

or locate an individual who is missing, is a lost relative, or is due a benefit, such as a pension, insurance, or unclaimed property benefits.
5. To a business acting pursuant to a court order, warrant, subpoena, or in response to a facially valid discovery request pursuant to rules applicable to a court or administrative body that has jurisdiction over the disclosing entity.
6. To a business providing the SSN to a federal, state, or local government entity, including a law enforcement agency, the department of public safety, or a court.
7. To an SSN that has been redacted.
8. To information obtained from a recorded document in the official records of the town clerk or municipality.
9. To information obtained from a document filed in the official records of the courts.[1]

Vermont law on SSN confidentiality as it pertains to a state agency

Requirements

Under the provisions of 9 V.S.A. § 2440(d), the state and any state agency, political subdivision of the state, and agent or employee of the state, a state agency, or a political subdivision of the state (hereinafter the State) may not do any of the following:

1. Collect an SSN from an individual unless authorized or required by state or federal law or regulation, or grant agreement, or unless the collection of the SSN or records containing the SSN is related to the performance of that agency's duties and responsibilities.
2. Fail, when collecting an SSN from an individual in a hard copy format, to segregate that number on a separate page from the rest of the record, or as otherwise appropriate, in order that the SSN can be more easily redacted pursuant to a valid public records request.
3. Fail to provide, upon request, at the time of or prior to the collection of an SSN, a statement of the purposes for which the SSN is being collected and used.
4. Use the SSN for any purpose other than the purpose set forth in the statement of purpose.
5. Intentionally print or imbed an individual's SSN on any card required for the individual to access government services.
6. Require an individual to transmit the individual's SSN over the internet, unless the connection is secure or the SSN is encrypted.
7. Require an individual to use the individual's SSN to access an internet website unless a password or unique personal identification number or other authentication device is also required to access the internet website.
8. Print an individual's SSN on any materials that are mailed to the individual, unless a state or federal law, regulation, or grant agreement requires that the SSN be on the document to be mailed. (No part of the SSN may be printed on a postcard or mailer not requiring an envelope, or be visible without the envelope having been opened.)

[1] If a business or the state has used an SSN prior to January 1, 2007, in a manner inconsistent with these provisions, it may continue to do so after January 1, 2007, if all of the following conditions are met:

- The use is continuous.
- The individual is provided an annual disclosure that informs the individual that he or she has the right to stop the use of his or her SSN.
- A written request by an individual to stop the use of his or her SSN is implemented within 30 days of the receipt of the request, and there shall be no fee or charge for implementing the request; and,
- The entity does not deny services to an individual because the individual makes a written request.

Exceptions

The requirements pertaining to use of an SSN by the State shall not apply to:

1. SSNs disclosed to another governmental entity, including contractors, grantees, or grantors, if disclosure is necessary for the receiving entity to perform its duties and responsibilities. The receiving entity shall maintain the confidential status of the SSNs. ("Necessary" means reasonably needed to promote the efficient, accurate, or economical conduct of the entity's duties and responsibilities.)
2. SSNs disclosed pursuant to a court order, warrant, or subpoena, or in response to a facially valid discovery request pursuant to rules applicable to a court or administrative body that has jurisdiction over the disclosing entity.
3. SSNs disclosed for public health purposes pursuant to and in compliance with requirements of the department of health under Title 18.
4. The collection, use, or release of an SSN reasonably necessary for administrative purposes or internal verification. Internal verification includes the sharing of information for internal verification between and among governmental entities, including contractors, grantees, and grantors.
5. SSNs that have been redacted.
6. Certified copies of vital records issued by the health department and other authorized officials pursuant to part 6 of Title 18.
7. A recorded document in the official records of the town clerk or municipality.
8. A document filed in the official records of the courts.
9. The collection, use, or dissemination of SSNs by law enforcement agencies and the department of public safety in the execution of their duties and responsibilities.
10. The collection, use, or release of an SSN to investigate or prevent fraud; conduct background checks; conduct social or scientific research; collect a debt; obtain a credit report from or furnish data to a consumer reporting agency pursuant to the Fair Credit Reporting Act; or locate an individual who is missing, is a lost relative, or is due a benefit, such as a pension, insurance, or unclaimed property benefit.[2]

Individual's right to request removal of personally identifiable information

Pursuant to 9 V.S.A. § 2440(f), any person has the right to request that a town clerk or clerk of court remove from an image or copy of an official record placed on a town's or court's internet website available to the general public the person's SSN, employer taxpayer identification number, driver's license number, state identification number, passport number, checking account number, savings account number, credit card or debit card number, or personal identification number (PIN) or password contained in that official record.

A town clerk or clerk of court is authorized to redact the personal information identified in a request submitted under this section. The request must be made in writing, legibly signed by the requester, and delivered by mail, facsimile, or electronic transmission, or delivered in person to the town clerk or clerk of court. The request must specify the personal information to be

[2] See footnote 5 for grandfathered practices for state agencies and businesses.

redacted, information that identifies the document that contains the personal information, and the location within the document that contains the information to be redacted.

The request for redaction shall be considered a public record with access restricted to the town clerk, the clerk of court, their staff, or upon order of the court. The town clerk or clerk of court shall have no duty to inquire beyond the written request to verify the identity of a person requesting redaction and shall have no duty to replace redacted information for any reason upon subsequent request by an individual or by order of the court, if impossible to do so.

No fee will be charged for the redaction. Any person who requests a redaction without proper authority to do so shall be guilty of an infraction, punishable by a fine not to exceed $500.00.

Other Laws Pertaining to Confidentiality of SSNs

Another Vermont law that pertains to the confidentiality of SSNs is 9 V.S.A. § 2445 (effective on January 1, 2007). This law requires the safe destruction of business records that contain SSNs, as well as other important personal information, and provides for enforcement by the Attorney General and State's Attorney, or by the Department of Banking, Insurance, Securities, and Health Care Administration with respect to a person or entity regulated by the Department. The law requires that such records be destroyed through shredding or other means that ensures the confidentiality of the SSNs. It also requires an entity that is in the business of disposing of personal financial information to implement and monitor compliance with policies and procedures that protect against unauthorized access to or use of personal information.

In addition, 9 V.S.A. § 2480m (effective on July 1, 2005) requires that prior to posting or requiring the posting of a document in a place of general public circulation, a state agency or political subdivision take all reasonable steps to redact SSNs from the document.

Recommended practices for protecting Social Security Numbers

These recommendations are intended to serve as guidelines to assist businesses and state agencies move towards aligning their information collection practices with the goals and the requirements of Vermont's Social Security Number Protection Act.

1. Reduce the collection of SSNs.

- Collect SSNs only where required to do so by federal or state law.
- When collecting SSNs as allowed, but not required, by law, do so only as reasonably necessary for the proper administration of lawful business activities.
- If a unique personal identifier is needed, develop your own unique identifier as a substitute for the SSN.

2. Inform individuals when you request their SSNs.

- Whenever you collect SSNs, inform the individuals of the purpose of the collection, the intended use, whether the law requires the SSN to be protected, and the consequences to the individual if he or she chooses not to provide the number.
- If required by law, notify individuals (customers, employees, business partners, etc.) annually of their right to request that you not post or publicly display their SSN.

3. Eliminate the public display of SSNs.

- Do not put SSNs on documents that are widely seen by others, such as identification cards, badges, time cards, employee rosters, and bulletin board postings.
- Do not send documents containing SSNs through the mail, except when required by law.
- When sending applications, forms, or other documents required by law to carry SSNs through the mail, place the SSN where it will not be revealed by an envelope window. Where possible, leave the SSN field on forms and applications blank and ask the individual to fill it in before returning the form or application.
- Do not send SSNs over the internet or by electronic mail, unless the communication is secure or the SSN is encrypted.
- Do not require an individual to send his or her SSN over the internet or by email, unless the connection is secure or the SSN is encrypted.
- Do not require individuals to use SSNs as passwords or codes for access to internet websites or other services.

4. Control access to SSNs.

- Limit access to records containing SSNs only to those who need to see the numbers for the performance of their duties.
- Use computer logs or electronic audit trails to monitor employees' access to records with SSNs.
- Protect records containing SSNs, including back-ups, by encrypting the numbers in electronic records or storing records in other media in locked cabinets.
- Do not store records containing SSNs on computers or other electronic devices that are not secured against unauthorized access.
- Avoid sharing SSNs with other entities, except where required by law.
- If you must share SSNs, including with contractors, use written agreements to protect confidentiality, prohibit re-disclosure of SSNs except as required by law, and require effective security controls on record systems containing SSNs.
- Hold third-party contractors and other entities with whom you share SSNs accountable for compliance with the restrictions you impose, and monitor or audit their practices.
- If SSNs are disclosed inappropriately and the individuals whose SSNs were disclosed are put at risk of identity theft or other harm, promptly notify individuals potentially affected as required by Vermont's Security Breach Notice Act, 9 V.S.A § 2435.

5. Develop internal security safeguard procedures to protect SSNs.

- Develop a written security plan for databases and other records that contain SSNs.
- Develop written policies for protecting the confidentiality of SSNs.
- Adopt "clean desk/work area" policy requiring employees to properly secure records containing SSNs.
- Do not leave voice mail messages containing SSNs and if you must send an SSN by fax, take special measures to ensure confidentiality.
- Require employees to ask individuals (employees, customers, etc.) for identifiers other than the SSN when looking up records for the individual.

- Require employees to promptly report any inappropriate disclosure or loss of records containing SSNs to their supervisors or to the organization's privacy officer.

6. Make your organization accountable for protecting SSNs.

- Designate an office or employee within the organization as responsible for ensuring compliance with policies and procedures for protecting SSNs.
- Train employees at least annually on their responsibilities in handling SSNs, and provide them with appropriate written protocols.
- Provide the same training and materials to all new employees, temporary employees, and contract employees.
- Discipline employees for non-compliance with organizational policies and practices for protecting SSNs.
- Conduct risk assessments and regular audits of record systems containing SSNs.

7. Institute safe destruction of SSNs and other personal information.

- When discarding or destroying records in any medium containing SSNs, do so in a way that protects their confidentiality, such as shredding.
- Ensure the information is not accessible by the public when being destroyed.

Examples of SSN usage

- The Retirement Division of the Treasurer's Office mails pension payments to retirees, refunds to retirees, and tax reporting forms that contain SSNs. This is permitted because state and federal law requires an SSN on these documents. However, the SSNs may not be printed, in whole or in part, on a postcard or other mail piece that does not require an envelope, and SSNs may not be visible on an envelope or through an envelope window.

- A state agency may respond to a valid public records request by supplying records that contain SSNs, so long as the SSNs have been redacted prior to the dissemination.

- A town clerk may receive for recording in the Land Records a transfer tax return containing the SSNs of parties to the land transaction. The town clerk may continue to record such documents in the Land Records without redacting the SSN.

- The Vermont Office of Child Support uses as its file number an individual client's SSN. This is permitted because the federal government requires the state to use SSNs as child welfare case identifiers and as internal verifiers.

- The Department of Personnel collects SSNs for payroll and for uses related to health benefits. This is permitted because the collection is required by state and federal law, and also because it is necessary to promote the efficient, accurate, and economical conduct of the Department's duties and responsibilities.

- A business wishes to verify that a consumer to whom it is speaking on the phone is in fact the person the consumer purports to be. The business has the consumer's SSN in its file. The business asks the consumer to inform the business of **the last four digits** of the consumer's SSN to verify the consumer's identity.