PARKER
COLORADO

TOWN COUNCIL STUDY SESSION AGENDA
February 11, 2019
5:30 PM

I. Town Council Items

II. Study Session Items

1. Security Breach Policy/Data Protection Procedures (HB18-1128) - Schledorn/Brown - 30 minutes
2. Economic Development Quarterly Update - Carlson - 45 minutes
3. Cultural Department "White Board" Discussion - Mariner - 30 minutes

MEMORANDUM

TO:	Mayor and Town Council
FROM:	Kristin Schledorn, Deputy Town Attorney Mary Lou Brown, Finance Director
DATE:	February 11, 2019
SUBJECT:	Security Breach Policy/Data Protection Procedures (HB18-1128)

ISSUE:

The purpose of this study session agenda item is to discuss amendment of the Parker Records Retention Schedule and adoption of a new Policy 4.3 to the Operations Manual regarding records containing personal identifying information, in response to HB 18-1128 and Division of Homeland Security and Emergency Management Performance Grant site visit.

FISCAL/BUDGET IMPACT:

None.

BACKGROUND:

Last year, the state legislature enacted HB 18-1128, which established specific notification requirements for security breaches of data containing personal identifying information (PII) and for the destruction of municipal records containing PII. A copy of the bill is attached to this memorandum.

Staff is proposing the addition of a new Policy 4.3 to the Operations Manual, entitled "Town Information Security Policy" and a proposed resolution to amend the Parker Records Retention Schedule, regarding the destruction of records containing PII. The Colorado Municipal Records Retention Schedule (which the Town has adopted) sets forth appropriate methods of records destruction in Appendix E. However, they do not adequately address the record destruction requirements of HB 18-1128.

Additionally, on December 4, 2018, the Division of Homeland Security and Emergency Management (DHSEM) monitoring team completed a site visit for the Emergency Management Performance Grant (EMPG) program from which the Town receives grant funding. The compliance team examined certain functions of the Town related to the administration of funds under the EMPG grant.

During the visit, the DHSEM identified the lack of a policy for the protection of PII. This was considered an area of improvement that required follow up. According to the Code of Federal Regulations (CFR) 200.303(e) “The non-Federal entity must take reasonable measures to safeguard protected personally identifiable information and other information the Federal awarding agency or pass-through entity designates as sensitive or the non-Federal entity considers sensitive consistent with applicable Federal, state, local, and tribal laws regarding privacy and obligations of confidentiality.”

The Town prepared a response to the DHSEM notifying them that the Town Attorney’s office, Technology Management and Accounting Division have drafted a PII policy that will be discussed with Town Council on February 11, 2019, and that following that discussion, the policy will be added to the Town’s General Operations Manual in the beginning of April. Once the policy is in place, the Town will send a copy of the policy to the DHSEM – Subrecipient Monitoring Team. The DHSEM approved the Town's response and proposed course of action.

Attached to this memorandum are the proposed resolution and Policy 4.3. Formal action will be required by Town Council to adopt the proposed resolution and amend the Parker Records Retention Schedule. Policy 4.3 is approved administratively by the Town Administrator and will be done in conjunction with approval of the attached resolution.

RECOMMENDATION:

Staff recommends proceeding with adoption of the resolution by Town Council, amending the Parker Records Retention Schedule, and approval of the addition of Policy 4.3 to the General Operations Manual by the Town Administrator.

REQUESTED DIRECTION:

Staff requests direction on this issue.

ATTACHMENT:

1. Proposed Record Retention Schedule Resoluton to Amend App E 20190206
2. Operations Manual - Sec 4.3 (New) Info Security Policy 20190206
3. HB 18-1128

RESOLUTION NO. 19-_____, Series of 2019

TITLE: A RESOLUTION TO AMEND RESOLUTION NO. 16-073, SERIES OF 2016, CONCERNING THE TOWN OF PARKER RECORDS RETENTION SCHEDULE APPENDIX E REGARDING METHODS OF RECORD DESTRUCTION PURSUANT TO HB 18-1128

WHEREAS, the Town Council of the Town of Parker adopted the Colorado Municipal Records Retention Schedule ("CMRRS") as the records retention schedule for the Town of Parker, with certain exceptions ("Parker Records Retention Schedule");

WHEREAS, the Town Council adopted Supplements 11 and 12 of the Parker Retention Schedule by Resolution No. 16-073, Series of 2016, concerning website, intranet and social media records on December 5, 2016;

WHEREAS, in its last session, the State General Assembly enacted HB 18-1128, which, in part, set forth specific requirements for the disposal of personal identifying information;

WHEREAS, the Methods of Record Destruction, set forth in Appendix E of the CMRRS, do not adequately address the requirements for the disposal of personal identifying information set forth in HB 18-1128;

WHEREAS, the Colorado State Archives authorizes municipalities to amend the CMRRS by formal direction of an entity's governing body followed by submittal to the Colorado State Archives of an Approval Request Form;

WHEREAS, the Town Council desires to amend Appendix E by incorporating the requirements of HB 18-1128; and

WHEREAS, the Town Council desires to amend the Parker Records Retention Schedule concerning methods of destroying records.

NOW, THEREFORE, BE IT RESOLVED BY THE TOWN COUNCIL OF THE TOWN OF PARKER, COLORADO, AS FOLLOWS:

Section 1. The Town Council of the Town of Parker hereby amends the Parker Records Retention Schedule, Exhibit E, Methods of Destruction, by addition of a new paragraph after section 4 of the Appendix's first paragraph to provide:

> "'Personal Identifying Information,' which means a social security number, a personal identification number, a password, a pass code, an official state or government-issued driver's license or identification car number, a government passport number, biometric data as defined in C.R.S. § 24-73-103(1)(a), an employer, student, or military identification number, or a financial transaction device, as defined in C.R.S. § 18-5-701(3), shall be destroyed 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."

Section 2. The Town Council of the Town of Parker hereby amends the Parker Records Retention Schedule, Exhibit E, Methods of Destruction, by addition of section 7 of the Appendix's last paragraph to provide:

"7. Where the destruction of records is performed by a third-party service provider, the Town shall ensure that the provider maintain reasonable security procedures and practices that are appropriate for the records subject to destruction and are reasonably designed to protect the records from unauthorized access, use, modification, disclosure, or destruction."

Section 3. The Town Council of the Town of Parker hereby directs the Town Clerk of the Town of Parker to file a copy of this Resolution with the Colorado State Archivist.

RESOLVED AND PASSED this _____ day of _____, 2019.

TOWN OF PARKER, COLORADO

_____

Mike Waid, Mayor

ATTEST:

_____

Carol Baumgartner, Town Clerk

PARKER
COLORADO

General Operations Manual

Issued by the Town Administrator's Office

4. Information Technology

….

4.3 Town Information Security Policy

It is the purpose of this policy to provide Town of Parker employees guidance on how to properly handle personally identifiable information (personal information). To strengthen the protections for consumer data privacy for those living, working, and doing business within the Town and to ensure a prompt response, the following standards have been adopted in compliance with HB 18-1128, which is codified at C.R.S. § 24-73-103, and is summarized below. Terms not defined in this Policy shall have the meaning given them in the statute and in the event of any inconsistency between C.R.S. § 24-73-103 and this Policy, the statute shall control.

4.3.1 Definition of Terms

"Redaction" means the process of deleting, blacking out, or otherwise making unreadable information or data before dissemination.

"Personal information" means information about a person that can be used to distinguish or determine a person's identity. The types of information that can be personal information include, but are not limited to:

- Social security number
- Username and password
- Passport number

- Credit card information
- Clearances
- Banking information
- Biometrics
- Date and place of birth
- Mother's maiden name
- Criminal, medical and financial records
- Educational transcripts
- Photos and video including any of the above

For purposes of compliance with C.R.S. § 24-73-103, "personal information" also means a Colorado resident's first name or first initial and last name in combination with any of the following data elements that relate to the resident, when the data elements are not encrypted, redacted, or secured by any other method rendering the name or the element unreadable or unusable: social security number; driver's license number or identification card number; student, military, or passport identification number; medical information; health insurance identification number; or biometric data. "Personal information" also means a Colorado resident's username or email address, in combination with a password or security questions and answers, that would permit access to an online account or a Colorado resident's account number or credit or debit card number in combination with any required security code, access code or password that would permit access to that account. "Personal information" does not include publicly available information that is lawfully made available to the general public from federal, state or local government records or widely distributed media, including, but not limited to:

- First and last name
- Address
- Work telephone number
- Work email address
- Home telephone number
- General educational credentials
- General photos and video

"Security breach" means the unauthorized acquisition of unencrypted computerized data that compromises the security, confidentiality, or integrity of personal information maintained by the Town.

4.3.2. Procedures for Protection of Personal Information

- **General**

  All electronic files that contain personal information will reside within a protected information system location. All physical files that contain personal information will reside within a locked file cabinet or room when not being actively viewed or modified. Files containing personal information are not to be downloaded to personally-owned mobile devices (such as laptops, mobile phones, tablets or removable media) or to systems outside the protection of the Town. Files containing personal information should not be sent through any form of unsecured electronic communication (email or instant messaging systems).

- **Redaction**

  Town employees must redact all personal information prior to dissemination to non-employees. Redaction may include making a photocopy of the document and using black permanent marker to conceal the personal information. Employees may also use Adobe Acrobat Pro to redact personal information for electronic dissemination. Documents containing personal information may be disclosed by the Town to third-party service providers only if the service provider implements and maintains reasonable security procedures to ensure the protection of such data.

- **Disposal**

  When paper or electronic documents containing personal information are no longer needed, Town employees must destroy or arrange for the documents destruction. Paper copies of documents containing personal information must be shredded securely or made indecipherable through any means available. Any electronic documents must be deleted from the computer file system, and the trash folder emptied to assure complete deletion of the file from the computer or storage system. Such destruction must also comply with the requirements for document destruction outlined in the Parker Records Retention Schedule, Exhibit E, Methods of Destruction.

- **Incident Reporting**

  Employees must immediately report all real or suspected disclosure of personal information immediately to the Information Technology Department. Examples of potential disclosure include misplacing a paper report, loss of a laptop, hard drive, mobile device, or removable media containing personal information, accidental email of personal information, possible virus, or malware infection of a computer containing personal information.

- **Audits**

  Periodic audits of Town-owned equipment and physical locations may be performed by the Chief Information Officer or delegate to ensure that personal information is stored in approved information systems or locations. The purpose of any audit is to ensure compliance with this policy and to provide information necessary to continuously improve business practices.

4.3.3 Investigation of Security Breach (C.R.S. § 24-73-103)

Upon becoming aware that a security breach may have occurred, the Town shall conduct a good faith and prompt investigation to determine the likelihood that personal information has been or will be misused.

- **Response to Suspected Security Breach**

  If this investigation shows that misuse has occurred or is likely to occur, the Town shall give notice to any affected Colorado residents in the most expedient time possible and without unreasonable delay, but not later than thirty days after the date of determination that a security breach occurred, consistent with the legitimate needs of law enforcement and consistent with any measures necessary to determine the scope of the breach and to restore the reasonable integrity of the computerized data system. If notice is delayed because law enforcement notifies the Town that it will impede a criminal investigation, notice will be made in the most expedient time possible and without unreasonable delay, but not later than thirty days after the law enforcement agency determines that

notification will no longer impede the investigation and has notified the Town that it is appropriate to send the notice.

Notice shall be provided using any of the following methods:

- Written notice to the postal address listed in the Town's records;
- Telephonic notice;
- Electronic notice, if this is the primary means of contact with this Colorado resident; or
- Substitute notice, including email, public posting on Town website, or notification to major statewide media, if the cost of providing notice will exceed $250,000 or affects more than 250,000 Colorado residents, or if contact information is insufficient to provide notice.

- **Notice Requirements**

Notice of a security breach to affected Colorado residents must include the following information:

- The date, estimated date or estimated date range of the security breach;
- A description of the personal information that was acquired or reasonably believed to have been acquired as part of the security breach;
- Information that the Colorado resident can use to contact the Town to inquire about the security breach;
- The toll-free numbers, addresses and websites for consumer reporting agencies;
- The toll-free number, address and website for the federal trade commission; and
- A statement that the Colorado resident can obtain information from the federal trade commission and the credit reporting agencies about fraud alerts and security freezes.

- **Additional Steps**

In addition to providing notice, the Town shall also, in the most expedient time possible and without unreasonable delay, but not later than thirty days after the date of determination that a security breach occurred:

- Direct those whose personal information has been breached to change their passwords and security questions and answers for that account immediately, as well as for any other accounts with the same user name and passwords;
- Send notices of a suspected security breach to alternate email addresses or other methods of communication, rather than to compromised accounts;
- Disclose the breach of encrypted or otherwise secure personal information if the encryption key or other means to decipher the secured information was also acquired or was reasonably believed to have been acquired in the security breach;

- Require third-party service providers who maintain computerized data for the Town to notify and cooperate with the Town in responding to and taking steps to resolve the breach;
- If the Town must notify more than 1,000 Colorado residents of a suspected breach, then it must also notify all consumer reporting agencies that a breach occurred as quickly as possible; and
- If more than 500 Colorado residents are believed to be affected by the breach, then the Town must notify the Colorado attorney general's office, as quickly as possible and no more than 30 days after the breach is discovered.

HOUSE BILL 18-1128

BY REPRESENTATIVE(S) Wist and Bridges, Arndt, Becker K., Buckner, Coleman, Danielson, Esgar, Exum, Foote, Garnett, Gray, Hamner, Hansen, Herod, Hooton, Jackson, Kraft-Tharp, Landgraf, Lawrence, Lee, Liston, Lontine, McLachlan, Melton, Michaelson Jenet, Neville P., Pettersen, Rankin, Ransom, Reyher, Roberts, Rosenthal, Saine, Sias, Singer, Valdez, Van Winkle, Weissman, Winkler, Winter, Young, Duran, Benavidez, Ginal, Humphrey, Kennedy, Salazar;
also SENATOR(S) Lambert and Court, Aguilar, Crowder, Donovan, Fenberg, Fields, Garcia, Gardner, Guzman, Jahn, Jones, Kefalas, Kerr, Lundberg, Marble, Martinez Humenik, Merrifield, Moreno, Neville T., Tate, Todd, Williams A., Zenzinger, Grantham.

CONCERNING STRENGTHENING PROTECTIONS FOR CONSUMER DATA PRIVACY.

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

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

6-1-713. Disposal of personal identifying information - policy - definitions. (1) Each ~~public and private~~ COVERED entity in the state that ~~uses~~ MAINTAINS PAPER OR ELECTRONIC documents during the course of

Capital letters or bold & italic numbers indicate new material added to existing statutes; dashes through words indicate deletions from existing statutes and such material not part of act.

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 COVERED ENTITY SHALL DESTROY OR ARRANGE FOR THE DESTRUCTION OF SUCH PAPER AND ELECTRONIC DOCUMENTS WITHIN ITS CUSTODY OR CONTROL THAT CONTAIN PERSONAL IDENTIFYING INFORMATION BY SHREDDING, ERASING, OR OTHERWISE MODIFYING THE PERSONAL IDENTIFYING INFORMATION IN THE PAPER OR ELECTRONIC DOCUMENTS TO MAKE THE PERSONAL IDENTIFYING INFORMATION UNREADABLE OR INDECIPHERABLE THROUGH ANY MEANS.

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

(a) "COVERED ENTITY" MEANS A PERSON, AS DEFINED IN SECTION 6-1-102 (6), THAT MAINTAINS, OWNS, OR LICENSES PERSONAL IDENTIFYING INFORMATION IN THE COURSE OF THE PERSON'S BUSINESS, VOCATION, OR OCCUPATION. "COVERED ENTITY" DOES NOT INCLUDE A PERSON ACTING AS A THIRD-PARTY SERVICE PROVIDER AS DEFINED IN SECTION 6-1-713.5.

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

(3) ~~A public entity that is managing its records in compliance with part 1 of article 80 of title 24, C.R.S., shall be deemed to have met its obligations under subsection (1) of this section~~ A COVERED 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.

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

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

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

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

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

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

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

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

(4) A COVERED ENTITY THAT IS REGULATED BY STATE OR FEDERAL LAW AND THAT MAINTAINS PROCEDURES FOR PROTECTION 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.

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

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

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

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

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

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

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

(e) "MEDICAL INFORMATION" MEANS ANY INFORMATION ABOUT A CONSUMER'S MEDICAL OR MENTAL HEALTH TREATMENT OR DIAGNOSIS BY A

HEALTH CARE PROFESSIONAL.

(f) "NOTICE" MEANS:

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

(II) TELEPHONIC NOTICE;

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

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

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

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

(C) NOTIFICATION TO MAJOR STATEWIDE MEDIA.

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

INFORMATION; HEALTH INSURANCE IDENTIFICATION NUMBER; OR BIOMETRIC DATA;

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

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

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

(h) "SECURITY BREACH" MEANS THE UNAUTHORIZED ACQUISITION OF UNENCRYPTED COMPUTERIZED DATA THAT COMPROMISES THE SECURITY, CONFIDENTIALITY, OR INTEGRITY OF PERSONAL INFORMATION MAINTAINED BY A COVERED ENTITY. GOOD FAITH ACQUISITION OF PERSONAL INFORMATION BY AN EMPLOYEE OR AGENT OF A COVERED ENTITY FOR THE COVERED ENTITY'S BUSINESS PURPOSES IS NOT A SECURITY BREACH IF THE PERSONAL INFORMATION IS NOT USED FOR A PURPOSE UNRELATED TO THE LAWFUL OPERATION OF THE BUSINESS OR IS NOT SUBJECT TO FURTHER UNAUTHORIZED DISCLOSURE.

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

(2) **Disclosure of breach.** (a) ~~An individual or a commercial~~ A COVERED entity ~~that conducts business in Colorado and~~ that MAINTAINS, owns, or licenses computerized data that includes personal information about a resident of Colorado shall, when it ~~becomes aware of a breach of the security of the system~~ BECOMES AWARE THAT A SECURITY BREACH MAY HAVE OCCURRED, conduct in good faith a prompt investigation to determine the likelihood that personal information has been or will be misused. The ~~individual or the commercial~~ COVERED entity shall give notice ~~as soon as possible~~ to the affected Colorado ~~resident~~ RESIDENTS unless the

investigation determines that the misuse of information about a Colorado resident has not occurred and is not reasonably likely to occur. Notice ~~shall~~ MUST be made in the most expedient time possible and without unreasonable delay, BUT NOT LATER THAN THIRTY DAYS AFTER THE DATE OF DETERMINATION THAT A SECURITY BREACH OCCURRED, consistent with the legitimate needs of law enforcement and consistent with any measures necessary to determine the scope of the breach and to restore the reasonable integrity of the computerized data system.

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

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

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

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

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

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

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

(a.3) IF AN INVESTIGATION BY THE COVERED ENTITY PURSUANT TO SUBSECTION (2)(a) OF THIS SECTION DETERMINES THAT THE TYPE OF PERSONAL INFORMATION DESCRIBED IN SUBSECTION (1)(g)(I)(B) OF THIS SECTION HAS BEEN MISUSED OR IS REASONABLY LIKELY TO BE MISUSED, THEN THE COVERED ENTITY SHALL, IN ADDITION TO THE NOTICE OTHERWISE REQUIRED BY SUBSECTION (2)(a.2) OF THIS SECTION AND IN THE MOST

EXPEDIENT TIME POSSIBLE AND WITHOUT UNREASONABLE DELAY, BUT NOT LATER THAN THIRTY DAYS AFTER THE DATE OF DETERMINATION THAT A SECURITY BREACH OCCURRED, CONSISTENT WITH THE LEGITIMATE NEEDS OF LAW ENFORCEMENT AND CONSISTENT WITH ANY MEASURES NECESSARY TO DETERMINE THE SCOPE OF THE BREACH AND TO RESTORE THE REASONABLE INTEGRITY OF THE COMPUTERIZED DATA SYSTEM:

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

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

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

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

(a.6) NOTHING IN THIS SUBSECTION (2) PROHIBITS THE NOTICE DESCRIBED IN THIS SUBSECTION (2) FROM CONTAINING ADDITIONAL

INFORMATION, INCLUDING ANY INFORMATION THAT MAY BE REQUIRED BY STATE OR FEDERAL LAW.

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

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

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

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

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

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

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

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

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

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

(b) ~~An individual or a commercial~~ A COVERED entity that is regulated by state or federal law and that maintains procedures for a SECURITY breach ~~of the security of the system~~ pursuant to the laws, rules, regulations, guidances, or guidelines established by its ~~primary or functional~~ state or federal regulator is ~~deemed to be~~ in compliance with this section; EXCEPT THAT NOTICE TO THE ATTORNEY GENERAL IS STILL REQUIRED PURSUANT TO SUBSECTION (2)(f) OF THIS SECTION. IN THE CASE OF A CONFLICT BETWEEN THE TIME PERIOD FOR NOTICE TO INDIVIDUALS THAT IS REQUIRED PURSUANT TO THIS SUBSECTION (3) AND THE APPLICABLE STATE OR 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~~ A COVERED 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, AND WITH EITHER A REQUEST FROM THE GOVERNOR TO PROSECUTE A PARTICULAR CASE OR WITH THE APPROVAL OF THE DISTRICT ATTORNEY WITH JURISDICTION TO PROSECUTE CASES IN THE JUDICIAL DISTRICT WHERE A CASE COULD BE BROUGHT, THE ATTORNEY GENERAL HAS THE AUTHORITY TO 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 REQUIRED BY THIS SECTION.

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

(a) "GOVERNMENTAL ENTITY" MEANS THE STATE AND ANY STATE AGENCY OR INSTITUTION, INCLUDING THE JUDICIAL DEPARTMENT, COUNTY, CITY AND COUNTY, INCORPORATED CITY OR TOWN, SCHOOL DISTRICT, SPECIAL IMPROVEMENT DISTRICT, AUTHORITY, AND EVERY OTHER KIND OF DISTRICT, INSTRUMENTALITY, OR POLITICAL SUBDIVISION OF THE STATE ORGANIZED PURSUANT TO LAW. "GOVERNMENTAL ENTITY" INCLUDES

ENTITIES GOVERNED BY HOME RULE CHARTERS. "GOVERNMENTAL ENTITY" DOES NOT INCLUDE AN ENTITY ACTING AS A THIRD-PARTY SERVICE PROVIDER AS DEFINED IN SECTION 24-73-102.

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

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

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

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

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

(3) FOR THE PURPOSES OF SUBSECTION (2) OF THIS SECTION, A DISCLOSURE OF PERSONAL IDENTIFYING INFORMATION DOES NOT INCLUDE DISCLOSURE OF INFORMATION TO A THIRD PARTY UNDER CIRCUMSTANCES WHERE THE GOVERNMENTAL ENTITY RETAINS PRIMARY RESPONSIBILITY FOR IMPLEMENTING AND MAINTAINING REASONABLE SECURITY PROCEDURES AND

PRACTICES APPROPRIATE TO THE NATURE OF THE PERSONAL IDENTIFYING INFORMATION AND THE GOVERNMENTAL ENTITY IMPLEMENTS AND MAINTAINS TECHNICAL CONTROLS REASONABLY DESIGNED TO:

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

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

(4) A GOVERNMENTAL ENTITY THAT IS REGULATED BY STATE OR FEDERAL LAW AND THAT MAINTAINS PROCEDURES FOR STORAGE 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.

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

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

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

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

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

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

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

(f) "NOTICE" MEANS:

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

(II) TELEPHONIC NOTICE;

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

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

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

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

(C) NOTIFICATION TO MAJOR STATEWIDE MEDIA.

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

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

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

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

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

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

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

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

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

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

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

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

(V) THE TOLL-FREE NUMBER, ADDRESS, AND WEBSITE FOR THE

FEDERAL TRADE COMMISSION; AND

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

(c) IF AN INVESTIGATION BY THE GOVERNMENTAL ENTITY PURSUANT TO SUBSECTION (2)(a) OF THIS SECTION DETERMINES THAT THE TYPE OF PERSONAL INFORMATION DESCRIBED IN SUBSECTION (1)(g)(I)(B) OF THIS SECTION HAS BEEN MISUSED OR IS REASONABLY LIKELY TO BE MISUSED, THEN THE GOVERNMENTAL ENTITY SHALL, IN ADDITION TO THE NOTICE OTHERWISE REQUIRED BY SUBSECTION (2)(b) OF THIS SECTION AND IN THE MOST EXPEDIENT TIME POSSIBLE AND WITHOUT UNREASONABLE DELAY, BUT NOT LATER THAN THIRTY DAYS AFTER THE DATE OF DETERMINATION THAT A SECURITY BREACH OCCURRED, CONSISTENT WITH THE LEGITIMATE NEEDS OF LAW ENFORCEMENT AND CONSISTENT WITH ANY MEASURES NECESSARY TO DETERMINE THE SCOPE OF THE BREACH AND TO RESTORE THE REASONABLE INTEGRITY OF THE COMPUTERIZED DATA SYSTEM:

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

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

(d) THE BREACH OF ENCRYPTED OR OTHERWISE SECURED PERSONAL INFORMATION MUST BE DISCLOSED IN ACCORDANCE WITH THIS SECTION IF

THE CONFIDENTIAL PROCESS, ENCRYPTION KEY, OR OTHER MEANS TO DECIPHER THE SECURED INFORMATION WAS ALSO ACQUIRED IN THE SECURITY BREACH OR WAS REASONABLY BELIEVED TO HAVE BEEN ACQUIRED.

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

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

(g) IF A GOVERNMENTAL ENTITY USES A THIRD-PARTY SERVICE PROVIDER TO MAINTAIN COMPUTERIZED DATA THAT INCLUDES PERSONAL INFORMATION, THEN THE THIRD-PARTY SERVICE PROVIDER SHALL GIVE NOTICE TO AND COOPERATE WITH THE GOVERNMENTAL ENTITY IN THE EVENT OF A SECURITY BREACH THAT COMPROMISES SUCH COMPUTERIZED DATA, INCLUDING NOTIFYING THE GOVERNMENTAL ENTITY OF ANY SECURITY BREACH IN THE MOST EXPEDIENT TIME AND WITHOUT UNREASONABLE DELAY FOLLOWING DISCOVERY OF A SECURITY BREACH, IF MISUSE OF PERSONAL INFORMATION ABOUT A COLORADO RESIDENT OCCURRED OR IS LIKELY TO OCCUR. COOPERATION INCLUDES SHARING WITH THE COVERED ENTITY INFORMATION RELEVANT TO THE SECURITY BREACH; EXCEPT THAT SUCH COOPERATION DOES NOT REQUIRE THE DISCLOSURE OF CONFIDENTIAL BUSINESS INFORMATION OR TRADE SECRETS.

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

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

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

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

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

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

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

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

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

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

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

SECTION 6. Safety clause. The general assembly hereby finds,

determines, and declares that this act is necessary for the immediate preservation of the public peace, health, and safety.

Crisanta Duran
SPEAKER OF THE HOUSE
OF REPRESENTATIVES

Kevin J. Grantham
PRESIDENT OF
THE SENATE

Marilyn Eddins
CHIEF CLERK OF THE HOUSE
OF REPRESENTATIVES

Effie Ameen
SECRETARY OF
THE SENATE

APPROVED 10:27 am 5/29/18

John W. Hickenlooper
GOVERNOR OF THE STATE OF COLORADO