

Second Regular Session
Seventy-first General Assembly
STATE OF COLORADO

REVISED

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

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

State, Veterans, & Military Affairs

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.

SENATE
Amended 2nd Reading
May 2, 2018

HOUSE
3rd Reading Unamended
April 20, 2018

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 THIRD-PARTY SERVICE PROVIDER; 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 _____ 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 PERSON ACTING
24 AS A THIRD-PARTY SERVICE PROVIDER AS DEFINED IN SUBSECTION (1)(i)
25 OF THIS SECTION.

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

1 CONCLUDE THAT A SECURITY BREACH HAS TAKEN PLACE.

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

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

9 (f) "NOTICE" MEANS:

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

12 (II) TELEPHONIC NOTICE;

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

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

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

1 RESIDENTS;

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

4 (C) NOTIFICATION TO MAJOR STATEWIDE MEDIA.

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

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

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

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

26 (h) "SECURITY BREACH" MEANS THE UNAUTHORIZED ACQUISITION
27 OF UNENCRYPTED COMPUTERIZED DATA THAT COMPROMISES THE

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

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

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

1 (a.2) 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 TO INQUIRE ABOUT THE 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 (a.3) IF AN INVESTIGATION BY THE COVERED ENTITY PURSUANT TO
20 SUBSECTION (2)(a) OF THIS SECTION DETERMINES THAT THE TYPE OF
21 PERSONAL INFORMATION DESCRIBED IN SUBSECTION (1)(g)(I)(B) OF THIS
22 SECTION HAS BEEN MISUSED OR IS REASONABLY LIKELY TO BE MISUSED,
23 THEN THE COVERED ENTITY SHALL, IN ADDITION TO THE NOTICE
24 OTHERWISE REQUIRED BY SUBSECTION (2)(a.2) OF THIS SECTION AND IN
25 THE MOST EXPEDIENT TIME POSSIBLE AND WITHOUT UNREASONABLE
26 DELAY, BUT NOT LATER THAN THIRTY DAYS AFTER THE DATE OF
27 DETERMINATION THAT A SECURITY BREACH OCCURRED, CONSISTENT WITH

1 THE LEGITIMATE NEEDS OF LAW ENFORCEMENT AND CONSISTENT WITH
2 ANY MEASURES NECESSARY TO DETERMINE THE SCOPE OF THE BREACH
3 AND TO RESTORE THE REASONABLE INTEGRITY OF THE COMPUTERIZED
4 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 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 THROUGH OTHER METHODS, AS DEFINED IN SUBSECTION
18 (1)(f) OF THIS SECTION, OR BY CLEAR AND CONSPICUOUS NOTICE
19 DELIVERED TO THE RESIDENT ONLINE WHEN THE RESIDENT IS CONNECTED
20 TO THE ONLINE ACCOUNT FROM AN INTERNET PROTOCOL ADDRESS OR
21 ONLINE LOCATION FROM WHICH THE COVERED ENTITY KNOWS THE
22 RESIDENT CUSTOMARILY ACCESSES THE 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 IN THE MOST EXPEDIENT
19 TIME POSSIBLE, AND WITHOUT UNREASONABLE DELAY following discovery
20 of a SECURITY breach, if misuse of personal information about a Colorado
21 resident occurred or is likely to occur. Cooperation includes sharing with
22 ~~the owner or licensee~~ COVERED ENTITY information relevant to the
23 SECURITY breach; except that such cooperation ~~shall not be deemed to~~
24 DOES NOT require the disclosure of confidential business information or
25 trade 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, IN THE MOST EXPEDIENT TIME POSSIBLE AND
5 without unreasonable delay and as soon as possible BUT NOT LATER THAN
6 THIRTY DAYS after the law enforcement agency determines that
7 notification will no longer impede the investigation and has notified the
8 individual or commercial COVERED entity that conducts business in
9 Colorado that it is appropriate to send the 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, IN THE MOST EXPEDIENT
14 TIME POSSIBLE AND without unreasonable delay, all consumer reporting
15 agencies that compile and maintain files on consumers on a nationwide
16 basis, as defined by THE FEDERAL "FAIR CREDIT REPORTING ACT", 15
17 U.S.C. sec. 1681a (p), of the anticipated date of the notification to the
18 residents and the approximate number of residents who are to be notified.
19 Nothing in this paragraph (d) shall be construed to require SUBSECTION
20 (2)(d) REQUIRES the individual or commercial COVERED entity to provide
21 to the consumer reporting agency the names or other personal information
22 of SECURITY breach notice recipients. This paragraph (d) shall
23 SUBSECTION (2)(d) DOES not apply to a person COVERED ENTITY who is
24 subject to Title V of the federal "Gramm-Leach-Bliley Act", 15 U.S.C.
25 sec. 6801 et seq.

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

1 (f) (I) THE COVERED ENTITY THAT MUST NOTIFY COLORADO
2 RESIDENTS OF A DATA BREACH PURSUANT TO THIS SECTION SHALL
3 PROVIDE NOTICE OF ANY SECURITY BREACH TO THE COLORADO ATTORNEY
4 GENERAL IN THE MOST EXPEDIENT TIME POSSIBLE AND WITHOUT
5 UNREASONABLE DELAY, BUT NOT LATER THAN THIRTY DAYS AFTER THE
6 DATE OF DETERMINATION THAT A SECURITY BREACH OCCURRED, IF THE
7 SECURITY BREACH IS REASONABLY BELIEVED TO HAVE AFFECTED FIVE
8 HUNDRED COLORADO RESIDENTS OR MORE, UNLESS THE INVESTIGATION
9 DETERMINES THAT THE MISUSE OF INFORMATION ABOUT A COLORADO
10 RESIDENT HAS NOT OCCURRED AND IS NOT LIKELY TO OCCUR.

11 (II) THE COLORADO ATTORNEY GENERAL SHALL DESIGNATE A
12 PERSON OR PERSONS AS A POINT OF CONTACT FOR FUNCTIONS SET FORTH
13 IN THIS SUBSECTION (2)(f) AND SHALL MAKE THE CONTACT INFORMATION
14 FOR THAT PERSON OR THOSE PERSONS PUBLIC ON THE ATTORNEY
15 GENERAL'S WEBSITE AND BY ANY OTHER APPROPRIATE MEANS.

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

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

1 compliance with the notice requirements of this section if the ~~individual~~
2 ~~or the commercial~~ COVERED entity notifies affected Colorado customers
3 RESIDENTS in accordance with its policies in the event of a ~~breach of~~
4 ~~security of the system~~ SECURITY BREACH; EXCEPT THAT NOTICE TO THE
5 ATTORNEY GENERAL IS STILL REQUIRED PURSUANT TO SUBSECTION (2)(f)
6 OF THIS SECTION.

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

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

27 (5) **Attorney general criminal authority.** UPON RECEIPT OF

1 NOTICE PURSUANT TO SUBSECTION (2) OF THIS SECTION, AND WITH EITHER
2 A REQUEST FROM THE GOVERNOR TO PROSECUTE A PARTICULAR CASE OR
3 WITH THE APPROVAL OF THE DISTRICT ATTORNEY WITH JURISDICTION TO
4 PROSECUTE CASES IN THE JUDICIAL DISTRICT WHERE A CASE ___ COULD BE
5 BROUGHT, THE ATTORNEY GENERAL HAS THE AUTHORITY TO PROSECUTE
6 ANY CRIMINAL VIOLATIONS OF SECTION 18-5.5-102.

7 **SECTION 4.** In Colorado Revised Statutes, **add** article 73 to title
8 24 as follows:

9 **ARTICLE 73**

10 **Security Breaches and Personal Information**

11 **24-73-101. Governmental entity - disposal of personal**
12 **identifying information - policy - definitions.** (1) EACH
13 GOVERNMENTAL ENTITY IN THE STATE THAT MAINTAINS PAPER OR
14 ELECTRONIC DOCUMENTS DURING THE COURSE OF BUSINESS THAT
15 CONTAIN PERSONAL IDENTIFYING INFORMATION SHALL DEVELOP A
16 WRITTEN POLICY FOR THE DESTRUCTION OR PROPER DISPOSAL OF THOSE
17 PAPER AND ELECTRONIC DOCUMENTS CONTAINING PERSONAL IDENTIFYING
18 INFORMATION. UNLESS OTHERWISE REQUIRED BY STATE OR FEDERAL LAW
19 OR REGULATION, THE WRITTEN POLICY MUST REQUIRE THAT, WHEN SUCH
20 PAPER OR ELECTRONIC DOCUMENTS ARE NO LONGER NEEDED, THE
21 GOVERNMENTAL ENTITY DESTROY OR ARRANGE FOR THE DESTRUCTION OF
22 SUCH PAPER AND ELECTRONIC DOCUMENTS WITHIN ITS CUSTODY OR
23 CONTROL THAT CONTAIN PERSONAL IDENTIFYING INFORMATION BY
24 SHREDDING, ERASING, OR OTHERWISE MODIFYING THE PERSONAL
25 IDENTIFYING INFORMATION IN THE PAPER OR ELECTRONIC DOCUMENTS TO
26 MAKE THE PERSONAL IDENTIFYING INFORMATION UNREADABLE OR
27 INDECIPHERABLE THROUGH ANY MEANS.

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

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

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

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

24 (b) "PERSONAL IDENTIFYING INFORMATION" MEANS A SOCIAL
25 SECURITY NUMBER; A PERSONAL IDENTIFICATION NUMBER; A PASSWORD;
26 A PASS CODE; AN OFFICIAL STATE OR GOVERNMENT-ISSUED DRIVER'S
27 LICENSE OR IDENTIFICATION CARD NUMBER; A GOVERNMENT PASSPORT

1 NUMBER; BIOMETRIC DATA, AS DEFINED IN SECTION 24-73-103 (1)(a); AN
2 EMPLOYER, STUDENT, OR MILITARY IDENTIFICATION NUMBER; OR A
3 FINANCIAL TRANSACTION DEVICE, AS DEFINED IN SECTION 18-5-701 (3).

4 **24-73-102. Governmental entity - protection of personal**
5 **identifying information - definition.** (1) TO PROTECT PERSONAL
6 IDENTIFYING INFORMATION, AS DEFINED IN SECTION 24-73-101 (4)(b),
7 FROM UNAUTHORIZED ACCESS, USE, MODIFICATION, DISCLOSURE, OR
8 DESTRUCTION, A GOVERNMENTAL ENTITY THAT MAINTAINS, OWNS, OR
9 LICENSES PERSONAL IDENTIFYING INFORMATION SHALL IMPLEMENT AND
10 MAINTAIN REASONABLE SECURITY PROCEDURES AND PRACTICES THAT ARE
11 APPROPRIATE TO THE NATURE OF THE PERSONAL IDENTIFYING
12 INFORMATION AND THE NATURE AND SIZE OF THE GOVERNMENTAL ENTITY.

13 (2) UNLESS A GOVERNMENTAL ENTITY AGREES TO PROVIDE ITS
14 OWN SECURITY PROTECTION FOR THE INFORMATION IT DISCLOSES TO A
15 THIRD-PARTY SERVICE PROVIDER, THE GOVERNMENTAL ENTITY SHALL
16 REQUIRE THAT THE THIRD-PARTY SERVICE PROVIDER IMPLEMENT AND
17 MAINTAIN REASONABLE SECURITY PROCEDURES AND PRACTICES THAT
18 ARE:

19 (a) APPROPRIATE TO THE NATURE OF THE PERSONAL IDENTIFYING
20 INFORMATION DISCLOSED TO THE THIRD-PARTY SERVICE PROVIDER; AND

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

24 (3) FOR THE PURPOSES OF SUBSECTION (2) OF THIS SECTION, A
25 DISCLOSURE OF PERSONAL IDENTIFYING INFORMATION DOES NOT INCLUDE
26 DISCLOSURE OF INFORMATION TO A THIRD PARTY UNDER CIRCUMSTANCES
27 WHERE THE GOVERNMENTAL ENTITY RETAINS PRIMARY RESPONSIBILITY

1 FOR IMPLEMENTING AND MAINTAINING REASONABLE SECURITY
2 PROCEDURES AND PRACTICES APPROPRIATE TO THE NATURE OF THE
3 PERSONAL IDENTIFYING INFORMATION AND THE GOVERNMENTAL ENTITY
4 IMPLEMENTS AND MAINTAINS TECHNICAL CONTROLS REASONABLY
5 DESIGNED TO:

6 (a) HELP PROTECT THE PERSONAL IDENTIFYING INFORMATION
7 FROM UNAUTHORIZED ACCESS, MODIFICATION, DISCLOSURE, OR
8 DESTRUCTION; OR

9 (b) EFFECTIVELY ELIMINATE THE THIRD PARTY'S ABILITY TO
10 ACCESS THE PERSONAL IDENTIFYING INFORMATION, NOTWITHSTANDING
11 THE THIRD PARTY'S PHYSICAL POSSESSION OF THE PERSONAL IDENTIFYING
12 INFORMATION.

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

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

22 **24-73-103. Governmental entity - notification of security**
23 **breach. (1) Definitions.** AS USED IN THIS SECTION, UNLESS THE CONTEXT
24 OTHERWISE REQUIRES:

25 (a) "BIOMETRIC DATA" MEANS UNIQUE BIOMETRIC DATA
26 GENERATED FROM MEASUREMENTS OR ANALYSIS OF HUMAN BODY
27 CHARACTERISTICS FOR THE PURPOSE OF AUTHENTICATING THE INDIVIDUAL

1 WHEN HE OR SHE ACCESSES AN ONLINE ACCOUNT.

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

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

9 (d) "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 SUBSECTION (1)(i) OF THIS
18 SECTION.

19 (e) "MEDICAL INFORMATION" MEANS ANY INFORMATION ABOUT A
20 CONSUMER'S MEDICAL OR MENTAL HEALTH TREATMENT OR DIAGNOSIS BY
21 A HEALTH CARE PROFESSIONAL.

22 (f) "NOTICE" MEANS:

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

25 (II) TELEPHONIC NOTICE;

26 (III) ELECTRONIC NOTICE, IF A PRIMARY MEANS OF
27 COMMUNICATION BY THE GOVERNMENTAL ENTITY WITH A COLORADO

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

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

14 (A) E-MAIL NOTICE IF THE GOVERNMENTAL ENTITY HAS E-MAIL
15 ADDRESSES FOR THE MEMBERS OF THE AFFECTED CLASS OF COLORADO
16 RESIDENTS;

17 (B) CONSPICUOUS POSTING OF THE NOTICE ON THE WEBSITE PAGE
18 OF THE GOVERNMENTAL ENTITY IF THE GOVERNMENTAL ENTITY
19 MAINTAINS ONE; AND

20 (C) NOTIFICATION TO MAJOR STATEWIDE MEDIA.

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

1 NUMBER; STUDENT, MILITARY, OR PASSPORT IDENTIFICATION NUMBER;
2 MEDICAL INFORMATION; HEALTH INSURANCE IDENTIFICATION NUMBER; OR
3 BIOMETRIC DATA, AS DEFINED IN SECTION 24-73-101 (1)(a);

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

7 (C) A COLORADO RESIDENT'S ACCOUNT NUMBER OR CREDIT OR
8 DEBIT CARD NUMBER IN COMBINATION WITH ANY REQUIRED SECURITY
9 CODE, ACCESS CODE, OR PASSWORD THAT WOULD PERMIT ACCESS TO THAT
10 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 (i) "THIRD-PARTY SERVICE PROVIDER" MEANS AN ENTITY THAT
25 HAS BEEN CONTRACTED TO MAINTAIN, STORE, OR PROCESS PERSONAL
26 INFORMATION ON BEHALF OF A GOVERNMENTAL ENTITY.

27 (2) **Disclosure of breach.** (a) A GOVERNMENTAL ENTITY THAT

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

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

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

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

26 (III) INFORMATION THAT THE RESIDENT CAN USE TO CONTACT THE
27 GOVERNMENTAL ENTITY TO INQUIRE ABOUT THE SECURITY BREACH;

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

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

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

8 (c) IF AN INVESTIGATION BY THE GOVERNMENTAL ENTITY
9 PURSUANT TO SUBSECTION (2)(a) OF THIS SECTION DETERMINES THAT THE
10 TYPE OF PERSONAL INFORMATION DESCRIBED IN SUBSECTION (1)(g)(I)(B)
11 OF THIS SECTION HAS BEEN MISUSED OR IS REASONABLY LIKELY TO BE
12 MISUSED, THEN THE GOVERNMENTAL ENTITY SHALL, IN ADDITION TO THE
13 NOTICE OTHERWISE REQUIRED BY SUBSECTION (2)(b) OF THIS SECTION AND
14 IN THE MOST EXPEDIENT TIME POSSIBLE AND WITHOUT UNREASONABLE
15 DELAY, BUT NOT LATER THAN THIRTY DAYS AFTER THE DATE OF
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:

21 (I) DIRECT THE PERSON WHOSE PERSONAL INFORMATION HAS BEEN
22 BREACHED TO PROMPTLY CHANGE HIS OR HER PASSWORD AND SECURITY
23 QUESTION OR ANSWER, AS APPLICABLE, OR TO TAKE OTHER STEPS
24 APPROPRIATE TO PROTECT THE ONLINE ACCOUNT WITH THE PERSON OR
25 BUSINESS AND ALL OTHER ONLINE ACCOUNTS FOR WHICH THE PERSON
26 WHOSE PERSONAL INFORMATION HAS BEEN BREACHED USES THE SAME
27 USERNAME OR E-MAIL ADDRESS AND PASSWORD OR SECURITY QUESTION

1 OR ANSWER.

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

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

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

22 (f) NOTHING IN THIS SUBSECTION (2) PROHIBITS THE NOTICE
23 DESCRIBED IN THIS SUBSECTION (2) FROM CONTAINING ADDITIONAL
24 INFORMATION, INCLUDING ANY INFORMATION THAT MAY BE REQUIRED BY
25 STATE OR FEDERAL LAW.

26 (g) IF A GOVERNMENTAL ENTITY USES A THIRD-PARTY SERVICE
27 PROVIDER TO MAINTAIN COMPUTERIZED DATA THAT INCLUDES PERSONAL

1 INFORMATION, THEN THE THIRD-PARTY SERVICE PROVIDER SHALL GIVE
2 NOTICE TO AND COOPERATE WITH THE GOVERNMENTAL ENTITY IN THE
3 EVENT OF A SECURITY BREACH THAT COMPROMISES SUCH COMPUTERIZED
4 DATA, INCLUDING NOTIFYING THE GOVERNMENTAL ENTITY OF ANY
5 SECURITY BREACH IN THE MOST EXPEDIENT TIME AND WITHOUT
6 UNREASONABLE DELAY FOLLOWING DISCOVERY OF A SECURITY BREACH,
7 IF MISUSE OF PERSONAL INFORMATION ABOUT A COLORADO RESIDENT
8 OCCURRED OR IS LIKELY TO OCCUR. COOPERATION INCLUDES SHARING
9 WITH THE COVERED ENTITY INFORMATION RELEVANT TO THE SECURITY
10 BREACH; EXCEPT THAT SUCH COOPERATION DOES NOT REQUIRE THE
11 DISCLOSURE OF CONFIDENTIAL BUSINESS INFORMATION OR TRADE
12 SECRETS.

13 (h) NOTICE REQUIRED BY THIS SECTION MAY BE DELAYED IF A LAW
14 ENFORCEMENT AGENCY DETERMINES THAT THE NOTICE WILL IMPEDE A
15 CRIMINAL INVESTIGATION AND THE LAW ENFORCEMENT AGENCY HAS
16 NOTIFIED THE GOVERNMENTAL ENTITY THAT OPERATES IN COLORADO NOT
17 TO SEND NOTICE REQUIRED BY THIS SECTION. NOTICE REQUIRED BY THIS
18 SECTION MUST BE MADE IN GOOD FAITH, IN THE MOST EXPEDIENT TIME
19 POSSIBLE AND WITHOUT UNREASONABLE DELAY, BUT NOT LATER THAN
20 THIRTY DAYS AFTER THE LAW ENFORCEMENT AGENCY DETERMINES THAT
21 NOTIFICATION WILL NO LONGER IMPEDE THE INVESTIGATION, AND HAS
22 NOTIFIED THE GOVERNMENTAL ENTITY THAT IT IS APPROPRIATE TO SEND
23 THE NOTICE REQUIRED BY THIS SECTION.

24 (i) IF A GOVERNMENTAL ENTITY IS REQUIRED TO NOTIFY MORE
25 THAN ONE THOUSAND COLORADO RESIDENTS OF A SECURITY BREACH
26 PURSUANT TO THIS SECTION, THE GOVERNMENTAL ENTITY SHALL ALSO
27 NOTIFY, IN THE MOST EXPEDIENT TIME POSSIBLE AND WITHOUT

1 UNREASONABLE DELAY, ALL CONSUMER REPORTING AGENCIES THAT
2 COMPILE AND MAINTAIN FILES ON CONSUMERS ON A NATIONWIDE BASIS,
3 AS DEFINED BY THE FEDERAL "FAIR CREDIT REPORTING ACT", 15 U.S.C.
4 SEC. 1681a (p), OF THE ANTICIPATED DATE OF THE NOTIFICATION TO THE
5 RESIDENTS AND THE APPROXIMATE NUMBER OF RESIDENTS WHO ARE TO BE
6 NOTIFIED. NOTHING IN THIS SUBSECTION (2)(i) REQUIRES THE
7 GOVERNMENTAL ENTITY TO PROVIDE TO THE CONSUMER REPORTING
8 AGENCY THE NAMES OR OTHER PERSONAL INFORMATION OF SECURITY
9 BREACH NOTICE RECIPIENTS. THIS SUBSECTION (2)(i) DOES NOT APPLY TO
10 A PERSON WHO IS SUBJECT TO TITLE V OF THE FEDERAL
11 "GRAMM-LEACH-BLILEY ACT", 15 U.S.C. SEC. 6801 ET SEQ.

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

14 (k) (I) THE GOVERNMENTAL ENTITY THAT MUST NOTIFY
15 COLORADO RESIDENTS OF A DATA BREACH PURSUANT TO THIS SECTION
16 SHALL PROVIDE NOTICE OF ANY SECURITY BREACH TO THE COLORADO
17 ATTORNEY GENERAL IN THE MOST EXPEDIENT TIME POSSIBLE AND
18 WITHOUT UNREASONABLE DELAY, BUT NOT LATER THAN THIRTY DAYS
19 AFTER THE DATE OF DETERMINATION THAT A SECURITY BREACH
20 OCCURRED, IF THE SECURITY BREACH IS REASONABLY BELIEVED TO HAVE
21 AFFECTED FIVE HUNDRED COLORADO RESIDENTS OR MORE, UNLESS THE
22 INVESTIGATION DETERMINES THAT THE MISUSE OF INFORMATION ABOUT
23 A COLORADO RESIDENT HAS NOT OCCURRED AND IS NOT LIKELY TO OCCUR.

24 (II) THE COLORADO ATTORNEY GENERAL SHALL DESIGNATE A
25 PERSON OR PERSONS AS A POINT OF CONTACT FOR FUNCTIONS SET FORTH
26 IN THIS SUBSECTION (2)(k) AND SHALL MAKE THE CONTACT INFORMATION
27 FOR THAT PERSON OR THOSE PERSONS PUBLIC ON THE ATTORNEY

1 GENERAL'S WEBSITE AND BY ANY OTHER APPROPRIATE MEANS.

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

8 **(3) Procedures deemed in compliance with notice**
9 **requirements.** (a) PURSUANT TO THIS SECTION, A GOVERNMENTAL
10 ENTITY THAT MAINTAINS ITS OWN NOTIFICATION PROCEDURES AS PART OF
11 AN INFORMATION SECURITY POLICY FOR THE TREATMENT OF PERSONAL
12 INFORMATION AND WHOSE PROCEDURES ARE OTHERWISE CONSISTENT
13 WITH THE TIMING REQUIREMENTS OF THIS SECTION IS IN COMPLIANCE WITH
14 THE NOTICE REQUIREMENTS OF THIS SECTION IF THE GOVERNMENTAL
15 ENTITY NOTIFIES AFFECTED COLORADO RESIDENTS IN ACCORDANCE WITH
16 ITS POLICIES IN THE EVENT OF A SECURITY BREACH; EXCEPT THAT NOTICE
17 TO THE ATTORNEY GENERAL IS STILL REQUIRED PURSUANT TO SUBSECTION
18 (2)(k) OF THIS SECTION.

19 (b) A GOVERNMENTAL ENTITY THAT IS REGULATED BY STATE OR
20 FEDERAL LAW AND THAT MAINTAINS PROCEDURES FOR A SECURITY
21 BREACH PURSUANT TO THE LAWS, RULES, REGULATIONS, GUIDANCES, OR
22 GUIDELINES ESTABLISHED BY ITS STATE OR FEDERAL REGULATOR IS IN
23 COMPLIANCE WITH THIS SECTION; EXCEPT THAT NOTICE TO THE ATTORNEY
24 GENERAL IS STILL REQUIRED PURSUANT TO SUBSECTION (2)(k) OF THIS
25 SECTION. IN THE CASE OF A CONFLICT BETWEEN THE TIME PERIOD FOR
26 NOTICE TO INDIVIDUALS, THE LAW OR REGULATION WITH THE SHORTEST
27 NOTICE PERIOD CONTROLS.

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

3 **(5) Attorney general criminal authority.** UPON RECEIPT OF
4 NOTICE PURSUANT TO SUBSECTION (2) OF THIS SECTION, AND WITH EITHER
5 A REQUEST FROM THE GOVERNOR TO PROSECUTE A PARTICULAR CASE OR
6 WITH THE APPROVAL OF THE DISTRICT ATTORNEY WITH JURISDICTION TO
7 PROSECUTE CASES IN THE JUDICIAL DISTRICT WHERE A CASE ___ COULD BE
8 BROUGHT, THE ATTORNEY GENERAL HAS THE AUTHORITY TO PROSECUTE
9 ANY CRIMINAL VIOLATIONS OF SECTION 18-5.5-102.

10 **SECTION 5. Effective date.** This act takes effect September 1,
11 2018.

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