

Second Regular Session  
Seventy-first General Assembly  
STATE OF COLORADO

**ENGROSSED**

*This Version Includes All Amendments Adopted  
on Second Reading in the House of Introduction*

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  
Appropriations

**Senate Committees**

---

**A BILL FOR AN ACT**

101 **CONCERNING STRENGTHENING PROTECTIONS FOR CONSUMER DATA**  
102 **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,

Shading denotes HOUSE amendment. Double underlining denotes SENATE amendment.  
Capital letters or bold & italic numbers indicate new material to be added to existing statute.  
Dashes through the words indicate deletions from existing statute.

HOUSE  
Amended 2nd Reading  
April 19, 2018

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.

---

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

2 **SECTION 1.** In Colorado Revised Statutes, 6-1-713, **amend** (1),  
3 (2), and (3) as follows:

4 **6-1-713. Disposal of personal identifying information - policy**  
5 **- definitions.** (1) Each ~~public and private~~ COVERED entity in the state that  
6 ~~uses~~ MAINTAINS PAPER OR ELECTRONIC documents during the course of  
7 business that contain personal identifying information shall develop a  
8 WRITTEN policy for the destruction or proper disposal of THOSE paper AND  
9 ELECTRONIC documents containing personal identifying information.  
10 UNLESS OTHERWISE REQUIRED BY STATE OR FEDERAL LAW OR  
11 REGULATION, THE WRITTEN POLICY MUST REQUIRE THAT, WHEN SUCH  
12 PAPER OR ELECTRONIC DOCUMENTS ARE NO LONGER NEEDED, THE  
13 COVERED ENTITY SHALL DESTROY OR ARRANGE FOR THE DESTRUCTION OF  
14 SUCH PAPER AND ELECTRONIC DOCUMENTS WITHIN ITS CUSTODY OR  
15 CONTROL THAT CONTAIN PERSONAL IDENTIFYING INFORMATION BY  
16 SHREDDING, ERASING, OR OTHERWISE MODIFYING THE PERSONAL  
17 IDENTIFYING INFORMATION IN THE PAPER OR ELECTRONIC DOCUMENTS TO  
18 MAKE THE PERSONAL IDENTIFYING INFORMATION UNREADABLE OR  
19 INDECIPHERABLE THROUGH ANY MEANS.

20 (2) For the purposes of this section AND SECTION 6-1-713.5:

21 (a) "COVERED ENTITY" MEANS A PERSON, AS DEFINED IN SECTION  
22 6-1-102(6), THAT MAINTAINS, OWNS, OR LICENSES PERSONAL IDENTIFYING

1 INFORMATION IN THE COURSE OF THE PERSON'S BUSINESS, VOCATION, OR  
2 OCCUPATION. "COVERED ENTITY" DOES NOT INCLUDE A PERSON ACTING  
3 AS A THIRD-PARTY SERVICE PROVIDER AS DEFINED IN SECTION 6-1-713.5.

4 (b) "Personal identifying information" means a social security  
5 number; a personal identification number; a password; a pass code; an  
6 official state or government-issued driver's license or identification card  
7 number; a government passport number; biometric data, AS DEFINED IN  
8 SECTION 6-1-716 (1)(a); an employer, student, or military identification  
9 number; or a financial transaction device, AS DEFINED IN SECTION  
10 18-5-701 (3).

11 (3) ~~A public entity that is managing its records in compliance with~~  
12 ~~part 1 of article 80 of title 24, C.R.S., shall be deemed to have met its~~  
13 ~~obligations under subsection (1) of this section~~ A COVERED ENTITY THAT  
14 IS REGULATED BY STATE OR FEDERAL LAW AND THAT MAINTAINS  
15 PROCEDURES FOR DISPOSAL OF PERSONAL IDENTIFYING INFORMATION  
16 PURSUANT TO THE LAWS, RULES, REGULATIONS, GUIDANCES, OR  
17 GUIDELINES ESTABLISHED BY ITS STATE OR FEDERAL REGULATOR IS IN  
18 COMPLIANCE WITH THIS SECTION.

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

21 **6-1-713.5. Protection of personal identifying information -**  
22 **definition.** (1) TO PROTECT PERSONAL IDENTIFYING INFORMATION, AS  
23 DEFINED IN SECTION 6-1-713 (2), FROM UNAUTHORIZED ACCESS, USE,  
24 MODIFICATION, DISCLOSURE, OR DESTRUCTION, A COVERED ENTITY THAT  
25 MAINTAINS, OWNS, OR LICENSES PERSONAL IDENTIFYING INFORMATION OF  
26 AN INDIVIDUAL RESIDING IN THE STATE SHALL IMPLEMENT AND MAINTAIN  
27 REASONABLE SECURITY PROCEDURES AND PRACTICES THAT ARE

1 APPROPRIATE TO THE NATURE OF THE PERSONAL IDENTIFYING  
2 INFORMATION AND THE NATURE AND SIZE OF THE BUSINESS AND ITS  
3 OPERATIONS.

4 (2) UNLESS A COVERED ENTITY AGREES TO PROVIDE ITS OWN  
5 SECURITY PROTECTION FOR THE INFORMATION IT DISCLOSES TO A  
6 THIRD-PARTY SERVICE PROVIDER, THE COVERED ENTITY SHALL REQUIRE  
7 THAT THE THIRD-PARTY SERVICE PROVIDER IMPLEMENT AND MAINTAIN  
8 REASONABLE SECURITY PROCEDURES AND PRACTICES THAT ARE:

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

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

14 (3) FOR THE PURPOSES OF SUBSECTION (2) OF THIS SECTION, A  
15 DISCLOSURE OF PERSONAL IDENTIFYING INFORMATION DOES NOT INCLUDE  
16 DISCLOSURE OF INFORMATION TO A THIRD PARTY UNDER CIRCUMSTANCES  
17 WHERE THE COVERED ENTITY RETAINS PRIMARY RESPONSIBILITY FOR  
18 IMPLEMENTING AND MAINTAINING REASONABLE SECURITY PROCEDURES  
19 AND PRACTICES APPROPRIATE TO THE NATURE OF THE PERSONAL  
20 IDENTIFYING INFORMATION AND THE COVERED ENTITY IMPLEMENTS AND  
21 MAINTAINS TECHNICAL CONTROLS THAT ARE REASONABLY DESIGNED TO:

22 (a) HELP PROTECT THE PERSONAL IDENTIFYING INFORMATION  
23 FROM UNAUTHORIZED ACCESS, USE, MODIFICATION, DISCLOSURE, OR  
24 DESTRUCTION; OR

25 (b) EFFECTIVELY ELIMINATE THE THIRD PARTY'S ABILITY TO  
26 ACCESS THE PERSONAL IDENTIFYING INFORMATION, NOTWITHSTANDING  
27 THE THIRD PARTY'S PHYSICAL POSSESSION OF THE PERSONAL IDENTIFYING

1 INFORMATION.

2 (4) A COVERED ENTITY THAT IS REGULATED BY STATE OR FEDERAL  
3 LAW AND THAT MAINTAINS PROCEDURES FOR PROTECTION OF PERSONAL  
4 IDENTIFYING INFORMATION PURSUANT TO THE LAWS, RULES,  
5 REGULATIONS, GUIDANCES, OR GUIDELINES ESTABLISHED BY ITS STATE OR  
6 FEDERAL REGULATOR IS IN COMPLIANCE WITH THIS SECTION.

7 (5) FOR THE PURPOSES OF THIS SECTION, "THIRD-PARTY SERVICE  
8 PROVIDER" MEANS AN ENTITY THAT HAS BEEN CONTRACTED WITH TO  
9 MAINTAIN, STORE, OR PROCESS PERSONAL IDENTIFYING INFORMATION ON  
10 BEHALF OF A COVERED ENTITY.

11 **SECTION 3.** In Colorado Revised Statutes, 6-1-716, **amend** (2),  
12 (3), and (4); **repeal and reenact, with amendments,** (1); and **add** (5) as  
13 follows:

14 **6-1-716. Notification of security breach. (1) Definitions.** AS  
15 USED IN THIS SECTION, UNLESS THE CONTEXT OTHERWISE REQUIRES:

16 (a) "BIOMETRIC DATA" MEANS UNIQUE BIOMETRIC DATA  
17 GENERATED FROM MEASUREMENTS OR ANALYSIS OF HUMAN BODY  
18 CHARACTERISTICS FOR THE PURPOSE OF AUTHENTICATING THE INDIVIDUAL  
19 WHEN HE OR SHE ACCESSES AN ONLINE ACCOUNT.

20 (b) "COVERED ENTITY" MEANS A PERSON, AS DEFINED IN SECTION  
21 6-1-102 (6), THAT MAINTAINS, OWNS, OR LICENSES PERSONAL  
22 INFORMATION IN THE COURSE OF THE PERSON'S BUSINESS, VOCATION, OR  
23 OCCUPATION. "COVERED ENTITY" DOES NOT INCLUDE A THIRD-PARTY  
24 SERVICE PROVIDER AS DEFINED IN SUBSECTION (1)(i) OF THIS SECTION.

25 (c) "DETERMINATION THAT A SECURITY BREACH OCCURRED"  
26 MEANS THE POINT IN TIME AT WHICH THERE IS SUFFICIENT EVIDENCE TO  
27 CONCLUDE THAT A SECURITY BREACH HAS TAKEN PLACE.

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

5 (e) "MEDICAL INFORMATION" MEANS ANY INFORMATION ABOUT A  
6 CONSUMER'S MEDICAL OR MENTAL HEALTH TREATMENT OR DIAGNOSIS BY  
7 A HEALTH CARE PROFESSIONAL.

8 (f) "NOTICE" MEANS:

9 (I) WRITTEN NOTICE TO THE POSTAL ADDRESS LISTED IN THE  
10 RECORDS OF THE COVERED ENTITY;

11 (II) TELEPHONIC NOTICE;

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

18 (IV) SUBSTITUTE NOTICE, IF THE COVERED ENTITY REQUIRED TO  
19 PROVIDE NOTICE DEMONSTRATES THAT THE COST OF PROVIDING NOTICE  
20 WILL EXCEED TWO HUNDRED FIFTY THOUSAND DOLLARS, THE AFFECTED  
21 CLASS OF PERSONS TO BE NOTIFIED EXCEEDS TWO HUNDRED FIFTY  
22 THOUSAND COLORADO RESIDENTS, OR THE COVERED ENTITY DOES NOT  
23 HAVE SUFFICIENT CONTACT INFORMATION TO PROVIDE NOTICE.

24 SUBSTITUTE NOTICE CONSISTS OF ALL OF THE FOLLOWING:

25 (A) E-MAIL NOTICE IF THE COVERED ENTITY HAS E-MAIL  
26 ADDRESSES FOR THE MEMBERS OF THE AFFECTED CLASS OF COLORADO  
27 RESIDENTS;

1 (B) CONSPICUOUS POSTING OF THE NOTICE ON THE WEBSITE PAGE  
2 OF THE COVERED ENTITY IF THE COVERED ENTITY MAINTAINS ONE; AND

3 (C) NOTIFICATION TO MAJOR STATEWIDE MEDIA.

4 (g) (I) (A) "PERSONAL INFORMATION" MEANS A COLORADO  
5 RESIDENT'S FIRST NAME OR FIRST INITIAL AND LAST NAME IN COMBINATION  
6 WITH ANY ONE OR MORE OF THE FOLLOWING DATA ELEMENTS THAT  
7 RELATE TO THE RESIDENT, WHEN THE DATA ELEMENTS ARE NOT  
8 ENCRYPTED, REDACTED, OR SECURED BY ANY OTHER METHOD RENDERING  
9 THE NAME OR THE ELEMENT UNREADABLE OR UNUSABLE: SOCIAL  
10 SECURITY NUMBER; STUDENT, MILITARY, OR PASSPORT IDENTIFICATION  
11 NUMBER; DRIVER'S LICENSE NUMBER OR IDENTIFICATION CARD NUMBER;  
12 MEDICAL INFORMATION; HEALTH INSURANCE IDENTIFICATION NUMBER; OR  
13 BIOMETRIC DATA;

14 (B) A COLORADO RESIDENT'S USERNAME OR E-MAIL ADDRESS, IN  
15 COMBINATION WITH A PASSWORD OR SECURITY QUESTIONS AND ANSWERS,  
16 THAT WOULD PERMIT ACCESS TO AN ONLINE ACCOUNT; OR

17 (C) A COLORADO RESIDENT'S ACCOUNT NUMBER OR CREDIT OR  
18 DEBIT CARD NUMBER IN COMBINATION WITH ANY REQUIRED SECURITY  
19 CODE, ACCESS CODE, OR PASSWORD THAT WOULD PERMIT ACCESS TO THAT  
20 ACCOUNT.

21 (II) "PERSONAL INFORMATION" DOES NOT INCLUDE PUBLICLY  
22 AVAILABLE INFORMATION THAT IS LAWFULLY MADE AVAILABLE TO THE  
23 GENERAL PUBLIC FROM FEDERAL, STATE, OR LOCAL GOVERNMENT  
24 RECORDS OR WIDELY DISTRIBUTED MEDIA.

25 (h) "SECURITY BREACH" MEANS THE UNAUTHORIZED ACQUISITION  
26 OF UNENCRYPTED COMPUTERIZED DATA THAT COMPROMISES THE  
27 SECURITY, CONFIDENTIALITY, OR INTEGRITY OF PERSONAL INFORMATION

1 MAINTAINED BY A COVERED ENTITY. GOOD FAITH ACQUISITION OF  
2 PERSONAL INFORMATION BY AN EMPLOYEE OR AGENT OF A COVERED  
3 ENTITY FOR THE COVERED ENTITY'S BUSINESS PURPOSES IS NOT A  
4 SECURITY BREACH IF THE PERSONAL INFORMATION IS NOT USED FOR A  
5 PURPOSE UNRELATED TO THE LAWFUL OPERATION OF THE BUSINESS OR IS  
6 NOT SUBJECT TO FURTHER UNAUTHORIZED DISCLOSURE.

7 (i) "THIRD-PARTY SERVICE PROVIDER" MEANS AN ENTITY THAT  
8 HAS BEEN CONTRACTED WITH TO MAINTAIN, STORE, OR PROCESS PERSONAL  
9 INFORMATION ON BEHALF OF A COVERED ENTITY.

10 (2) **Disclosure of breach.** (a) ~~An individual or a commercial~~ A  
11 COVERED entity that conducts business in Colorado and that MAINTAINS,  
12 owns, or licenses computerized data that includes personal information  
13 about a resident of Colorado shall, when it becomes aware of a breach, of  
14 ~~the security of the system~~ DETERMINES THAT A SECURITY BREACH HAS  
15 OCCURRED, conduct in good faith a prompt investigation to determine the  
16 likelihood that personal information has been or will be misused. The  
17 ~~individual or the commercial~~ COVERED entity shall give notice as soon as  
18 possible to the affected Colorado resident RESIDENTS unless the  
19 investigation determines that the misuse of information about a Colorado  
20 resident has not occurred and is not reasonably likely to occur. Notice  
21 shall MUST be made in the most expedient time possible and without  
22 unreasonable delay, BUT NOT LATER THAN THIRTY DAYS AFTER THE DATE  
23 OF DETERMINATION THAT A SECURITY BREACH OCCURRED, consistent with  
24 the legitimate needs of law enforcement and consistent with any measures  
25 necessary to determine the scope of the breach and to restore the  
26 reasonable integrity of the computerized data system.

27 (a.2) EXCEPT AS OTHERWISE PROVIDED FOR IN SUBSECTION (2)(a.3)



1 OF THIS SECTION, IN THE CASE OF A BREACH OF PERSONAL INFORMATION,  
2 NOTICE REQUIRED BY THIS SUBSECTION (2) TO AFFECTED COLORADO  
3 RESIDENTS MUST INCLUDE, BUT NEED NOT BE LIMITED TO, THE FOLLOWING  
4 INFORMATION:

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

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

10 (III) INFORMATION THAT THE RESIDENT CAN USE TO CONTACT THE  
11 COVERED ENTITY THAT WAS BREACHED TO INQUIRE ABOUT THE SECURITY  
12 BREACH;

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

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

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

20 (a.3) IF AN INVESTIGATION BY THE COVERED ENTITY PURSUANT TO  
21 SUBSECTION (2)(a) OF THIS SECTION DETERMINES THAT THE TYPE OF  
22 PERSONAL INFORMATION DESCRIBED IN SUBSECTION (1)(g)(I)(B) OF THIS  
23 SECTION HAS BEEN MISUSED OR IS REASONABLY LIKELY TO BE MISUSED,  
24 THEN THE COVERED ENTITY SHALL, IN ADDITION TO THE NOTICE  
25 OTHERWISE REQUIRED BY THIS SECTION AND IN THE MOST EXPEDIENT TIME  
26 POSSIBLE AND WITHOUT UNREASONABLE DELAY, BUT NO LATER THAN  
27 THIRTY DAYS AFTER THE DATE OF DETERMINATION THAT A SECURITY

1 BREACH OCCURRED, CONSISTENT WITH THE LEGITIMATE NEEDS OF LAW  
2 ENFORCEMENT AND CONSISTENT WITH ANY MEASURES NECESSARY TO  
3 DETERMINE THE SCOPE OF THE BREACH AND TO RESTORE THE REASONABLE  
4 INTEGRITY OF THE COMPUTERIZED DATA SYSTEM:

5 (I) DIRECT THE PERSON WHOSE PERSONAL INFORMATION HAS BEEN  
6 BREACHED TO PROMPTLY CHANGE HIS OR HER PASSWORD AND SECURITY  
7 QUESTION OR ANSWER, AS APPLICABLE, OR TO TAKE OTHER STEPS  
8 APPROPRIATE TO PROTECT THE ONLINE ACCOUNT WITH THE COVERED  
9 ENTITY AND ALL OTHER ONLINE ACCOUNTS FOR WHICH THE PERSON WHOSE  
10 PERSONAL INFORMATION HAS BEEN BREACHED THAT USES THE SAME USER  
11 NAME OR E-MAIL ADDRESS AND PASSWORD OR SECURITY QUESTION OR  
12 ANSWER.

13 (II) FOR LOG-IN CREDENTIALS OF AN E-MAIL ACCOUNT FURNISHED  
14 BY THE COVERED ENTITY, THE COVERED ENTITY SHALL NOT COMPLY WITH  
15 THIS SECTION BY PROVIDING THE SECURITY BREACH NOTIFICATION TO  
16 THAT E-MAIL ADDRESS, BUT MAY INSTEAD COMPLY WITH THIS SECTION BY  
17 PROVIDING NOTICE, AS DEFINED IN SUBSECTION (1)(f) OF THIS SECTION, OR  
18 BY CLEAR AND CONSPICUOUS NOTICE DELIVERED TO THE RESIDENT ONLINE  
19 WHEN THE RESIDENT IS CONNECTED TO THE ONLINE ACCOUNT FROM AN  
20 INTERNET PROTOCOL ADDRESS OR ONLINE LOCATION FROM WHICH THE  
21 COVERED ENTITY KNOWS THE RESIDENT CUSTOMARILY ACCESSES THE  
22 ACCOUNT.

23 (a.4) THE BREACH OF ENCRYPTED OR OTHERWISE SECURED  
24 PERSONAL INFORMATION MUST BE DISCLOSED IN ACCORDANCE WITH THIS  
25 SECTION IF THE CONFIDENTIAL PROCESS, ENCRYPTION KEY, OR OTHER  
26 MEANS TO DECIPHER THE SECURED INFORMATION WAS ALSO ACQUIRED IN  
27 THE SECURITY BREACH OR WAS REASONABLY BELIEVED TO HAVE BEEN

1 ACQUIRED.

2 (a.5) A COVERED ENTITY THAT IS REQUIRED TO PROVIDE NOTICE TO  
3 AFFECTED COLORADO RESIDENTS PURSUANT TO THIS SUBSECTION (2) IS  
4 PROHIBITED FROM CHARGING THE COST OF PROVIDING SUCH NOTICE TO  
5 SUCH RESIDENTS.

6 (a.6) NOTHING IN THIS SUBSECTION (2) PROHIBITS THE NOTICE  
7 DESCRIBED IN THIS SUBSECTION (2) FROM CONTAINING ADDITIONAL  
8 INFORMATION, INCLUDING ANY INFORMATION THAT MAY BE REQUIRED BY  
9 STATE OR FEDERAL LAW.

10 (b) ~~An individual or a commercial entity that maintains~~ IF A  
11 COVERED ENTITY USES A THIRD-PARTY SERVICE PROVIDER TO MAINTAIN  
12 computerized data that includes personal information, ~~that the individual~~  
13 ~~or the commercial entity does not own or license~~ THEN THE THIRD-PARTY  
14 SERVICE PROVIDER shall give notice to and cooperate with ~~the owner or~~  
15 ~~licensee of the information of any breach of the security of the system~~  
16 ~~immediately~~ THE COVERED ENTITY IN THE EVENT OF A SECURITY BREACH  
17 THAT COMPROMISES SUCH COMPUTERIZED DATA, INCLUDING NOTIFYING  
18 THE COVERED ENTITY OF ANY SECURITY BREACH AS SOON AS POSSIBLE  
19 AND WITHOUT UNREASONABLE DELAY following discovery of a SECURITY  
20 breach, if misuse of personal information about a Colorado resident  
21 occurred or is likely to occur. Cooperation includes sharing with the  
22 ~~owner or licensee~~ COVERED ENTITY information relevant to the SECURITY  
23 breach; except that such cooperation ~~shall not be deemed to~~ DOES NOT  
24 require the disclosure of confidential business information or trade  
25 secrets.

26 (c) Notice required by this section may be delayed if a law  
27 enforcement agency determines that the notice will impede a criminal

1 investigation and the law enforcement agency has notified the individual  
2 or commercial COVERED entity that conducts business in Colorado not to  
3 send notice required by this section. Notice required by this section shall  
4 MUST be made in good faith, without unreasonable delay and as soon as  
5 possible BUT NOT LATER THAN THIRTY DAYS after the law enforcement  
6 agency determines that notification will no longer impede the  
7 investigation and has notified the individual or commercial COVERED  
8 entity that conducts business in Colorado that it is appropriate to send the  
9 notice required by this section.

10 (d) If an individual or commercial A COVERED entity is required  
11 to notify more than one thousand Colorado residents of a SECURITY  
12 breach of the security of the system pursuant to this section, the individual  
13 or commercial COVERED entity shall also notify, without unreasonable  
14 delay, all consumer reporting agencies that compile and maintain files on  
15 consumers on a nationwide basis, as defined by THE FEDERAL "FAIR  
16 CREDIT REPORTING ACT", 15 U.S.C. sec. 1681a (p), of the anticipated  
17 date of the notification to the residents and the approximate number of  
18 residents who are to be notified. Nothing in this paragraph (d) shall be  
19 construed to require SUBSECTION (2)(d) REQUIRES the individual or  
20 commercial COVERED entity to provide to the consumer reporting agency  
21 the names or other personal information of SECURITY breach notice  
22 recipients. This paragraph (d) shall SUBSECTION (2)(d) DOES not apply to  
23 a person COVERED ENTITY who is subject to Title V of the federal  
24 "Gramm-Leach-Bliley Act", 15 U.S.C. sec. 6801 et seq.

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

27 (f) (I) THE INDIVIDUAL OR COMMERCIAL ENTITY THAT WAS

1 BREACHED SHALL PROVIDE NOTICE OF ANY SECURITY BREACH TO THE  
2 COLORADO ATTORNEY GENERAL AS SOON AS PRACTICABLE BUT NOT  
3 LATER THAN THIRTY DAYS AFTER THE DATE OF DETERMINATION THAT A  
4 SECURITY BREACH OCCURRED IF THE SECURITY BREACH IS REASONABLY  
5 BELIEVED TO HAVE AFFECTED FIVE HUNDRED COLORADO RESIDENTS OR  
6 MORE, UNLESS THE INVESTIGATION DETERMINES THAT THE MISUSE OF  
7 INFORMATION ABOUT A COLORADO RESIDENT HAS NOT OCCURRED AND IS  
8 NOT LIKELY TO OCCUR.

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

15 (3) **Procedures deemed in compliance with notice**  
16 **requirements.** (a) ~~Under~~ PURSUANT TO this section, ~~an individual or a~~  
17 ~~commercial~~ A COVERED entity that maintains its own notification  
18 procedures as part of an information security policy for the treatment of  
19 personal information and whose procedures are otherwise consistent with  
20 the timing requirements of this section ~~shall be deemed to be~~ IS in  
21 compliance with the notice requirements of this section if the ~~individual~~  
22 ~~or the commercial~~ COVERED entity notifies affected Colorado customers  
23 in accordance with its policies in the event of a ~~breach of security of the~~  
24 ~~system~~ SECURITY BREACH; EXCEPT THAT NOTICE TO THE ATTORNEY  
25 GENERAL IS STILL REQUIRED PURSUANT TO SUBSECTION (2)(f) OF THIS  
26 SECTION.

27 (b) ~~An individual or a commercial~~ A COVERED entity that is

1 regulated by state or federal law and that maintains procedures for a  
2 SECURITY breach of the security of the system pursuant to the laws, rules,  
3 regulations, guidances, or guidelines established by its ~~primary or~~  
4 ~~functional~~ state or federal regulator is ~~deemed to be~~ in compliance with  
5 this section; EXCEPT THAT NOTICE TO THE ATTORNEY GENERAL IS STILL  
6 REQUIRED PURSUANT TO SUBSECTION (2)(f) OF THIS SECTION. IN THE CASE  
7 OF A CONFLICT BETWEEN THE TIME PERIOD FOR NOTICE TO INDIVIDUALS  
8 THAT IS REQUIRED PURSUANT TO THIS SUBSECTION (2) AND THE  
9 APPLICABLE STATE OR FEDERAL LAW OR REGULATION, THE LAW OR  
10 REGULATION WITH THE SHORTEST TIME FRAME FOR NOTICE TO THE  
11 INDIVIDUAL CONTROLS.

12 (4) **Violations.** The attorney general may bring an action in law  
13 or equity to address violations of this section, SECTION 6-1-713, OR  
14 SECTION 6-1-713.5, and for other relief that may be appropriate to ensure  
15 compliance with this section or to recover direct economic damages  
16 resulting from a violation, or both. The provisions of this section are not  
17 exclusive and do not relieve ~~an individual or a commercial~~ A COVERED  
18 entity subject to this section from compliance with all other applicable  
19 provisions of law.

20 (5) **Attorney general criminal authority.** UPON RECEIPT OF  
21 NOTICE PURSUANT TO SUBSECTION (2) OF THIS SECTION, AND WITH EITHER  
22 A REQUEST FROM THE GOVERNOR TO PROSECUTE A PARTICULAR CASE OR  
23 WITH THE APPROVAL OF THE DISTRICT ATTORNEY WITH JURISDICTION TO  
24 PROSECUTE CASES IN THE JUDICIAL DISTRICT WHERE A CASE HAS BEEN,  
25 WILL BE, OR COULD BE BROUGHT, THE ATTORNEY GENERAL HAS THE  
26 AUTHORITY TO PROSECUTE ANY CRIMINAL VIOLATIONS OF SECTION  
27 18-5.5-102.

1           **SECTION 4.** In Colorado Revised Statutes, **add** article 73 to title  
2 24 as follows:

3   **ARTICLE 73**

4                                   **Security Breaches and Personal Information**

5           **24-73-101. Governmental entity - disposal of personal**  
6 **identifying information - policy - definitions.** (1) EACH

7 GOVERNMENTAL ENTITY IN THE STATE THAT MAINTAINS PAPER OR  
8 ELECTRONIC DOCUMENTS DURING THE COURSE OF BUSINESS THAT  
9 CONTAIN PERSONAL IDENTIFYING INFORMATION SHALL DEVELOP A  
10 WRITTEN POLICY FOR THE DESTRUCTION OR PROPER DISPOSAL OF THOSE  
11 PAPER AND ELECTRONIC DOCUMENTS CONTAINING PERSONAL IDENTIFYING  
12 INFORMATION. UNLESS OTHERWISE REQUIRED BY STATE OR FEDERAL LAW  
13 OR REGULATION, THE WRITTEN POLICY MUST REQUIRE THAT, WHEN SUCH  
14 PAPER OR ELECTRONIC DOCUMENTS ARE NO LONGER NEEDED, THE  
15 GOVERNMENTAL ENTITY DESTROY OR ARRANGE FOR THE DESTRUCTION OF  
16 SUCH PAPER AND ELECTRONIC DOCUMENTS WITHIN ITS CUSTODY OR  
17 CONTROL THAT CONTAIN PERSONAL IDENTIFYING INFORMATION BY  
18 SHREDDING, ERASING, OR OTHERWISE MODIFYING THE PERSONAL  
19 IDENTIFYING INFORMATION IN THE PAPER OR ELECTRONIC DOCUMENTS TO  
20 MAKE THE PERSONAL IDENTIFYING INFORMATION UNREADABLE OR  
21 INDECIPHERABLE THROUGH ANY MEANS.

22           (2) A GOVERNMENTAL ENTITY THAT IS REGULATED BY STATE OR  
23 FEDERAL LAW AND THAT MAINTAINS PROCEDURES FOR DISPOSAL OF  
24 PERSONAL IDENTIFYING INFORMATION PURSUANT TO THE LAWS, RULES,  
25 REGULATIONS, GUIDANCES, OR GUIDELINES ESTABLISHED BY ITS STATE OR  
26 FEDERAL REGULATOR IS IN COMPLIANCE WITH THIS SECTION.

27           (3) UNLESS A GOVERNMENTAL ENTITY SPECIFICALLY CONTRACTS

1 WITH A RECYCLER OR DISPOSAL FIRM FOR DESTRUCTION OF DOCUMENTS  
2 THAT CONTAIN PERSONAL IDENTIFYING INFORMATION, NOTHING IN THIS  
3 SECTION REQUIRES A RECYCLER OR DISPOSAL FIRM TO VERIFY THAT THE  
4 DOCUMENTS CONTAINED IN THE PRODUCTS IT RECEIVES FOR DISPOSAL OR  
5 RECYCLING HAVE BEEN PROPERLY DESTROYED OR DISPOSED OF AS  
6 REQUIRED BY THIS SECTION.

7 (4) FOR THE PURPOSES OF THIS SECTION AND SECTION 24-73-102,  
8 UNLESS THE CONTEXT OTHERWISE REQUIRES:

9 (a) "GOVERNMENTAL ENTITY" MEANS THE STATE AND ANY STATE  
10 AGENCY OR INSTITUTION, INCLUDING THE JUDICIAL DEPARTMENT,  
11 COUNTY, CITY AND COUNTY, INCORPORATED CITY OR TOWN, SCHOOL  
12 DISTRICT, SPECIAL IMPROVEMENT DISTRICT, AUTHORITY, AND EVERY  
13 OTHER KIND OF DISTRICT, INSTRUMENTALITY, OR POLITICAL SUBDIVISION  
14 OF THE STATE ORGANIZED PURSUANT TO LAW. "GOVERNMENTAL ENTITY"  
15 INCLUDES ENTITIES GOVERNED BY HOME RULE CHARTERS.  
16 "GOVERNMENTAL ENTITY" DOES NOT INCLUDE AN ENTITY ACTING AS A  
17 THIRD-PARTY SERVICE PROVIDER AS DEFINED IN SECTION 24-73-102.

18 (b) "PERSONAL IDENTIFYING INFORMATION" MEANS A SOCIAL  
19 SECURITY NUMBER; A PERSONAL IDENTIFICATION NUMBER; A PASSWORD;  
20 A PASS CODE; AN OFFICIAL STATE OR GOVERNMENT-ISSUED DRIVER'S  
21 LICENSE OR IDENTIFICATION CARD NUMBER; A GOVERNMENT PASSPORT  
22 NUMBER; BIOMETRIC DATA, AS DEFINED IN SECTION 24-73-103 (1)(a); AN  
23 EMPLOYER, STUDENT, OR MILITARY IDENTIFICATION NUMBER; OR A  
24 FINANCIAL TRANSACTION DEVICE, AS DEFINED IN SECTION 18-5-701 (3).

25 **24-73-102. Governmental entity - protection of personal**  
26 **identifying information - definition.** (1) TO PROTECT PERSONAL  
27 IDENTIFYING INFORMATION, AS DEFINED IN SECTION 24-73-101 (4)(b),



1 FROM UNAUTHORIZED ACCESS, USE, MODIFICATION, DISCLOSURE, OR  
2 DESTRUCTION, A GOVERNMENTAL ENTITY THAT MAINTAINS, OWNS, OR  
3 LICENSES PERSONAL IDENTIFYING INFORMATION SHALL IMPLEMENT AND  
4 MAINTAIN REASONABLE SECURITY PROCEDURES AND PRACTICES THAT ARE  
5 APPROPRIATE TO THE NATURE OF THE PERSONAL IDENTIFYING  
6 INFORMATION AND THE NATURE AND SIZE OF THE GOVERNMENTAL ENTITY.

7 (2) UNLESS A GOVERNMENTAL ENTITY AGREES TO PROVIDE ITS  
8 OWN SECURITY PROTECTION FOR THE INFORMATION IT DISCLOSES TO A  
9 THIRD-PARTY SERVICE PROVIDER, THE GOVERNMENTAL ENTITY SHALL  
10 REQUIRE THAT THE THIRD-PARTY SERVICE PROVIDER IMPLEMENT AND  
11 MAINTAIN REASONABLE SECURITY PROCEDURES AND PRACTICES THAT  
12 ARE:

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

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

18 (3) FOR THE PURPOSES OF SUBSECTION (2) OF THIS SECTION, A  
19 DISCLOSURE OF PERSONAL IDENTIFYING INFORMATION DOES NOT INCLUDE  
20 DISCLOSURE OF INFORMATION TO A THIRD PARTY UNDER CIRCUMSTANCES  
21 WHERE THE GOVERNMENTAL ENTITY RETAINS PRIMARY RESPONSIBILITY  
22 FOR IMPLEMENTING AND MAINTAINING REASONABLE SECURITY  
23 PROCEDURES AND PRACTICES APPROPRIATE TO THE NATURE OF THE  
24 PERSONAL IDENTIFYING INFORMATION AND THE GOVERNMENTAL ENTITY  
25 IMPLEMENTS AND MAINTAINS TECHNICAL CONTROLS REASONABLY  
26 DESIGNED TO:

27 (a) HELP PROTECT THE PERSONAL IDENTIFYING INFORMATION

1 FROM UNAUTHORIZED ACCESS, MODIFICATION, DISCLOSURE, OR  
2 DESTRUCTION; OR

3 (b) EFFECTIVELY ELIMINATE THE THIRD PARTY'S ABILITY TO  
4 ACCESS THE PERSONAL IDENTIFYING INFORMATION, NOTWITHSTANDING  
5 THE THIRD PARTY'S PHYSICAL POSSESSION OF THE PERSONAL IDENTIFYING  
6 INFORMATION.

7 (4) A GOVERNMENTAL ENTITY THAT IS REGULATED BY STATE OR  
8 FEDERAL LAW AND THAT MAINTAINS PROCEDURES FOR STORAGE OF  
9 PERSONAL IDENTIFYING INFORMATION PURSUANT TO THE LAWS, RULES,  
10 REGULATIONS, GUIDANCES, OR GUIDELINES ESTABLISHED BY ITS STATE OR  
11 FEDERAL REGULATOR IS IN COMPLIANCE WITH THIS SECTION.

12 (5) FOR THE PURPOSES OF THIS SECTION, "THIRD-PARTY SERVICE  
13 PROVIDER" MEANS AN ENTITY THAT HAS BEEN CONTRACTED WITH TO  
14 MAINTAIN, STORE, OR PROCESS PERSONAL IDENTIFYING INFORMATION ON  
15 BEHALF OF A GOVERNMENTAL ENTITY.

16 **24-73-103. Governmental entity - notification of security**  
17 **breach. (1) Definitions.** AS USED IN THIS SECTION, UNLESS THE CONTEXT  
18 OTHERWISE REQUIRES:

19 (a) "BIOMETRIC DATA" MEANS UNIQUE BIOMETRIC DATA  
20 GENERATED FROM MEASUREMENTS OR ANALYSIS OF HUMAN BODY  
21 CHARACTERISTICS FOR THE PURPOSE OF AUTHENTICATING THE INDIVIDUAL  
22 WHEN HE OR SHE ACCESSES AN ONLINE ACCOUNT.

23 (b) "DETERMINATION THAT A SECURITY BREACH OCCURRED"  
24 MEANS THE POINT IN TIME AT WHICH THERE IS SUFFICIENT EVIDENCE TO  
25 CONCLUDE THAT A SECURITY BREACH HAS TAKEN PLACE.

26 (c) "ENCRYPTED" MEANS RENDERED UNUSABLE, UNREADABLE, OR  
27 INDECIPHERABLE TO AN UNAUTHORIZED PERSON THROUGH A SECURITY

1 TECHNOLOGY OR METHODOLOGY GENERALLY ACCEPTED IN THE FIELD OF  
2 INFORMATION SECURITY.

3 (d) "GOVERNMENTAL ENTITY" MEANS THE STATE AND ANY STATE  
4 AGENCY OR INSTITUTION, INCLUDING THE JUDICIAL DEPARTMENT,  
5 COUNTY, CITY AND COUNTY, INCORPORATED CITY OR TOWN, SCHOOL  
6 DISTRICT, SPECIAL IMPROVEMENT DISTRICT, AUTHORITY, AND EVERY  
7 OTHER KIND OF DISTRICT, INSTRUMENTALITY, OR POLITICAL SUBDIVISION  
8 OF THE STATE ORGANIZED PURSUANT TO LAW. "GOVERNMENTAL ENTITY"  
9 INCLUDES ENTITIES GOVERNED BY HOME RULE CHARTERS.  
10 "GOVERNMENTAL ENTITY" DOES NOT INCLUDE AN ENTITY ACTING AS A  
11 THIRD-PARTY SERVICE PROVIDER AS DEFINED IN SUBSECTION (1)(i) OF THIS  
12 SECTION.

13 (e) "MEDICAL INFORMATION" MEANS ANY INFORMATION ABOUT A  
14 CONSUMER'S MEDICAL OR MENTAL HEALTH TREATMENT OR DIAGNOSIS BY  
15 A HEALTH CARE PROFESSIONAL.

16 (f) "NOTICE" MEANS:

17 (I) WRITTEN NOTICE TO THE POSTAL ADDRESS LISTED IN THE  
18 RECORDS OF THE GOVERNMENTAL ENTITY;

19 (II) TELEPHONIC NOTICE;

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

26 OR

27 (IV) SUBSTITUTE NOTICE, IF THE GOVERNMENTAL ENTITY

1 REQUIRED TO PROVIDE NOTICE DEMONSTRATES THAT THE COST OF  
2 PROVIDING NOTICE WILL EXCEED TWO HUNDRED FIFTY THOUSAND  
3 DOLLARS, THE AFFECTED CLASS OF PERSONS TO BE NOTIFIED EXCEEDS TWO  
4 HUNDRED FIFTY THOUSAND COLORADO RESIDENTS, OR THE  
5 GOVERNMENTAL ENTITY DOES NOT HAVE SUFFICIENT CONTACT  
6 INFORMATION TO PROVIDE NOTICE. SUBSTITUTE NOTICE CONSISTS OF ALL  
7 OF THE FOLLOWING:

8 (A) E-MAIL NOTICE IF THE GOVERNMENTAL ENTITY HAS E-MAIL  
9 ADDRESSES FOR THE MEMBERS OF THE AFFECTED CLASS OF COLORADO  
10 RESIDENTS;

11 (B) CONSPICUOUS POSTING OF THE NOTICE ON THE WEBSITE PAGE  
12 OF THE GOVERNMENTAL ENTITY IF THE GOVERNMENTAL ENTITY  
13 MAINTAINS ONE; AND

14 (C) NOTIFICATION TO MAJOR STATEWIDE MEDIA.

15 (g) (I) (A) "PERSONAL INFORMATION" MEANS A COLORADO  
16 RESIDENT'S FIRST NAME OR FIRST INITIAL AND LAST NAME IN COMBINATION  
17 WITH ANY ONE OR MORE OF THE FOLLOWING DATA ELEMENTS THAT  
18 RELATE TO THE RESIDENT, WHEN THE DATA ELEMENTS ARE NOT  
19 ENCRYPTED, REDACTED, OR SECURED BY ANY OTHER METHOD RENDERING  
20 THE NAME OR THE ELEMENT UNREADABLE OR UNUSABLE: SOCIAL  
21 SECURITY NUMBER; DRIVER'S LICENSE NUMBER OR IDENTIFICATION CARD  
22 NUMBER; STUDENT, MILITARY, OR PASSPORT IDENTIFICATION NUMBER;  
23 MEDICAL INFORMATION; HEALTH INSURANCE IDENTIFICATION NUMBER; OR  
24 BIOMETRIC DATA, AS DEFINED IN SECTION 24-73-101 (1)(a);

25 (B) A COLORADO RESIDENT'S USER NAME OR E-MAIL ADDRESS, IN  
26 COMBINATION WITH A PASSWORD OR SECURITY QUESTIONS AND ANSWERS,  
27 THAT WOULD PERMIT ACCESS TO AN ONLINE ACCOUNT; OR

1 (C) A COLORADO RESIDENT'S ACCOUNT NUMBER OR CREDIT OR  
2 DEBIT CARD NUMBER IN COMBINATION WITH ANY REQUIRED SECURITY  
3 CODE, ACCESS CODE, OR PASSWORD THAT WOULD PERMIT ACCESS TO THAT  
4 ACCOUNT.

5 (II) "PERSONAL INFORMATION" DOES NOT INCLUDE PUBLICLY  
6 AVAILABLE INFORMATION THAT IS LAWFULLY MADE AVAILABLE TO THE  
7 GENERAL PUBLIC FROM FEDERAL, STATE, OR LOCAL GOVERNMENT  
8 RECORDS OR WIDELY DISTRIBUTED MEDIA.

9 (h) "SECURITY BREACH" MEANS THE UNAUTHORIZED ACQUISITION  
10 OF UNENCRYPTED COMPUTERIZED DATA THAT COMPROMISES THE  
11 SECURITY, CONFIDENTIALITY, OR INTEGRITY OF PERSONAL INFORMATION  
12 MAINTAINED BY A GOVERNMENTAL ENTITY. GOOD FAITH ACQUISITION OF  
13 PERSONAL INFORMATION BY AN EMPLOYEE OR AGENT OF A  
14 GOVERNMENTAL ENTITY FOR THE PURPOSES OF THE GOVERNMENTAL  
15 ENTITY IS NOT A SECURITY BREACH IF THE PERSONAL INFORMATION IS NOT  
16 USED FOR A PURPOSE UNRELATED TO THE LAWFUL GOVERNMENT PURPOSE  
17 OR IS NOT SUBJECT TO FURTHER UNAUTHORIZED DISCLOSURE.

18 (i) "THIRD-PARTY SERVICE PROVIDER" MEANS AN ENTITY THAT  
19 HAS BEEN CONTRACTED WITH TO MAINTAIN, STORE, OR PROCESS PERSONAL  
20 INFORMATION ON BEHALF OF A GOVERNMENTAL ENTITY.

21 (2) **Disclosure of breach.** (a) A GOVERNMENTAL ENTITY THAT  
22 MAINTAINS, OWNS, OR LICENSES COMPUTERIZED DATA THAT INCLUDES  
23 PERSONAL INFORMATION ABOUT A RESIDENT OF COLORADO SHALL, WHEN  
24 IT DETERMINES THAT A SECURITY BREACH HAS OCCURRED, CONDUCT IN  
25 GOOD FAITH A PROMPT INVESTIGATION TO DETERMINE THE LIKELIHOOD  
26 THAT PERSONAL INFORMATION HAS BEEN OR WILL BE MISUSED. THE  
27 GOVERNMENTAL ENTITY SHALL GIVE NOTICE TO THE AFFECTED COLORADO

1 RESIDENTS UNLESS THE INVESTIGATION DETERMINES THAT THE MISUSE OF  
2 INFORMATION ABOUT A COLORADO RESIDENT HAS NOT OCCURRED AND IS  
3 NOT REASONABLY LIKELY TO OCCUR. NOTICE MUST BE MADE IN THE MOST  
4 EXPEDIENT TIME POSSIBLE AND WITHOUT UNREASONABLE DELAY, BUT NOT  
5 LATER THAN THIRTY DAYS AFTER THE DATE OF DETERMINATION THAT A  
6 SECURITY BREACH OCCURRED, CONSISTENT WITH THE LEGITIMATE NEEDS  
7 OF LAW ENFORCEMENT AND CONSISTENT WITH ANY MEASURES NECESSARY  
8 TO DETERMINE THE SCOPE OF THE BREACH AND TO RESTORE THE  
9 REASONABLE INTEGRITY OF THE COMPUTERIZED DATA SYSTEM.

10 (b) EXCEPT AS PROVIDED FOR IN SUBSECTION (2)(c) OF THIS  
11 SECTION, IN THE CASE OF A BREACH OF PERSONAL INFORMATION, NOTICE  
12 REQUIRED BY THIS SUBSECTION (2) TO AFFECTED COLORADO RESIDENTS  
13 MUST INCLUDE, BUT NEED NOT BE LIMITED TO, THE FOLLOWING  
14 INFORMATION:

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

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

20 (III) INFORMATION THAT THE RESIDENT CAN USE TO CONTACT THE  
21 GOVERNMENTAL ENTITY THAT WAS BREACHED TO INQUIRE ABOUT THE  
22 SECURITY BREACH;

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

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

27 (VI) A STATEMENT THAT THE RESIDENT CAN OBTAIN INFORMATION

1 FROM THE FEDERAL TRADE COMMISSION AND THE CREDIT REPORTING  
2 AGENCIES ABOUT FRAUD ALERTS AND SECURITY FREEZES.

3 (c) IF AN INVESTIGATION BY THE GOVERNMENTAL ENTITY  
4 PURSUANT TO SUBSECTION (2)(a) OF THIS SECTION DETERMINES THAT THE  
5 TYPE OF PERSONAL INFORMATION DESCRIBED IN SUBSECTION (1)(g)(I)(B)  
6 OF THIS SECTION HAS BEEN MISUSED OR IS REASONABLY LIKELY TO BE  
7 MISUSED, THEN THE GOVERNMENTAL ENTITY SHALL, IN ADDITION TO THE  
8 NOTICE OTHERWISE REQUIRED BY THIS SECTION AND IN THE MOST  
9 EXPEDIENT TIME POSSIBLE AND WITHOUT UNREASONABLE DELAY, BUT NO  
10 LATER THAN THIRTY DAYS AFTER THE DATE OF DETERMINATION THAT A  
11 SECURITY BREACH OCCURRED, CONSISTENT WITH THE LEGITIMATE NEEDS  
12 OF LAW ENFORCEMENT AND CONSISTENT WITH ANY MEASURES NECESSARY  
13 TO DETERMINE THE SCOPE OF THE BREACH AND TO RESTORE THE  
14 REASONABLE INTEGRITY OF THE COMPUTERIZED DATA SYSTEM:

15 (I) DIRECT THE PERSON WHOSE PERSONAL INFORMATION HAS BEEN  
16 BREACHED TO PROMPTLY CHANGE HIS OR HER PASSWORD AND SECURITY  
17 QUESTION OR ANSWER, AS APPLICABLE, OR TO TAKE OTHER STEPS  
18 APPROPRIATE TO PROTECT THE ONLINE ACCOUNT WITH THE PERSON OR  
19 BUSINESS AND ALL OTHER ONLINE ACCOUNTS FOR WHICH THE PERSON  
20 WHOSE PERSONAL INFORMATION HAS BEEN BREACHED THAT USES THE  
21 SAME USERNAME OR E-MAIL ADDRESS AND PASSWORD OR SECURITY  
22 QUESTION OR ANSWER.

23 (II) FOR LOG-IN CREDENTIALS OF AN E-MAIL ACCOUNT FURNISHED  
24 BY THE GOVERNMENTAL ENTITY, THE GOVERNMENTAL ENTITY SHALL NOT  
25 COMPLY WITH THIS SECTION BY PROVIDING THE SECURITY BREACH  
26 NOTIFICATION TO THAT E-MAIL ADDRESS, BUT MAY INSTEAD COMPLY WITH  
27 THIS SECTION BY PROVIDING NOTICE, AS DEFINED IN SUBSECTION (1)(f) OF

1 THIS SECTION, OR BY CLEAR AND CONSPICUOUS NOTICE DELIVERED TO THE  
2 RESIDENT ONLINE WHEN THE RESIDENT IS CONNECTED TO THE ONLINE  
3 ACCOUNT FROM AN INTERNET PROTOCOL ADDRESS OR ONLINE LOCATION  
4 FROM WHICH THE GOVERNMENTAL ENTITY KNOWS THE RESIDENT  
5 CUSTOMARILY ACCESSES THE ACCOUNT.

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

12 (e) A GOVERNMENTAL ENTITY THAT IS REQUIRED TO PROVIDE  
13 NOTICE PURSUANT TO THIS SUBSECTION (2) IS PROHIBITED FROM CHARGING  
14 THE COST OF PROVIDING SUCH NOTICE TO INDIVIDUALS.

15 (f) NOTHING IN THIS SUBSECTION (2) PROHIBITS THE NOTICE  
16 DESCRIBED IN THIS SUBSECTION (2) FROM CONTAINING ADDITIONAL  
17 INFORMATION, INCLUDING ANY INFORMATION THAT MAY BE REQUIRED BY  
18 STATE OR FEDERAL LAW.

19 (g) IF A GOVERNMENTAL ENTITY USES A THIRD-PARTY SERVICE  
20 PROVIDER TO MAINTAIN COMPUTERIZED DATA THAT INCLUDES PERSONAL  
21 INFORMATION, THEN THE THIRD-PARTY SERVICE PROVIDER SHALL GIVE  
22 NOTICE TO AND COOPERATE WITH THE GOVERNMENTAL ENTITY IN THE  
23 EVENT OF A SECURITY BREACH THAT COMPROMISES SUCH COMPUTERIZED  
24 DATA, INCLUDING NOTIFYING THE GOVERNMENTAL ENTITY OF ANY  
25 SECURITY BREACH AS SOON AS POSSIBLE AND WITHOUT UNREASONABLE  
26 DELAY FOLLOWING DISCOVERY OF A SECURITY BREACH, IF MISUSE OF  
27 PERSONAL INFORMATION ABOUT A COLORADO RESIDENT OCCURRED OR IS



1 LIKELY TO OCCUR. COOPERATION INCLUDES SHARING WITH THE COVERED  
2 ENTITY INFORMATION RELEVANT TO THE SECURITY BREACH; EXCEPT THAT  
3 SUCH COOPERATION DOES NOT REQUIRE THE DISCLOSURE OF  
4 CONFIDENTIAL BUSINESS INFORMATION OR TRADE SECRETS.

5 (h) NOTICE REQUIRED BY THIS SECTION MAY BE DELAYED IF A LAW  
6 ENFORCEMENT AGENCY DETERMINES THAT THE NOTICE WILL IMPEDE A  
7 CRIMINAL INVESTIGATION AND THE LAW ENFORCEMENT AGENCY HAS  
8 NOTIFIED THE GOVERNMENTAL ENTITY THAT OPERATES IN COLORADO NOT  
9 TO SEND NOTICE REQUIRED BY THIS SECTION. NOTICE REQUIRED BY THIS  
10 SECTION MUST BE MADE IN GOOD FAITH, WITHOUT UNREASONABLE DELAY  
11 BUT NOT LATER THAN THIRTY DAYS AFTER THE LAW ENFORCEMENT  
12 AGENCY DETERMINES THAT NOTIFICATION WILL NO LONGER IMPEDE THE  
13 INVESTIGATION AND HAS NOTIFIED THE GOVERNMENTAL ENTITY THAT IT  
14 IS APPROPRIATE TO SEND THE NOTICE REQUIRED BY THIS SECTION.

15 (i) IF A GOVERNMENTAL ENTITY IS REQUIRED TO NOTIFY MORE  
16 THAN ONE THOUSAND COLORADO RESIDENTS OF A SECURITY BREACH  
17 PURSUANT TO THIS SECTION, THE GOVERNMENTAL ENTITY SHALL ALSO  
18 NOTIFY, WITHOUT UNREASONABLE DELAY, ALL CONSUMER REPORTING  
19 AGENCIES THAT COMPILE AND MAINTAIN FILES ON CONSUMERS ON A  
20 NATIONWIDE BASIS, AS DEFINED BY THE FEDERAL "FAIR CREDIT  
21 REPORTING ACT", 15 U.S.C. SEC. 1681a (p), OF THE ANTICIPATED DATE OF  
22 THE NOTIFICATION TO THE RESIDENTS AND THE APPROXIMATE NUMBER OF  
23 RESIDENTS WHO ARE TO BE NOTIFIED. NOTHING IN THIS SUBSECTION (2)(i)  
24 REQUIRES THE GOVERNMENTAL ENTITY TO PROVIDE TO THE CONSUMER  
25 REPORTING AGENCY THE NAMES OR OTHER PERSONAL INFORMATION OF  
26 SECURITY BREACH NOTICE RECIPIENTS. THIS SUBSECTION (2)(i) DOES NOT  
27 APPLY TO A PERSON WHO IS SUBJECT TO TITLE V OF THE FEDERAL

1 "GRAMM-LEACH-BLILEY ACT", 15 U.S.C. SEC. 6801 ET SEQ.

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

4 (k) (I) THE GOVERNMENTAL ENTITY SHALL NOTIFY COLORADO  
5 RESIDENTS OF A SECURITY BREACH AS SOON AS PRACTICABLE BUT NOT  
6 LATER THAN THIRTY DAYS AFTER THE DATE OF DETERMINATION THAT A  
7 SECURITY BREACH OCCURRED IF THE SECURITY BREACH IS REASONABLY  
8 BELIEVED TO HAVE AFFECTED FIVE HUNDRED COLORADO RESIDENTS OR  
9 MORE, UNLESS THE INVESTIGATION DETERMINES THAT THE MISUSE OF  
10 INFORMATION ABOUT A COLORADO RESIDENT HAS NOT OCCURRED AND IS  
11 NOT LIKELY TO OCCUR.

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

18 (3) **Procedures deemed in compliance with notice**  
19 **requirements.** (a) PURSUANT TO THIS SECTION, A GOVERNMENTAL  
20 ENTITY THAT MAINTAINS ITS OWN NOTIFICATION PROCEDURES AS PART OF  
21 AN INFORMATION SECURITY POLICY FOR THE TREATMENT OF PERSONAL  
22 INFORMATION AND WHOSE PROCEDURES ARE OTHERWISE CONSISTENT  
23 WITH THE TIMING REQUIREMENTS OF THIS SECTION IS IN COMPLIANCE WITH  
24 THE NOTICE REQUIREMENTS OF THIS SECTION IF THE GOVERNMENTAL  
25 ENTITY NOTIFIES AFFECTED COLORADO CUSTOMERS IN ACCORDANCE WITH  
26 ITS POLICIES IN THE EVENT OF A SECURITY BREACH; EXCEPT THAT NOTICE  
27 TO THE ATTORNEY GENERAL IS STILL REQUIRED PURSUANT TO SUBSECTION

1 (2)(k) OF THIS SECTION.

2 (b) A GOVERNMENTAL ENTITY THAT IS REGULATED BY STATE OR  
3 FEDERAL LAW AND THAT MAINTAINS PROCEDURES FOR A SECURITY  
4 BREACH PURSUANT TO THE LAWS, RULES, REGULATIONS, GUIDANCES, OR  
5 GUIDELINES ESTABLISHED BY ITS STATE OR FEDERAL REGULATOR IS IN  
6 COMPLIANCE WITH THIS SECTION; EXCEPT THAT NOTICE TO THE ATTORNEY  
7 GENERAL IS STILL REQUIRED PURSUANT TO SUBSECTION (2)(k) OF THIS  
8 SECTION. IN THE CASE OF A CONFLICT BETWEEN THE TIME PERIOD FOR  
9 NOTICE TO INDIVIDUALS, THE LAW OR REGULATION WITH THE SHORTEST  
10 NOTICE PERIOD CONTROLS.

11 (4) **Violations.** THE ATTORNEY GENERAL MAY BRING AN ACTION  
12 FOR INJUNCTIVE RELIEF TO ENFORCE THE PROVISIONS OF THIS SECTION.

13 (5) **Attorney general criminal authority.** UPON RECEIPT OF  
14 NOTICE PURSUANT TO SUBSECTION (2) OF THIS SECTION, AND WITH EITHER  
15 A REQUEST FROM THE GOVERNOR TO PROSECUTE A PARTICULAR CASE OR  
16 WITH THE APPROVAL OF THE DISTRICT ATTORNEY WITH JURISDICTION TO  
17 PROSECUTE CASES IN THE JUDICIAL DISTRICT WHERE A CASE HAS BEEN,  
18 WILL BE, OR COULD BE BROUGHT, THE ATTORNEY GENERAL HAS THE  
19 AUTHORITY TO PROSECUTE ANY CRIMINAL VIOLATIONS OF SECTION  
20 18-5.5-102.

21 **SECTION 5. Effective date.** This act takes effect September 1,  
22 2018.

23 **SECTION 6. Safety clause.** The general assembly hereby finds,  
24 determines, and declares that this act is necessary for the immediate  
25 preservation of the public peace, health, and safety.