

HB1128_L.003

HOUSE COMMITTEE OF REFERENCE AMENDMENT

Committee on State, Veterans, & Military Affairs.HB18-1128 be amended as follows:

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

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

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

38 **6-1-713.5. Protection of personal identifying information.**

39 (1) TO PROTECT PERSONAL IDENTIFYING INFORMATION, AS DEFINED IN
40 SECTION 6-1-713 (2), FROM UNAUTHORIZED ACCESS, USE, MODIFICATION,
41 DISCLOSURE, OR DESTRUCTION, A PERSON THAT MAINTAINS, OWNS, OR

1 LICENSES PERSONAL IDENTIFYING INFORMATION OF AN INDIVIDUAL
2 RESIDING IN THE STATE SHALL IMPLEMENT AND MAINTAIN REASONABLE
3 SECURITY PROCEDURES AND PRACTICES THAT ARE APPROPRIATE TO THE
4 NATURE OF THE PERSONAL IDENTIFYING INFORMATION AND THE NATURE
5 AND SIZE OF THE BUSINESS AND ITS OPERATIONS.

6 (2) A PERSON THAT USES A NONAFFILIATED THIRD PARTY AS A
7 SERVICE PROVIDER TO PERFORM SERVICES FOR THE PERSON AND
8 DISCLOSES PERSONAL IDENTIFYING INFORMATION ABOUT AN INDIVIDUAL
9 RESIDING IN THE STATE WITH THE NONAFFILIATED THIRD PARTY SHALL
10 REQUIRE THAT THE NONAFFILIATED THIRD PARTY 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 NONAFFILIATED THIRD PARTY UNDER
21 CIRCUMSTANCES WHERE THE PERSON 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 PERSON IMPLEMENTS AND
25 MAINTAINS TECHNICAL CONTROLS THAT ARE REASONABLY DESIGNED TO:

26 (a) HELP PROTECT THE PERSONAL IDENTIFYING INFORMATION
27 FROM UNAUTHORIZED ACCESS, USE, MODIFICATION, DISCLOSURE, OR
28 DESTRUCTION; OR

29 (b) EFFECTIVELY ELIMINATE THE NONAFFILIATED THIRD PARTY'S
30 ABILITY TO ACCESS THE PERSONAL IDENTIFYING INFORMATION,
31 NOTWITHSTANDING THE THIRD PARTY'S PHYSICAL POSSESSION OF THE
32 PERSONAL IDENTIFYING INFORMATION.

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

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

41 **6-1-716. Notification of security breach.** (1) **Definitions.** As
42 USED IN THIS SECTION, UNLESS THE CONTEXT OTHERWISE REQUIRES:

43 (a) "BIOMETRIC DATA" MEANS UNIQUE BIOMETRIC DATA
44 GENERATED FROM MEASUREMENTS OR ANALYSIS OF HUMAN BODY
45 CHARACTERISTICS FOR THE PURPOSE OF AUTHENTICATING THE INDIVIDUAL

1 WHEN HE OR SHE ACCESSES AN ONLINE ACCOUNT.

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

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

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

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

14 (f) "NOTICE" MEANS:

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

17 (II) TELEPHONIC NOTICE;

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

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

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

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

39 (C) NOTIFICATION TO MAJOR STATEWIDE MEDIA.

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

1 SECURITY NUMBER; DRIVER'S LICENSE NUMBER OR IDENTIFICATION CARD
2 NUMBER; ACCOUNT NUMBER OR CREDIT CARD OR DEBIT CARD NUMBER;
3 MEDICAL INFORMATION; HEALTH INSURANCE IDENTIFICATION NUMBER; OR
4 BIOMETRIC DATA; OR

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

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

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

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

39 (a.2) EXCEPT AS OTHERWISE PROVIDED FOR IN SUBSECTION (2)(a.3)
40 OF THIS SECTION, IN THE CASE OF A BREACH OF PERSONAL INFORMATION,
41 NOTICE REQUIRED BY THIS SUBSECTION (2) TO AFFECTED COLORADO
42 RESIDENTS MUST INCLUDE, BUT NEED NOT BE LIMITED TO, THE FOLLOWING
43 INFORMATION:

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

1 (II) A DESCRIPTION OF THE PERSONAL INFORMATION THAT WAS
2 ACQUIRED OR REASONABLY BELIEVED TO HAVE BEEN ACQUIRED AS PART
3 OF THE SECURITY BREACH;
4 (III) INFORMATION THAT THE RESIDENT CAN USE TO CONTACT THE
5 INDIVIDUAL OR COMMERCIAL ENTITY THAT WAS BREACHED TO INQUIRE
6 ABOUT THE SECURITY BREACH;
7 (IV) THE TOLL-FREE NUMBERS, ADDRESSES, AND WEBSITES FOR
8 CONSUMER REPORTING AGENCIES;
9 (V) THE TOLL-FREE NUMBER, ADDRESS, AND WEBSITE FOR THE
10 FEDERAL TRADE COMMISSION; AND
11 (VI) A STATEMENT THAT THE RESIDENT CAN OBTAIN INFORMATION
12 FROM THE FEDERAL TRADE COMMISSION AND THE CREDIT REPORTING
13 AGENCIES ABOUT FRAUD ALERTS AND SECURITY FREEZES.
14 (a.3) IF NOTICE OF A SECURITY BREACH INVOLVING PERSONAL
15 INFORMATION IS GIVEN NO LATER THAN FIVE DAYS AFTER THE
16 DETERMINATION THAT A SECURITY BREACH OCCURRED, CONSISTENT WITH
17 THE LEGITIMATE NEEDS OF LAW ENFORCEMENT AND CONSISTENT WITH
18 ANY MEASURES NECESSARY TO DETERMINE THE SCOPE OF THE BREACH
19 AND TO RESTORE THE REASONABLE INTEGRITY OF THE COMPUTERIZED
20 DATA SYSTEM, NOTICE MAY BE GIVEN AS FOLLOWS, INSTEAD OF AS
21 OUTLINED IN SUBSECTION (2)(a.2) OF THIS SECTION:
22 (I) THE INDIVIDUAL OR COMMERCIAL ENTITY MAY PROVIDE THE
23 SECURITY BREACH NOTIFICATION IN ELECTRONIC OR OTHER FORM THAT
24 DIRECTS THE PERSON WHOSE PERSONAL INFORMATION HAS BEEN
25 BREACHED TO PROMPTLY CHANGE HIS OR HER PASSWORD AND SECURITY
26 QUESTION OR ANSWER, AS APPLICABLE, OR TO TAKE OTHER STEPS
27 APPROPRIATE TO PROTECT THE ONLINE ACCOUNT WITH THE PERSON OR
28 BUSINESS AND ALL OTHER ONLINE ACCOUNTS FOR WHICH THE PERSON
29 WHOSE PERSONAL INFORMATION HAS BEEN BREACHED THAT USES THE
30 SAME USER NAME OR E-MAIL ADDRESS AND PASSWORD OR SECURITY
31 QUESTION OR ANSWER.
32 (II) FOR LOG-IN CREDENTIALS OF AN E-MAIL ACCOUNT FURNISHED
33 BY THE INDIVIDUAL OR COMMERCIAL ENTITY, THE INDIVIDUAL OR
34 COMMERCIAL ENTITY SHALL NOT COMPLY WITH THIS SECTION BY
35 PROVIDING THE SECURITY BREACH NOTIFICATION TO THAT E-MAIL
36 ADDRESS, BUT MAY INSTEAD COMPLY WITH THIS SECTION BY PROVIDING
37 NOTICE, AS DEFINED IN SUBSECTION (1)(f) OF THIS SECTION, OR BY CLEAR
38 AND CONSPICUOUS NOTICE DELIVERED TO THE RESIDENT ONLINE WHEN
39 THE RESIDENT IS CONNECTED TO THE ONLINE ACCOUNT FROM AN INTERNET
40 PROTOCOL ADDRESS OR ONLINE LOCATION FROM WHICH THE INDIVIDUAL
41 OR COMMERCIAL ENTITY KNOWS THE RESIDENT CUSTOMARILY ACCESSES
42 THE ACCOUNT.
43 (a.4) THE BREACH OF ENCRYPTED OR OTHERWISE SECURED
44 PERSONAL INFORMATION MUST BE DISCLOSED IN ACCORDANCE WITH THIS
45 SECTION IF THE CONFIDENTIAL PROCESS, ENCRYPTION KEY, OR OTHER

1 MEANS TO DECIPHER THE SECURED INFORMATION WAS ALSO ACQUIRED IN
2 THE SECURITY BREACH OR WAS REASONABLY BELIEVED TO HAVE BEEN
3 ACQUIRED.

4 (a.5) AN INDIVIDUAL OR COMMERCIAL ENTITY THAT IS REQUIRED
5 TO PROVIDE NOTICE TO AFFECTED COLORADO RESIDENTS PURSUANT TO
6 THIS SUBSECTION (2) IS PROHIBITED FROM CHARGING THE COST OF
7 PROVIDING SUCH NOTICE TO SUCH RESIDENTS.

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

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

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

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

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

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

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

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

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

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

SHORTEST TIME FRAME FOR NOTICE TO THE INDIVIDUAL CONTROLS.

(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 CRIMINAL VIOLATIONS OF SECTION 18-5.5-102.

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

ARTICLE 73

Security Breaches and Personal Information

24-73-101. Governmental entity - disposal of personal identifying information - policy - definitions. (1) EACH GOVERNMENTAL ENTITY IN THE STATE THAT 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 STATE OR FEDERAL LAW OR REGULATION, THE WRITTEN POLICY MUST REQUIRE THAT, WHEN SUCH PAPER OR ELECTRONIC DOCUMENTS ARE NO LONGER NEEDED, THE GOVERNMENTAL 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) A GOVERNMENTAL ENTITY THAT IS REGULATED BY STATE OR FEDERAL LAW AND THAT MAINTAINS PROCEDURES FOR DISPOSAL OF PERSONAL IDENTIFYING INFORMATION PURSUANT TO THE LAWS, RULES, REGULATIONS, GUIDANCES, OR GUIDELINES ESTABLISHED BY ITS STATE OR FEDERAL REGULATOR IS IN COMPLIANCE WITH THIS SECTION.

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

1 REQUIRED BY THIS SECTION.

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

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

11 (b) "PERSONAL IDENTIFYING INFORMATION" MEANS A SOCIAL
12 SECURITY NUMBER; A PERSONAL IDENTIFICATION NUMBER; A PASSWORD;
13 A PASS CODE; AN OFFICIAL STATE OR GOVERNMENT-ISSUED DRIVER'S
14 LICENSE OR IDENTIFICATION CARD NUMBER; A GOVERNMENT PASSPORT
15 NUMBER; BIOMETRIC DATA; AN EMPLOYER, STUDENT, OR MILITARY
16 IDENTIFICATION NUMBER; OR A FINANCIAL TRANSACTION DEVICE, AS
17 DEFINED IN SECTION 18-5-701 (3).

18 **24-73-102. Governmental entity - protection of personal**
19 **identifying information.** (1) TO PROTECT PERSONAL IDENTIFYING
20 INFORMATION, AS DEFINED IN SECTION 24-73-101 (4)(b), FROM
21 UNAUTHORIZED ACCESS, USE, MODIFICATION, DISCLOSURE, OR
22 DESTRUCTION, A GOVERNMENTAL ENTITY THAT MAINTAINS, OWNS, OR
23 LICENSES PERSONAL IDENTIFYING INFORMATION SHALL IMPLEMENT AND
24 MAINTAIN REASONABLE SECURITY PROCEDURES AND PRACTICES THAT ARE
25 APPROPRIATE TO THE NATURE OF THE PERSONAL IDENTIFYING
26 INFORMATION AND THE NATURE AND SIZE OF THE GOVERNMENTAL ENTITY.

27 (2) A GOVERNMENTAL ENTITY THAT USES A NONAFFILIATED THIRD
28 PARTY AS A SERVICE PROVIDER TO PERFORM SERVICES FOR THE
29 GOVERNMENTAL ENTITY AND DISCLOSES PERSONAL IDENTIFYING
30 INFORMATION ABOUT AN INDIVIDUAL RESIDING IN THE STATE WITH THE
31 NONAFFILIATED THIRD PARTY SHALL REQUIRE THAT THE NONAFFILIATED
32 THIRD PARTY IMPLEMENT AND MAINTAIN REASONABLE SECURITY
33 PROCEDURES AND PRACTICES THAT ARE:

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

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

39 (3) FOR THE PURPOSES OF SUBSECTION (2) OF THIS SECTION, A
40 DISCLOSURE OF PERSONAL IDENTIFYING INFORMATION DOES NOT INCLUDE
41 DISCLOSURE OF INFORMATION TO A NONAFFILIATED THIRD PARTY UNDER
42 CIRCUMSTANCES WHERE THE GOVERNMENTAL ENTITY RETAINS PRIMARY
43 RESPONSIBILITY FOR IMPLEMENTING AND MAINTAINING REASONABLE
44 SECURITY PROCEDURES AND PRACTICES APPROPRIATE TO THE NATURE OF
45 THE PERSONAL IDENTIFYING INFORMATION AND THE GOVERNMENTAL

1 ENTITY IMPLEMENTS AND MAINTAINS TECHNICAL CONTROLS REASONABLY
2 DESIGNED TO:

3 (a) HELP PROTECT THE PERSONAL IDENTIFYING INFORMATION
4 FROM UNAUTHORIZED ACCESS, MODIFICATION, DISCLOSURE, OR
5 DESTRUCTION; OR

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

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

15 **24-73-103. Governmental entity - notification of security**
16 **breach. (1) Definitions.** AS USED IN THIS SECTION, UNLESS THE CONTEXT
17 OTHERWISE REQUIRES:

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

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

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

29 (d) "GOVERNMENTAL ENTITY" MEANS THE STATE AND ANY STATE
30 AGENCY OR INSTITUTION, COUNTY, CITY AND COUNTY, INCORPORATED
31 CITY OR TOWN, SCHOOL DISTRICT, SPECIAL IMPROVEMENT DISTRICT,
32 AUTHORITY, AND EVERY OTHER KIND OF DISTRICT, INSTRUMENTALITY, OR
33 POLITICAL SUBDIVISION OF THE STATE ORGANIZED PURSUANT TO LAW.
34 "GOVERNMENTAL ENTITY" INCLUDES ENTITIES GOVERNED BY HOME RULE
35 CHARTERS.

36 (e) "MEDICAL INFORMATION" MEANS ANY INFORMATION ABOUT A
37 CONSUMER'S MEDICAL OR MENTAL HEALTH TREATMENT OR DIAGNOSIS BY
38 A HEALTH CARE PROFESSIONAL.

39 (f) "NOTICE" MEANS:

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

42 (II) TELEPHONIC NOTICE;

43 (III) ELECTRONIC NOTICE, IF A PRIMARY MEANS OF
44 COMMUNICATION BY THE GOVERNMENTAL ENTITY WITH A COLORADO
45 RESIDENT IS BY ELECTRONIC MEANS OR THE NOTICE PROVIDED IS

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

5 (IV) SUBSTITUTE NOTICE, IF THE GOVERNMENTAL ENTITY
6 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
10 GOVERNMENTAL 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 GOVERNMENTAL ENTITY HAS E-MAIL
14 ADDRESSES FOR THE MEMBERS OF THE AFFECTED CLASS OF COLORADO
15 RESIDENTS;

16 (B) CONSPICUOUS POSTING OF THE NOTICE ON THE WEBSITE PAGE
17 OF THE GOVERNMENTAL ENTITY IF THE GOVERNMENTAL ENTITY
18 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; DRIVER'S LICENSE NUMBER OR IDENTIFICATION CARD
27 NUMBER; ACCOUNT NUMBER OR CREDIT CARD OR DEBIT CARD NUMBER;
28 MEDICAL INFORMATION; HEALTH INSURANCE IDENTIFICATION NUMBER; OR
29 BIOMETRIC DATA; OR

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

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

37 (h) "SECURITY BREACH" MEANS THE UNAUTHORIZED ACQUISITION
38 OF UNENCRYPTED COMPUTERIZED DATA THAT COMPROMISES THE
39 SECURITY, CONFIDENTIALITY, OR INTEGRITY OF PERSONAL INFORMATION
40 MAINTAINED BY A GOVERNMENTAL ENTITY. GOOD FAITH ACQUISITION OF
41 PERSONAL INFORMATION BY AN EMPLOYEE OR AGENT OF A
42 GOVERNMENTAL ENTITY FOR THE PURPOSES OF THE GOVERNMENTAL
43 ENTITY IS NOT A SECURITY BREACH IF THE PERSONAL INFORMATION IS NOT
44 USED FOR A PURPOSE UNRELATED TO THE LAWFUL GOVERNMENT PURPOSE
45 OR IS NOT SUBJECT TO FURTHER UNAUTHORIZED DISCLOSURE.

1 (2) **Disclosure of breach.** (a) A GOVERNMENTAL ENTITY THAT
2 MAINTAINS, OWNS, OR LICENSES COMPUTERIZED DATA THAT INCLUDES
3 PERSONAL INFORMATION ABOUT A RESIDENT OF COLORADO SHALL, WHEN
4 IT DETERMINES THAT A SECURITY BREACH HAS OCCURRED, CONDUCT IN
5 GOOD FAITH A PROMPT INVESTIGATION TO DETERMINE THE LIKELIHOOD
6 THAT PERSONAL INFORMATION HAS BEEN OR WILL BE MISUSED. THE
7 GOVERNMENTAL ENTITY SHALL GIVE NOTICE TO THE AFFECTED COLORADO
8 RESIDENTS UNLESS THE INVESTIGATION DETERMINES THAT THE MISUSE OF
9 INFORMATION ABOUT A COLORADO RESIDENT HAS NOT OCCURRED AND IS
10 NOT REASONABLY LIKELY TO OCCUR. NOTICE MUST BE MADE IN THE MOST
11 EXPEDIENT TIME POSSIBLE AND WITHOUT UNREASONABLE DELAY, BUT NOT
12 LATER THAN THIRTY DAYS AFTER THE DATE OF DETERMINATION THAT A
13 SECURITY BREACH OCCURRED, CONSISTENT WITH THE LEGITIMATE NEEDS
14 OF LAW ENFORCEMENT AND CONSISTENT WITH ANY MEASURES NECESSARY
15 TO DETERMINE THE SCOPE OF THE BREACH AND TO RESTORE THE
16 REASONABLE INTEGRITY OF THE COMPUTERIZED DATA SYSTEM.

17 (b) EXCEPT AS PROVIDED FOR IN SUBSECTION (2)(c) OF THIS
18 SECTION, IN THE CASE OF A BREACH OF PERSONAL INFORMATION, NOTICE
19 REQUIRED BY THIS SUBSECTION (2) TO AFFECTED COLORADO RESIDENTS
20 MUST INCLUDE, BUT NEED NOT BE LIMITED TO, THE FOLLOWING
21 INFORMATION:

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

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

27 (III) INFORMATION THAT THE RESIDENT CAN USE TO CONTACT THE
28 GOVERNMENTAL ENTITY THAT WAS BREACHED TO INQUIRE ABOUT THE
29 SECURITY BREACH;

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

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

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

37 (c) IF NOTICE OF A SECURITY BREACH INVOLVING PERSONAL
38 INFORMATION IS GIVEN NO LATER THAN FIVE DAYS AFTER THE
39 DETERMINATION THAT A SECURITY BREACH OCCURRED, CONSISTENT WITH
40 THE LEGITIMATE NEEDS OF LAW ENFORCEMENT AND CONSISTENT WITH
41 ANY MEASURES NECESSARY TO DETERMINE THE SCOPE OF THE BREACH
42 AND TO RESTORE THE REASONABLE INTEGRITY OF THE COMPUTERIZED
43 DATA SYSTEM, NOTICE MAY BE GIVEN AS FOLLOWS RATHER THAN AS
44 OUTLINED IN SUBSECTION (2)(a) OF THIS SECTION:

45 (I) THE GOVERNMENTAL ENTITY MAY PROVIDE THE SECURITY

1 BREACH NOTIFICATION IN ELECTRONIC OR OTHER FORM THAT DIRECTS THE
2 PERSON WHOSE PERSONAL INFORMATION HAS BEEN BREACHED TO
3 PROMPTLY CHANGE HIS OR HER PASSWORD AND SECURITY QUESTION OR
4 ANSWER, AS APPLICABLE, OR TO TAKE OTHER STEPS APPROPRIATE TO
5 PROTECT THE ONLINE ACCOUNT WITH THE PERSON OR BUSINESS AND ALL
6 OTHER ONLINE ACCOUNTS FOR WHICH THE PERSON WHOSE PERSONAL
7 INFORMATION HAS BEEN BREACHED THAT USES THE SAME USERNAME OR
8 E-MAIL ADDRESS AND PASSWORD OR SECURITY QUESTION OR ANSWER.

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

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

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

28 (f) NOTHING IN THIS SUBSECTION (2) PROHIBITS THE NOTICE
29 DESCRIBED IN THIS SUBSECTION (2) FROM CONTAINING ADDITIONAL
30 INFORMATION, INCLUDING ANY INFORMATION THAT MAY BE REQUIRED BY
31 STATE OR FEDERAL LAW.

32 (g) IF A GOVERNMENTAL ENTITY USES A THIRD-PARTY SERVICE
33 PROVIDER TO MAINTAIN COMPUTERIZED DATA THAT INCLUDES PERSONAL
34 INFORMATION, THEN THE THIRD-PARTY SERVICE PROVIDER SHALL GIVE
35 NOTICE TO AND COOPERATE WITH THE GOVERNMENTAL ENTITY IN THE
36 EVENT OF A SECURITY BREACH THAT COMPROMISES SUCH COMPUTERIZED
37 DATA, INCLUDING NOTIFYING THE GOVERNMENTAL ENTITY OF ANY
38 SECURITY BREACH AS SOON AS POSSIBLE AND WITHOUT UNREASONABLE
39 DELAY FOLLOWING DISCOVERY OF A SECURITY BREACH, IF MISUSE OF
40 PERSONAL INFORMATION ABOUT A COLORADO RESIDENT OCCURRED OR IS
41 LIKELY TO OCCUR. COOPERATION INCLUDES SHARING WITH THE OWNER OR
42 LICENSEE INFORMATION RELEVANT TO THE SECURITY BREACH; EXCEPT
43 THAT SUCH COOPERATION DOES NOT REQUIRE THE DISCLOSURE OF
44 CONFIDENTIAL BUSINESS INFORMATION OR TRADE SECRETS.

45 (h) NOTICE REQUIRED BY THIS SECTION MAY BE DELAYED IF A LAW

1 ENFORCEMENT AGENCY DETERMINES THAT THE NOTICE WILL IMPEDE A
2 CRIMINAL INVESTIGATION AND THE LAW ENFORCEMENT AGENCY HAS
3 NOTIFIED THE GOVERNMENTAL ENTITY THAT OPERATES IN COLORADO NOT
4 TO SEND NOTICE REQUIRED BY THIS SECTION. NOTICE REQUIRED BY THIS
5 SECTION MUST BE MADE IN GOOD FAITH, WITHOUT UNREASONABLE DELAY,
6 AND AS SOON AS POSSIBLE AFTER THE LAW ENFORCEMENT AGENCY
7 DETERMINES THAT NOTIFICATION WILL NO LONGER IMPEDE THE
8 INVESTIGATION AND HAS NOTIFIED THE GOVERNMENTAL ENTITY THAT IT
9 IS APPROPRIATE TO SEND THE NOTICE REQUIRED BY THIS SECTION.

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

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

26 (k) (I) THE GOVERNMENTAL ENTITY THAT WAS BREACHED SHALL
27 PROVIDE NOTICE OF ANY SECURITY BREACH TO THE COLORADO ATTORNEY
28 GENERAL AS SOON AS PRACTICABLE BUT NOT LATER THAN THIRTY DAYS
29 AFTER THE DATE OF DETERMINATION THAT A SECURITY BREACH
30 OCCURRED IF THE SECURITY BREACH IS REASONABLY BELIEVED TO HAVE
31 AFFECTED FIVE HUNDRED COLORADO RESIDENTS OR MORE, UNLESS THE
32 INVESTIGATION DETERMINES THAT THE MISUSE OF INFORMATION ABOUT
33 A COLORADO RESIDENT HAS NOT OCCURRED AND IS NOT LIKELY TO OCCUR.

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

40 (3) **Procedures deemed in compliance with notice**
41 **requirements.** (a) PURSUANT TO THIS SECTION, A GOVERNMENTAL
42 ENTITY THAT MAINTAINS ITS OWN NOTIFICATION PROCEDURES AS PART OF
43 AN INFORMATION SECURITY POLICY FOR THE TREATMENT OF PERSONAL
44 INFORMATION AND WHOSE PROCEDURES ARE OTHERWISE CONSISTENT
45 WITH THE TIMING REQUIREMENTS OF THIS SECTION IS IN COMPLIANCE WITH

1 THE NOTICE REQUIREMENTS OF THIS SECTION IF THE GOVERNMENTAL
2 ENTITY NOTIFIES AFFECTED COLORADO CUSTOMERS IN ACCORDANCE WITH
3 ITS POLICIES IN THE EVENT OF A SECURITY BREACH; EXCEPT THAT NOTICE
4 TO THE ATTORNEY GENERAL IS STILL REQUIRED PURSUANT TO SUBSECTION
5 (2)(k) OF THIS SECTION.

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

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

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

** **