LEGISLATIVE BUDGET BOARD
Austin, Texas

FISCAL NOTE, 85TH LEGISLATIVE REGULAR SESSION

April 23, 2017

TO: Honorable René Oliveira, Chair, House Committee on Business & Industry

FROM: Ursula Parks, Director, Legislative Budget Board

IN RE: **HB2333** by Elkins (Relating to a breach of system security of a business that exposes consumer credit card or debit card information; providing a civil penalty.), **As Introduced**

Estimated Two-year Net Impact to General Revenue Related Funds for HB2333, As Introduced: a negative impact of ($30,621,082) through the biennium ending August 31, 2019 associated with the administrative aspects of the legislation.

Due to insufficient information available to calculate the total number of data security breaches that would be subject to civil penalty as well as the number of eligible participants in the compensation program, the fiscal implication of program revenue and disbursements cannot be determined. Therefore, only the costs to administer the program are reflected in the fiscal note.

The bill would make no appropriation but could provide the legal basis for an appropriation of funds to implement the provisions of the bill.

General Revenue-Related Funds, Five-Year Impact:

Fiscal Year	Probable Net Positive/(Negative) Impact to General Revenue Related Funds
2018	($16,298,751)
2019	($14,322,331)
2020	($14,322,331)
2021	($14,322,331)
2022	($14,322,331)

All Funds, Five-Year Impact:

Fiscal Year	Probable Savings/(Cost) from *General Revenue Fund* 1	Change in Number of State Employees from FY 2017
2018	($16,298,751)	183.0
2019	($14,322,331)	183.0
2020	($14,322,331)	183.0
2021	($14,322,331)	183.0
2022	($14,322,331)	183.0

Fiscal Analysis

The bill would amend the Business and Commerce Code to require that a business that accepts a credit card or debit card for payment and retains any data related to the card, other than a confirmation number, shall secure the retained information from a breach of a security system. In the event of a security breach, the bill provides direction for the reporting of the security breach to the Attorney General and to each financial institution that issued a credit or debit card effected by the breach.

The bill would create a data security breach victim compensation fund as a dedicated account in the general revenue fund. The fund would consist of revenues collected as civil penalites paid by businesses who suffer a breach of system security for each credit card and debit card from which information was compromised. The money collected in this fund may be used to pay claims to consumers who have suffered financial loss in relation to a breach of system security and to reimburse a financial institution for costs associated with a breach of system security.

The bill would direct the Attorney General to develop a claims process to make payments from the data security breach victims compensation fund.

The bill would create a civil penalty of $50 for each credit card and debit card from which information was compromised to be paid to the data security breach victim compensation fund. The bill would authorize the Attorney General to bring an action to recover a penalty and then deposit the recovered penalty to the credit of the data security breach compensation fund.

This legislation would do one or more of the following: create or recreate a dedicated account in the General Revenue Fund, create or recreate a special or trust fund either with or outside of the Treasury, or create a dedicated revenue source. The fund, account, or revenue dedication included in this bill would be subject to funds consolidation review by the current Legislature. Although this bill would not make an appropriation, it would establish the basis for an appropriation.

The bill would take effect September 1, 2017.

Methodology

The bill would establish a data security breach victim compensation fund. Revenues to the fund are to be generated from a business which suffers a breach of system security and pays a civil penalty of $50 for each credit and debit card from which information was compromised. Inadequate data is available to determine the number of companies that will be required to pay this civil penalty. The fund will disburse funds to consumers who have suffered a financial loss in relation to a breach of system security and to financial institutions for costs associated with a breach of system security. The bill does not specify a minimum or maximum amount of compensation to be paid per victim or financial institution. Furthermore, the bill does not address what funds will be used to cover additional disbursements if the fund was completely depleted but requests for reimbursements remained. Inadequate data is available to determine the number of individuals and financial institutions who would request compensation under the provisions of the bill.

The Office of the Attorney General (OAG) anticipates significant administrative costs associated with the duties prescribed by the bill concerning the collection of funds and operation of the data security breach victim compensation fund. Estimated administrative costs include a one-time technology costs of $1,158,620 and recurring technology costs of $888,920 for the modifications

of the current crime victims compensation claims processing system and the funds necessary to hire 183 FTEs to manage the compensation program.

Utilizing the best available data, the OAG has based its cost estimate on the assumption that 7 percent of the projected 2017 state population of 28,797,290 (population estimate according to the Department of State Health Services) or 2,015,810 individuals would be a victim of a data breach under this legislation. Of this subset, the OAG estimates, using available data, that 14 percent of victims, or 70,553 per year, might be new applicants as individual victims seeking compensation under this legislation. In addition, under this same methodology, it is expected that 100 percent of financial institutions would suffer an out-of-pocket expense anytime an individual is a victim of this crime and 10 percent would seek compensation under this bill, or 201,581 incidents for which a financial institution can be reimbursed.

To administer the data security breach victim compensation fund, the OAG estimates this legislation would require a similar process, infrastructure, and staff to the agency's Crime Victim's Compensation (CVC) Program, which reimburses victims for losses related to violent crime. Currently the program has 94 FTEs who processed 24,718 applications for victim compensation in fiscal year 2016. Assuming 70,553 applications received from individual victims and 201,581 incidents for which financial institutions could be reimbursed, the OAG estimates 183 additional FTEs would be needed for the administration of the data security breach victim compensation program.

The cost for the 183 additional FTEs would be $10,300,903 in fiscal year 2018 and each subsequent year for salary and benefits. An additional $2,763,928 would be needed in fiscal year 2018 with $2,718,928 in each subsequent year for other operating expenses (general overhead, lease space, travel, telephone system, and payroll contribution).

Technology

FTE related technology costs include a one-time cost of $772,800 in fiscal year 2018 for FTE equipment startup (computers, printers, phone, and software) and $413,580 each year in ongoing charges for network storage and software.

The OAG currently operates a CVC claim processing system that the agency assumes could be modified to assume the additional duties of a data security breach compensation program. The claims processing system technology cost in fiscal year 2018 is a one-time cost of $1,158,620 and a recurring cost in each subsequent year of $888,920. The one-time cost estimate includes programmer costs and a security penetration test for the system modification. Recurring costs include software licensing, cloud hosting and support, as well as contract support personnel to maintain the system.

Local Government Impact

No significant fiscal implication to units of local government is anticipated.

Source Agencies: 302 Office of the Attorney General, 304 Comptroller of Public Accounts

LBB Staff: UP, CL, WP, JSm, RC