Second Regular Session
Seventy-first General Assembly
STATE OF COLORADO

INTRODUCED

LLS NO. 18-0270.02 Jane Ritter x4342 **HOUSE BILL 18-1128**

HOUSE SPONSORSHIP

Wist and Bridges,

SENATE SPONSORSHIP

Lambert and Court,

House Committees
State, Veterans, & Military Affairs

Senate Committees

A BILL FOR AN ACT

CONCERNING STRENGTHENING PROTECTIONS FOR CONSUMER DATA PRIVACY.

Bill Summary

(Note: This summary applies to this bill as introduced and does not reflect any amendments that may be subsequently adopted. If this bill passes third reading in the house of introduction, a bill summary that applies to the reengrossed version of this bill will be available at http://leg.colorado.gov.)

Except for conduct in compliance with applicable federal, state, or local law, the bill requires public and private entities in Colorado that maintain paper or electronic documents (documents) that contain personal identifying information (personal information) to develop and maintain a written policy for the destruction and proper disposal of those documents. Entities that maintain, own, or license personal information,

including those that use a nonaffiliated third party as a service provider, shall implement and maintain reasonable security procedures for the personal information. The notification laws governing disclosure of unauthorized acquisitions of unencrypted and encrypted computerized data are expanded to specify who must be notified following such unauthorized acquisition and what must be included in such notification.

Be it enacted by the General Assembly of the State of Colorado:

SECTION 1. In Colorado Revised Statutes, 6-1-713, **amend** (1) and (2) as follows:

6-1-713. Disposal of personal identifying documents - policy - definition. (1) Each public and private entity in the state that ~~uses~~ MAINTAINS PAPER OR ELECTRONIC documents during the course of business that contain personal identifying information shall develop a WRITTEN policy for the destruction or proper disposal of THOSE paper AND ELECTRONIC documents containing personal identifying information. UNLESS OTHERWISE REQUIRED BY FEDERAL LAW OR REGULATION, THE WRITTEN POLICY MUST REQUIRE THAT, WHEN SUCH PAPER OR ELECTRONIC DOCUMENTS ARE NO LONGER NEEDED, THE PUBLIC OR PRIVATE ENTITY DESTROY OR ARRANGE FOR THE DESTRUCTION OF SUCH PAPER AND ELECTRONIC DOCUMENTS WITHIN ITS CUSTODY OR CONTROL THAT CONTAIN PERSONAL IDENTIFYING INFORMATION BY SHREDDING, ERASING, OR OTHERWISE MODIFYING THE PERSONAL IDENTIFYING INFORMATION IN THE PAPER OR ELECTRONIC DOCUMENTS TO MAKE THE PERSONAL IDENTIFYING INFORMATION UNREADABLE OR INDECIPHERABLE THROUGH ANY MEANS.

(2) For the purposes of this section AND SECTION 6-1-713.5, "personal identifying information" means a social security number; a personal identification number; a password; a pass code; an official state

or government-issued driver's license or identification card number; a government passport number; biometric data; an employer, student, or military identification number; or a financial transaction device.

SECTION 2. In Colorado Revised Statutes, **add** 6-1-713.5 as follows:

6-1-713.5. Protection of electronic customer records. (1) TO PROTECT PERSONAL IDENTIFYING INFORMATION, AS DEFINED IN SECTION 6-1-713 (2), FROM UNAUTHORIZED ACCESS, USE, MODIFICATION, DISCLOSURE, OR DESTRUCTION, A PERSON WHO MAINTAINS, OWNS, OR LICENSES PERSONAL IDENTIFYING INFORMATION OF AN INDIVIDUAL RESIDING IN THE STATE SHALL IMPLEMENT AND MAINTAIN REASONABLE SECURITY PROCEDURES AND PRACTICES THAT ARE APPROPRIATE TO THE NATURE OF THE PERSONAL IDENTIFYING INFORMATION AND THE NATURE AND SIZE OF THE BUSINESS AND ITS OPERATIONS.

(2) A PERSON WHO USES A NONAFFILIATED THIRD PARTY AS A SERVICE PROVIDER TO PERFORM SERVICES FOR THE PERSON AND DISCLOSES PERSONAL IDENTIFYING INFORMATION ABOUT AN INDIVIDUAL RESIDING IN THE STATE WITH THE NONAFFILIATED THIRD PARTY SHALL REQUIRE THAT THE NONAFFILIATED THIRD PARTY IMPLEMENT AND MAINTAIN REASONABLE SECURITY PROCEDURES AND PRACTICES THAT ARE:

(a) APPROPRIATE TO THE NATURE OF THE PERSONAL IDENTIFYING INFORMATION DISCLOSED TO THE NONAFFILIATED THIRD PARTY; AND

(b) REASONABLY DESIGNED TO HELP PROTECT THE PERSONAL IDENTIFYING INFORMATION FROM UNAUTHORIZED ACCESS, USE, MODIFICATION, DISCLOSURE, OR DESTRUCTION.

SECTION 3. In Colorado Revised Statutes, 6-1-716, **amend** (2),

(3), and (4); **repeal and reenact, with amendments,** (1); and **add** (5) as follows:

6-1-716. Notification of security breach. (1) **Definitions.** AS USED IN THIS SECTION, UNLESS THE CONTEXT OTHERWISE REQUIRES:

(a) "COMMERCIAL ENTITY" MEANS ANY PRIVATE LEGAL ENTITY, WHETHER FOR-PROFIT OR NOT-FOR-PROFIT.

(b) "ENCRYPTED" MEANS RENDERED UNUSABLE, UNREADABLE, OR INDECIPHERABLE TO AN UNAUTHORIZED PERSON THROUGH A SECURITY TECHNOLOGY OR METHODOLOGY GENERALLY ACCEPTED IN THE FIELD OF INFORMATION SECURITY.

(c) "NOTICE" MEANS:

(I) WRITTEN NOTICE TO THE POSTAL ADDRESS LISTED IN THE RECORDS OF THE INDIVIDUAL OR COMMERCIAL ENTITY;

(II) TELEPHONIC NOTICE;

(III) ELECTRONIC NOTICE, IF A PRIMARY MEANS OF COMMUNICATION BY THE INDIVIDUAL OR COMMERCIAL ENTITY WITH A COLORADO RESIDENT IS BY ELECTRONIC MEANS OR THE NOTICE PROVIDED IS CONSISTENT WITH THE PROVISIONS REGARDING ELECTRONIC RECORDS AND SIGNATURES SET FORTH IN THE FEDERAL "ELECTRONIC SIGNATURES IN GLOBAL AND NATIONAL COMMERCE ACT", 15 U.S.C. SEC. 7001 ET SEQ.; OR

(IV) SUBSTITUTE NOTICE, IF THE INDIVIDUAL OR THE COMMERCIAL ENTITY REQUIRED TO PROVIDE NOTICE DEMONSTRATES THAT THE COST OF PROVIDING NOTICE WILL EXCEED TWO HUNDRED FIFTY THOUSAND DOLLARS, THE AFFECTED CLASS OF PERSONS TO BE NOTIFIED EXCEEDS TWO HUNDRED FIFTY THOUSAND COLORADO RESIDENTS, OR THE INDIVIDUAL OR THE COMMERCIAL ENTITY DOES NOT HAVE SUFFICIENT CONTACT

INFORMATION TO PROVIDE NOTICE. SUBSTITUTE NOTICE CONSISTS OF ALL OF THE FOLLOWING:

(A) E-MAIL NOTICE IF THE INDIVIDUAL OR THE COMMERCIAL ENTITY HAS E-MAIL ADDRESSES FOR THE MEMBERS OF THE AFFECTED CLASS OF COLORADO RESIDENTS;

(B) CONSPICUOUS POSTING OF THE NOTICE ON THE WEBSITE PAGE OF THE INDIVIDUAL OR THE COMMERCIAL ENTITY IF THE INDIVIDUAL OR THE COMMERCIAL ENTITY MAINTAINS ONE; AND

(C) NOTIFICATION TO MAJOR STATEWIDE MEDIA.

(d) (I) "PERSONAL INFORMATION" MEANS A COLORADO RESIDENT'S FIRST NAME OR FIRST INITIAL AND LAST NAME IN COMBINATION WITH ANY ONE OR MORE OF THE FOLLOWING DATA ELEMENTS THAT RELATE TO THE RESIDENT, WHEN THE DATA ELEMENTS ARE NOT ENCRYPTED, REDACTED, OR SECURED BY ANY OTHER METHOD RENDERING THE NAME OR THE ELEMENT UNREADABLE OR UNUSABLE:

(A) SOCIAL SECURITY NUMBER;

(B) DRIVER'S LICENSE NUMBER OR IDENTIFICATION CARD NUMBER;

(C) ACCOUNT NUMBER OR CREDIT CARD OR DEBIT CARD NUMBER;

(D) MEDICAL INFORMATION;

(E) HEALTH INSURANCE INFORMATION;

(F) BIOMETRIC DATA; AND

(G) USER NAME OR E-MAIL ADDRESS, IN COMBINATION WITH A PASSWORD OR SECURITY QUESTIONS AND ANSWERS, THAT WOULD PERMIT ACCESS TO AN ONLINE ACCOUNT.

(II) "PERSONAL INFORMATION" DOES NOT INCLUDE PUBLICLY AVAILABLE INFORMATION THAT IS LAWFULLY MADE AVAILABLE TO THE GENERAL PUBLIC FROM FEDERAL, STATE, OR LOCAL GOVERNMENT

RECORDS OR WIDELY DISTRIBUTED MEDIA.

(e) "SECURITY BREACH" MEANS THE UNAUTHORIZED ACQUISITION OF UNENCRYPTED COMPUTERIZED DATA THAT COMPROMISES THE SECURITY, CONFIDENTIALITY, OR INTEGRITY OF PERSONAL INFORMATION MAINTAINED BY AN INDIVIDUAL OR A COMMERCIAL ENTITY. GOOD FAITH ACQUISITION OF PERSONAL INFORMATION BY AN EMPLOYEE OR AGENT OF AN INDIVIDUAL OR COMMERCIAL ENTITY FOR THE PURPOSES OF THE INDIVIDUAL OR COMMERCIAL ENTITY IS NOT A SECURITY BREACH IF THE PERSONAL INFORMATION IS NOT USED FOR OR IS NOT SUBJECT TO FURTHER UNAUTHORIZED DISCLOSURE.

(2) **Disclosure of breach.** (a) An individual or a commercial entity that conducts business in Colorado and that MAINTAINS, owns, or licenses computerized data that includes personal information about a resident of Colorado shall, when it becomes aware of a SECURITY breach, ~~of the security of the system,~~ conduct in good faith a prompt investigation to determine the likelihood that personal information has been or will be misused. The individual or the commercial entity shall give notice ~~as soon as possible~~ to the affected Colorado ~~resident~~ RESIDENTS unless the investigation determines that the misuse of information about a Colorado resident has not occurred and is not reasonably likely to occur. Notice ~~shall~~ MUST be made in the most expedient time possible and without unreasonable delay, BUT NOT LATER THAN FORTY-FIVE DAYS FROM THE DATE OF THE SECURITY BREACH, 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.

(a.3) NOTICE REQUIRED BY THIS SUBSECTION (2) TO AFFECTED

COLORADO RESIDENTS MUST INCLUDE, BUT NEED NOT BE LIMITED TO, THE FOLLOWING INFORMATION:

(I) THE DATE, ESTIMATED DATE, OR ESTIMATED DATE RANGE OF THE SECURITY BREACH;

(II) A DESCRIPTION OF THE PERSONAL INFORMATION THAT WAS ACQUIRED OR REASONABLY BELIEVED TO HAVE BEEN ACQUIRED AS PART OF THE SECURITY BREACH;

(III) INFORMATION THAT THE RESIDENT CAN USE TO CONTACT THE INDIVIDUAL OR COMMERCIAL ENTITY THAT WAS BREACHED TO INQUIRE ABOUT THE SECURITY BREACH;

(IV) THE TOLL-FREE NUMBERS, ADDRESSES, AND WEBSITES FOR CONSUMER REPORTING AGENCIES;

(V) THE TOLL-FREE NUMBER, ADDRESS, AND WEBSITE FOR THE FEDERAL TRADE COMMISSION; AND

(VI) A STATEMENT THAT THE RESIDENT CAN OBTAIN INFORMATION FROM THE FEDERAL TRADE COMMISSION AND THE CREDIT REPORTING AGENCIES ABOUT FRAUD ALERTS AND SECURITY FREEZES.

(a.5) THE BREACH OF ENCRYPTED OR OTHERWISE SECURED PERSONAL INFORMATION MUST BE DISCLOSED IN ACCORDANCE WITH THIS SECTION IF THE CONFIDENTIAL PROCESS, ENCRYPTION KEY, OR OTHER MEANS TO DECIPHER THE SECURED INFORMATION WAS ALSO ACQUIRED IN THE SECURITY BREACH OR WAS REASONABLY BELIEVED TO HAVE BEEN ACQUIRED.

(a.7) AN INDIVIDUAL OR COMMERCIAL ENTITY THAT IS REQUIRED TO PROVIDE NOTICE PURSUANT TO THIS SUBSECTION (2) IS PROHIBITED FROM CHARGING THE COST OF PROVIDING SUCH NOTICE TO INDIVIDUALS.

(b) An individual or a commercial entity that maintains

computerized data that includes personal information that the individual or the commercial entity does not own or license shall give notice to and cooperate with the owner or licensee of the information of any SECURITY breach ~~of the security of the system~~ immediately following discovery of a SECURITY breach, if misuse of personal information about a Colorado resident occurred or is likely to occur. Cooperation includes sharing with the owner or licensee information relevant to the SECURITY breach; except that such cooperation ~~shall not be deemed to~~ DOES NOT require the disclosure of confidential business information or trade secrets.

(c) Notice required by this section may be delayed if a law enforcement agency determines that the notice will impede a criminal investigation and the law enforcement agency has notified the individual or commercial entity that conducts business in Colorado not to send notice required by this section. Notice required by this section ~~shall~~ MUST be made in good faith, without unreasonable delay, and as soon as possible after the law enforcement agency determines that notification will no longer impede the investigation and has notified the individual or commercial entity that conducts business in Colorado that it is appropriate to send the notice required by this section.

(d) If an individual or commercial entity is required to notify more than one thousand Colorado residents of a SECURITY breach ~~of the security of the system~~ pursuant to this section, the individual or commercial entity shall also notify, without unreasonable delay, all consumer reporting agencies that compile and maintain files on consumers on a nationwide basis, as defined by THE FEDERAL "FAIR CREDIT REPORTING ACT", 15 U.S.C. sec. 1681a (p), of the anticipated date of the notification to the residents and the approximate number of

residents who are to be notified. Nothing in this ~~paragraph (d) shall be construed to require~~ SUBSECTION (2)(d) REQUIRES the individual or commercial entity to provide to the consumer reporting agency the names or other personal information of SECURITY breach notice recipients. This ~~paragraph (d) shall~~ SUBSECTION (2)(d) DOES not apply to a person who is subject to Title V of the federal "Gramm-Leach-Bliley Act", 15 U.S.C. sec. 6801 et seq.

(e) A WAIVER OF THESE NOTIFICATION RIGHTS OR RESPONSIBILITIES IS VOID AS AGAINST PUBLIC POLICY.

(f) REGARDLESS OF THE NEED TO PROVIDE NOTICE TO AFFECTED COLORADO RESIDENTS PURSUANT TO THIS SECTION, THE INDIVIDUAL OR COMMERCIAL ENTITY THAT WAS BREACHED SHALL PROVIDE NOTICE OF ANY UNAUTHORIZED ACQUISITION OF UNENCRYPTED OR ENCRYPTED COMPUTERIZED DATA THAT COMPROMISES THE SECURITY, CONFIDENTIALITY, OR INTEGRITY OF PERSONAL INFORMATION MAINTAINED BY AN INDIVIDUAL OR COMMERCIAL ENTITY TO THE COLORADO ATTORNEY GENERAL AS SOON AS PRACTICABLE BUT NOT LATER THAN SEVEN DAYS AFTER DISCOVERY OF THE UNAUTHORIZED ACQUISITION OF DATA IF SUCH UNAUTHORIZED ACQUISITION AFFECTED OR IS REASONABLY BELIEVED TO HAVE AFFECTED FIVE HUNDRED COLORADO RESIDENTS OR MORE.

(3) **Procedures deemed in compliance with notice requirements.** (a) ~~Under~~ PURSUANT TO this section, an individual or a commercial entity that maintains its own notification procedures as part of an information security policy for the treatment of personal information and whose procedures are otherwise consistent with the timing requirements of this section ~~shall be deemed to be~~ IS in compliance with the notice requirements of this section if the individual or the

commercial entity notifies affected Colorado customers in accordance with its policies in the event of a SECURITY breach. ~~of security of the system.~~

(b) An individual or a commercial entity that is regulated by state or federal law and that maintains procedures for a SECURITY breach ~~of the security of the system~~ pursuant to the laws, rules, regulations, guidances, or guidelines established by its primary or functional state or federal regulator is ~~deemed to be~~ in compliance with this section.

(4) **Violations.** The attorney general may bring an action in law or equity to address violations of this section, SECTION 6-1-713, OR SECTION 6-1-713.5, and for other relief that may be appropriate to ensure compliance with this section or to recover direct economic damages resulting from a violation, 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.

(5) **Attorney general criminal authority.** UPON RECEIPT OF NOTICE PURSUANT TO SUBSECTION (2) OF THIS SECTION, THE ATTORNEY GENERAL HAS THE AUTHORITY TO INVESTIGATE AND PROSECUTE ANY RELATED CRIMINAL VIOLATIONS OF SECTION 18-5.5-102.

SECTION 4. Effective date. This act takes effect September 1, 2018.

SECTION 5. Safety clause. The general assembly hereby finds, determines, and declares that this act is necessary for the immediate preservation of the public peace, health, and safety.