Understanding & Preparing for the Colorado Cybersecurity Regulation (HB 18-1128)

Introduction

On January 19, 2018, the General Assembly of the State of Colorado introduced House Bill 18-1128, Concerning Strengthening Protections for Consumer Data Privacy. The new regulation comes from an effort to improve protection for Colorado businesses, consumers, and government agencies from the ever-growing threat of cyber-attacks. The regulation was signed into law on May 29, 2018 and goes into effect on September 1, 2018.

The wording in the **Section Text** column alternates between uppercase and lowercase words. The reason for this is to show the difference between existing regulation and new regulatory text. All uppercase wording is new, whereas all lowercase wording is preexisting language.

This resource is for information purposes only. It serves to provide Tandem's opinion of the regulatory language included in HB 18-1128. You may use this resource to assist in your understanding of the regulation, but you should interpret the regulation, as appropriate, for your organization.

This resource also serves to identify areas in Tandem where regulation topics are addressed and does not guarantee that a financial institution using the Tandem software is in compliance with the regulation.

Tandem is a tool designed to work with financial institutions to assist with compliance goals. Use the details in the **Tandem Mapping** column to help determine whether the institution's controls and documentation align with the regulation.

For any questions about this resource, contact Tandem Support:

800-356-6568

Tandem@CoNetrix.com

Section	Section Title / *Section Text*	Tandem Opinion	Tandem Mapping
1	6-1-713. Disposal of Personal Identifying Information		**Policies** Data Retention and Destruction
1(1)	*Each COVERED 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 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.*	Each covered entity must have a written data destruction policy that addresses the disposal of physical and electronic documents that contain personally identifiable information (PII).	**Policies** Data Retention and Destruction See the **Implementation** section of the policy.
1(2)(a)	*"COVERED ENTITY" MEANS A PERSON, AS DEFINED IN SECTION 6- I- 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 DEFNED IN SECTION 6- I -713.5.*	The regulation defines a “covered entity” as a person who maintains, owns, or licenses PII in the course of their business, vocation, or occupation. Per Section 6-1-102(6), a “person” is an: Individual Corporation Business Trust Estate Trust Partnership Unincorporated Association The term “covered entity” does not apply to third parties.	N/A

Section	Section Title / *Section Text*	Tandem Opinion	Tandem Mapping
1(2)(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 (l)(a); an employer, student, or military identification number; or a financial transaction device, AS DEFINED IN SECTION 18-5-701*	The regulation defines PII as: Social Security Number Personal Identification Number Password Pass Code Driver's License Number State Issued ID Card Number Passport Number Biometric Data Employer, Student, or Military ID Number Financial Transaction Device Per Section 18-5-205, a "financial transaction device" is a: Credit Card Banking Card Debit Card Electronic Fund Transfer Card Guaranteed Check Card Account Number But it does not include: Checks Negotiable Order of Withdrawal Share Draft	**Policies** Data Retention and Destruction While the "Data Retention and Destruction" policy includes examples of PII, users are welcome to customize the policy further to include these more specific examples at ***Policies > Global > Policies > Edit "Data Retention and Destruction"***. A good section to put this information would be in the **Commentary** field.
1(3)	*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.*	If the covered entity is already regulated by state or federal law (e.g., GLBA), the requirements in Section 1 should already be met.	N/A

Section	Section Title / *Section Text*	Tandem Opinion	Tandem Mapping
2	6-1-713.5. Protection of Personal Identifying Information		Each module in the Tandem product is designed to help financial institutions protect their personally identifying information. See the Tandem Knowledge Base articles for more information about each product and how the module plays a part in protecting personal identifying information: https://secure.conetrix.com/KnowledgeBaseArticles
2(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.*	Covered entities must "implement and maintain reasonable security procedures and practices" to protect PII from unauthorized access, use, modification, disclosure, or destruction. This is similar language to the Interagency Guidelines Establishing Information Security Standards' UMAD threat types: Unauthorized Disclosure = Disclosure Misuse = Use Alteration = Modification Destruction = Destruction The Colorado regulation also includes unauthorized "access."	**Risk Assessment** The Tandem Risk Assessment module allows users to document threats that could result in unauthorized disclosure, misuse, alteration, or destruction of personally identifiable information, along with the controls that are used to reduce the likelihood and potential damage of each threat's occurrence.
2(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:*	Unless otherwise agreed, if a covered entity provides PII to a third party, the covered entity must require the third party to implement controls to protect it.	**Vendor Management** The Tandem Vendor Management module allows users to document their third party oversight, contract requirements, and notification procedures.

Section	Section Title / *Section Text*	Tandem Opinion	Tandem Mapping
2(2)(a)	*APPROPRIATE TO THE NATURE OF THE PERSONAL IDENTIFYING INFORMATION DISCLOSED TO THE THIRD-PARTY SERVICE PROVIDER; AND*	The third party's controls should be appropriate for the PII data it's protecting.	**Vendor Management** Required Document Types Significance Questions For example, if a third party stores your organization's PII data, you would want to ensure the third party has a SOC Report that addresses the protections the third party has in place.
2(2)(b)	*REASONABLY DESIGNED TO HELP PROTECT THE PERSONAL IDENTIFYING INFORMATION FROM UNAUTHORIZED ACCESS, USE, MODIFICATION, DISCLOSURE, OR DESTRUCTION.*	The third party's controls should be designed to protect the PII the same way the covered entity's controls would protect it.	**Vendor Management** Required Document Types Significance Questions These controls should be discovered and evaluated through the vendor due diligence process.
2(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 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 ARE REASONABLY DESIGNED TO:*	There may be times when the covered entity is providing PII to a third party in which the covered entity retains responsibility for protecting the data.	This concept is typically referred to as "complimentary user entity controls" and is one of the areas that should be considered when performing a SOC Report review. **Vendor Management** SOC Report Review Template
2(3)(a)	*HELP PROTECT THE PERSONAL IDENTIFYING INFORMATION FROM UNAUTHORIZED ACCESS, USE, MODIFICATION, DISCLOSURE, OR DESTRUCTION; OR*	In this case, the covered entity should implement its own controls to help protect the PII during the relationship with the third party.	**Risk Assessment** Create asset-based risk assessments to document the threats and controls applicable to systems that may house PII. **Vendor Management** SOC Report Review Template

Section	Section Title / *Section Text*	Tandem Opinion	Tandem Mapping
2(3)(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.*	The covered entity should also have a plan in place to completely remove the third party's ability to access the PII, including any physical documentation to which the third party may have access.	**Policies** Cloud Computing Vendors, Contractors, and Partners **Vendor Management** Contract Review Template
2(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 GUIDELNES ESTABLISHED BY ITS STATE OR FEDERAL REGULATOR IS IN COMPLIANCE WITH THIS SECTION.*	If the covered entity is already regulated by state or federal law (e.g., GLBA), the requirements in Section 2 should already be met.	N/A
2(5)	*FOR THE PURPOSES OF THIS SECTION, "THIRD-PARTY SERVICE PROVIDER" MEANS AN ENTITY THAT HAS BEEN CONTRACTED TO MAINTAN, STORE, OR PROCESS PERSONAL IDENTIFYING INFORMATION ON BEHALF OF A COVERED ENTITY.*	The regulation defines a "third-party service provider" as someone who has been contracted to work with a covered entity's PII.	N/A
3	6-1-716. Notification of Security Breach.		**Policies** Incident Response **Resources** Incident Response Checklist This section primarily focuses on incident response and notification procedures. The Tandem "Incident Response" policy that addresses many of the generic requirements from this section. However, Tandem users can customize the policy to include their state's specific notification requirements.
3(1)	*Definitions. As USED IN THIS SECTION, UNLESS THE CONTEXT OTHERWISE REQUIRES:*	These are the definitions for terms used in the following sections.	While the "Incident Response" policy includes examples of incidents and PII,

Section	Section Title / *Section Text*	Tandem Opinion	Tandem Mapping
3(1)(a)	*"BIOMETRIC DATA" MEANS UNIQUE BIOMETRIC DATA GENERATED FROM MEASUREMENTS OR ANALYSIS OF BODY CHARACTERISTICS FOR THE PURPOSE OF AUTHENTICATING THE INDIVIDUAL WHEN HE OR SHE ACCESSES AN ONLINE ACCOUNT.*	The regulation defines "biometric data" as the use of body characteristics to authenticate someone's identity.	users are welcome to customize the policy further to include these more specific examples and definitions at ***Policies > Global > Policies > Edit "Incident Response"***. A good section to put this information would be in the **Commentary** field.
3(1)(b)	*"COVERED ENTITY" MEANS A PERSON, AS DEFINED IN SECTION 6- I- 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.*	This is a restating of the regulation's definition of a "covered entity." It's essentially the same as the definition in subsection 1(2)(a), except it refers to PII as "personal information."	
3(1)(c)	*"DETERMINATION THAT A SECURITY BREACH OCCURRED" MEANS THE POINT TIME AT WHICH THERE IS SUFFICIENT EVIDENCE TO CONCLUDE THAT A SECURITY BREACH HAS TAKEN PLACE.*	The regulation provides this definition for the event in which the covered entity realizes there is enough evidence to determine a security breach occurred.	
3(1)(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.*	The regulation defines "encrypted" data as data that cannot be used, read, or otherwise deciphered.	
3(1)(e)	*"MEDICAL INFORMATION" MEANS ANY INFORMATION ABOUT A CONSUMER'S MEDICAL OR MENTAL HEALTH TREATMENT OR DIAGNOSIS BY A HEALTH CARE PROFESSIONAL.*	This definition does not apply to financial institutions.	
3(1)(f)(I – III)	*"NOTICE" MEANS:* *WRITTEN NOTICE TO THE POSTAL ADDRESS LISTED IN THE RECORDS OF THE COVERED ENTITY;* *TELEPHONIC NOTICE;* *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*	If a covered entity must provide notice of a security breach, the covered entity can either: Write via postal mail Call Send electronic notice (if permissible)	**Policies** Incident Response This is addressed in the **Implementation** section, under the "Notification" subheading.

Section	Section Title / *Section Text*	Tandem Opinion	Tandem Mapping
3(1)(f)(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:*	If providing notice will cost the covered entity more than $250,000, the covered entity is notifying more than 250,000 people, or the covered entity does not have contact information to communicate with the affected persons, an alternative notification option may be used.	This specific requirement of "substitute notice" is not included in the Tandem "Incident Response" policy, but it could be included in the **Implementation** section, under the "Notification" subheading.
3(1)(f)(IV)(a – c)	*E-MAIL NOTICE IF THE COVERED ENTITY HAS E-MAIL ADDRESSES FOR THE MEMBERS OF THE AFFECTED CLASS OF COLORADO RESIDENTS;* *CONSPICUOUS POSTING OF THE NOTICE ON THE WEBSITE PAGE OF THE COVERED ENTITY IF THE COVERED ENTITY MAINTANS ONE; AND* *NOTIFICATION TO MAJOR STATEWIDE MEDIA.*	The alternative notification options include: Email Posting on website Notifying statewide media	
3(1)(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, 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;*	For this section, PII is defined as a Colorado resident's first name (or first initial) and last name, paired with the following unencrypted information: Social Security Number Student, Military, or Passport ID Number Driver's License Number State Issued ID Card Number Medical Information Health Insurance ID Number Biometric Data	This specific definition of "personal information" (i.e., section 3(1)(g) and applicable subsections) is not included in the Tandem "Incident Response" policy, but it could be included in the **Commentary** section.
3(1)(g)(I)(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*	PII also includes a Colorado resident's username/email address, if a password, security question, or security question answer is also compromised.	
3(1)(g)(I)(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.*	PII also includes a Colorado resident's account number, credit card number, or debit card number, if a security code, access code, or password is also compromised.	

Section	Section Title / *Section Text*	Tandem Opinion	Tandem Mapping
3(1)(g)(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.*	If the data can be accessed publicly from government records or "widely distributed media," it's not PII. The regulation does not define "widely distributed media."	
3(1)(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.*	An event can be defined as a security breach if unencrypted computerized data is acquired without authorization and the acquiring party plans to compromise the security, confidentiality, or integrity of the data. If the covered entity provides data to a third party in the course of business, as long as the data is used for business purposes, that is not considered a security breach.	This specific definition for "security breach" is not included in the Tandem "Incident Response" policy, but it could be included in the **Implementation** section, under the "Initiation" and/or "Assessment" subheadings.
3(1)(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.*	This is the same definition that was used in subsection 2(5) to define "third-party service provider."	N/A
3(2)(a.1)	*A COVERED 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 COVERED 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.*	If a covered entity thinks a security breach occurred, they must conduct an investigation ASAP to determine if the event was actually a security breach (i.e., data was compromised with an intent to misuse the data). If the covered entity determines that the information has been or will be misused, the covered entity must notify the affected Colorado residents ASAP, but no later than 30 days after the "determination that a security breach occurred," as long as the notification does not interfere with law enforcement and the covered entity has made plans or changes to secure the compromised system again.	**Policies** Incident Response See the **Implementation** section, under the "Assessment" subheading. The specific notification requirements are not included in the Tandem "Incident Response" policy, but it could be included in the **Implementation** field, under the "Notification" subheading.
3(2)(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:*	If the covered entity determined a breach occurred, the consumer notice must include (at minimum):	**Policies** Incident Response

Section	Section Title / *Section Text*	Tandem Opinion	Tandem Mapping
3(2)(a.2)(I)	*THE DATE, ESTIMATED DATE, OR ESTIMATED DATE RANGE OF THE SECURITY BREACH;*	The date (or date range) of the breach.	The Tandem "Incident Response" policy language does address the requirements in subsections (I – VI) in generic terms. If you would like to provide additional clarification, you may do so by updating the **Implementation** field, under the "Notification" subheading.
3(2)(a.2)(II)	*A DESCRIPTION OF THE PERSONAL INFORMATION THAT WAS ACQUIRED OR REASONABLY BELIEVED TO HAVE BEEN ACQUIRED AS PART OF THE SECURITY BREACH;*	A description of the data that was compromised by the breach.	
3(2)(a.2)(III)	*INFORMATION THAT THE RESIDENT CAN USE TO CONTACT THE COVERED ENTITY TO INQUIRE ABOUT THE SECURITY BREACH;*	The covered entity's contact information, if the affected parties want to learn more.	
3(2)(a.2)(IV)	*THE TOLL-FREE NUMBERS, ADDRESSES, AND WEBSITES FOR CONSUMER REPORTING AGENCIES;*	Contact information for the consumer reporting agencies: **Equifax** 888-548-7878 P.O. Box 740241 Atlanta, GA 30374 www.equifax.com **Experian** 888-397-3742 P.O. Box 9530 Allen, TX 75013 www.experian.com **TransUnion** 800-916-8800 P.O. Box 6790 Fullerton, CA 92834 www.transunion.com	
3(2)(a.2)(V)	*THE TOLL-FREE NUMBER, ADDRESS, AND WEBSITE FOR THE FEDERAL TRADE COMMISSION; AND*	Contact information for the FTC: **Federal Trade Commission** 877-382-4357 600 Pennsylvania Ave, NW Washington, DC 20580 www.ftc.gov	
3(2)(a.2)(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.*	Educational information to let the affected parties know how they can receive information about fraud alerts and security freezes (e.g., credit freezes).	

Section	Section Title / *Section Text*	Tandem Opinion	Tandem Mapping
3(2)(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:*	If an affected party's username/email address was compromised in conjunction with a password or security question/answer, the notice must also:	This specific kind of security breach is not mentioned in the Tandem "Incident Response" policy, but additional language could be included in the **Implementation** section, under the "Notification" subheading.
3(2)(a.3)(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.*	Include instructions about changing their passwords, security questions, and/or security question answers for both the affected account and any other online accounts that use the same data as that which was compromised.	
3(2)(a.3)(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 (I)(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.*	Not be sent to the email address that was compromised, but be delivered through another form of communication. An alternative method of communication recommended here is displaying a web banner to a user when they're logged in to their account from a frequently used IP address.	
3(2)(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.*	If encrypted PII data was compromised, notice must be provided only if the encryption key (or another form of deciphering the data) was also acquired.	The Tandem "Incident Response" policy does not differentiate between encrypted and unencrypted data, but additional language could be included in the **Commentary** section.

Section	Section Title / *Section Text*	Tandem Opinion	Tandem Mapping
3(2)(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.*	The covered entity cannot charge consumers for this notification service.	N/A
3(2)(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.*	This regulation does not restrict what information may be included in a notice, especially if the covered entity is required to provide additional information by state or federal law.	Any other information you would like to include in your notice can be documented in the Tandem "Incident Response" policy's **Implementation** section, under the "Notification" subheading.
3(2)(b)	*IF A COVERED 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 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 COVERED ENTITY information relevant to the SECURITY breach; except that such cooperation DOES NOT require the disclosure of confidential business information or trade secrets.*	If a third party experiences a security breach that affects the PII entrusted to a covered entity by a Colorado resident, the third party must let the covered entity know ASAP. The third party must cooperate with the covered entity and provide information relevant to the security breach, but the third party does not have to provide information that could disclose business information or trade secrets.	**Vendor Management** Contract Review Template Use the Tandem "Contract Review Template" to ensure breach notification requirements are addressed prior to contracting with a vendor.
3(2)(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 COVERED entity that conducts business 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 COVERED entity that conducts business in Colorado that it is appropriate to send the notice required by this section.*	If law enforcement determines that providing notice could compromise a criminal investigation, they may instruct the covered entity to delay sending the notification. Once law enforcement approves notifying the affected parties, the covered entity must do so ASAP, but no later than 30 days after being given approval.	**Policies** Incident Response The Tandem "Incident Response" policy does address working with law enforcement. However, it does not include the specific timeframe for notice. Additional language could be included in the **Implementation** section, under the "Notification" subheading.

Section	Section Title / *Section Text*	Tandem Opinion	Tandem Mapping
3(2)(d)	*If A COVERED entity is required to notify more than one thousand Colorado residents of a SECURITY breach pursuant to this section, the 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. 1681 a (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)(d) REQUIRES the COVERED entity to provide to the consumer reporting agency the names or other personal information of SECURITY breach notice recipients. This 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.*	If a covered entity must notify more than 1,000 people, the covered entity must also notify all consumer reporting agencies (e.g., Equifax, Experian, and Transunion) ASAP. The notification must include: The date the covered entity plans to contact the affected parties. The approximate number of affected parties. This regulation does not require the covered entity to provide the names of the affected parties or other PII. If the covered entity is subject to GLBA, this subsection does not apply.	**Policies** Incident Response The Tandem "Incident Response" policy does address notifying consumer reporting agencies. However, it does not include the specific requirement of 1,000 people or what the notification must include. Additional language could be included in the **Implementation** section, under the "Notification" subheading.
3(2)(e)	*A WAIVER OF THESE NOTIFICATION RIGHTS OR RESPONSIBILITIES IS VOID AS AGAINST PUBLIC POLICY.*	This rule is in the best interest of the public, so a covered entity cannot obtain a waiver for this required notification	N/A
3(2)(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.*	If the security breach affected more than 500 Colorado residents, the covered entity must notify the Colorado attorney general ASAP, but no later than 30 days after determining a security breach occurred.	This requirement is specific to Colorado organizations, but could be included in the Tandem "Incident Response" policy in the **Implementation** section, under the "Notification" subheading.
3(2)(f)(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.*	The Colorado attorney general will designate a person to receive these reports and will publish that person's contact information on the attorney general's website: https://coag.gov	N/A

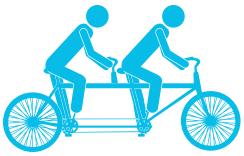
Section	Section Title / *Section Text*	Tandem Opinion	Tandem Mapping
3(2)(g)	*THE BREACH OF ENCRYPTED OR OTHERWISE SECURED PERSONAL INFORMATION MUST BE DISCLOSED IN ACCORDANCE WITH THIS SECTION IF THE CONFIDENTIAL PROCESS, ENCRYPTION KEY, OR OTHER MEANS TO DECIPHER THE SECURED INFORMATION WAS ALSO ACQUIRED OR WAS REASONABLY BELIEVED TO HAVE BEEN ACQUIRED IN THE SECURITY BREACH.*	If encrypted PII data was compromised, notice must be provided only if the encryption key (or another form of deciphering the data) was also acquired. This is restating Section 3(2)(a.4).	The Tandem "Incident Response" policy does not differentiate between encrypted and unencrypted data, but additional language could be included in the **Commentary** section.
3(3)	*Procedures deemed in compliance with notice requirements.*		N/A
3(3)(a)	*PURSUANT TO this section, 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 IS in compliance with the notice requirements of this section if the COVERED 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)(f) OF THIS SECTION.*	A covered entity is in compliance with this regulation if they have an information security policy that outlines specific notification requirements that align with the requirements of this regulation. If the breach affects more than 500 Colorado residents, notification still must be provided to the Colorado attorney general.	These requirements are specific to Colorado organizations, but could be included in the Tandem "Incident Response" policy in the **Implementation** section, under the "Notification" subheading.
3(3)(b)	*A COVERED 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)(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.*	A covered entity is in compliance with this regulation if they are required to maintain security breach procedures by state or federal law. If the breach affects more than 500 Colorado residents, notification still must be provided to the Colorado attorney general. If there are conflicting timeframes for notification of a security breach, the covered entity must follow the shortest timeframe.	
3(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 A COVERED entity subject to this section from compliance with all other applicable provisions of law.*	The Colorado attorney general reserves the right to pursue legal action if a covered entity violates this regulation. The Colorado attorney general may also pursue legal action to provide regulatory relief or to assist with recovery following a security breach. However, this does not excuse covered entities from complying with the regulation.	N/A

Section	Section Title / *Section Text*	Tandem Opinion	Tandem Mapping
3(5)	*Attorney general criminal authority. UPON RECEIPT OFNOTICE 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 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.*	When the Colorado attorney general receives notice of a security breach from a covered entity, the Colorado attorney general may criminally prosecute those who breach the security of a covered entity, as long as they have a request from the Colorado governor or permission of a district attorney to do so.	N/A
4	Security Breaches and Personal Information	Section 4 applies to Colorado governmental entities (see section 24-73-101(4)(a) for a definition of a "governmental entity"). In essence, the language is just a restating of Sections 1 – 3, with minor grammatical, terminology, and subsection changes.	N/A
5	Effective date. This act takes effect September 1, 2018.	The act goes into effect on September 1, 2018.	**Compliance Management** Use the Tandem Compliance Management module to document and create reminders about upcoming compliance events.
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.	The General Assembly of the State of Colorado created this law because it is necessary to protect the peace, health, and safety of Colorado residents.	N/A

Tandem™

What is Tandem?

It's all in the name. Tandem is an online solution designed by CoNetrix to help ease the burden of regulatory compliance. We have done the research up front so you can be compliant with information security regulations in much less time. Don't struggle with complex or technical language and spend time tracking updates through multiple documents. Let Tandem work with you to streamline your efforts and guide your compliance operations.



Who can benefit from using Tandem?

Tandem was built specifically for financial institutions to help increase security, stay in compliance, and lower overhead costs.

Over 16,000 active users, representing more than 1000 financial institutions across the U.S., are using one or more modules in Tandem. Ask us for a reference and view a demo to see how Tandem can work for you.

Used by more than
1000
financial institutions

Tandem Features

- An online framework created and updated by security and compliance experts
- Professional documents downloadable in Microsoft Word and/ or Adobe PDF formats
- One simple license fee with free automatic updates during subscription term
- Easy to use, integrated modules
- Dashboards & email reminders
- Unlimited storage
- Multi-user access & access roles
- No software installation or equipment costs
- The ability to manage several companies' programs with one login (requires a subscription for each company)

Tandem is safe to use online!

Access the web-based application anywhere you have an Internet connection using a secure login to our SOC examined data center. Set up password expiration and multi-factor login authentication for additional security measures.

Tandem

Risk Assessment – Develop your Information Security Risk Assessment and individual risk assessments for your critical assets. Tandem helps you identify reasonably foreseeable threats, assign risk levels, and define controls.

Business Continuity Planning – Be prepared to address adverse events such as natural disasters, biological pandemics, technological failures, human error, and terrorism. Define and manage business process recovery through the formal Business Impact Analysis (BIA) process, and take advantage of template checklists and MMS emergency notification.

Information Security Policies – Jumpstart your custom security plan with over 50 pre-populated polices, and the ability to create your own policies, manage policy implementation, identify verification, and build an acceptable use policy.

Internet Banking Security Program – Create risk assessments for different types of online customer accounts (e.g. corporate and retail), identify risk levels, and assign layered security controls to mitigate risk. Use the customizable security awareness material for educating your customers.

Compliance Management – Easily identify, schedule and track important compliance projects and deadlines, such as reporting, audits, training, and operations. Free and Pro versions available.

Cybersecurity – Complete the FFIEC Cybersecurity Self-Assessment Tool in an electronic interface. Report results to the board, track progress, and compare results with similar institutions (optional).

Vendor Management – Manage third party vendors and assess risk. Tandem streamlines the process of collecting, reviewing, and documenting pertinent information about your service providers.

Identity Theft Prevention Program – Develop and manage your Identity Theft Prevention Program document per the FACT Act, and use the online employee training customized for your red flags.

Social Media Management – Manage all of your social media profiles with one login. Create a custom review process for authoring, approving, and scheduling posts. Post to all accounts from one place, keep track of employee access to social media accounts, and conduct regular social media risk assessments.

Audit Management – Keep track of various audits (e.g., IT, Compliance, Safety and Soundness, Exam), assign responsibility, and manage findings. View trends, risks, and costs of findings and assign tasks for response. Pro version available to conduct audits and manage work programs.

Phishing – Safely create phishing scenarios and tests. Use results to gauge security awareness among your employees.

Support

- Ask questions and get support from our responsive support team, which is backed by an entire department of IT security auditors.
- Jump in with Knowledge Base, help text, recorded demos, and workshop webinars.
- Attend our annual User Group to learn more about Tandem and see how other institutions are using it.

KEYS CONFERENCE

Request a quote

conetrix.com/tandem

Need more assistance? Ask us about our consulting services through CoNetrix Security. Our security experts hold numerous security certifications and understand the real-life challenges facing the financial industry.