



www.lsc.ohio.gov

# OHIO LEGISLATIVE SERVICE COMMISSION

Office of Research  
and Drafting

Legislative Budget  
Office

H.B. 432  
134<sup>th</sup> General Assembly

## Fiscal Note & Local Impact Statement

[Click here for H.B. 432's Bill Analysis](#)

**Version:** As Introduced

**Primary Sponsors:** Reps. Crossman and Sobecki

**Local Impact Statement Procedure Required:** No

Tom Wert, Senior Budget Analyst

### Highlights

- Expenditures from the Risk Management Reserve Fund (Fund 1300) to provide credit monitoring service to Ohio residents whose personal information was exposed as a result of a state agency computer data breach could range from thousands to several million dollars per year depending on the number of individuals receiving the service.
- Costs paid from the Information Technology Governance Fund (Fund 2290) would likely increase by several hundred thousand dollars per year to provide salaries and benefits and other tools needed for the State Chief Information Officer to comply with the bill's requirements to examine and report on data security risks of state agency computer systems every two years.

### Detailed Analysis

#### Credit monitoring

Under the bill, a state agency that suffers a computer data breach must ensure that Ohio residents whose personal information was exposed as a result of that breach can obtain credit monitoring for a period of three years following the date that the state agency discloses the breach. Currently, the Department of Administrative Services (DAS) contracts for credit monitoring services in the event of computer data exposure. According to DAS, prices for these services range from \$1.49 to \$28.99 per year for each individual whose credit is monitored, depending on the specific services included in the monitoring services. Costs to provide credit monitoring services are paid from the Risk Management Reserve Fund (Fund 1300), which receives revenue from fees assessed to state agencies. Total costs to provide credit monitoring services in the event of a computer data breach would depend on the number of individuals

receiving the service and could range from thousands to several million dollars per year for each year that the credit monitoring services are provided.

### **State Chief Information Officer examination and report**

The bill requires the State Chief Information Officer (SCIO) to examine, every two years, each state agency's computer system to assess the risk of a data breach that could compromise the confidentiality of an Ohio resident's personal information. After an examination, the bill requires the SCIO to issue a report to the examined agency that identifies all risks and makes recommendations on how to mitigate those risks. After receiving the report, state agencies must mitigate those risks. According to DAS, to accomplish this, the SCIO would require between five and ten additional employees and potentially additional computer hardware, software, or other diagnostic tools. As a result, costs paid from the Information Technology Governance Fund (Fund 2290) could increase by several hundred thousand dollars per year or more to provide the new employees' salaries, benefits, and to pay the costs of other tools that may be necessary. Fund 2290 receives revenue from charges assessed to state agencies.