


Government of the District of Columbia
Office of the Chief Financial Officer



Jeffrey S. DeWitt
Chief Financial Officer

MEMORANDUM

TO: The Honorable Phil Mendelson
Chairman, Council of the District of Columbia

FROM: Jeffrey S. DeWitt
Chief Financial Officer 

DATE: January 17, 2020

SUBJECT: Fiscal Impact Statement - Security Breach Protection Amendment Act
of 2020

REFERENCE: Bill 23-215, Committee print provided to the Office of Revenue Analysis
on January 15, 2020

Conclusion

Funds are sufficient in the fiscal year 2020 through fiscal year 2023 budget and financial plan to implement the bill.

Background

The bill updates definitions and requirements associated with personal data security breaches at businesses and organizations and establishes notification requirements and remedies for failing to meet the requirements. It sets standards for entities to reasonably secure data and makes violation of requirements to protect personal information an unfair or deceptive trade practice, allowing for prosecution under those laws.

The bill requires that a person or entity¹ conducting business in the District notify the Office of the Attorney General (OAG) of an unauthorized acquisition of data or equipment that compromises personal information² if the breach affects 50 or more District residents. Notification cannot be

¹ A person or entity is defined in the bill as an individual, firm, corporation, partnership, company, cooperative, association, trust, or any other organization, legal entity, or group of individuals, but excludes the Government of the District of Columbia and its agencies.

² Personal information is defined in the bill to include names or other personal identifier including social security number, taxpayer identification number, account numbers, credit card numbers, medical information, genetic information, health insurance information, biometric data, email addresses, or any combination that allows for identification or access to an individual email account.

The Honorable Phil Mendelson

FIS: "Warehousing and Storage Eminent Domain Authority Emergency Amendment Act of 2019," Draft bill provided to the Office of Revenue Analysis on December 18, 2019.

delayed on the grounds that the exact number of District residents is not yet determined. Entities must continue to provide notification to the affected parties as already established in current law. The bill requires that notification to affected parties include categories of information that were exposed, information about the right to obtain a security freeze, and contact information for the entity, consumer reporting agencies, the Federal Trade Commission and the OAG.

The bill requires entities to maintain reasonable security safeguards, including procedures and practices appropriate for the type of information and size of the entity. Entities must have a written agreement with any third-party service provider requiring that the third party also maintain reasonable security procedures. The reasonable safeguards must be also be maintained when destroying records.

When a breach occurs in which it is believed a social security number or tax identification number may have been released, entities must offer each affected District resident identity theft protection services for no fewer than 18 months at no cost.

Financial Plan Impact

Funds are sufficient in the fiscal year 2020 through fiscal year 2023 budget and financial plan to implement the bill. The bill imposes requirements on the private sector to report security breaches and provide remedies. The bill excludes the District government and its agencies from the security requirements of the bill, so there is no fiscal exposure to the specific remedies outlined in the bill. The Office of the Attorney General can absorb the cost of collecting notification of security breaches by entities, as well as all other provisions authorizing action by OAG, such as rulemaking.