First Regular Session
Sixty-eighth General Assembly
STATE OF COLORADO

INTRODUCED

LLS NO. 11-0510.01 Julie Pelegrin **HOUSE BILL 11-1225**

HOUSE SPONSORSHIP

Pabon, Court, Duran, Hullinghorst, McCann, Miklosi

SENATE SPONSORSHIP

(None),

House Committees
Judiciary

Senate Committees

A BILL FOR AN ACT

CONCERNING LEGAL ACTIONS ADDRESSING BREACHES OF DATA SECURITY THAT INVOLVE PERSONAL INFORMATION.

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.)

Under the bill, an individual or commercial entity is not liable for civil damages resulting from a breach of data security made possible by acts or omissions made in good faith, so long as the acts or omissions were not grossly negligent or willful and wanton, if:

! The breach of data security is committed by a third party

without authorized access or by an employee or agent operating outside the scope of employment; and

! The individual or commercial entity that holds the personal information has been audited by a qualified information technology auditor and found to be implementing best practices and meeting information technology security standards.

If the individual or commercial entity has not been audited, the individual or commercial entity may raise a rebuttable presumption at trial that it was not negligent in making possible the breach of data security if the individual or commercial entity demonstrates that it was operating in accordance with the best practices and standards.

The state's chief information officer will identify an entity that will identify national organizations that certify persons with the expertise to act as data security auditors, and the entity will identify the best practices and data security standards that an individual or commercial entity should follow.

A person who is the victim of a computer crime or breach of data security may petition the court for a subpoena to require the individual or commercial entity whose data system was breached to provide any information it may have concerning the perpetrators of the crime or breach. If the individual or commercial entity provides the information, it will be immune for the direct use of the information against the individual or commercial entity in a civil suit brought by a person other than the victim, so long as the individual or commercial entity or its employees or agents were not grossly negligent and did not act willfully or wantonly.

The bill creates a new class 1 misdemeanor computer crime if a person receives stolen computer-related property, including data, and intends to use it in a way that deprives the lawful owner of its use, to commit another crime with it, or to use it to damage the lawful owner's reputation.

The bill makes conforming amendments.

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

SECTION 1. Article 21 of title 13, Colorado Revised Statutes, is amended BY THE ADDITION OF A NEW PART to read:

PART 12

LIABILITY FOR DATA SECURITY BREACHES

INVOLVING PERSONAL INFORMATION

13-21-1201. Definitions. AS USED IN THIS PART 12, UNLESS THE CONTEXT OTHERWISE REQUIRES:

(1) "AUTHORIZATION" SHALL HAVE THE SAME MEANING AS PROVIDED IN SECTION 18-5.5-101 (1), C.R.S.

(2) "BREACH OF DATA SECURITY" SHALL HAVE THE SAME MEANING AS THE PHRASE "BREACH OF THE SECURITY OF A SYSTEM" AS PROVIDED IN SECTION 6-1-716 (1) (a), C.R.S.

(3) "COMPUTER" SHALL HAVE THE SAME MEANING AS PROVIDED IN SECTION 18-5.5-101 (2), C.R.S.

(4) "COMPUTER CRIME" MEANS IDENTITY THEFT AS DESCRIBED IN SECTION 18-5-902, C.R.S., COMMITTED WHOLLY OR IN PART BY USING A COMPUTER, COMPUTER NETWORK, OR COMPUTER SYSTEM, OR COMPUTER CRIME AS DESCRIBED IN SECTION 18-5.5-102, C.R.S.

(5) "COMPUTER NETWORK" SHALL HAVE THE SAME MEANING AS PROVIDED IN SECTION 18-5.5-101 (3), C.R.S.

(6) "COMPUTER SYSTEM" SHALL HAVE THE SAME MEANING AS PROVIDED IN SECTION 18-5.5-101 (6), C.R.S.

(7) "EXCEED AUTHORIZED ACCESS" SHALL HAVE THE SAME MEANING AS PROVIDED IN SECTION 18-5.5-101 (6.7), C.R.S.

(8) (a) "PERSONAL INFORMATION" MEANS:

(I) 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; OR

(II) 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; A DATE OF BIRTH; A SOCIAL SECURITY NUMBER; A PASSWORD; A PASS CODE; AN OFFICIAL, GOVERNMENT-ISSUED DRIVER'S LICENSE OR IDENTIFICATION CARD NUMBER; A GOVERNMENT PASSPORT NUMBER; BIOMETRIC DATA; OR AN EMPLOYER, STUDENT, OR MILITARY IDENTIFICATION NUMBER.

(b) "PERSONAL INFORMATION" DOES NOT INCLUDE PUBLICLY AVAILABLE INFORMATION THAT IS LAWFULLY MADE AVAILABLE TO THE GENERAL PUBLIC BY THE PERSON TO WHOM THE INFORMATION PERTAINS OR WHOSE FINANCIAL ACCOUNTS IT CONCERNS OR FROM FEDERAL, STATE, OR LOCAL GOVERNMENT RECORDS OR WIDELY DISTRIBUTED MEDIA.

(9) "QUALIFIED INFORMATION TECHNOLOGY SECURITY AUDITOR OR ASSESSOR" MEANS A PERSON WHO:

(a) IS CERTIFIED BY ONE OR MORE NATIONALLY RECOGNIZED ORGANIZATIONS OR ASSOCIATIONS IN THE INFORMATION TECHNOLOGY INDUSTRY AS HAVING EXPERTISE IN DATA SECURITY; AND

(b) HAS NOT BEEN CONVICTED OF OR PLED GUILTY OR NOLO CONTENDERE TO A FELONY OR MISDEMEANOR OFFENSE INVOLVING MORAL TURPITUDE, INCLUDING BUT NOT LIMITED TO OFFENSES INVOLVING FRAUD AS DESCRIBED IN ARTICLE 5 OF TITLE 18, C.R.S., COMPUTER CRIMES AS DESCRIBED IN ARTICLE 5.5 OF TITLE 18, C.R.S., FAILURE TO PAY CHILD SUPPORT, OR ANY COMPARABLE OFFENSE UNDER THE LAWS OF ANY OTHER

STATE, THE UNITED STATES, OR A FOREIGN COUNTRY.

13-21-1202. Immunity from liability for breach of data security - audit. (1) AN INDIVIDUAL OR COMMERCIAL ENTITY THAT OPERATES IN COLORADO AND THAT OWNS, LICENSES, OR MAINTAINS COMPUTERIZED DATA THAT INCLUDES PERSONAL INFORMATION SHALL NOT BE LIABLE FOR CIVIL DAMAGES RESULTING FROM A BREACH OF DATA SECURITY MADE POSSIBLE BY ACTS OR OMISSIONS MADE IN GOOD FAITH BY THE INDIVIDUAL OR COMMERCIAL ENTITY OR ITS AGENTS OR EMPLOYEES, SO LONG AS THE ACTS OR OMISSIONS WERE NOT GROSSLY NEGLIGENT OR WILLFUL AND WANTON, IF:

(a) THE BREACH OF DATA SECURITY IS COMMITTED BY A THIRD PARTY WITHOUT AUTHORIZATION OR WHOSE ACTIONS EXCEED AUTHORIZED ACCESS TO THE INDIVIDUAL'S OR COMMERCIAL ENTITY'S COMPUTER, COMPUTER NETWORK, OR COMPUTER SYSTEM, OR BY AN EMPLOYEE OR AGENT OF THE INDIVIDUAL OR COMMERCIAL ENTITY ACTING OUTSIDE THE SCOPE OF HIS OR HER EMPLOYMENT IN CAUSING THE BREACH; AND

(b) PRIOR TO THE BREACH OF DATA SECURITY, THE INDIVIDUAL OR COMMERCIAL ENTITY IS CERTIFIED BY A QUALIFIED INFORMATION TECHNOLOGY SECURITY AUDITOR OR ASSESSOR AS IMPLEMENTING BEST PRACTICES IN THE AREA OF DATA SECURITY AND MEETING INFORMATION TECHNOLOGY SECURITY STANDARDS, AS IDENTIFIED BY THE ENTITY IDENTIFIED PURSUANT TO SECTION 13-21-1204.

(2) AN INDIVIDUAL OR A COMMERCIAL ENTITY THAT CLAIMS IMMUNITY PURSUANT TO THIS SECTION IS RESPONSIBLE FOR VERIFYING THAT THE PERSON WHO AUDITS OR ASSESSES THE INDIVIDUAL'S OR COMMERCIAL ENTITY'S IMPLEMENTATION OF BEST PRACTICES AND

COMPLIANCE WITH TECHNOLOGY SECURITY STANDARDS IS A QUALIFIED INFORMATION TECHNOLOGY SECURITY AUDITOR OR ASSESSOR.

13-21-1203. Breach of data security - rebuttable presumption. AN INDIVIDUAL OR A COMMERCIAL ENTITY THAT IS NOT IMMUNE FROM CIVIL LIABILITY PURSUANT TO SECTION 13-21-1202 FOR A BREACH OF DATA SECURITY MAY ESTABLISH A REBUTTABLE PRESUMPTION THAT THE INDIVIDUAL OR COMMERCIAL ENTITY, AND THE EMPLOYEES OR AGENTS OF THE INDIVIDUAL OR COMMERCIAL ENTITY, WERE NOT NEGLIGENT IN MAKING POSSIBLE THE BREACH OF DATA SECURITY BY INTRODUCING EVIDENCE THAT THE INDIVIDUAL OR COMMERCIAL ENTITY IMPLEMENTED THE BEST PRACTICES AND WAS IN COMPLIANCE WITH THE TECHNOLOGY SECURITY STANDARDS IDENTIFIED BY THE ENTITY IDENTIFIED PURSUANT TO SECTION 13-21-1204.

13-21-1204. Office of information technology - selection of entity - certifications - best practices and standards. (1) THE CHIEF INFORMATION OFFICER APPOINTED PURSUANT TO SECTION 24-37.5-103, C.R.S., SHALL IDENTIFY AN ENTITY IN THIS STATE, REFERRED TO IN THIS SECTION AS THE "ENTITY", TO CARRY OUT THE DUTIES SPECIFIED IN THIS SECTION. THE ENTITY IDENTIFIED BY THE CHIEF INFORMATION OFFICER SHALL HAVE EXPERTISE IN THE LAWS AND PRACTICES SURROUNDING DATA SECURITY AND PRIVACY. THE CHIEF INFORMATION OFFICER SHALL PUBLICIZE THE NAME AND INTERNET ADDRESS OF THE ENTITY ON THE STATEWIDE INTERNET PORTAL ESTABLISHED PURSUANT TO ARTICLE 37.7 OF THIS TITLE.

(2) THE ENTITY SHALL PROVIDE ON ITS WEB SITE FOR PUBLIC ACCESS A LIST OF THE NATIONALLY RECOGNIZED ORGANIZATIONS OR ASSOCIATIONS IN THE INFORMATION TECHNOLOGY INDUSTRY THAT

CERTIFY A PERSON'S QUALIFICATIONS IN DATA SECURITY SYSTEMS. THE ENTITY SHALL REVIEW AND UPDATE THE LIST AT LEAST ANNUALLY.

(3) THE ENTITY SHALL IDENTIFY THE BEST PRACTICES THAT AN INDIVIDUAL OR A COMMERCIAL ENTITY MAY IMPLEMENT AND INFORMATION TECHNOLOGY SECURITY STANDARDS WITH WHICH AN INDIVIDUAL OR A COMMERCIAL ENTITY MAY COMPLY IF THE INDIVIDUAL OR COMMERCIAL ENTITY OWNS, LICENSES, OR MAINTAINS COMPUTERIZED DATA THAT INCLUDES PERSONAL INFORMATION. THE ENTITY SHALL POST THE LIST OF BEST PRACTICES AND INFORMATION TECHNOLOGY SECURITY STANDARDS ON ITS WEB SITE FOR PUBLIC ACCESS AND SHALL REVIEW AND UPDATE THE BEST PRACTICES AND STANDARDS AT LEAST ANNUALLY.

13-21-1205. Consumers - investigation of breach of data security - authority to issue subpoenas. (1) A PERSON WHO IS THE VICTIM OF A COMPUTER CRIME OR WHOSE PERSONAL INFORMATION IS LOST, STOLEN, OR COMPROMISED AS A RESULT OF A BREACH OF DATA SECURITY MAY PETITION THE COURT FOR THE ISSUANCE OF A SUBPOENA COMMANDING AN INDIVIDUAL OR COMMERCIAL ENTITY THAT WAS THE SUBJECT OF A DATA SECURITY BREACH OR ANY THIRD PARTY TO PRODUCE ANY INFORMATION IN ITS POSSESSION, CUSTODY, OR CONTROL REGARDING THE COMPUTER CRIME OR THE UNAUTHORIZED ACCESS TO THE PETITIONER'S PERSONAL INFORMATION TO FACILITATE THE DETECTION, APPREHENSION, AND PROSECUTION OF ANY PERPETRATOR OF THE COMPUTER CRIME OR BREACH OF DATA SECURITY.

(2) A PERSON WHO SEEKS A SUBPOENA PURSUANT TO THIS SECTION SHALL FILE WITH A COURT OF COMPETENT JURISDICTION IN THE JUDICIAL DISTRICT IN WHICH THE INDIVIDUAL OR COMMERCIAL ENTITY IS LOCATED OR DOING BUSINESS, A VERIFIED PETITION EX PARTE ALLEGING UNDER

OATH THE OCCURRENCE OF THE COMPUTER CRIME OR BREACH OF DATA SECURITY AND THE LOSS OF PERSONAL INFORMATION. THE COURT SHALL ISSUE THE SUBPOENA UPON A FINDING THAT THE PETITION SETS FORTH A SHOWING OF PROBABLE CAUSE TO BELIEVE THAT THE PETITIONER HAS BEEN THE VICTIM OF A COMPUTER CRIME OR BREACH OF DATA SECURITY AND THAT THE INDIVIDUAL OR COMMERCIAL ENTITY FOR WHOM THE SUBPOENA IS SOUGHT IS IN POSSESSION, CUSTODY, OR CONTROL OF EVIDENCE LIKELY TO FACILITATE THE DETECTION, APPREHENSION, AND PROSECUTION OF ANY PERPETRATOR.

(3) A PETITION FILED PURSUANT TO THIS SECTION MAY BE FILED UNDER SEAL IF A PUBLIC FILING WOULD SUBJECT THE PETITIONER OR ANY INNOCENT THIRD PARTY TO FURTHER RISK OF HARM OR WOULD RISK HINDERING THE DETECTION, APPREHENSION, OR PROSECUTION OF ANY PERPETRATOR.

(4) THE COURT MAY CONSIDER A MOTION TO QUASH A SUBPOENA ISSUED PURSUANT TO THIS SECTION, TO LIMIT PRODUCTION SOUGHT BY THE SUBPOENA, OR TO ISSUE PROTECTIVE ORDERS TO PROTECT THE RIGHTS OF THIRD PARTIES, OTHER THAN A PERPETRATOR.

(5) AN INDIVIDUAL OR COMMERCIAL ENTITY, OTHER THAN A PERPETRATOR, THAT PRODUCES INFORMATION IN RESPONSE TO A SUBPOENA AUTHORIZED AND ISSUED PURSUANT TO THIS SECTION SHALL BE IMMUNE FROM THE DIRECT USE OF SAID INFORMATION IN ANY CIVIL ACTION BROUGHT BY A PARTY OTHER THAN THE VICTIM OF THE COMPUTER CRIME OR BREACH OF DATA SECURITY AGAINST THE INDIVIDUAL OR COMMERCIAL ENTITY FOR ACTS OR OMISSIONS MADE IN GOOD FAITH BY THE INDIVIDUAL OR COMMERCIAL ENTITY OR ITS AGENTS OR EMPLOYEES, SO LONG AS THE ACTS OR OMISSIONS WERE NOT GROSSLY NEGLIGENT OR

WILLFUL AND WANTON.

SECTION 2. 18-5.5-102 (1) (g), Colorado Revised Statutes, is amended, and the said 18-5.5-102 (1) is further amended BY THE ADDITION OF A NEW PARAGRAPH, to read:

18-5.5-102. Computer crime. (1) A person commits computer crime if the person knowingly:

(g) Uses or causes to be used a software application that runs automated tasks over the internet to access a computer, computer network, or computer system, or any part thereof, that circumvents or disables any electronic queues, waiting periods, or other technological measure intended by the seller to limit the number of event tickets that may be purchased by any single person in an on-line event ticket sale as defined in section 6-1-720, C.R.S.; OR

(h) RECEIVES, RETAINS, POSSESSES, OR DISPOSES OF PROPERTY KNOWING OR BELIEVING THAT THE PROPERTY HAS BEEN STOLEN OR OBTAINED, BY MEANS OF ACCESS THAT IS NOT AUTHORIZED OR THAT EXCEEDS AUTHORIZED ACCESS, FROM A COMPUTER, COMPUTER NETWORK, OR COMPUTER SYSTEM, AND THE PERSON INTENDS TO:

(I) USE OR DISPOSE OF THE PROPERTY IN A WAY THAT DEPRIVES THE LAWFUL OWNER OR ANY LAWFUL LICENSEE OF THE PROPERTY OF ITS USE OR BENEFIT;

(II) USE OR DISPOSE OF THE PROPERTY IN ORDER TO COMMIT, ATTEMPT, OR SOLICIT THE COMMISSION OF ANY OTHER OFFENSE IN VIOLATION OF THIS TITLE OR THE LAWS OF ANY OTHER STATE OR OF THE UNITED STATES; OR

(III) DAMAGE THE REPUTATION OF THE LAWFUL OWNER OR ANY LAWFUL LICENSEE OF THE PROPERTY.

SECTION 3. 18-5.5-102 (3) (a), Colorado Revised Statutes, is amended, and the said 18-5.5-102 (3) is further amended BY THE ADDITION OF A NEW PARAGRAPH, to read:

18-5.5-102. Computer crime. (3) (a) Except as provided in paragraphs ~~(b) and (c)~~ (b), (c), AND (e) of this subsection (3), if the loss, damage, value of services, or thing of value taken, or cost of restoration or repair caused by a violation of this section is less than five hundred dollars, computer crime is a class 2 misdemeanor; if five hundred dollars or more but less than one thousand dollars, computer crime is a class 1 misdemeanor; if one thousand dollars or more but less than twenty thousand dollars, computer crime is a class 4 felony; if twenty thousand dollars or more, computer crime is a class 3 felony.

(e) COMPUTER CRIME COMMITTED IN VIOLATION OF PARAGRAPH (h) OF SUBSECTION (1) OF THIS SECTION IS A CLASS 1 MISDEMEANOR.

SECTION 4. 24-37.5-106 (1) (r) and (1) (s), Colorado Revised Statutes, are amended, and the said 24-37.5-106 (1) is further amended BY THE ADDITION OF A NEW PARAGRAPH, to read:

24-37.5-106. Chief information officer - duties and responsibilities - broadband inventory fund created. (1) The chief information officer shall:

(r) In consultation with the government data advisory board created in section 24-37.5-703, adopt rules and procedures for responding to data requests submitted by an entity outside of state government; ~~and~~

(s) In consultation with the government data advisory board created in section 24-37.5-703, adopt a schedule of fees that the office may charge to state agencies to supervise and administer interdepartmental and external data requests, that a state agency may

charge another state agency in responding to an interdepartmental data request, and that a state agency may charge to respond to a data request submitted by an entity outside of state government. The chief information officer shall ensure that the amount of the fees does not exceed the direct and indirect costs incurred by the office or by the state agency that is responding to a data request; AND

(t) IDENTIFY AN ENTITY AS DESCRIBED IN SECTION 13-21-1204, C.R.S., TO PERFORM THE DUTIES RELATED TO DATA SECURITY SPECIFIED IN SAID SECTION AND TO POST THE NAME AND INTERNET ADDRESS OF THE ENTITY ON THE STATEWIDE DATA PORTAL.

SECTION 5. Effective date - applicability. This act shall take effect July 1, 2011, and sections 2 and 3 of this act shall apply to offenses committed on or after said date.

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.