A BILL FOR AN ACT

CONCERNING THE REQUIREMENTS OF A STATE ENTITY WHEN THE STATE ENTITY EXPERIENCES AN INCIDENT THAT COULD COMPROMISE THE SECURITY OF SENSITIVE PERSONAL INFORMATION HELD BY THE STATE ENTITY.

Bill Summary

(Note: This summary applies to this bill as introduced and does not reflect any amendments that may be subsequently adopted. If this bill passes third reading in the house of introduction, a bill summary that applies to the reengrossed version of this bill will be available at http://www.leg.state.co.us/billsummaries.)

If a state entity experiences an accidental or deliberate event that results in or constitutes a threat of the unauthorized access, loss,
disclosure, modification, disruption, or destruction of personal or financial identifying information (security incident) and determines that the security incident occurred due to an error of the state entity or any employee of the state entity or due to a lack of security protecting the personal or financial identifying information held by the state entity, the state entity must notify any person who may be impacted by the security incident of the following:

- That a security incident occurred and that the security of the person's personal or financial identifying information held by the state entity may have been compromised;
- That the person is entitled to have the state entity pay for identity theft protection services on the person's behalf for a limited time after the security incident occurred; and
- That the person may contact the state entity for further information. The state entity shall include relevant contact information for the state entity in the notification.

The bill requires the chief information officer of the office of information technology to promulgate rules necessary for the implementation of these requirements. The rules promulgated by the chief information officer apply to each executive branch department of the state and may be adopted by any state entity that is not an executive branch department. A state entity that is not an executive branch department and that does not adopt the rules of the chief information officer is required to promulgate its own rules or adopt its own policies as necessary for the implementation of these requirements.

---

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

**SECTION 1.** In Colorado Revised Statutes, add article 10.5 to title 24 as follows:

**ARTICLE 10.5**

**Compromised Personal or Financial Identifying Information**

**24-10.5-101. Definitions.** As used in this article, unless the context otherwise requires:

1. "Financial identifying information" means any of the following that can be used, alone or in conjunction with any other information, to obtain cash, credit, property, services, or any other thing of value or to make a financial payment:
(a) A PERSONAL IDENTIFICATION NUMBER, CREDIT CARD NUMBER, BANKING CARD NUMBER, CHECKING ACCOUNT NUMBER, DEBIT CARD NUMBER, ELECTRONIC FUND TRANSFER CARD NUMBER, GUARANTEED CHECK CARD NUMBER, OR ROUTING NUMBER; OR

(b) A NUMBER REPRESENTING A FINANCIAL ACCOUNT OR A NUMBER AFFECTING THE FINANCIAL INTEREST, STANDING, OR OBLIGATION OF OR TO THE ACCOUNT HOLDER.

(2) "IDENTITY THEFT PROTECTION SERVICE" MEANS AN ORGANIZATION THAT PROTECTS ITS CUSTOMERS AGAINST CREDIT FRAUD AND IDENTITY THEFT, ALERTS CUSTOMERS WHEN IT DETECTS THE UNAUTHORIZED USE OF PERSONAL IDENTIFYING INFORMATION OR FINANCIAL IDENTIFYING INFORMATION, AND HELPS CUSTOMERS RECOVER FROM IDENTITY THEFT.

(3) "PERSONAL IDENTIFYING INFORMATION" MEANS INFORMATION THAT MAY BE USED, ALONE OR IN CONJUNCTION WITH ANY OTHER INFORMATION, TO IDENTIFY A SPECIFIC INDIVIDUAL, INCLUDING BUT NOT LIMITED TO A NAME; DATE OF BIRTH; SOCIAL SECURITY NUMBER; PASSWORD; PASS CODE; AN OFFICIAL, GOVERNMENT-ISSUED DRIVER'S LICENSE OR IDENTIFICATION CARD NUMBER; GOVERNMENT PASSPORT NUMBER; BIOMETRIC DATA; OR EMPLOYER, STUDENT, OR MILITARY IDENTIFICATION NUMBER.

(4) "SECURITY INCIDENT" MEANS AN ACCIDENTAL OR DELIBERATE EVENT THAT RESULTS IN OR CONSTITUTES A THREAT OF THE UNAUTHORIZED ACCESS, LOSS, DISCLOSURE, MODIFICATION, DISRUPTION, OR DESTRUCTION OF PERSONAL IDENTIFYING INFORMATION OR FINANCIAL IDENTIFYING INFORMATION.

(5) "STATE ENTITY" MEANS THE STATE OF COLORADO AND ANY
BOARD, COMMISSION, DEPARTMENT, CORPORATION, INSTRUMENTALITY, OR AGENCY THEREOF.

24-10.5-102. State compromise of personal or financial identifying information. (1) If a state entity experiences a security incident and determines that the security incident occurred due to an error of the state entity or any employee of the state entity or due to a lack of reasonable security protecting the personal identifying information or financial identifying information held by the state entity, the state entity must notify any person who may be impacted by the security incident of the following:

(a) That a security incident occurred, the date and nature of the security incident, the nature of the information that was the target of the security incident, and that the security of the person's personal identifying information or financial identifying information held by the state entity may have been compromised;

(b) That a person whose personal identifying information or financial identifying information may have been compromised is entitled to have the state entity pay for identity theft protection services on the person's behalf for one year after the security incident occurred pursuant to subsection (2) of this section; and

(c) That the person may contact the state entity for further information or if the person has questions. The notification must include the contact information for the state entity, including any special telephone numbers, web sites, or
ADDRESSES ESTABLISHED FOR PEOPLE WHO ARE INQUIRING ABOUT THE
SECURITY INCIDENT.

(2) A STATE ENTITY THAT DETERMINES THAT A SECURITY INCIDENT
OCCURRED DUE TO AN ERROR OF THE STATE ENTITY OR ANY EMPLOYEE OF
THE STATE ENTITY OR DUE TO A LACK OF SECURITY PROTECTING PERSONAL
IDENTIFYING INFORMATION OR FINANCIAL IDENTIFYING INFORMATION
SHALL CONTRACT WITH AN IDENTITY THEFT PROTECTION SERVICE TO
PROVIDE IDENTITY THEFT PROTECTION SERVICES TO ANY PERSON WHOSE
PERSONAL IDENTIFYING INFORMATION OR FINANCIAL IDENTIFYING
INFORMATION MAY HAVE BEEN COMPROMISED DUE TO THE SECURITY
INCIDENT. THE STATE ENTITY SHALL PROVIDE THE PROTECTION FOR ONE
YEAR AFTER THE DATE OF THE SECURITY INCIDENT.

24-10.5-103. Rules. (1) The chief information officer of the
office of information technology created pursuant to section
24-37.5-103 shall promulgate rules necessary for the
implementation of this article in accordance with article 4 of
this title. The rules promulgated by the chief information
officer apply to each executive branch department of the state.

(2) Any state entity that is not an executive branch
department must either promulgate rules or procedures
necessary for the implementation of this article or determine,
as a matter of policy, to follow the rules promulgated pursuant
to subsection (1) of this section. Any state entity that is not an
executive branch department and that promulgates rules or
procedures pursuant to this subsection (2) must promulgate such
rules or procedures in accordance with article 4 of this title.

SECTION 2. Act subject to petition - effective date. This act
takes effect at 12:01 a.m. on the day following the expiration of the ninety-day period after final adjournment of the general assembly (August 6, 2014, if adjournment sine die is on May 7, 2014); except that, if a referendum petition is filed pursuant to section 1 (3) of article V of the state constitution against this act or an item, section, or part of this act within such period, then the act, item, section, or part will not take effect unless approved by the people at the general election to be held in November 2014 and, in such case, will take effect on the date of the official declaration of the vote thereon by the governor.