

Wyo. Stat. § 40-12-501, 502

ARTICLE 5 - CREDIT FREEZE REPORTS

40-12-501. Definitions.

(a) As used in this act:

(i) "Breach of the security of the data system" means unauthorized acquisition of computerized data that materially compromises the security, confidentiality or integrity of personal identifying information maintained by a person or business and causes or is reasonably believed to cause loss or injury to a resident of this state. Good faith acquisition of personal identifying information by an employee or agent of a person or business for the purposes of the person or business is not a breach of the security of the data system, provided that the personal identifying information is not used or subject to further unauthorized disclosure;

(ii) "Consumer" means any person who is utilizing or seeking credit for personal, family or household purposes;

(iii) "Consumer reporting agency" means any person whose business is the assembling and evaluating of information as to the credit standing and credit worthiness of a consumer, for the purposes of furnishing credit reports, for monetary fees and dues to third parties;

(iv) "Credit report" means any written or oral report, recommendation or representation of a consumer reporting agency as to the credit worthiness, credit standing or credit capacity of any consumer and includes any information which is sought or given for the purpose of serving as the basis for determining eligibility for credit to be used primarily for personal, family or household purposes;

(v) "Creditor" means the lender of money or vendor of goods, services or property, including a lessor under a lease intended as a security, rights or privileges, for which payment is arranged through a credit transaction, or any successor to the right, title or interest of any such lender or vendor, and an affiliate, associate or subsidiary of any of them or any director, officer or

employee of any of them or any other person in any way associated with any of them;

(vi) "Financial institution" means any person licensed or chartered under the laws of any state or the United States as a bank holding company, bank, savings and loan association, credit union, trust company or subsidiary thereof doing business in this state;

(vii) "Personal identifying information" means the first name or first initial and last name of a person in combination with one (1) or more of the data elements specified in W.S. 6-3-901(b)(iii) through (xiv), when the data elements are not redacted.

(A) Repealed by Laws 2015, ch. 63, § 2.

(B) Repealed by Laws 2015, ch. 63, § 2.

(C) Repealed by Laws 2015, ch. 63, § 2.

(D) Repealed by Laws 2015, ch. 63, § 2.

(E) Repealed by Laws 2015, ch. 63, § 2.

(viii) "Redact" means alteration or truncation of data such that no more than five (5) digits of the data elements provided in subparagraphs (vii)(A) through (D) of this subsection are accessible as part of the personal information;

(ix) "Security freeze" means a notice placed in a consumer's credit report, at the request of the consumer, that prohibits the credit rating agency from releasing the consumer's credit report or any information from it relating to an extension of credit or the opening of a new account, without the express authorization of the consumer;

(x) "Substitute notice" means:

(A) An electronic mail notice when the person or business has an electronic mail address for the subject persons;

(B) Conspicuous posting of the notice on the website page of the person or business if the person or business maintains one; and

(C) Publication in applicable local or statewide media.

(xi) "This act" means W.S. 40-12-501 through 40-12-511.

(b) "Personal identifying information" as defined in paragraph (a)(vii) of this section does not include information, regardless of its source, contained in any federal, state or local government records or in widely distributed media that are lawfully made available to the general public.

40-12-502. Computer security breach; notice to affected persons.

(a) An individual or commercial entity that conducts business in Wyoming and that owns or licenses computerized data that includes personal identifying information about a resident of Wyoming shall, when it becomes aware of a breach of the security of the system, conduct in good faith a reasonable and prompt investigation to determine the likelihood that personal identifying information has been or will be misused. If the investigation determines that the misuse of personal identifying information about a Wyoming resident has occurred or is reasonably likely to occur, the individual or the commercial entity shall give notice as soon as possible to the affected Wyoming resident. Notice shall be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement and consistent with any measures necessary to determine the scope of the breach and to restore the reasonable integrity of the computerized data system.

(b) The notification required by this section may be delayed if a law enforcement agency determines in writing that the notification may seriously impede a criminal investigation.

(c) Any financial institution as defined in 15 U.S.C. 6809 or federal credit union as defined by 12 U.S.C. 1752 that maintains notification procedures subject to the requirements of 15 U.S.C. 6801(b)(3) and 12 C.F.R. Part 364 Appendix B or Part 748 Appendix B, is deemed to be in compliance with this section if the financial institution

July 2, 2017

notifies affected Wyoming customers in compliance with the requirements of 15 U.S.C. 6801 through 6809 and 12 C.F.R. Part 364 Appendix B or Part 748 Appendix B.

(d) For purposes of this section, notice to consumers may be provided by one (1) of the following methods:

(i) Written notice;

(ii) Electronic mail notice;

(iii) Substitute notice, if the person demonstrates:

(A) That the cost of providing notice would exceed ten thousand dollars (\$10,000.00) for Wyoming-based persons or businesses, and two hundred fifty thousand dollars (\$250,000.00) for all other businesses operating but not based in Wyoming;

(B) That the affected class of subject persons to be notified exceeds ten thousand (10,000) for Wyoming-based persons or businesses and five hundred thousand (500,000) for all other businesses operating but not based in Wyoming; or

(C) The person does not have sufficient contact information.

(iv) Substitute notice shall consist of all of the following:

(A) Conspicuous posting of the notice on the Internet, the World Wide Web or a similar proprietary or common carrier electronic system site of the person collecting the data, if the person maintains a public Internet, the World Wide Web or a similar proprietary or common carrier electronic system site; and

(B) Notification to major statewide media. The notice to media shall include a toll-free phone number where an individual can learn whether or not that individual's personal data is included in the security breach.

(e) Notice required under subsection (a) of this section shall be clear and conspicuous and shall include, at a minimum:

(i) A toll-free number:

(A) That the individual may use to contact the person collecting the data, or his agent; and

(B) From which the individual may learn the toll-free contact telephone numbers and addresses for the major credit reporting agencies.

(ii) The types of personal identifying information that were or are reasonably believed to have been the subject of the breach;

(iii) A general description of the breach incident;

(iv) The approximate date of the breach of security, if that information is reasonably possible to determine at the time notice is provided;

(v) In general terms, the actions taken by the individual or commercial entity to protect the system containing the personal identifying information from further breaches;

(vi) Advice that directs the person to remain vigilant by reviewing account statements and monitoring credit reports;

(vii) Whether notification was delayed as a result of a law enforcement investigation, if that information is reasonably possible to determine at the time the notice is provided.

(f) The attorney general may bring an action in law or equity to address any violation of this section and for other relief that may be appropriate to ensure proper compliance with this section, to recover damages, or both. The provisions of this section are not exclusive and do not relieve an individual or a commercial entity subject to this section from compliance with all other applicable provisions of law.

July 2, 2017

(g) Any person who maintains computerized data that includes personal identifying information on behalf of another business entity shall disclose to the business entity for which the information is maintained any breach of the security of the system as soon as practicable following the determination that personal identifying information was, or is reasonably believed to have been, acquired by an unauthorized person. The person who maintains the data on behalf of another business entity and the business entity on whose behalf the data is maintained may agree which person or entity will provide any required notice as provided in subsection (a) of this section, provided only a single notice for each breach of the security of the system shall be required. If agreement regarding notification cannot be reached, the person who has the direct business relationship with the resident of this state shall provide notice subject to the provisions of subsection (a) of this section.

(h) A covered entity or business associate that is subject to and complies with the Health Insurance Portability and Accountability Act, and the regulations promulgated under that act, 45 C.F.R. Parts 160 and 164, is deemed to be in compliance with this section if the covered entity or business associate notifies affected Wyoming customers or entities in compliance with the requirements of the Health Insurance Portability and Accountability Act and 45 C.F.R. Parts 160 and 164.

Wyo. Stat. § 6-3-901

6-3-901. Unauthorized use of personal identifying information; penalties; restitution.

(a) Every person who willfully obtains personal identifying information of another person, and uses that information for any unlawful purpose, including to obtain, or attempt to obtain, credit, goods, services or medical information in the name of the other person without the consent of that person is guilty of theft of identity.

(b) As used in this section "personal identifying information" means the name or any of the following data elements of an individual person:

- (i) Address;
- (ii) Telephone number;
- (iii) Social security number;
- (iv) Driver's license number;
- (v) Account number, credit card number or debit card number in combination with any security code, access code or password that would allow access to a financial account of the person;
- (vi) Tribal identification card;
- (vii) Federal or state government issued identification card;
- (viii) Shared secrets or security tokens that are known to be used for data based authentication;
- (ix) A username or email address, in combination with a password or security question and answer that would permit access to an online account;
- (x) A birth or marriage certificate;
- (xi) Medical information, meaning a person's medical history, mental or physical condition, or medical treatment or diagnosis by a health care professional;

(xii) Health insurance information, meaning a person's health insurance policy number or subscriber identification number, any unique identifier used by a health insurer to identify the person or information related to a person's application and claims history;

(xiii) Unique biometric data, meaning data generated from measurements or analysis of human body characteristics for authentication purposes;

(xiv) An individual taxpayer identification number.

(c) Theft of identity is:

(i) A misdemeanor punishable by imprisonment for not more than six (6) months, a fine of not more than seven hundred fifty dollars (\$750.00), or both, if no economic benefit was gained or was attempted to be gained, or if an economic benefit of less than one thousand dollars (\$1,000.00) was gained or was attempted to be gained by the defendant; or

(ii) A felony punishable by imprisonment for not more than ten (10) years, a fine of not more than ten thousand dollars (\$10,000.00), or both, if an economic benefit of one thousand dollars (\$1,000.00) or more was gained or was attempted to be gained by the defendant.

(d) If a restitution plan is ordered pursuant to W.S. 7-9-101 through 7-9-115, the court may include, as part of its determination of amount owed pursuant to W.S. 7-9-103, payment for any costs incurred by the victim, including attorney fees, any costs incurred in clearing the credit history or credit rating of the victim or in connection with any civil or administrative proceeding to satisfy any debt, lien or other obligation of the victim arising as a result of the actions of the defendant.

(e) In any case in which a person willfully obtains personal identifying information of another person, and without the authorization of that person uses that information to commit a crime in addition to a violation of subsection (a) of this section, and is convicted of that crime, the court records shall reflect that the person whose identity was falsely used to commit the crime did not commit the crime.