white paper

SAFE DESTRUCTION OF DOCUMENTS

Federal and State Requirements for Proper Disposal of Information Contained in Consumer Reports

OVERVIEW

With the growth in popularity for organizations to utilize electronic data storage and data becoming more easily accessible and transferable between parties, a key concern for consumer protection and privacy advocates has been the potential for private and sensitive information to fall into the wrong hands.

In light of this growing concern, state and federal legislators have passed laws to mitigate the risk of unauthorized persons gaining access to such information.

In 2003, a federal law was enacted that is designed to reduce the risk of consumer fraud and related harms, including identity theft, created by the improper disposal of consumer information. Individual states have also passed laws—most recently in Delaware—governing the proper disposal of sensitive consumer information. Organizations that procure consumer reports on individuals must be aware of these various data disposal laws and regulations, and should ensure that their procedures and methods for disposing of consumer reports and other sensitive consumer information are in full compliance.

FEDERAL DATA DISPOSAL LAWS & REGULATIONS

The Fair and Accurate Credit Transactions Act of 2003[1] ("FACTA") directed certain government agencies to issue final regulations requiring any person that maintains or otherwise possesses consumer information derived from consumer reports for a business purpose to properly dispose of any such information.

In response, the Federal Trade Commission ("FTC") promulgated a rule in 2005 to set forth the proper disposal procedures for consumer reports ("Disposal Rule").[2]

The Disposal Rule applies specifically to individuals and organizations that use consumer reports and information derived from consumer reports as defined under the Fair Credit Reporting Act ("FCRA").[3] The Disposal Rule provides such individuals and organizations with the discretion to determine the proper disposal procedures based on the sensitivity of the information, the costs and benefits of different disposal methods and changes in technology.[4]

Section 682.3 of the Disposal Rule provides that:

> Any person who maintains or otherwise possesses consumer information for a business purpose must properly dispose of such information by taking reasonable measures to protect against unauthorized access to or use of the information in connection with its disposal.

Consumer information is defined as: "any record about an individual, whether in paper, electronic, or other form, that is a consumer report or is derived from a consumer report. Consumer information also means a compilation of such records. Consumer information does not include information that does not identify individuals, such as aggregate information or blind data."

Section 682.3 goes on to provide a non-exhaustive list of examples to illustrate some reasonable measures that can be taken to protect against unauthorized access to or use of consumer information, including:

> (1) requiring the burning, pulverizing, or shredding of papers containing consumer information so that the information cannot practicably be read or reconstructed;
>
> (2) requiring the destruction or erasure of electronic media containing consumer information so that the information cannot practicably be read or reconstructed; and
>
> (3) conducting due diligence[5] before entering into and monitoring compliance with a contract with another party engaged in the business of record destruction to dispose of material, specifically identified as consumer information, in a manner consistent with the Disposal Rule.

[1] W Pub. L. No. 108-159.

[2] 16 C.F.R. pt. 682.

[3] 15 U.S.C. § 1681. The FCRA defines a "consumer report" as: "any written, oral, or other communication of any information by a consumer reporting agency bearing on a consumer's credit worthiness, credit standing, credit capacity, character, general reputation, personal characteristics, or mode of living which is used or expected to be used or collected in whole or in part for the purpose of serving as a factor in establishing the consumer's eligibility for (A) credit or insurance to be used primarily for personal, family, or household purposes; (B) employment purposes; or (C) any other purpose authorized under section 604 [§ 1681b]."

[4] *Protecting Personal Information: A Guide for Business*, FED. TRADE COMM'N 12 (Nov. 2011), http://www.business.ftc.gov/sites/default/files/pdf/bus69-protecting-personal-information-guide-business_0.pdf.

Persons or entities who maintain or otherwise possess consumer information through their provision of services directly to a person subject to the Disposal Rule should implement and monitor compliance with policies and procedures that protect against unauthorized or unintentional disposal of consumer information and should dispose of such information in accordance with examples (1) and (2) above. Persons subject to the Gramm-Leach-Bliley Act, 15 U.S.C. 6081 et seq., and the Federal Trade Commission's Standards for Safeguarding Customer Information, 16 C.F.R. pt. 314 ("Safeguards Rule"), should take reasonable measures by incorporating the proper disposal of consumer information as required by the Disposal Rule into the information security program required by the Safeguards Rule.

Organizations that fail to comply with the aforementioned federal disposal requirements could face lawsuits and liability for actual damages or up to $1,000 in statutory damages per violation.

[5] The Disposal Rule defines "due diligence" to include "reviewing an independent audit of the disposal company's operations and/or its compliance with this rule, obtaining information about the disposal company from several references or other reliable sources, requiring that the disposal company be certified by a recognized trade association or similar third party, reviewing and evaluating the disposal company's information security policies or procedures, or taking other appropriate measures to determine the competency and integrity of the potential disposal company."

STATE DISPOSAL LAWS

A number of states have also passed laws governing the proper disposal of personally identifiable information and other sensitive consumer data.

However, the scope and requirements of each law vary from state to state.[6] Some states have adopted very detailed statutory and regulatory guidelines in order to ensure the confidentiality and proper disposal of private consumer information. For example, Massachusetts[7] requires every covered entity to develop, implement and maintain a comprehensive written information security program that contains administrative, technical and physical safeguards to ensure the security and confidentiality of records—both paper and electronic—containing personal information. In Oregon,[8] covered businesses must implement an information security and disposal program that includes certain minimum administrative, technical and physical safeguards in order to comply with the requirement that they "develop, implement and maintain reasonable safeguards to protect the security, confidentiality and integrity of the personal information, including disposal of the data."

In contrast, other states—such as Indiana[9] and Texas[10] —have a more general requirement that covered entities implement and maintain "reasonable procedures" to protect against unauthorized access to or improper disposal of sensitive consumer information. Nonetheless, the common thread across most states is that covered businesses must destroy or arrange for the destruction of records containing sensitive consumer information by shredding, erasing or otherwise making the information unreadable or indecipherable.

Most recently, Delaware passed laws, effective January 1, 2015, that "create potential liability for companies that fail to destroy records or documents that contain personal

[6] For a detailed analysis of various state laws governing disposal of sensitive consumer information, *see*: Bruce A Radke & Michael J. Waters, *Selected State Laws Governing the Safeguarding & Disposing of Personal Information*, VEDDER PRICE PC (Sept. 30, 2014), http://www.vedderprice.com/selected-state-laws-governing-safeguarding-and-disposing-of-personal-information/.

[7] The Massachusetts Data Security Regulations, 201 C.M.R. 17.00 et seq.

[8] The Oregon Consumer Identity Theft Protection Act, O.R.S. § 646A.622.

[9] IC 24-4.9-3-3.5; IC 24-4.9-2-3; IC 24-4.9-2-10.

[10] Tex. Bus. & Com. Code Ann. 521.052.

identifying information in a manner that renders them unreadable or indecipherable."[11] The laws are located at 6 Del. Code §§ 50C-101 to 50C-104 (hereinafter "Section 50C") and 7 Del. Code § 736 (hereinafter "Section 736").

Under Section 50C, commercial entities are required to take reasonable steps to destroy records containing a consumer's personally identifiable information ("PII"). PII is defined as:

> [A] consumer's first initial and last name in combination with any one of the following data elements that relate to the consumer, when either the name or the data elements are not encrypted: his or her signature, full date of birth, social security number, passport number, driver's license or state identification card number, insurance policy number, financial services account number, bank account number, credit card number, debit card number, any other financial information or confidential health care information including all information relating to a patient's health care history, diagnosis condition, treatment, or evaluation obtained from a health care provider who has treated the patient which explicitly or by implication identifies a particular patient.

Section 50C also requires that commercial entities take all reasonable steps to destroy or arrange for the destruction of a consumer's personally identifiable information within its custody and control by shredding, erasing or otherwise destroying or modifying the personally identifiable information in those records to make it entirely unreadable or indecipherable through any means for the purpose of:

> (1) Ensuring the security and confidentiality of consumer's personally identifiable information;
>
> (2) Protecting against any reasonably foreseeable threats or hazards to the security or integrity of consumer's personally identifiable information; and
>
> (3) Protecting against unauthorized access to or use of consumer's personally identifiable information that could result in substantial harm or inconvenience to any consumer.

[11] Sharon R. Klein & T. Stephen Jenkins, *Inside Delaware's New Laws On Destroying Consumer Info*, LAW360 (Oct. 15, 2014), http://www.law360.com/articles/586986/inside-delaware-s-new-laws-on-destroying-consumer-info.

Section 50C does, however, exempt several entities including banks, credit unions, financial institutions, health insurers or healthcare facilities, consumer reporting agencies and governments and their subdivisions. It is also important to note that Section 50C defines "consumer" as an individual who enters into a transaction primarily for personal, family or household purposes.

Additionally, Section 736 sets forth requirements for the safe destruction of employee records containing PII, and unlike Section 50C, does not exempt any entities from its requirements. Section 736 states:

> In the event that an employer seeks permanently to dispose of records[12] containing employees' personally identifiable information within its custody and control, such employer shall take all reasonable steps to destroy or arrange for the destruction of each such record by shredding, erasing, or otherwise destroying or modifying the personally identifiable information in those records to make it unreadable or indecipherable.

[12] Section 736 defines "record" to mean "information that is inscribed on a tangible medium, or that is stored in an electronic or other medium and is retrievable in perceivable form on which personally identifiable information is recorded or preserved. 'Record' does not include publicly available directories or sources containing information an employee has voluntarily consented to have publicly disseminated or listed or which is disseminated as provided for by applicable law or regulation, such as name, address, or telephone number, or other directories or sources as are derived solely from such directories or sources."

CONCLUSION

Organizations that handle private consumer information, including employers who obtain consumer reports for employment purposes, must ensure that they safeguard and dispose of such information in accordance with all federal and state requirements.

Generally, this includes having safeguards in place to ensure that only authorized personnel can access the sensitive information and procedures in place to destroy the information that include burning, shredding, pulverizing or any other method of destruction that makes the information unreadable or indecipherable.

Additionally, the FTC recommends taking the following measures to help ensure that sensitive information is properly disposed of:

- Making shredders available throughout the workplace, including next to the photocopier;

- When disposing of old computers and portable storage devices, using software to securely erase data, usually called a wipe utility program (deleting files using the keyboard or mouse commands usually isn't sufficient because the files may continue to exist on the computer's hard drive and could easily be retrieved); and

- Making sure employees who work from home follow the same procedures for disposing of sensitive documents, old computers and portable storage devices.[13]

The procedures used by Certiphi Screening, Inc. to destroy sensitive information depend upon the type and intended disposition of the media. One way we destroy sensitive information is through data wiping, using Department of Defense sanctioned methods that include multi-pass data overwrites. Other methods utilized by our company include degaussing and the use of a National Association for Information Destruction (NAID) AAA certified shredding company. These procedures are mentioned in Section 682.3 of the Disposal Rule as examples of reasonable measures that can be taken to protect against the unauthorized access to or use of sensitive consumer information, and thus comply with the FACTA requirements for the proper disposal of such information.

[13] FED. TRADE COMM'N, *supra note* 4, at 12.

ONE WAY WE DESTROY SENSITIVE INFORMATION IS THROUGH DATA WIPING, USING DEPARTMENT OF DEFENSE SANCTIONED METHODS THAT INCLUDE MULTI-PASS DATA OVERWRITES.