HB 18-1128

Legislative Council Staff
Nonpartisan Services for Colorado's Legislature

FINAL FISCAL NOTE

Drafting Number:	LLS 18-0270	**Date:**	June 26, 2018
Prime Sponsors:	Rep. Wist; Bridges Sen. Lambert; Court	**Bill Status:**	Signed into Law
		Fiscal Analyst:	Chris Creighton | 303-866-5834 Chris.Creighton@state.co.us

Bill Topic: PROTECTIONS FOR CONSUMER DATA PRIVACY

Summary of Fiscal Impact:

- ☒ State Revenue *(minimal)*
- ☒ State Expenditure
- ☐ State Transfer
- ☒ TABOR Refund
- ☒ Local Government
- ☐ Statutory Public Entity

This bill makes changes related to the handling of personally identifying information and required procedures and notifications if this information is breached. This bill increases state and local government revenue, expenditures, and workload. These impacts continue in future years.

Appropriation Summary: No appropriation is required.

Fiscal Note Status: This fiscal note reflects the enacted bill.

Table 1
State Fiscal Impacts Under HB 18-1128

			FY 2018-19	FY 2019-20
Revenue	General Fund and Cash Funds		less than $5,000	less than $5,000
Expenditures			-	-
Transfers			-	-
TABOR Refund		General Fund	less than $5,000	less than $5,000

Summary of Legislation

This bill adds definitions and makes changes related to the handling of personally identifying information and required procedures and notifications if this information is breached.

Record disposal policy. This bill requires each governmental and covered entity that owns, maintains, or licenses personal identifying information in the state that maintains paper or electronic documents that contain personally identifying information to develop a written policy for the disposal of such records. When these records no longer need to be stored, unless otherwise required by state or federal law, this policy must require the destruction of these records in a manner that ensures the personally identifying information is unreadable.

Governmental entities that are regulated by state or federal law and maintain disposal procedures in accordance with any applicable state or federal law, rules, procedures, or guidelines are in compliance with the disposal requirements of this bill.

Security procedures. A covered entity that maintains, owns, or licenses personally identifying information or uses a third party as a service provider must implement and maintain reasonable security procedures and practices that are appropriate to the information stored and size and nature of the entity to protect personally identifying information from unauthorized access.

Governmental entities must also maintain reasonable security measures to protect personal identifying information from unauthorized access, use, modification, disclosure, or destruction. Governmental entities that use third-party service providers must require the providers to implement reasonable security measures. Governmental entities are in compliance with this bill if they maintain security measurers in accordance with state and federal law, rules, procedures, or guidelines regulating them.

Breach notification. This bill adds definitions related to the disclosure of a security breach and requires a covered or governmental entity to give written notice to affected Colorado residents upon discovery of a security breach as soon as possible, but no later than 30 days from the date of the breach. Prior to providing this notice and consistent with current law for individual and commercial entities, governmental entities must conduct a prompt investigation when it is determined that a information breach has occurred. Notice is not required if the investigation determines misuse of the information has or is not likely to occur.

This bill describes what information must be included in such a notification including, but not limited to, the date of the breach, a description of the information accessed in the breach, and information for contacting credit agencies and the Federal Trade Commission. Covered and governmental entities are prohibited from charging for the cost of providing this notice. Electronic breach notifications may be provided in certain situations, such as when individuals whose information was breached and notification is needed promptly to change a password or log-in credentials. Consistent with current law for individual and commercial entities, covered and governmental entities must notify all consumer reporting agencies for any breach affecting more than 1,000 Colorado residents.

Breach reporting to the Attorney General. A covered or governmental entity is required to provide notice to the Colorado Attorney General within 30 days of any breach if the breach is believed to impact 500 or more Colorado residents. The Attorney General is authorized to investigate and prosecute the breach upon receipt of this notice.

Background

As defined under current law, in the Colorado Consumer Protection Act, a person is an individual, corporation, business trust, estate, trust, partnership, or unincorporated association. Under current law, a person breaching computerized data can be charged with a misdemeanor or felony depending on the nature of the crime.

For FY 2018-19, the Department of Personnel and Administration (DPA) budget includes funding for $375,000 to purchase a cybersecurity insurance policy. Of this, $325,000 is for the annual insurance premium and $50,000 is for expenses related to minor cybersecurity incidents. This policy would provide cybersecurity coverage of up to $5 million per incident for all state agencies beginning in FY 2018-19. This includes crisis mitigation, incident response including providing required notifications, data recovery, and annual cybersecurity training for state agencies. Beginning in FY 2018-19, state agencies would pay for their portion of this policy through reappropriated funds to DPA, similar to other risk management policies.

Assumptions

For this analysis, all state and local government agencies were canvassed and the majority responded that they already have compliant records disposal policies and security procedures or that they are in compliance because requirements in other applicable state or federal laws, such as Medicaid requirements. Therefore, this analysis assumes that most agencies can implement this bill within existing appropriations. To the extent these agencies require additional appropriations for reviewing and updating their records disposal policies and security procedures, to respond to breaches within 30 days, or to purchase additional cybersecurity protection, its is assumed they will be requested through the annual budget process.

State Revenue

Beginning in FY 2018-19, this bill may increase state revenue from criminal fines and court administrative fees by less than $5,000 per year.

Criminal fines. To the extent that reporting breaches to the Colorado Attorney General increases the number of computer crime offenses prosecuted, this bill will increase state revenue credited to the Fines Collection Cash Fund in the Judicial Department. It is unknown if these will be misdemeanor or felony computer crime offenses. Depending on the nature of the crime, a computer crime can range from a petty 1 misdemeanor to a class 2 felony with a fine penalty range of no more than $500 (petty 1 misdemeanor) up to $1.0 million (class 2 felony). Because the courts have the discretion of incarceration, imposing a fine, or both, the precise impact to state revenue cannot be determined, but is assumed to be minimal and less than $5,000 per year.

Court and administrative fees. The bill may also increase state fee revenue credited to the General Fund and various cash funds. Fees are imposed for a variety of court-related costs, which vary based on the offense but may include probation supervision, drug or sex offender surcharges, victim compensation, and late fees, among others. Some fee revenue is shared with local governments; refer to the Local Government Impact section for additional information.

TABOR Refund

This bill increases state revenue from criminal fines and fees, which will increase the amount of money required to be refunded under TABOR for FY 2018-19 and FY 2019-20. Since the bill increases the TABOR refund obligation without a corresponding change in General Fund revenue, the amount of money available in the General Fund for the budget will decrease by an identical amount. State revenue subject to TABOR is not estimated for years beyond FY 2019-20.

State Expenditures

Beginning in FY 2018-19, this bill increases state agency workload as described below.

Department of Law/Attorney General's Office. This bill increases workload in the Consumer Protection Section of the Department of Law, also known as the Attorney General's Office, to receive data breach notifications from covered and governmental entities that experience a breach of data. Because data breach notices are currently provided to the department on a voluntary basis, its is assumed that this workload increase will be minimal and can be accomplished within existing appropriations. Workload also increases to investigate and prosecute data breach computer crimes. The number of crimes requiring investigation is unknown and it is assumed the department will request an increase in appropriations though the annual budget process, if needed.

Judicial Department. To the extent that this bill increases the number of computer crime offenses prosecuted workload for the trial courts will increase. Given that a Judicial Officer can handle 511 cases per year and the increase in cases resulting from this bill is expected to be well below this level, no additional appropriations are required.

Department of Higher Education. The Department of Higher Education will conduct an IT risk assessment to review current IT business functions and determine if additional IT support or technology is needed and if separate cybersecurity insurance is needed. The cost of this assessment is expected to be between $12,000 and $20,000 and will be paid for using existing appropriations. The department will request additional appropriations through the annual budget process if they are required, based on the outcome of the assessment.

State agencies. State agency workload will increase to review record disposal policies and security procedures to ensure such policies are in compliance with this bill. To the extent that encryption, redaction, or other means are needed to ensure these records are unreadable costs may increase. Workload also increases to review third-party service provider contracts to ensure they are in compliance. To the extent that any breaches occur, workload increases to investigate the breach and provide the required notifications. This analysis assumes additional appropriations will be requested through the annual budget process, if needed.

Local Government

Overall, this bill is expected to increase local government revenue, costs, and workload starting in FY 2018-19, as described below. The exact impact to a particular local government will vary depending on existing record disposal policies and security procedures, cybersecurity breaches, and the number of new computer crime offenses committed within its jurisdiction.

Record disposal policies. Beginning in FY 2018-19, this bill increases local government workload to update record disposal policies. To the extent that encryption, redaction, or other means are needed to ensure these records are unreadable, costs may increase. These potential costs have not been estimated.

Security procedures. This bill increases workload for local governments to review and update security procedures to ensure the protection of personally identifying information. Workload also increases to review third-party service agreements to ensure vendors are complaint with the requirements established by this bill.

Breach notification. To the extent that breaches occur, this bill increases workload and costs to provide notifications to those impacted by the breach, the Attorney General, and consumer reporting agencies if the breach affects more than 1,000 Colorado residents. To the extent that local governments do not have cybersecurity insurance policies and choose to purchase them as a result of this bill, costs will increase. This cost will vary by the size of the government and amount of coverage needed and have not been estimated.

District attorneys. The bill may increase workload and costs for district attorneys to prosecute any new computer crime offenses, discovered from the new reporting requirements created by this bill.

County jails. Under current law, a court may sentence an offender to jail for a misdemeanor or petty offense computer crime. The sentence period varies depending on the nature of the offense and can be up to 18 months. Because the courts have the discretion of incarceration or imposing a fine, the precise impact at the local level cannot be determined. Estimated costs to house an offender in a county jail vary from $53 to $114 per day. For the current fiscal year, the state reimburses county jails at a daily rate of $54.39 to house state inmates.

Denver County Court. The bill may increase criminal fine and court fee revenue, costs, and workload for the Denver County Court, managed and funded by the City and County of Denver from any new misdemeanor computer crime cases. Probation services in the Denver County Courts may also experience a minimal increase in revenue and workload to supervise persons convicted under the bill within Denver County.

Effective Date

This bill was signed into law by the Governor on May 29, 2018, and takes effect September 1, 2018.

Departmental Difference

The Department of Health Care Policy and Financing (HCPF) estimates it will have costs of $120,051 and 1.5 FTE in FY 2018-19 and $69,450 and 1.0 FTE in FY 2019-20 and beyond paid the General Fund (17 percent), the Healthcare Affordability and Sustainability Fee Cash Fund (33 percent), and federal funds (50 percent) to implement this bill. This is to update policies, procedures, training materials, and 300 contracts regarding the storage, disposal, and breach notification within 30 days for Health Insurance Portability and Accountability Act (HIPPA) records. However, the fiscal note does not include these costs because this analysis assumes, the

department is already in compliance with this bill, will be covered by the DPA cybersecurity insurance policy, and that because it is unknown when a breach may occur, any workload created by a breach will be handled within existing staff with additional appropriations for staff being requested through the annual budget process, if needed.

State and Local Government Contacts

All Local Government Agencies All State Agencies