COMMITTEE ON LEGISLATIVE RESEARCH
OVERSIGHT DIVISION

FISCAL NOTE

L.R. No.: 0794-04
Bill No.: SCS for SBs 207 & 245
Subject: State Attorney General; Business and Commerce; Consumer Protection
Type: Original
Date: March 18, 2009

Bill Summary: The proposal creates consumer notification requirements for data security breaches.

FISCAL SUMMARY

ESTIMATED NET EFFECT ON GENERAL REVENUE FUND			
FUND AFFECTED	FY 2010	FY 2011	FY 2012
General Revenue	$0 or (More than $100,000)	$0 or (More than $100,000)	$0 or (More than $100,000)
Total Estimated Net Effect on General Revenue Fund	**$0 or (More than $100,000)**	**$0 or (More than $100,000)**	**$0 or (More than $100,000)**

ESTIMATED NET EFFECT ON OTHER STATE FUNDS			
FUND AFFECTED	FY 2010	FY 2011	FY 2012
Various State Funds	$0 or (More than $100,000)	$0 or (More than $100,000)	$0 or (More than $100,000)
Total Estimated Net Effect on Other State Funds	**$0 or (More than $100,000)**	**$0 or (More than $100,000)**	**$0 or (More than $100,000)**

Numbers within parentheses: ( ) indicate costs or losses.
This fiscal note contains 10 pages.

ESTIMATED NET EFFECT ON FEDERAL FUNDS			
FUND AFFECTED	FY 2010	FY 2011	FY 2012
Total Estimated Net Effect on All Federal Funds	**$0**	**$0**	**$0**

ESTIMATED NET EFFECT ON FULL TIME EQUIVALENT (FTE)			
FUND AFFECTED	FY 2010	FY 2011	FY 2012
Total Estimated Net Effect on FTE	**0**	**0**	**0**

☐ Estimated Total Net Effect on All funds expected to exceed $100,000 savings or (cost).

☐ Estimated Net Effect on General Revenue Fund expected to exceed $100,000 (cost).

ESTIMATED NET EFFECT ON LOCAL FUNDS			
FUND AFFECTED	FY 2010	FY 2011	FY 2012
Local Government	**$0 or (More than $100,000)**	**$0 or (More than $100,000)**	**$0 or (More than $100,000)**

FISCAL ANALYSIS

ASSUMPTION

Officials from the **Office of Administration – Administrative Hearing Commission, Department of Mental Health, Department of Corrections, Department of Revenue, Department of Insurance, Financial Institutions, and Professional Registration, Missouri Consolidated Health Care Plan,** and the **Department of Public Safety – Missouri State Highway Patrol** assume the proposal would have no fiscal impact on their agencies.

Officials from the **Office of the Attorney General (AGO)** assume any potential costs arising from this proposal can be absorbed within existing resources, but if there is a significant increase in cases over time, the AGO may seek appropriation to adequately enforce the provisions of the proposal.

Officials from the **Office of State Courts Administrator** assume the proposed legislation would have no fiscal impact on the courts.

Officials from the **Department of Public Safety – Director's Office** assume any costs associated with this proposal could be absorbed within existing resources.

Officials from the **Office of Administration – Division of Purchasing and Materials Management (DPMM)** assume, in order to comply with Section 407.1500.10, DPMM would have to develop bid language that required a contractor that has access to individuals' personal data to disclose any breach of security of their system following discovery or notification of the breach. Notification would have to be made to nay resident of the state whose personal information was disclosed. Also, the contractor would have to notify the owner or licensee of the personal information indicating there was a breach of security.

Currently, DPMM has a contract that requires the contractor to immediately suspend contract performance and notify the contract administrator if there has been a breach of security, fraud, or misrepresentation in connection with the services being provided under the contract.

Officials from the **Department of Elementary and Secondary Education (DESE)** assume, per Office of Administration – Information Technology Services Division (OA ITSD) staff, the proposal would require anyone with personal information to notify consumers if there is a security breach.

ASSUMPTION (continued)

The cost to post notice would depend on the number of people involved in a breach – but if the MOSIS system was breached, the cost would be around $500,000 to mail out letters or contact parents in another manner. The number of kids in the MOSIS system is around 1,000,000. Costs would be similar if a breach occurred in teacher certification. This would not include time to gather the information, compose the notice, and other tasks.

There would be a cost to handle inquires and other administrative tasks. If there is a breach, much work will be required to field questions and answer phone calls. The amount of time would depend on the severity and size of the breach. A "normal" breach could result in approximately 800 hours of additional administrative support.

Should the new crimes and amendments to current law result in additional fines or penalties, DESE cannot know how much additional money might be collected by local governments or the DOR to distribute to schools. To the extent fine revenues exceed 2004-2005 collections, any increase in this money distributed to schools increases the deduction in the foundation formula the following year. Therefore, the affected districts will see an equal decrease in the amount of funding received through the formula the following year; unless the affected districts are hold-harmless, in which case the districts will not see a decrease in the amount of funding received through the formula (any increase in fine money distributed to the hold-harmless districts will simply be additional money). An increase in the deduction (all other factors remaining constant) reduces the cost to the state of funding the formula.

Oversight assumes any increase or decrease in fine or penalty revenues generated cannot be determined. Therefore, the fiscal note does not reflect any fine or penalty revenues for the local school districts.

ASSUMPTION (continued)

Officials from the **Department of Health and Senior Services (DHSS)** assume Section 407.1500 of the proposed legislation creates a new section relating to security breaches. The definitions differ from those used by the Health Insurance Portability and Accountability Act of 1996 (HIPAA). DHSS is composed of some parts that are regulated by HIPAA and some parts that are not, which makes it a "hybrid entity" as defined by HIPAA. The covered entity parts of the department that are regulated by HIPAA fit within the proposed Section 407.1500.3(2) so they would not have increased costs under SB 207. However, the non-covered entity parts of DHSS fit within the definition of "person" in Section 407.1500.1(8) provided in the proposed statute and would be subject to the new notification requirement because they acquire personal information regarding residents of Missouri. The number of licensees/registrants/clients in the various databases within DHSS, not covered by HIPAA, varies significantly and depending on the situation, a breach could impact more than one database. It is impossible to determine the costs related to an unforeseen breach; therefore, the fiscal impact for this legislation is unknown.

Officials from the **Department of Labor and Industrial Relations (DOLIR)** assume this bill would apply to all DOLIR entities by virtue of Section 407.1500.1(8). Strict compliance with the provisions of the bill would need to be maintained due to the substantial penalties that could be imposed under proposed Section 407.1500.4.

Sections 407.1500.2(1) and (1)(a); 407.1500.2(2); 407.1500.2(4); 407.1500.2(6); and 407.1500.2(7) state a security breach, would result in the need to notify all individuals whose information was compromised. This could result in the preparation of a massive number of documents in a short period of time. These documents could be computer generated and could result in administrative expense. The proposed legislation provides that if there is a breach, DOLIR would need to "provide notice to the affected consumer that there has been a breach of security following discovery or notification of the breach." The legislation requires this notice to be made "without unreasonable delay." Section 407.1500.2(1) and (1)(a). This expense could be absorbed through current funds.

Officials from the **Department of Social Services (DOS)** assume DOS and the Information Technology Services Division in the Office of Administration (OA – ITSD) maintain security for all their databases and has policy and procedures in place for employees to minimize the possibility of a security breach. Therefore, DOS does not anticipate cost. However, if a breach were to occur, the cost of notification as outlined in the bill could exceed $100,000 (GR). DOS does not anticipate a need for additional FTEs.

ASSUMPTION (continued)

DOS assumes it is hard to estimate the actual cost of this bill, as it is unknown how many security breaches may happen in a years time. DOS would incur costs to notify the persons in case of a security breach. Some of these notifications are already covered under HIPAA since we are a covered entity, but it does not correspond directly to our HIPAA obligations, as some of the definitions are different. It is unknown as to what costs would be, as the numbers of security breaches, the number of people involved, and the cost of notifying them are all unknown. Since there is a clause in the legislation that allows a different path to be taken if the cost is greater than 250,000.00, it is assumed that our costs would be unknown to $250,000.00, as the alternate routes are not as costly. However, this is per incident and it is unknown if there would be more than one incident per year.

OA – ITSD has security measures in place to prevent breaches. However, if a breach were to occur OA – ITSD would have to notify the Attorney General. OA – ITSD would also work with the appropriate Division to generate and send letters to the customers involved. OA – ITSD considers this as part of their normal job duties and therefore, would have no fiscal impact. Any associated costs, such as paper or postage, would not be the responsibility of ITSD.

Officials from the **Department of Conservation (MDC)** assume the proposal would have a fiscal impact on MDC funds if a data security breach did occur, but MDC does not anticipate any breaches. MDC has two million plus records for permit customers. However, if a breach did occur, the exact amount of the impact is unknown, but is expected to exceed $100,000.

Officials from the **Office of the Secretary of State (SOS)** assume many bills considered by the General Assembly include provisions allowing or requiring agencies to submit rules and regulations to implement the act. The SOS is provided with core funding to handle a certain amount of normal activity resulting from each year's legislative session. The fiscal impact for this proposal for Administrative Rules is less than $2,500. The SOS recognizes this is a small amount and does not expect additional funding would be required to meet these costs. However, SOS also recognizes that many such bills may be passed in a given year and that collectively the costs may be in excess of what the SOS can sustain with their core budget. Any additional required funding would be handled through the budget process.

Oversight assumes the fiscal impact to various state agencies and local government in the event of a data security breach could exceed $100,000 per year. As the likelihood or frequency of a data security breach is unknown, Oversight has reflected the cost to the general revenue fund, various state funds, and local government as $0 or (more than $100,000) per fiscal year.

ASSUMPTION (continued)

Officials from Missouri State Employees' Retirement System did not respond to Oversight's request for fiscal impact.

FISCAL IMPACT - State Government	FY 2010 (10 Mo.)	FY 2011	FY 2012
GENERAL REVENUE FUND			
Costs – Various state agencies			
Consumer notification of data security breach	$0 or (More than $100,000)	$0 or (More than $100,000)	$0 or (More than $100,000)
ESTIMATED NET EFFECT ON GENERAL REVENUE FUND	**$0 or (More than $100,000)**	**$0 or (More than $100,000)**	**$0 or (More than $100,000)**
VARIOUS STATE FUNDS			
Costs – Various state agencies			
Consumer notification of data security breach	$0 or (More than $100,000)	$0 or (More than $100,000)	$0 or (More than $100,000)
ESTIMATED NET EFFECT ON VARIOUS STATE FUNDS	**$0 or (More than $100,000)**	**$0 or (More than $100,000)**	**$0 or (More than $100,000)**

FISCAL IMPACT - Local Government	FY 2010 (10 Mo.)	FY 2011	FY 2012
LOCAL GOVERNMENT			
Costs – Various political subdivisions			
Consumer notification of data security breaches	$0 or (More than $100,000)	$0 or (More than $100,000)	$0 or (More than $100,000)
ESTIMATED NET EFFECT ON LOCAL GOVERNMENT	**$0 or (More than $100,000)**	**$0 or (More than $100,000)**	**$0 or (More than $100,000)**

FISCAL IMPACT - Small Business

Small businesses who have had a data security breach and need to notify consumers could experience a fiscal impact as a result of this proposal.

FISCAL DESCRIPTION

The proposal requires any person (as defined) that owns or licenses personal information about Missouri residents to notify the affected individuals if the company discovers that security of the personal information has been breached. The notification must be made without unreasonable delay, but may be delayed by a law enforcement agency if the notification would compromise an investigation or homeland security.

Certain pieces of information must be included in the notification, such as the type of personal information compromised, the steps being taken to protect further breaches, and certain advice and contact information.

The proposal provides an exception to the notification requirements if it is determined that a risk of identity theft or other fraud to any consumer is not reasonably likely to occur as a result of the breach.

FISCAL DESCRIPTION (continued)

Notification to affected consumers of a breach may be made in writing, via e-mail, or by telephone. In cases when the cost of notifying would exceed $250,000, when there are over 500,000 affected people to notify, when the company does not have sufficient contact information, or if the company cannot determine which consumers are affected by a breach, the company may use alternate notification procedures as described.

Persons shall notify the Attorney General in cases where the personal information of over 1,000 Missourians has been breached.

Persons that maintain their own notification procedures for security breaches that are consistent with this act shall be deemed in compliance with this act if they follow their procedures. Similarly, if a person maintains procedures for security breaches under another state's laws or federal law, and it follows those procedures, the company shall be deemed in compliance with this act.

The Attorney General shall have exclusive authority to bring action for actual damages for willful and knowing violations of this act as well as may seek a civil penalty of up to $150,000 per security breach.

This legislation is not federally mandated, would not duplicate any other program and would not require additional capital improvements or rental space.

SOURCES OF INFORMATION

Office of the Attorney General
Office of Administration
- – Division of Purchasing and Materials Management
- – Administrative Hearing Commission

Office of State Courts Administrator
Department of Elementary and Secondary Education
Department of Insurance, Financial Institutions, and Professional Registration
Department of Mental Health
Department of Corrections
Department of Health and Senior Services
Department of Labor and Industrial Relations
Department of Revenue
Department of Social Services
Department of Public Safety
- – Missouri State Highway Patrol
- – Director's Office

Missouri Consolidated Health Care Plan
Department of Conservation
Office of the Secretary of State

NOT RESPONDING

Missouri State Employees' Retirement System

Mickey Wilson, CPA
Director
March 18, 2009

BLG:LR:OD (12/02)