# Department of Legislative Services

Maryland General Assembly
2017 Session

## FISCAL AND POLICY NOTE
**First Reader**

House Bill 704 (Delegate Vogt, *et al.*)
Ways and Means

**Education - Identity Protection and Credit Monitoring Services (Student Identity Protection Act)**

This bill requires the State Board of Education to provide identity protection and credit monitoring services for at least five years to any current or former student whose personal information has been compromised by a breach of a public school's or local school system's computer network, computer control language, computer, computer software, computer system, computer service, or computer database in violation of the Criminal Law Article. The board must adopt regulations to implement the bill.

## Fiscal Summary

**State Effect:** General fund expenditures increase, potentially significantly, for the State Board of Education to provide the identity protection and credit monitoring services required under the bill, as discussed below. Revenues are not affected.

**Local Effect:** None. The bill requires the State to pay for identity protection and credit monitoring services for local student data breaches.

**Small Business Effect:** None.

## Analysis

**Current Law/Background:** There is no requirement under State law for the State Board of Education, or any unit of State or local government, to provide identity protection or credit monitoring services for students as specified under the bill.

Disclosure of personally identifiable information by a public school or a local board of education is not specifically addressed in State statute; however, educational agencies and institutions that receive federal education funds are bound by the federal Family Educational Rights and Privacy Act (FERPA) (20 U.S.C. § 1232g) to protect the privacy of student and family information. According to federal regulations, "personally identifiable information" includes, but is not limited to, (1) the student's name; (2) the name of the student's parent or other family members; (3) the address of the student or the student's family; (4) a personal identifier, such as the student's Social Security number (SSN), student number, or biometric record; (5) other indirect identifiers, such as the student's date of birth, place of birth, and mother's maiden name; (6) other information that, alone or in combination, is linked or linkable to a specific student that would allow a reasonable person in the school community, who does not have personal knowledge of the relevant circumstances, to identity the student with reasonable certainty; or (7) information requested by a person who the educational agency or institution reasonably believes knows the identity of the student to whom the education record relates.

Under State law, public schools are prohibited from using SSNs on student (and teacher) identification cards; there is no prohibition on *storing* students' (or teachers') SSNs.

*Protection of Information by Units of Local and State Government*

Chapter 304 of 2013 required units of local and State government – which includes public school systems – to implement and maintain reasonable security procedures and practices appropriate to the nature of the information collected and the nature of the unit and its operations. A unit that uses a nonaffiliated third party as a service provider (and discloses personal information about an individual) must require that the third party implement and maintain reasonable security procedures and practices.

If a government unit that collects computerized data containing an individual's personal information discovers (or is notified of) a breach of the security system, the unit must conduct, in good faith, a reasonable and prompt investigation to determine whether the unauthorized acquisition of personal information has resulted in (or is likely to result in) the misuse of the information – in which case the unit (or the nonaffiliated third party, if authorized under a written contract or agreement) generally must notify the individual of the breach, as specified. A unit must also provide notice of a breach of security to the Office of the Attorney General (OAG), the Department of Information Technology (DoIT), and consumer reporting agencies under specified conditions.

Similarly, a nonaffiliated third party that maintains computerized data containing personal information provided by a unit generally must notify the unit, as specified, of a breach of the security of a system if the unauthorized acquisition of the individual's personal information has occurred or is likely to occur.

Notice to an individual must include specified information and may be given by written notice, telephonic notice, or (under specified circumstances) electronic mail. Substitute notice may be given if the unit demonstrates that the cost of providing notice would exceed $100,000 or that the affected class of individuals to be notified exceeds 175,000 (or if the unit does not have sufficient contact information to give regular notice).

*Identity Theft in Maryland*

In February 2016, the Consumer Sentinel Network, a consortium of national and international law enforcement and private security entities, released the *Consumer Sentinel Network Data Book* for calendar 2015. In calendar 2015, the Federal Trade Commission received 490,220 identity theft complaints compared to 332,647 in calendar 2014 and 290,102 in calendar 2013. In Maryland, residents reported 11,006 instances of identity theft in 2015, or 183.2 complaints per 100,000 population, ranking Maryland fourth in the nation for identity theft. This was a significant increase compared to 2014, when residents reported 5,734 instances of identity theft (95.9 complaints per 100,000 population). In 2014, Maryland ranked tenth in the nation for identity theft. The most common type of identity theft in Maryland was government documents or benefits fraud, which comprised 57% of all complaints. The second most prevalent type of identity fraud involved credit card fraud and represented 14% of all complaints.

According to OAG, there were 497 security breach notices sent in 2016 to Maryland consumers, compared to 482 in 2015 and 333 in 2014.

*Frederick County Student Data Breach*

In December 2016, Frederick County Public Schools (FCPS) announced that the names, SSNs, and dates of birth of about 1,000 former FCPS students were stolen. The information belonged to students who were enrolled in 2005-2006. After discovering the breach in August 2016, FCPS launched an internal investigation and contacted local law enforcement and the Federal Bureau of Investigation. FCPS also contacted the Maryland State Department of Education (MSDE), which investigated as well. According to FCPS, several agencies were ultimately involved in the matter, including OAG, DoIT, MSDE, and the U.S. Department of Homeland Security's Multi-State Information Sharing and Analysis Center (center). The investigation ended in December 2016. According to MSDE, the center found no evidence of a breach of MSDE's data system.

FCPS is providing credit monitoring and identity restoration services for individuals who were affected by the breach for 24 months at no cost. After 24 months, FCPS will consider extending the services, if needed. FCPS reports that it has strengthened its information technology security processes and procedures and is no longer collecting students' SSNs.

**State Expenditures:** The bill requires the State board to provide identity protection and credit monitoring services for at least five years following a breach of personal student information of a local school system or public school. (The bill does not address breaches of student information stored in MSDE or other State data systems.) There are numerous services available that provide "identity protection services," although the Federal Trade Commission (FTC) notes that no service can protect a person from having his or her personal information stolen. Rather, what these services offer are *monitoring services* and *recovery services*.

- *Monitoring services* watch for signs that an identity thief may be using someone's personal information.

- *Recovery services* help a person deal with the effects of identity theft after it happens.

The price of these services varies widely based on the company and the specific types of services offered. (FTC also notes that monitoring and recovery services are often sold together, and may include options like regular access to a person's credit reports or credit scores.)

The exact number of students who will have his or her information compromised each year in the State is unknown. Thus, a reliable estimate of the cost cannot be made at this time. However, *for illustrative purposes only*, assuming the board expends approximately $240 per year (or $20 per month) per person on identity protection and credit monitoring services, and assuming approximately 1,000 students annually have his or her personal information compromised, general fund expenditures increase in fiscal 2018 by $180,000, reflecting the bill's October 1, 2017 effective date.

The bill requires identity protection and credit monitoring services to be provided for *five years* following the compromise. Thus, the effect on expenditures is compounded over time as additional breaches transpire and the State continues to pay for breaches that happened over the previous five years.

**Exhibit 1** shows the hypothetical cost to the State, assuming 1,000 new students each year have his or her information compromised, and the board expends $240 annually for each student who previously had his or her information compromised for five years. As indicated, although the initial cost for 1,000 students is approximately $180,000 ($240,000 annualized), costs grow significantly over time as additional students have his or her information compromised. By fiscal 2022, general fund expenditures could increase by as much as $1.2 million. Actual costs will depend on the number of students affected by breaches each year and the cost of the services required.

**Exhibit 1**
**General Fund Expenditures Assuming 1,000 Student Data Breaches Per Year**
**Fiscal 2018-2022**

| | FY 2018[1] | FY 2019 | FY 2020 | FY 2021 | FY 2022 |
|---|---|---|---|---|---|
| New breaches | 1,000 | 1,000 | 1,000 | 1,000 | 1,000 |
| Prior breaches | | 1,000 | 2,000 | 3,000 | 4,000 |
| Total breaches | 1,000 | 2,000 | 3,000 | 4,000 | 5,000 |
| Cost per year per breach | $240 | $240 | $240 | $240 | $240 |
| **Total cost** | **$180,000** | **$480,000** | **$720,000** | **$960,000** | **$1,200,000** |

[1]FY 2018 reflects the bill's October 1, 2017 effective date.

## Additional Information

**Prior Introductions:** None.

**Cross File:** None.

**Information Source(s):** Anne Arundel, Charles, Frederick, and Montgomery counties; Judiciary (Administrative Office of the Courts); www.fcps.org; *The Baltimore Sun*; Maryland State Department of Education; Department of Legislative Services

**Fiscal Note History:** First Reader - February 27, 2017
fn/rhh

Analysis by: Eric Pierce

Direct Inquiries to:
(410) 946-5510
(301) 970-5510