

HOUSE COMMITTEE OF REFERENCE REPORT

Chairman of Committee

February 14, 2018
Date

Committee on State, Veterans, & Military Affairs.

After consideration on the merits, the Committee recommends the following:

HB18-1128 be amended as follows, and as so amended, be referred to the Committee on Appropriations with favorable recommendation:

- 1 Amend printed bill, strike everything below the enacting clause and
2 substitute:
- 3 "SECTION 1. In Colorado Revised Statutes, 6-1-713, amend (1),
4 (2), and (3) as follows:
- 5 **6-1-713. Disposal of personal identifying information - policy**
6 **- definition.** (1) Each public and private entity in the state that uses
7 MAINTAINS PAPER OR ELECTRONIC documents during the course of
8 business that contain personal identifying information shall develop a
9 WRITTEN policy for the destruction or proper disposal of THOSE paper AND
10 ELECTRONIC documents containing personal identifying information.
11 UNLESS OTHERWISE REQUIRED BY STATE OR FEDERAL LAW OR
12 REGULATION, THE WRITTEN POLICY MUST REQUIRE THAT, WHEN SUCH
13 PAPER OR ELECTRONIC DOCUMENTS ARE NO LONGER NEEDED, THE PUBLIC
14 OR PRIVATE ENTITY SHALL DESTROY OR ARRANGE FOR THE DESTRUCTION
15 OF SUCH PAPER AND ELECTRONIC DOCUMENTS WITHIN ITS CUSTODY OR
16 CONTROL THAT CONTAIN PERSONAL IDENTIFYING INFORMATION BY
17 SHREDDING, ERASING, OR OTHERWISE MODIFYING THE PERSONAL
18 IDENTIFYING INFORMATION IN THE PAPER OR ELECTRONIC DOCUMENTS TO
19 MAKE THE PERSONAL IDENTIFYING INFORMATION UNREADABLE OR
20 INDECIPHERABLE THROUGH ANY MEANS.
- 21 (2) For the purposes of this section AND SECTION 6-1-713.5,
22 "personal identifying information" means a social security number; a
23 personal identification number; a password; a pass code; an official state
24 or government-issued driver's license or identification card number; a

1 government passport number; biometric data; an employer, student, or
2 military identification number; or a financial transaction device, AS
3 DEFINED IN SECTION 18-5-701 (3).

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

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

14 **6-1-713.5. Protection of personal identifying information.**

15 (1) TO PROTECT PERSONAL IDENTIFYING INFORMATION, AS DEFINED IN
16 SECTION 6-1-713 (2), FROM UNAUTHORIZED ACCESS, USE, MODIFICATION,
17 DISCLOSURE, OR DESTRUCTION, A PERSON THAT MAINTAINS, OWNS, OR
18 LICENSES PERSONAL IDENTIFYING INFORMATION OF AN INDIVIDUAL
19 RESIDING IN THE STATE SHALL IMPLEMENT AND MAINTAIN REASONABLE
20 SECURITY PROCEDURES AND PRACTICES THAT ARE APPROPRIATE TO THE
21 NATURE OF THE PERSONAL IDENTIFYING INFORMATION AND THE NATURE
22 AND SIZE OF THE BUSINESS AND ITS OPERATIONS.

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

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

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

35 (3) FOR THE PURPOSES OF SUBSECTION (2) OF THIS SECTION, A
36 DISCLOSURE OF PERSONAL IDENTIFYING INFORMATION DOES NOT INCLUDE
37 DISCLOSURE OF INFORMATION TO A NONAFFILIATED THIRD PARTY UNDER
38 CIRCUMSTANCES WHERE THE PERSON RETAINS PRIMARY RESPONSIBILITY
39 FOR IMPLEMENTING AND MAINTAINING REASONABLE SECURITY
40 PROCEDURES AND PRACTICES APPROPRIATE TO THE NATURE OF THE
41 PERSONAL IDENTIFYING INFORMATION AND THE PERSON IMPLEMENTS AND

1 MAINTAINS TECHNICAL CONTROLS THAT ARE REASONABLY DESIGNED TO:
2 (a) HELP PROTECT THE PERSONAL IDENTIFYING INFORMATION
3 FROM UNAUTHORIZED ACCESS, USE, MODIFICATION, DISCLOSURE, OR
4 DESTRUCTION; OR

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

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

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

17 **6-1-716. Notification of security breach. (1) Definitions.** AS
18 USED IN THIS SECTION, UNLESS THE CONTEXT 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) "COMMERCIAL ENTITY" MEANS ANY PRIVATE LEGAL ENTITY,
24 WHETHER FOR-PROFIT OR NOT-FOR-PROFIT.

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.

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

32 (e) "MEDICAL INFORMATION" MEANS ANY INFORMATION ABOUT A
33 CONSUMER'S MEDICAL OR MENTAL HEALTH TREATMENT OR DIAGNOSIS BY
34 A HEALTH CARE PROFESSIONAL.

35 (f) "NOTICE" MEANS:

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

38 (II) TELEPHONIC NOTICE;

39 (III) ELECTRONIC NOTICE, IF A PRIMARY MEANS OF
40 COMMUNICATION BY THE INDIVIDUAL OR COMMERCIAL ENTITY WITH A
41 COLORADO RESIDENT IS BY ELECTRONIC MEANS OR THE NOTICE PROVIDED

1 IS CONSISTENT WITH THE PROVISIONS REGARDING ELECTRONIC RECORDS
2 AND SIGNATURES SET FORTH IN THE FEDERAL "ELECTRONIC SIGNATURES
3 IN GLOBAL AND NATIONAL COMMERCE ACT", 15 U.S.C. SEC. 7001 ET
4 SEQ.; OR

5 (IV) SUBSTITUTE NOTICE, IF THE INDIVIDUAL OR THE COMMERCIAL
6 ENTITY REQUIRED TO PROVIDE NOTICE DEMONSTRATES THAT THE COST OF
7 PROVIDING NOTICE WILL EXCEED TWO HUNDRED FIFTY THOUSAND
8 DOLLARS, THE AFFECTED CLASS OF PERSONS TO BE NOTIFIED EXCEEDS TWO
9 HUNDRED FIFTY THOUSAND COLORADO RESIDENTS, OR THE INDIVIDUAL OR
10 THE COMMERCIAL ENTITY DOES NOT HAVE SUFFICIENT CONTACT
11 INFORMATION TO PROVIDE NOTICE. SUBSTITUTE NOTICE CONSISTS OF ALL
12 OF THE FOLLOWING:

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

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

19 (C) NOTIFICATION TO MAJOR STATEWIDE MEDIA.

20 (g) (I) (A) "PERSONAL INFORMATION" MEANS A COLORADO
21 RESIDENT'S FIRST NAME OR FIRST INITIAL AND LAST NAME IN COMBINATION
22 WITH ANY ONE OR MORE OF THE FOLLOWING DATA ELEMENTS THAT
23 RELATE TO THE RESIDENT, WHEN THE DATA ELEMENTS ARE NOT
24 ENCRYPTED, REDACTED, OR SECURED BY ANY OTHER METHOD RENDERING
25 THE NAME OR THE ELEMENT UNREADABLE OR UNUSABLE: SOCIAL
26 SECURITY NUMBER; STUDENT, MILITARY, OR PASSPORT IDENTIFICATION
27 NUMBER; DRIVER'S LICENSE NUMBER OR IDENTIFICATION CARD NUMBER;
28 ACCOUNT NUMBER OR CREDIT CARD OR DEBIT CARD NUMBER; MEDICAL
29 INFORMATION; HEALTH INSURANCE IDENTIFICATION NUMBER; OR
30 BIOMETRIC DATA; OR

31 (B) A COLORADO RESIDENT'S USERNAME OR E-MAIL ADDRESS, IN
32 COMBINATION WITH A PASSWORD OR SECURITY QUESTIONS AND ANSWERS,
33 THAT WOULD PERMIT ACCESS TO AN ONLINE ACCOUNT.

34 (II) "PERSONAL INFORMATION" DOES NOT INCLUDE PUBLICLY
35 AVAILABLE INFORMATION THAT IS LAWFULLY MADE AVAILABLE TO THE
36 GENERAL PUBLIC FROM FEDERAL, STATE, OR LOCAL GOVERNMENT
37 RECORDS OR WIDELY DISTRIBUTED MEDIA.

38 (h) "SECURITY BREACH" MEANS THE UNAUTHORIZED ACQUISITION
39 OF UNENCRYPTED COMPUTERIZED DATA THAT COMPROMISES THE
40 SECURITY, CONFIDENTIALITY, OR INTEGRITY OF PERSONAL INFORMATION
41 MAINTAINED BY AN INDIVIDUAL OR A COMMERCIAL ENTITY. GOOD FAITH

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

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

24 (a.2) EXCEPT AS OTHERWISE PROVIDED FOR IN SUBSECTION (2)(a.3)
25 OF THIS SECTION, IN THE CASE OF A BREACH OF PERSONAL INFORMATION,
26 NOTICE REQUIRED BY THIS SUBSECTION (2) TO AFFECTED COLORADO
27 RESIDENTS MUST INCLUDE, BUT NEED NOT BE LIMITED TO, THE FOLLOWING
28 INFORMATION:

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

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

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

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

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

41 (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 (a.3) IF NOTICE OF A SECURITY BREACH INVOLVING PERSONAL
4 INFORMATION, AS DEFINED IN SUBSECTION (1)(g)(I)(B) OF THIS SECTION,
5 IS GIVEN NO LATER THAN FIVE DAYS AFTER THE 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, NOTICE
10 MAY BE GIVEN AS FOLLOWS, INSTEAD OF AS OUTLINED IN SUBSECTION
11 (2)(a.2) OF THIS SECTION:

12 (I) THE INDIVIDUAL OR COMMERCIAL ENTITY MAY PROVIDE THE
13 SECURITY BREACH NOTIFICATION IN ELECTRONIC OR OTHER FORM THAT
14 DIRECTS THE PERSON WHOSE PERSONAL INFORMATION HAS BEEN
15 BREACHED TO PROMPTLY CHANGE HIS OR HER PASSWORD AND SECURITY
16 QUESTION OR ANSWER, AS APPLICABLE, OR TO TAKE OTHER STEPS
17 APPROPRIATE TO PROTECT THE ONLINE ACCOUNT WITH THE PERSON OR
18 BUSINESS AND ALL OTHER ONLINE ACCOUNTS FOR WHICH THE PERSON
19 WHOSE PERSONAL INFORMATION HAS BEEN BREACHED THAT USES THE
20 SAME USER NAME OR E-MAIL ADDRESS AND PASSWORD OR SECURITY
21 QUESTION OR ANSWER.

22 (II) FOR LOG-IN CREDENTIALS OF AN E-MAIL ACCOUNT FURNISHED
23 BY THE INDIVIDUAL OR COMMERCIAL ENTITY, THE INDIVIDUAL OR
24 COMMERCIAL ENTITY SHALL NOT COMPLY WITH THIS SECTION BY
25 PROVIDING THE SECURITY BREACH NOTIFICATION TO THAT E-MAIL
26 ADDRESS, BUT MAY INSTEAD COMPLY WITH THIS SECTION BY PROVIDING
27 NOTICE, AS DEFINED IN SUBSECTION (1)(f) OF THIS SECTION, OR BY CLEAR
28 AND CONSPICUOUS NOTICE DELIVERED TO THE RESIDENT ONLINE WHEN
29 THE RESIDENT IS CONNECTED TO THE ONLINE ACCOUNT FROM AN INTERNET
30 PROTOCOL ADDRESS OR ONLINE LOCATION FROM WHICH THE INDIVIDUAL
31 OR COMMERCIAL ENTITY KNOWS THE RESIDENT CUSTOMARILY ACCESSES
32 THE ACCOUNT.

33 (a.4) THE BREACH OF ENCRYPTED OR OTHERWISE SECURED
34 PERSONAL INFORMATION MUST BE DISCLOSED IN ACCORDANCE WITH THIS
35 SECTION IF THE CONFIDENTIAL PROCESS, ENCRYPTION KEY, OR OTHER
36 MEANS TO DECIPHER THE SECURED INFORMATION WAS ALSO ACQUIRED IN
37 THE SECURITY BREACH OR WAS REASONABLY BELIEVED TO HAVE BEEN
38 ACQUIRED.

39 (a.5) AN INDIVIDUAL OR COMMERCIAL ENTITY THAT IS REQUIRED
40 TO PROVIDE NOTICE TO AFFECTED COLORADO RESIDENTS PURSUANT TO
41 THIS SUBSECTION (2) IS PROHIBITED FROM CHARGING THE COST OF

1 PROVIDING SUCH NOTICE TO SUCH RESIDENTS.

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

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

22 (c) Notice required by this section may be delayed if a law
23 enforcement agency determines that the notice will impede a criminal
24 investigation and the law enforcement agency has notified the individual
25 or commercial entity that conducts business in Colorado not to send
26 notice required by this section. Notice required by this section ~~shall~~ MUST
27 be made in good faith, without unreasonable delay ~~and as soon as possible~~
28 BUT NOT LATER THAN THIRTY DAYS after the law enforcement agency
29 determines that notification will no longer impede the investigation and
30 has notified the individual or commercial entity that conducts business in
31 Colorado that it is appropriate to send the notice required by this section.

32 (d) If an individual or commercial entity is required to notify more
33 than one thousand Colorado residents of a SECURITY breach ~~of the~~
34 ~~security of the system~~ pursuant to this section, the individual or
35 commercial entity shall also notify, without unreasonable delay, all
36 consumer reporting agencies that compile and maintain files on
37 consumers on a nationwide basis, as defined by THE FEDERAL "FAIR
38 CREDIT REPORTING ACT", 15 U.S.C. sec. 1681a (p), of the anticipated
39 date of the notification to the residents and the approximate number of
40 residents who are to be notified. Nothing in this ~~paragraph (d) shall be~~
41 ~~construed to require~~ SUBSECTION (2)(d) REQUIRES the individual or

1 commercial entity to provide to the consumer reporting agency the names
2 or other personal information of SECURITY breach notice recipients. This
3 ~~paragraph (d) shall~~ SUBSECTION (2)(d) DOES not apply to a person who is
4 subject to Title V of the federal "Gramm-Leach-Bliley Act", 15 U.S.C.
5 sec. 6801 et seq.

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

8 (f) (I) THE INDIVIDUAL OR COMMERCIAL ENTITY THAT WAS
9 BREACHED SHALL PROVIDE NOTICE OF ANY SECURITY BREACH TO THE
10 COLORADO ATTORNEY GENERAL AS SOON AS PRACTICABLE BUT NOT
11 LATER THAN THIRTY DAYS AFTER THE DATE OF DETERMINATION THAT A
12 SECURITY BREACH OCCURRED IF THE SECURITY BREACH IS REASONABLY
13 BELIEVED TO HAVE AFFECTED FIVE HUNDRED COLORADO RESIDENTS OR
14 MORE, UNLESS THE INVESTIGATION DETERMINES THAT THE MISUSE OF
15 INFORMATION ABOUT A COLORADO RESIDENT HAS NOT OCCURRED AND IS
16 NOT LIKELY TO OCCUR.

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

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

34 (b) An individual or a commercial entity that is regulated by state
35 or federal law and that maintains procedures for a SECURITY breach ~~of the~~
36 ~~security of the system~~ pursuant to the laws, rules, regulations, guidances,
37 or guidelines established by its ~~primary or functional~~ state or federal
38 regulator is ~~deemed to be~~ in compliance with this section; EXCEPT THAT
39 NOTICE TO THE ATTORNEY GENERAL IS STILL REQUIRED PURSUANT TO
40 SUBSECTION (2)(f) OF THIS SECTION. IN THE CASE OF A CONFLICT BETWEEN
41 THE TIME PERIOD FOR NOTICE TO INDIVIDUALS THAT IS REQUIRED

1 PURSUANT TO THIS SUBSECTION (2) AND THE APPLICABLE STATE OR
2 FEDERAL LAW OR REGULATION, THE LAW OR REGULATION WITH THE
3 SHORTEST TIME FRAME FOR NOTICE TO THE INDIVIDUAL CONTROLS.

4 (4) **Violations.** The attorney general may bring an action in law
5 or equity to address violations of this section, SECTION 6-1-713, OR
6 SECTION 6-1-713.5, and for other relief that may be appropriate to ensure
7 compliance with this section or to recover direct economic damages
8 resulting from a violation, or both. The provisions of this section are not
9 exclusive and do not relieve an individual or a commercial entity subject
10 to this section from compliance with all other applicable provisions of
11 law.

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

20 **SECTION 4.** In Colorado Revised Statutes, **add** article 73 to title
21 24 as follows:

22 **ARTICLE 73**

23 **Security Breaches and Personal Information**

24 **24-73-101. Governmental entity - disposal of personal**
25 **identifying information - policy - definitions.** (1) EACH
26 GOVERNMENTAL ENTITY IN THE STATE THAT MAINTAINS PAPER OR
27 ELECTRONIC DOCUMENTS DURING THE COURSE OF BUSINESS THAT
28 CONTAIN PERSONAL IDENTIFYING INFORMATION SHALL DEVELOP A
29 WRITTEN POLICY FOR THE DESTRUCTION OR PROPER DISPOSAL OF THOSE
30 PAPER AND ELECTRONIC DOCUMENTS CONTAINING PERSONAL IDENTIFYING
31 INFORMATION. UNLESS OTHERWISE REQUIRED BY STATE OR FEDERAL LAW
32 OR REGULATION, THE WRITTEN POLICY MUST REQUIRE THAT, WHEN SUCH
33 PAPER OR ELECTRONIC DOCUMENTS ARE NO LONGER NEEDED, THE
34 GOVERNMENTAL ENTITY DESTROY OR ARRANGE FOR THE DESTRUCTION OF
35 SUCH PAPER AND ELECTRONIC DOCUMENTS WITHIN ITS CUSTODY OR
36 CONTROL THAT CONTAIN PERSONAL IDENTIFYING INFORMATION BY
37 SHREDDING, ERASING, OR OTHERWISE MODIFYING THE PERSONAL
38 IDENTIFYING INFORMATION IN THE PAPER OR ELECTRONIC DOCUMENTS TO
39 MAKE THE PERSONAL IDENTIFYING INFORMATION UNREADABLE OR
40 INDECIPHERABLE THROUGH ANY MEANS.

41 (2) A GOVERNMENTAL ENTITY THAT IS REGULATED BY STATE OR

1 FEDERAL LAW AND THAT MAINTAINS PROCEDURES FOR DISPOSAL OF
2 PERSONAL IDENTIFYING INFORMATION PURSUANT TO THE LAWS, RULES,
3 REGULATIONS, GUIDANCES, OR GUIDELINES ESTABLISHED BY ITS STATE OR
4 FEDERAL REGULATOR IS IN COMPLIANCE WITH THIS SECTION.

5 (3) UNLESS A GOVERNMENTAL ENTITY SPECIFICALLY CONTRACTS
6 WITH A RECYCLER OR DISPOSAL FIRM FOR DESTRUCTION OF DOCUMENTS
7 THAT CONTAIN PERSONAL IDENTIFYING INFORMATION, NOTHING IN THIS
8 SECTION REQUIRES A RECYCLER OR DISPOSAL FIRM TO VERIFY THAT THE
9 DOCUMENTS CONTAINED IN THE PRODUCTS IT RECEIVES FOR DISPOSAL OR
10 RECYCLING HAVE BEEN PROPERLY DESTROYED OR DISPOSED OF AS
11 REQUIRED BY THIS SECTION.

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

14 (a) "GOVERNMENTAL ENTITY" MEANS THE STATE AND ANY STATE
15 AGENCY OR INSTITUTION, COUNTY, CITY AND COUNTY, INCORPORATED
16 CITY OR TOWN, SCHOOL DISTRICT, SPECIAL IMPROVEMENT DISTRICT,
17 AUTHORITY, AND EVERY OTHER KIND OF DISTRICT, INSTRUMENTALITY, OR
18 POLITICAL SUBDIVISION OF THE STATE ORGANIZED PURSUANT TO LAW.
19 "GOVERNMENTAL ENTITY" INCLUDES ENTITIES GOVERNED BY HOME RULE
20 CHARTERS.

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

28 **24-73-102. Governmental entity - protection of personal**
29 **identifying information.** (1) TO PROTECT PERSONAL IDENTIFYING
30 INFORMATION, AS DEFINED IN SECTION 24-73-101 (4)(b), FROM
31 UNAUTHORIZED ACCESS, USE, MODIFICATION, DISCLOSURE, OR
32 DESTRUCTION, A GOVERNMENTAL ENTITY THAT MAINTAINS, OWNS, OR
33 LICENSES PERSONAL IDENTIFYING INFORMATION SHALL IMPLEMENT AND
34 MAINTAIN REASONABLE SECURITY PROCEDURES AND PRACTICES THAT ARE
35 APPROPRIATE TO THE NATURE OF THE PERSONAL IDENTIFYING
36 INFORMATION AND THE NATURE AND SIZE OF THE GOVERNMENTAL ENTITY.

37 (2) A GOVERNMENTAL ENTITY THAT USES A NONAFFILIATED THIRD
38 PARTY AS A SERVICE PROVIDER TO PERFORM SERVICES FOR THE
39 GOVERNMENTAL ENTITY AND DISCLOSES PERSONAL IDENTIFYING
40 INFORMATION ABOUT AN INDIVIDUAL RESIDING IN THE STATE WITH THE
41 NONAFFILIATED THIRD PARTY SHALL REQUIRE THAT THE NONAFFILIATED

1 THIRD PARTY IMPLEMENT AND MAINTAIN REASONABLE SECURITY
2 PROCEDURES AND PRACTICES THAT ARE:

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

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

8 (3) FOR THE PURPOSES OF SUBSECTION (2) OF THIS SECTION, A
9 DISCLOSURE OF PERSONAL IDENTIFYING INFORMATION DOES NOT INCLUDE
10 DISCLOSURE OF INFORMATION TO A NONAFFILIATED THIRD PARTY UNDER
11 CIRCUMSTANCES WHERE THE GOVERNMENTAL ENTITY RETAINS PRIMARY
12 RESPONSIBILITY FOR IMPLEMENTING AND MAINTAINING REASONABLE
13 SECURITY PROCEDURES AND PRACTICES APPROPRIATE TO THE NATURE OF
14 THE PERSONAL IDENTIFYING INFORMATION AND THE GOVERNMENTAL
15 ENTITY IMPLEMENTS AND MAINTAINS TECHNICAL CONTROLS REASONABLY
16 DESIGNED TO:

17 (a) HELP PROTECT THE PERSONAL IDENTIFYING INFORMATION
18 FROM UNAUTHORIZED ACCESS, MODIFICATION, DISCLOSURE, OR
19 DESTRUCTION; OR

20 (b) EFFECTIVELY ELIMINATE THE NONAFFILIATED THIRD PARTY'S
21 ABILITY TO ACCESS THE PERSONAL IDENTIFYING INFORMATION,
22 NOTWITHSTANDING THE THIRD PARTY'S PHYSICAL POSSESSION OF THE
23 PERSONAL IDENTIFYING INFORMATION.

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

29 **24-73-103. Governmental entity - notification of security**
30 **breach. (1) Definitions.** AS USED IN THIS SECTION, UNLESS THE CONTEXT
31 OTHERWISE REQUIRES:

32 (a) "BIOMETRIC DATA" MEANS UNIQUE BIOMETRIC DATA
33 GENERATED FROM MEASUREMENTS OR ANALYSIS OF HUMAN BODY
34 CHARACTERISTICS FOR THE PURPOSE OF AUTHENTICATING THE INDIVIDUAL
35 WHEN HE OR SHE ACCESSES AN ONLINE ACCOUNT.

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

39 (c) "ENCRYPTED" MEANS RENDERED UNUSABLE, UNREADABLE, OR
40 INDECIPHERABLE TO AN UNAUTHORIZED PERSON THROUGH A SECURITY
41 TECHNOLOGY OR METHODOLOGY GENERALLY ACCEPTED IN THE FIELD OF

1 INFORMATION SECURITY.

2 (d) "GOVERNMENTAL ENTITY" MEANS THE STATE AND ANY STATE
3 AGENCY OR INSTITUTION, COUNTY, CITY AND COUNTY, INCORPORATED
4 CITY OR TOWN, SCHOOL DISTRICT, SPECIAL IMPROVEMENT DISTRICT,
5 AUTHORITY, AND EVERY OTHER KIND OF DISTRICT, INSTRUMENTALITY, OR
6 POLITICAL SUBDIVISION OF THE STATE ORGANIZED PURSUANT TO LAW.
7 "GOVERNMENTAL ENTITY" INCLUDES ENTITIES GOVERNED BY HOME RULE
8 CHARTERS.

9 (e) "MEDICAL INFORMATION" MEANS ANY INFORMATION ABOUT A
10 CONSUMER'S MEDICAL OR MENTAL HEALTH TREATMENT OR DIAGNOSIS BY
11 A HEALTH CARE PROFESSIONAL.

12 (f) "NOTICE" MEANS:

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

15 (II) TELEPHONIC NOTICE;

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

23 (IV) SUBSTITUTE NOTICE, IF THE GOVERNMENTAL ENTITY
24 REQUIRED TO PROVIDE NOTICE DEMONSTRATES THAT THE COST OF
25 PROVIDING NOTICE WILL EXCEED TWO HUNDRED FIFTY THOUSAND
26 DOLLARS, THE AFFECTED CLASS OF PERSONS TO BE NOTIFIED EXCEEDS TWO
27 HUNDRED FIFTY THOUSAND COLORADO RESIDENTS, OR THE
28 GOVERNMENTAL ENTITY DOES NOT HAVE SUFFICIENT CONTACT
29 INFORMATION TO PROVIDE NOTICE. SUBSTITUTE NOTICE CONSISTS OF ALL
30 OF THE FOLLOWING:

31 (A) E-MAIL NOTICE IF THE GOVERNMENTAL ENTITY HAS E-MAIL
32 ADDRESSES FOR THE MEMBERS OF THE AFFECTED CLASS OF COLORADO
33 RESIDENTS;

34 (B) CONSPICUOUS POSTING OF THE NOTICE ON THE WEBSITE PAGE
35 OF THE GOVERNMENTAL ENTITY IF THE GOVERNMENTAL ENTITY
36 MAINTAINS ONE; AND

37 (C) NOTIFICATION TO MAJOR STATEWIDE MEDIA.

38 (g) (I) (A) "PERSONAL INFORMATION" MEANS A COLORADO
39 RESIDENT'S FIRST NAME OR FIRST INITIAL AND LAST NAME IN COMBINATION
40 WITH ANY ONE OR MORE OF THE FOLLOWING DATA ELEMENTS THAT
41 RELATE TO THE RESIDENT, WHEN THE DATA ELEMENTS ARE NOT

1 ENCRYPTED, REDACTED, OR SECURED BY ANY OTHER METHOD RENDERING
2 THE NAME OR THE ELEMENT UNREADABLE OR UNUSABLE: SOCIAL
3 SECURITY NUMBER; DRIVER'S LICENSE NUMBER OR IDENTIFICATION CARD
4 NUMBER; STUDENT, MILITARY, OR PASSPORT IDENTIFICATION NUMBER;
5 ACCOUNT NUMBER OR CREDIT CARD OR DEBIT CARD NUMBER; MEDICAL
6 INFORMATION; HEALTH INSURANCE IDENTIFICATION NUMBER; OR
7 BIOMETRIC DATA; OR

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

11 (II) "PERSONAL INFORMATION" DOES NOT INCLUDE PUBLICLY
12 AVAILABLE INFORMATION THAT IS LAWFULLY MADE AVAILABLE TO THE
13 GENERAL PUBLIC FROM FEDERAL, STATE, OR LOCAL GOVERNMENT
14 RECORDS OR WIDELY DISTRIBUTED MEDIA.

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

24 (2) **Disclosure of breach.** (a) A GOVERNMENTAL ENTITY THAT
25 MAINTAINS, OWNS, OR LICENSES COMPUTERIZED DATA THAT INCLUDES
26 PERSONAL INFORMATION ABOUT A RESIDENT OF COLORADO SHALL, WHEN
27 IT DETERMINES THAT A SECURITY BREACH HAS OCCURRED, CONDUCT IN
28 GOOD FAITH A PROMPT INVESTIGATION TO DETERMINE THE LIKELIHOOD
29 THAT PERSONAL INFORMATION HAS BEEN OR WILL BE MISUSED. THE
30 GOVERNMENTAL ENTITY SHALL GIVE NOTICE TO THE AFFECTED COLORADO
31 RESIDENTS UNLESS THE INVESTIGATION DETERMINES THAT THE MISUSE OF
32 INFORMATION ABOUT A COLORADO RESIDENT HAS NOT OCCURRED AND IS
33 NOT REASONABLY LIKELY TO OCCUR. NOTICE MUST BE MADE IN THE MOST
34 EXPEDIENT TIME POSSIBLE AND WITHOUT UNREASONABLE DELAY, BUT NOT
35 LATER THAN THIRTY DAYS AFTER THE DATE OF DETERMINATION THAT A
36 SECURITY BREACH OCCURRED, CONSISTENT WITH THE LEGITIMATE NEEDS
37 OF LAW ENFORCEMENT AND CONSISTENT WITH ANY MEASURES NECESSARY
38 TO DETERMINE THE SCOPE OF THE BREACH AND TO RESTORE THE
39 REASONABLE INTEGRITY OF THE COMPUTERIZED DATA SYSTEM.

40 (b) EXCEPT AS PROVIDED FOR IN SUBSECTION (2)(c) OF THIS
41 SECTION, IN THE CASE OF A BREACH OF PERSONAL INFORMATION, NOTICE

1 REQUIRED BY THIS SUBSECTION (2) TO AFFECTED COLORADO RESIDENTS
2 MUST INCLUDE, BUT NEED NOT BE LIMITED TO, THE FOLLOWING
3 INFORMATION:

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

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

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

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

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

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

19 (c) IF NOTICE OF A SECURITY BREACH INVOLVING PERSONAL
20 INFORMATION, AS DEFINED IN SUBSECTION (1)(g)(I)(B) OF THIS SECTION,
21 IS GIVEN NO LATER THAN FIVE DAYS AFTER THE DETERMINATION THAT A
22 SECURITY BREACH OCCURRED, CONSISTENT WITH THE LEGITIMATE NEEDS
23 OF LAW ENFORCEMENT AND CONSISTENT WITH ANY MEASURES NECESSARY
24 TO DETERMINE THE SCOPE OF THE BREACH AND TO RESTORE THE
25 REASONABLE INTEGRITY OF THE COMPUTERIZED DATA SYSTEM, NOTICE
26 MAY BE GIVEN AS FOLLOWS RATHER THAN AS OUTLINED IN SUBSECTION
27 (2)(a) OF THIS SECTION:

28 (I) THE GOVERNMENTAL ENTITY MAY PROVIDE THE SECURITY
29 BREACH NOTIFICATION IN ELECTRONIC OR OTHER FORM THAT DIRECTS THE
30 PERSON WHOSE PERSONAL INFORMATION HAS BEEN BREACHED TO
31 PROMPTLY CHANGE HIS OR HER PASSWORD AND SECURITY QUESTION OR
32 ANSWER, AS APPLICABLE, OR TO TAKE OTHER STEPS APPROPRIATE TO
33 PROTECT THE ONLINE ACCOUNT WITH THE PERSON OR BUSINESS AND ALL
34 OTHER ONLINE ACCOUNTS FOR WHICH THE PERSON WHOSE PERSONAL
35 INFORMATION HAS BEEN BREACHED THAT USES THE SAME USERNAME OR
36 E-MAIL ADDRESS AND PASSWORD OR SECURITY QUESTION OR ANSWER.

37 (II) FOR LOG-IN CREDENTIALS OF AN E-MAIL ACCOUNT FURNISHED
38 BY THE GOVERNMENTAL ENTITY, THE GOVERNMENTAL ENTITY SHALL NOT
39 COMPLY WITH THIS SECTION BY PROVIDING THE SECURITY BREACH
40 NOTIFICATION TO THAT E-MAIL ADDRESS, BUT MAY INSTEAD COMPLY WITH
41 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
28 LIKELY TO OCCUR. COOPERATION INCLUDES SHARING WITH THE OWNER OR
29 LICENSEE INFORMATION RELEVANT TO THE SECURITY BREACH; EXCEPT
30 THAT SUCH COOPERATION DOES NOT REQUIRE THE DISCLOSURE OF
31 CONFIDENTIAL BUSINESS INFORMATION OR TRADE SECRETS.

32 (h) NOTICE REQUIRED BY THIS SECTION MAY BE DELAYED IF A LAW
33 ENFORCEMENT AGENCY DETERMINES THAT THE NOTICE WILL IMPEDE A
34 CRIMINAL INVESTIGATION AND THE LAW ENFORCEMENT AGENCY HAS
35 NOTIFIED THE GOVERNMENTAL ENTITY THAT OPERATES IN COLORADO NOT
36 TO SEND NOTICE REQUIRED BY THIS SECTION. NOTICE REQUIRED BY THIS
37 SECTION MUST BE MADE IN GOOD FAITH, WITHOUT UNREASONABLE DELAY
38 BUT NOT LATER THAN THIRTY DAYS AFTER THE LAW ENFORCEMENT
39 AGENCY DETERMINES THAT NOTIFICATION WILL NO LONGER IMPEDE THE
40 INVESTIGATION AND HAS NOTIFIED THE GOVERNMENTAL ENTITY THAT IT
41 IS APPROPRIATE TO SEND THE NOTICE REQUIRED BY THIS SECTION.

1 (i) IF A GOVERNMENTAL ENTITY IS REQUIRED TO NOTIFY MORE
2 THAN ONE THOUSAND COLORADO RESIDENTS OF A SECURITY BREACH
3 PURSUANT TO THIS SECTION, THE GOVERNMENTAL ENTITY SHALL ALSO
4 NOTIFY, WITHOUT UNREASONABLE DELAY, ALL CONSUMER REPORTING
5 AGENCIES THAT COMPILE AND MAINTAIN FILES ON CONSUMERS ON A
6 NATIONWIDE BASIS, AS DEFINED BY THE FEDERAL "FAIR CREDIT
7 REPORTING ACT", 15 U.S.C. SEC. 1681a (p), OF THE ANTICIPATED DATE OF
8 THE NOTIFICATION TO THE RESIDENTS AND THE APPROXIMATE NUMBER OF
9 RESIDENTS WHO ARE TO BE NOTIFIED. NOTHING IN THIS SUBSECTION (2)(i)
10 REQUIRES THE GOVERNMENTAL ENTITY TO PROVIDE TO THE CONSUMER
11 REPORTING AGENCY THE NAMES OR OTHER PERSONAL INFORMATION OF
12 SECURITY BREACH NOTICE RECIPIENTS. THIS SUBSECTION (2)(i) DOES NOT
13 APPLY TO A PERSON WHO IS SUBJECT TO TITLE V OF THE FEDERAL
14 "GRAMM-LEACH-BLILEY ACT", 15 U.S.C. SEC. 6801 ET SEQ.

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

17 (k) (I) THE GOVERNMENTAL ENTITY THAT WAS BREACHED SHALL
18 PROVIDE NOTICE OF ANY SECURITY BREACH TO THE COLORADO ATTORNEY
19 GENERAL AS SOON AS PRACTICABLE BUT NOT LATER THAN THIRTY DAYS
20 AFTER THE DATE OF DETERMINATION THAT A SECURITY BREACH
21 OCCURRED IF THE SECURITY BREACH IS REASONABLY BELIEVED TO HAVE
22 AFFECTED FIVE HUNDRED COLORADO RESIDENTS OR MORE, UNLESS THE
23 INVESTIGATION DETERMINES THAT THE MISUSE OF INFORMATION ABOUT
24 A COLORADO RESIDENT HAS NOT OCCURRED AND IS NOT LIKELY TO OCCUR.

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

31 (3) **Procedures deemed in compliance with notice**
32 **requirements.** (a) PURSUANT TO THIS SECTION, A GOVERNMENTAL
33 ENTITY THAT MAINTAINS ITS OWN NOTIFICATION PROCEDURES AS PART OF
34 AN INFORMATION SECURITY POLICY FOR THE TREATMENT OF PERSONAL
35 INFORMATION AND WHOSE PROCEDURES ARE OTHERWISE CONSISTENT
36 WITH THE TIMING REQUIREMENTS OF THIS SECTION IS IN COMPLIANCE WITH
37 THE NOTICE REQUIREMENTS OF THIS SECTION IF THE GOVERNMENTAL
38 ENTITY NOTIFIES AFFECTED COLORADO CUSTOMERS IN ACCORDANCE WITH
39 ITS POLICIES IN THE EVENT OF A SECURITY BREACH; EXCEPT THAT NOTICE
40 TO THE ATTORNEY GENERAL IS STILL REQUIRED PURSUANT TO SUBSECTION
41 (2)(k) OF THIS SECTION.

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

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

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

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

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

** *** ** *** **