

REPORT OF THE WAYS AND MEANS FULL COMMITTEE

Senate Bill 334

S. 334 -- Senators Leatherman, O'Dell, Bryant, Matthews, Jackson, Malloy, McGill, Fair, Coleman, Ford, Johnson, McElveen, Pinckney, Scott, Setzler, Williams, Nicholson, Allen, Lourie and Reese: A BILL TO AMEND THE CODE OF LAWS OF SOUTH CAROLINA, 1976, BY ADDING SECTION 12-4-352 SO AS TO REQUIRE THE GOVERNOR TO DEVELOP A PROTECTION PLAN TO MINIMIZE THE ACTUAL AND POTENTIAL COSTS AND EFFECTS OF IDENTITY THEFT DUE TO THE CYBER SECURITY BREACH AT THE DEPARTMENT OF REVENUE BY PROVIDING IDENTITY THEFT PROTECTION AND IDENTITY THEFT RESOLUTION SERVICES, TO REQUIRE THE GOVERNOR TO DEVELOP A POLICY THAT ENSURES THE SAFETY OF ALL PERSONALLY IDENTIFIABLE INFORMATION IN THE POSSESSION OF THE DEPARTMENT OF REVENUE, INCLUDING THE ENCRYPTION OF PERSONALLY IDENTIFIABLE INFORMATION, TO SET FORTH THE PROCESS BY WHICH IDENTITY THEFT PROTECTION AND RESOLUTION SERVICES ARE PROCURED, TO REQUIRE THE GOVERNOR AND THE DEPARTMENT OF REVENUE TO ATTEMPT TO MAKE ENROLLMENT IN THESE PROGRAMS AS EASY AS POSSIBLE, TO PROVIDE THAT THESE PROGRAMS MUST BE FREE OF CHARGE TO THE ELIGIBLE PERSONS, AND TO DEFINE TERMS; BY ADDING SECTION 12-6-1141, SO AS TO PROVIDE AN INDIVIDUAL INCOME TAX DEDUCTION FOR THE ACTUAL COSTS, BUT NOT EXCEEDING TWO HUNDRED DOLLARS FOR AN INDIVIDUAL TAXPAYER, AND NOT EXCEEDING THREE HUNDRED DOLLARS FOR A JOINT RETURN OR A RETURN CLAIMING DEPENDENTS, INCURRED BY A TAXPAYER IN THE TAXABLE YEAR TO PURCHASE IDENTITY THEFT PROTECTION AND IDENTITY THEFT RESOLUTION SERVICES; BY ADDING PART 7 TO CHAPTER 6, TITLE 37 SO AS TO ESTABLISH WITHIN THE DEPARTMENT OF CONSUMER AFFAIRS THE IDENTITY THEFT UNIT AND TO PROVIDE ITS DUTIES; BY ADDING CHAPTER 36 TO TITLE 1 SO AS TO ESTABLISH THE DEPARTMENT OF INFORMATION SECURITY, TO PROVIDE THAT THE MISSION OF THE DEPARTMENT OF INFORMATION SECURITY IS TO PROTECT THE STATE'S INFORMATION AND CYBER SECURITY INFRASTRUCTURE, TO PROVIDE THAT THE DIRECTOR OF THE DEPARTMENT OF INFORMATION SECURITY IS THE CHIEF INFORMATION SECURITY OFFICER OF THE STATE AND TO PROVIDE THE CHIEF INFORMATION SECURITY OFFICER IS APPOINTED BY THE GOVERNOR, AND TO DEFINE TERMS, TO ESTABLISH THE TECHNOLOGY INVESTMENT COUNCIL TO ADOPT AND ANNUALLY REVIEW A STATEWIDE TECHNOLOGY PLAN, TO PROVIDE FOR THE MEMBERSHIP OF THE COUNCIL, AND TO REQUIRE REPORTS; TO AMEND SECTION 1-3-240, AS AMENDED, RELATING TO OFFICERS THAT ONLY MAY BE REMOVED BY THE GOVERNOR FOR CAUSE, SO AS TO ADD THE CHIEF INFORMATION SECURITY OFFICER; TO AMEND SECTION 1-30-10, AS AMENDED, RELATING TO DEPARTMENTS WITHIN THE EXECUTIVE BRANCH OF STATE GOVERNMENT, SO AS TO ADD THE DEPARTMENT OF INFORMATION SECURITY; AND BY ADDING CHAPTER 79 TO TITLE 2 SO AS TO CREATE THE JOINT INFORMATION SECURITY OVERSIGHT COMMITTEE TO CONDUCT A CONTINUING STUDY OF THE LAWS OF THIS STATE AFFECTING CYBER SECURITY, INCLUDING THE RECEIPT OF IMPEDIMENTS TO IMPROVED CYBER SECURITY, AND TO PROVIDE FOR THE MEMBERSHIP OF THE COMMITTEE.

Summary of Bill:

The bill requires the Governor to provide a protection plan to those citizens effected by the data breach at DOR. It also provides a tax deduction if a taxpayer purchases their own protection up to \$300 for an individual taxpayer and \$1,000 for a joint return or a return claiming dependants. This deduction sunsets after the 2018 tax year. Establishes the Identity Theft Unit at the Dept. of Consumer Affairs. Creates a Division of Information Security as a distinct division of the Budget and Control Board. Establishes the Technology Investment Council and the Joint Information Oversight Committee. The DOR Identity Theft Reimbursement Fund and the Spartanburg County Amusement Train Disaster Fund are also established.

Introduced:

01/10/2013

Received by Ways and Means:

04/17/2013

Estimated Fiscal Impact:

According to OSB, the fiscal impact is estimated that a recurring cost of \$1,525,784 for the requirements of the Information Security (Section 3.A) of the Bill creating the Division of Information Security. Primarily, these are personal service and employer contribution costs for a Chief Information Security Officer and 10 FTE positions. Additionally, the Board estimates \$154,992 for duties associated with the Technology Investment Council and the Joint Information Security Oversight Committee. Non-recurring costs are estimated at \$70,032.

The Department estimates this Bill will have a fiscal impact on the agency's recurring and non-recurring funds. The Department estimates recurring costs of \$662,722. Recurring costs include \$387,000 for 10 new FTE positions and \$96,750 for employer contributions. In addition, operating costs for office space, office supplies, technology, and 2 vehicles are estimated at \$178,972. Non-recurring costs are estimated at \$537,690 for computer equipment, software, and telephone lines. Total estimated costs for the agency are \$1,200,412.

The Clerks of the Senate and House of Representatives estimate a daily cost per meeting of approximately \$1600. These costs include mileage, per diem and subsistence for 6 members (3 Senate, 3 House).

The Department reports that this Bill requires the agency to develop policies to ensure maximum enrollments. It also requires the agency to develop forms and an ability to sign up through DOR's website. In addition, there is also a reporting

requirement. DOR indicates the expenditure impact to the agency is minimal.

The Governor's Office states that there would be no fiscal impact to develop a plan for an Identify Theft Protection and Fraud Resolution Services Plan. However, The Governor's Office does not have sufficient information to determine the cost of such protection/insurance at this time. The necessary funding for these services would be included in the Governor's Executive Budget.

Total recurring costs for the State Budget & Control Board and the Department of Consumer Affairs for Personal Identity and Theft Protection are estimated at \$2,188,506 and 21.00 FTE positions. Nonrecurring costs are estimated at \$607,722. Note the cost of Identify Theft Protection/Insurance is not included in these estimates.

According to the BEA Fiscal Impact Statement, the bill will decrease the General Fund individual income tax revenue by \$45,394 in FY13-14.

Subcommittee Recommendation: Recalled to Full Committee on May 16, 2013

Full Committee Recommendation: Pending

Other Notes/Comments:

FISCAL IMPACT STATEMENT ON BILL NO. **S.334, Senate Amendment**
(Doc. No. 334C004.NL.DG13)

TO:	The Honorable Hugh K. Leatherman, Sr., Chairperson, Senate Finance Committee		
FROM:	State Budget Division, Budget and Control Board		
ANALYSTS:	K. Earle Powell, Stephen Gardner, Brenda Hart		
DATE:	March 21, 2013	SBD:	2013192

AUTHOR:	Unknown	PRIMARY CODE CITE:	12-6-1141
SUBJECT:	Identity Theft Protection		

ESTIMATED FISCAL IMPACT ON GENERAL FUND EXPENDITURES:
A Cost to the General Fund (See Below)

ESTIMATED FISCAL IMPACT ON FEDERAL & OTHER FUND EXPENDITURES:
A Cost of Federal and/or Other Funds (See Below)

BILL SUMMARY:

This is a proposed amendment to Senate Bill 334 regarding identity theft protection. The amendment requires the Governor to develop a protection plan to minimize the actual and potential costs of identity theft protection. In addition, the amendment directs the Governor to develop and implement a policy that is designed to ensure the safety of all personally identifiable information at the Department of Revenue. The amendment also creates an Identity Theft Unit at the Department of Consumer Affairs. Also, created within the State Budget and Control Board, is a Division of Information headed by a Chief Information Security Officer. Finally, the amendment establishes a Joint Information Security Oversight Committee comprised of six members of the General Assembly and two members appointed by the Governor.

EXPLANATION OF IMPACT:

State Budget and Control Board

The Board estimates a recurring cost of \$1,525,784 for the requirements of the Information Security (Section 3.A) of the Bill creating the Division of Information Security. Primarily, these are personal service and employer contribution costs for a Chief Information Security Officer and 10 FTE positions. Additionally, the Board estimates \$154,992 for duties associated with the Technology Investment Council and the Joint Information Security Oversight Committee. Non-recurring costs are estimated at \$70,032.

Department of Consumer Affairs

The Department estimates this Bill will have a fiscal impact on the agency's recurring and non-recurring funds. The Department estimates recurring costs of \$662,722. Recurring costs include \$387,000 for 10 new FTE positions and \$96,750 for employer contributions. In addition, operating costs for office space, office supplies, technology, and 2 vehicles are estimated at \$178,972. Non-recurring costs are estimated at \$537,690 for computer equipment, software, and telephone lines. Total estimated costs for the agency are \$1,200,412.

The Senate and House of Representatives

The Clerks of the Senate and House of Representatives estimate a daily cost per meeting of approximately \$1600. These costs include mileage, per diem and subsistence for 6 members (3 Senate, 3 House).

Department of Revenue (DOR)

The Department reports that this Bill requires the agency to develop policies to ensure maximum enrollments. It also requires the agency to develop forms and an ability to sign up through DOR's website. In addition, there is also a reporting requirement. DOR indicates the expenditure impact to the agency is minimal.

The Governor's Office

The Governor's Office states that there would be no fiscal impact to develop a plan for an Identify Theft Protection and Fraud Resolution Services Plan. However, The Governor's Office does not have sufficient information to determine the cost of such protection/insurance at this time. The necessary funding for these services would be included in the Governor's Executive Budget.

RECAP

Total recurring costs for the State Budget & Control Board and the Department of Consumer Affairs for Personal Identity and Theft Protection are estimated at \$2,188,506 and 21.00 FTE positions. Nonrecurring costs are estimated at \$607,722. Note the cost of Identify Theft Protection/Insurance is not included in these estimates.

LOCAL GOVERNMENT IMPACT:

None.

SPECIAL NOTES:

None.

Approved by:



Brenda Hart
Assistant Director, State Budget Division

Statement of Estimated State Revenue Impact

Date: February 7, 2013

Bill Number: S.334

Authors: Leatherman, O'Dell, Bryant, Matthews, *et al.*

Committee Requesting Impact: Finance

Bill Summary

TO AMEND THE CODE OF LAWS OF SOUTH CAROLINA, 1976, BY ADDING SECTION 12-4-352 SO AS TO REQUIRE THE GOVERNOR TO DEVELOP A PROTECTION PLAN TO MINIMIZE THE ACTUAL AND POTENTIAL COSTS AND EFFECTS OF IDENTITY THEFT DUE TO THE CYBER SECURITY BREACH AT THE DEPARTMENT OF REVENUE BY PROVIDING IDENTITY THEFT PROTECTION AND IDENTITY THEFT RESOLUTION SERVICES, TO REQUIRE THE GOVERNOR TO DEVELOP A POLICY THAT ENSURES THE SAFETY OF ALL PERSONALLY IDENTIFIABLE INFORMATION IN THE POSSESSION OF THE DEPARTMENT OF REVENUE, INCLUDING THE ENCRYPTION OF PERSONALLY IDENTIFIABLE INFORMATION, TO SET FORTH THE PROCESS BY WHICH IDENTITY THEFT PROTECTION AND RESOLUTION SERVICES ARE PROCURED, TO REQUIRE THE GOVERNOR AND THE DEPARTMENT OF REVENUE TO ATTEMPT TO MAKE ENROLLMENT IN THESE PROGRAMS AS EASY AS POSSIBLE, TO PROVIDE THAT THESE PROGRAMS MUST BE FREE OF CHARGE TO THE ELIGIBLE PERSONS, AND TO DEFINE TERMS; BY ADDING SECTION 12-6-1141, SO AS TO PROVIDE AN INDIVIDUAL INCOME TAX DEDUCTION FOR THE ACTUAL COSTS, BUT NOT EXCEEDING TWO HUNDRED DOLLARS FOR AN INDIVIDUAL TAXPAYER, AND NOT EXCEEDING THREE HUNDRED DOLLARS FOR A JOINT RETURN OR A RETURN CLAIMING DEPENDENTS, INCURRED BY A TAXPAYER IN THE TAXABLE YEAR TO PURCHASE IDENTITY THEFT PROTECTION AND IDENTITY THEFT RESOLUTION SERVICES; BY ADDING PART 7 TO CHAPTER 6, TITLE 37 SO AS TO ESTABLISH WITHIN THE DEPARTMENT OF CONSUMER AFFAIRS THE IDENTITY THEFT UNIT AND TO PROVIDE ITS DUTIES; BY ADDING CHAPTER 36 TO TITLE 1 SO AS TO ESTABLISH THE DEPARTMENT OF INFORMATION SECURITY, TO PROVIDE THAT THE MISSION OF THE DEPARTMENT OF INFORMATION SECURITY IS TO PROTECT THE STATE'S INFORMATION AND CYBER SECURITY INFRASTRUCTURE, TO PROVIDE THAT THE DIRECTOR OF THE DEPARTMENT OF INFORMATION SECURITY IS THE CHIEF INFORMATION SECURITY OFFICER OF THE STATE AND TO PROVIDE THE CHIEF INFORMATION SECURITY OFFICER IS APPOINTED BY THE GOVERNOR, AND TO DEFINE TERMS, TO ESTABLISH THE TECHNOLOGY INVESTMENT COUNCIL TO ADOPT AND ANNUALLY REVIEW A STATEWIDE TECHNOLOGY PLAN, TO PROVIDE FOR THE MEMBERSHIP OF THE COUNCIL, AND TO REQUIRE REPORTS; TO AMEND SECTION 1-3-240, AS AMENDED, RELATING TO OFFICERS THAT ONLY MAY BE REMOVED BY THE GOVERNOR FOR CAUSE, SO AS TO ADD THE CHIEF INFORMATION SECURITY OFFICER; TO AMEND SECTION 1-30-10, AS AMENDED, RELATING TO DEPARTMENTS WITHIN THE EXECUTIVE BRANCH OF STATE GOVERNMENT, SO AS TO ADD THE DEPARTMENT OF INFORMATION SECURITY; AND BY ADDING CHAPTER 79 TO TITLE 2 SO AS TO CREATE THE JOINT INFORMATION SECURITY OVERSIGHT COMMITTEE TO CONDUCT A CONTINUING STUDY OF THE LAWS OF THIS STATE AFFECTING CYBER SECURITY, INCLUDING THE RECEIPT OF IMPEDIMENTS TO IMPROVED CYBER SECURITY, AND TO PROVIDE FOR THE MEMBERSHIP OF THE COMMITTEE.

REVENUE IMPACT ^{1/}

This bill will decrease General Fund individual income tax revenue by \$45,394 in FY 2013-14.

Explanation

Section 1.B. of this bill creates a deduction from South Carolina taxable income for actual costs incurred by a taxpayer to purchase identity theft protection and resolution services. The deduction may not exceed \$200 for an individual taxpayer or \$300 for joint or head of

Statement of Estimated State Revenue Impact

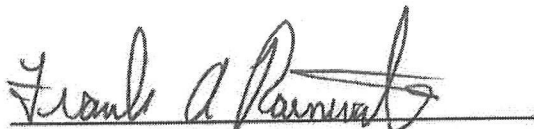
household returns. Expenditures on identity theft protection and resolution services that qualify as a business expense are not eligible for the deduction. Taxpayers eligible for the proposed identity theft protection and resolution services program contained in Section 1.A. of this bill are not eligible for the deduction. This excludes taxpayers that filed a return with the South Carolina Department of Revenue for any year after 1997 and before 2013 from the proposed deduction. Currently, 1,281,547 individuals and families have enrolled in the Experian ProtectMyID or Family Secure programs provided at no cost to taxpayers that have filed a South Carolina tax return since 1998. These taxpayers will receive the free services provided under the provisions of this bill, but will not be eligible for the deduction.

Persons eligible for the proposed deduction include new taxpayers filing their first return in 2013 or later. We anticipate that one percent, or 21,762, of the 2,176,159 individual income tax returns filed for the 2013 tax year will result from new taxpayers filing their first return in South Carolina. An estimated 9,219 returns that are non-taxable or have less than \$3,000 of taxable income further reduces the potential number of returns that could claim the deduction. If 100% of the remaining 12,543 eligible returns claim the deduction at an average cost of \$260, this would result in deductions totaling \$3,261,067. At an average tax rate of 5.8%, these deductions could reduce income tax revenue by \$189,142 in FY 2013-14.

We further reduce the expected revenue impact based on a U.S. survey on identity theft in November 2010 that reported only 12% of consumers were enrolled in an identity theft protection program. To account for additional uncertainty felt by taxpayers from the recent data breach in South Carolina, we expect that 3010, or 24%, of the new returns will claim the proposed deduction at an average of \$260 resulting in total deductions of \$782,656. At an average tax rate of 5.8%, these deductions would reduce General Fund individual income tax revenue by \$45,394 in FY 2013-14.

Unless reauthorized by the General Assembly, taxpayers would be eligible for these deductions for five years, or through FY 2017-18.

We do not anticipate that other sections of this bill would not have any affect on General Fund or other agency revenue.



Frank A. Rainwater
Chief Economist

Analyst: Shuford

^{1/} This statement meets the requirement of Section 2-7-71 for a state revenue impact by the BEA, or Section 2-7-76 for a local revenue impact or Section 6-1-85(B) for an estimate of the shift in local property tax incidence by the Office of Economic Research.

South Carolina General Assembly
120th Session, 2013-2014

S. 334

STATUS INFORMATION

General Bill

Sponsors: Senators Leatherman, O'Dell, Bryant, Matthews, Jackson, Malloy, McGill, Fair, Coleman, Ford, Johnson, McElveen, Pinckney, Scott, Setzler, Williams, Nicholson, Allen, Lourie and Reese
Document Path: I:\council\bill\13125dg13.docx

Introduced in the Senate on February 6, 2013

Introduced in the House on April 17, 2013

Last Amended on April 11, 2013

Currently residing in the House Committee on **Ways and Means**

Summary: Identity Theft Protection

HISTORY OF LEGISLATIVE ACTIONS

Date	Body	Action Description with journal page number
2/6/2013	Senate	Introduced and read first time (Senate Journal-page 5)
2/6/2013	Senate	Referred to Committee on Finance (Senate Journal-page 5)
3/20/2013	Senate	Committee report: Favorable with amendment Finance (Senate Journal-page 12)
3/21/2013		Scrivener's error corrected
4/9/2013	Senate	Committee Amendment Adopted (Senate Journal-page 50)
4/10/2013		Scrivener's error corrected
4/10/2013	Senate	Amended (Senate Journal-page 50)
4/11/2013	Senate	Amended (Senate Journal-page 14)
4/11/2013	Senate	Roll call Ayes-41 Nays-0 (Senate Journal-page 14)
4/11/2013	Senate	Read second time (Senate Journal-page 14)
4/11/2013	Senate	Roll call Ayes-40 Nays-0 (Senate Journal-page 14)
4/12/2013		Scrivener's error corrected
4/15/2013		Scrivener's error corrected
4/16/2013	Senate	Read third time and sent to House (Senate Journal-page 20)
4/17/2013	House	Introduced and read first time (House Journal-page 16)
4/17/2013	House	Referred to Committee on Ways and Means (House Journal-page 16)

View the latest [legislative information](#) at the LPITS web site

VERSIONS OF THIS BILL

[2/6/2013](#)

[3/20/2013](#)

[3/21/2013](#)

[4/9/2013](#)

[4/10/2013](#)

[4/11/2013](#)

[4/12/2013](#)

[4/15/2013](#)

1 AMENDED
2 April 11, 2013
3

S. 334

4
5
6 Introduced by Senators Leatherman, O'Dell, Bryant, Matthews,
7 Jackson, Malloy, McGill, Fair, Coleman, Ford, Johnson,
8 McElveen, Pinckney, Scott, Setzler, Williams, Nicholson, Allen,
9 Lourie and Reese

10
11 S. Printed 4/11/13--S. [SEC 4/15/13 1:35 PM]
12 Read the first time February 6, 2013.
13 _____

1
2
3
4
5
6
7
8
9
10

A BILL

11 TO AMEND THE CODE OF LAWS OF SOUTH CAROLINA,
12 1976, BY ADDING SECTION 12-4-352 SO AS TO REQUIRE
13 THE GOVERNOR TO DEVELOP A PROTECTION PLAN TO
14 MINIMIZE THE ACTUAL AND POTENTIAL COSTS AND
15 EFFECTS OF IDENTITY THEFT DUE TO THE CYBER
16 SECURITY BREACH AT THE DEPARTMENT OF REVENUE
17 BY PROVIDING IDENTITY THEFT PROTECTION AND
18 IDENTITY THEFT RESOLUTION SERVICES, TO REQUIRE
19 THE GOVERNOR TO DEVELOP A POLICY THAT ENSURES
20 THE SAFETY OF ALL PERSONALLY IDENTIFIABLE
21 INFORMATION IN THE POSSESSION OF THE
22 DEPARTMENT OF REVENUE, INCLUDING THE
23 ENCRYPTION OF PERSONALLY IDENTIFIABLE
24 INFORMATION, TO SET FORTH THE PROCESS BY WHICH
25 IDENTITY THEFT PROTECTION AND RESOLUTION
26 SERVICES ARE PROCURED, TO REQUIRE THE
27 GOVERNOR AND THE DEPARTMENT OF REVENUE TO
28 ATTEMPT TO MAKE ENROLLMENT IN THESE PROGRAMS
29 AS EASY AS POSSIBLE, TO PROVIDE THAT THESE
30 PROGRAMS MUST BE FREE OF CHARGE TO THE
31 ELIGIBLE PERSONS, AND TO DEFINE TERMS; BY ADDING
32 SECTION 12-6-1141, SO AS TO PROVIDE AN INDIVIDUAL
33 INCOME TAX DEDUCTION FOR THE ACTUAL COSTS, BUT
34 NOT EXCEEDING TWO HUNDRED DOLLARS FOR AN
35 INDIVIDUAL TAXPAYER, AND NOT EXCEEDING THREE
36 HUNDRED DOLLARS FOR A JOINT RETURN OR A
37 RETURN CLAIMING DEPENDENTS, INCURRED BY A
38 TAXPAYER IN THE TAXABLE YEAR TO PURCHASE
39 IDENTITY THEFT PROTECTION AND IDENTITY THEFT
40 RESOLUTION SERVICES; BY ADDING PART 7 TO
41 CHAPTER 6, TITLE 37 SO AS TO ESTABLISH WITHIN THE
42 DEPARTMENT OF CONSUMER AFFAIRS THE IDENTITY

1 THEFT UNIT AND TO PROVIDE ITS DUTIES; BY ADDING
2 CHAPTER 36 TO TITLE 1 SO AS TO ESTABLISH THE
3 DEPARTMENT OF INFORMATION SECURITY, TO
4 PROVIDE THAT THE MISSION OF THE DEPARTMENT OF
5 INFORMATION SECURITY IS TO PROTECT THE STATE'S
6 INFORMATION AND CYBER SECURITY
7 INFRASTRUCTURE, TO PROVIDE THAT THE DIRECTOR
8 OF THE DEPARTMENT OF INFORMATION SECURITY IS
9 THE CHIEF INFORMATION SECURITY OFFICER OF THE
10 STATE AND TO PROVIDE THE CHIEF INFORMATION
11 SECURITY OFFICER IS APPOINTED BY THE GOVERNOR,
12 AND TO DEFINE TERMS, TO ESTABLISH THE
13 TECHNOLOGY INVESTMENT COUNCIL TO ADOPT AND
14 ANNUALLY REVIEW A STATEWIDE TECHNOLOGY PLAN,
15 TO PROVIDE FOR THE MEMBERSHIP OF THE COUNCIL,
16 AND TO REQUIRE REPORTS; TO AMEND SECTION 1-3-240,
17 AS AMENDED, RELATING TO OFFICERS THAT ONLY
18 MAY BE REMOVED BY THE GOVERNOR FOR CAUSE, SO
19 AS TO ADD THE CHIEF INFORMATION SECURITY
20 OFFICER; TO AMEND SECTION 1-30-10, AS AMENDED,
21 RELATING TO DEPARTMENTS WITHIN THE EXECUTIVE
22 BRANCH OF STATE GOVERNMENT, SO AS TO ADD THE
23 DEPARTMENT OF INFORMATION SECURITY; AND BY
24 ADDING CHAPTER 79 TO TITLE 2 SO AS TO CREATE THE
25 JOINT INFORMATION SECURITY OVERSIGHT
26 COMMITTEE TO CONDUCT A CONTINUING STUDY OF
27 THE LAWS OF THIS STATE AFFECTING CYBER
28 SECURITY, INCLUDING THE RECEIPT OF IMPEDIMENTS
29 TO IMPROVED CYBER SECURITY, AND TO PROVIDE FOR
30 THE MEMBERSHIP OF THE COMMITTEE.

31 Amend Title To Conform

32

33 Whereas, between August 13, 2012 and September 15, 2012, a
34 cyber criminal gained unprecedented access to forty-four South
35 Carolina Department of Revenue computer systems utilizing
36 thirty-three unique and undetected pieces of malicious software,
37 leading to the ultimate theft of more than six million of the state's
38 taxpayers' most sensitive pieces of personal identifying
39 information that were not encrypted, including social security
40 numbers, bank account information, and credit card numbers; and

41

42 Whereas, at no time during this extended period did the
43 Department of Revenue prevent, mitigate, or detect the presence of

1 the cyber criminal, who ultimately uploaded nearly seventy-five
2 gigabytes of data containing millions of pieces of the state's
3 citizens' personal and financial information; and

4
5 Whereas, the Department of Revenue did not discover this
6 unprecedented crime until October 10, 2012, almost two months
7 after the attack began, when a law enforcement agency contacted
8 the Department of Revenue with evidence that a cyber security
9 breach had occurred; and

10
11 Whereas, the public was notified by the Governor of South
12 Carolina of the cyber security breach at the Department of
13 Revenue, the largest to date in United States history, on October
14 26, 2012, at which time the public was informed of the initial steps
15 that were being taken by the Governor and the Department of
16 Revenue to mitigate the damaging effects of the cyber security
17 breach; and

18
19 Whereas, at a cost of more than twenty million dollars to date, the
20 Governor and the Department of Revenue have utilized emergency
21 procurement laws of this State, to both investigate and close the
22 unprecedented breach, as well as to provide victims of this breach,
23 identity theft protection and resolution services; and

24
25 Whereas, the contract negotiated by the Governor and the
26 Department of Revenue under emergency procurement laws of this
27 State, include differing levels of credit report access, monitoring,
28 alerts and identity theft insurance for free, for the initial year, after
29 which time taxpayers would have to purchase the credit report
30 access, monitoring, alerts and identity theft insurance portions of
31 their current coverage at their own expense; and

32
33 Whereas, taxpayers whose personally identifiable information was
34 stolen as a result of this unprecedented cyber security breach were
35 victims through no fault of their own, and trusted the Department
36 of Revenue to protect their most personal and valuable financial
37 information from criminal attacks that could expose them, and
38 their children, to long-term identity theft vulnerabilities; and

39
40 Whereas, the failure of the Department of Revenue to adequately
41 protect taxpayers from this cyber security breach, warrants the
42 provision of identity theft protection and resolution services to
43 eligible persons beyond the initial year, free of charge; and

1
2 Whereas, the Department of Revenue declined technology
3 services, including cyber security services, that had been offered
4 free of charge by another entity of state government; and

5
6 Whereas, the Department of Revenue determined that the
7 encryption of taxpayers' personally identifiable information was
8 too costly and cumbersome to pursue; and

9
10 Whereas, security techniques were known and available but the
11 Department of Revenue decided that the risk of such a breach was
12 small enough to warrant inaction regarding the application of such
13 security techniques; and

14
15 Whereas, this cyber security breach at the Department of Revenue
16 was not primarily about the failure of technology, but was about
17 the failure to deploy even the most basic technology and a failure
18 of organizational structure; and

19
20 Whereas, under the state's current decentralized approach to
21 information security, each agency decides its own risk tolerance
22 for data loss and creates its own information security plan, absent
23 statewide oversight and standards, thereby undermining the state's
24 overall cyber security posture and creating unacceptable risks for
25 data breaches throughout all of state government; and

26
27 Whereas, the creation of a centralized Division of Information
28 Security is necessary to provide statewide oversight and standards
29 to all South Carolina State and local governments to protect the
30 personally identifiable information of all citizens and taxpayers of
31 this State; and

32
33 Whereas, the development and implementation of a single,
34 common, statewide technology direction is fundamental to every
35 aspect of state government, and that the creation of the Division of
36 Information Security will best support the State in this endeavor to
37 unify its technology strategies while identifying those solutions
38 which best improve the protection of the personally identifiable
39 information of the state's citizens. Now, therefore,

40
41 Be it enacted by the General Assembly of the State of South
42 Carolina:

1 SECTION 1. A. Article 3, Chapter 4, Title 12 of the 1976 Code
2 is amended by adding:

3

4 “Section 12-4-352. (A) As used in this section:

5 (1) ‘Eligible person’ means a taxpayer that filed a return
6 with the department for any taxable year after 1997 and before
7 2013, whether by paper or electronic transmission, or any person
8 whose personally identifiable information was contained on the
9 return of another eligible person, including minor dependents.

10 (2) ‘Identity theft protection’ means identity fraud and
11 protection products and services that attempt to proactively detect,
12 notify, or prevent unauthorized access or misuse of a person’s
13 identifying information or financial information to fraudulently
14 obtain resources, credit, government documents or benefits, phone
15 or other utility services, bank or savings accounts, loans, or other
16 benefits in the person’s name.

17 (3) ‘Identity theft resolution services’ means products and
18 services that attempt to mitigate the effects of identity fraud after
19 personally identifiable information has been fraudulently obtained
20 by a third party, including, but not limited to, identity theft
21 insurance and other identity theft resolution services that are
22 designed to resolve actual and potential identity theft and related
23 matters.

24 (4) ‘Person’ means an individual, corporation, firm,
25 association, joint venture, partnership, limited liability corporation,
26 or any other business entity.

27 (5) ‘Personally identifiable information’ means information
28 that can be used to uniquely identify, contact, or locate a single
29 person or can be used with other sources to uniquely identify a
30 single individual, including, but not limited to, social security
31 numbers, debit card numbers, credit card numbers, and bank
32 account numbers.

33 (B)(1) The Governor shall develop a protection plan to
34 minimize the actual and potential costs and effects of identity theft
35 perpetrated upon all eligible persons by providing identity theft
36 protection and identity theft resolution services. The identity theft
37 protection and identity theft resolution services must be free of
38 charge to each eligible person.

39 (2) The Governor shall develop and implement a policy that
40 is designed to ensure the safety of all personally identifiable
41 information in possession of the Department of Revenue. The
42 policy shall include, but is not limited to, the encryption of

1 personally identifiable information both during transmission and at
2 rest.

3 (3) The protection plan and policy implemented pursuant to
4 items (1) and (2) may include assistance from or services provided
5 by any executive branch agency of state government, including the
6 Department of Consumer Affairs.

7 (C)(1) The protection plan implemented pursuant to subsection
8 (B)(1) must include procurement by the Governor of one or more
9 contracts for identity theft protection and identity theft resolution
10 services for all eligible persons, including, but not limited to, credit
11 monitoring and alerts. In implementing the protection plan, the
12 Governor must also consider including protections against
13 government documents and benefits fraud, phone and other
14 utilities fraud, bank fraud and loan fraud. The procurement of
15 identity theft protection shall be governed by the South Carolina
16 Consolidated Procurement Code and conducted in compliance with
17 the following additional requirements. Any contract for identity
18 theft protection or identity theft resolution services entered into by
19 the Governor must be solicited through the Materials Management
20 Office using the process set forth in Section 11-35-1530. Prior to
21 issuance, the Governor's request for proposals must be reviewed
22 and approved by an advisory panel composed of three members
23 appointed by the Governor, Chairman of the Senate Finance
24 Committee, and Chairman of the House Ways and Means
25 Committee. The evaluation and ranking required by Section
26 11-35-1530 must be conducted by an evaluation panel composed
27 of at least three members. The advisory panel must approve
28 anyone selected to serve or otherwise participate with the
29 evaluation panel and anyone authorized by the procurement officer
30 to participate, directly or indirectly, in the selection process.

31 (2) Any contract entered into pursuant to subsection (B)(1)
32 must be for a term of no more than five years. Upon the expiration
33 of a contract or contracts, the Governor shall issue a report to the
34 General Assembly containing findings and recommendations
35 concerning the ongoing risk of identity theft to eligible persons, the
36 services the contract or contracts provided, and the need, if any, for
37 extending the period for the contracted services, including the
38 levels of service required if such a need exists. Based on the
39 findings of the report, the Governor may extend the provision of
40 one or more services offered pursuant to subsection (B)(1) for one
41 additional term of up to five years; however, the provisions of item
42 (1) of this subsection must be complied with in procuring another
43 contract.

1 (3) No service provided pursuant to subsection (B)(1) may
2 be procured for a cost if the same service is available to eligible
3 persons for free under state or federal law.

4 (D)(1) In order to ensure that every eligible person obtains
5 identity theft protection and identity theft resolution services
6 pursuant to subsection (B)(1), to the extent allowed by federal or
7 state law, including Section 30-2-320, the Governor and the
8 Department of Revenue must develop and implement a policy to
9 make enrollment as simple as possible for each eligible person.
10 The policy may include, but is not limited to, automatic
11 enrollment, provided that there is an opt-out mechanism for
12 otherwise eligible persons, enrollment authorization on a tax return
13 filed in this State, and enrollment authorization through a secure
14 protected server on the department's website.

15 (2) By March fifteenth of each year, the Department of
16 Revenue shall issue a report to the Governor and the General
17 Assembly detailing the number of eligible persons that enrolled in
18 the identity theft protection and identity theft resolution services
19 program procured by the Governor pursuant to subsection (B)(1) in
20 the most recent tax year for which there is an accurate figure and
21 the number of people eligible to enroll. The report also must detail
22 the efforts of the Governor and the Department of Revenue to
23 increase enrollment in the programs.

24 (E) The Governor must include the estimated costs of
25 implementing this section when submitting the executive budget
26 pursuant to Article 1, Chapter 11, Title 11. Also, if the
27 department, or an executive branch of state government, including
28 the Department of Consumer Affairs, anticipate funds are
29 necessary to implement the provisions of this section, they must
30 account specifically for such estimated costs in making their
31 annual budget request to the Office of State Budget pursuant to
32 Article 1, Chapter 11, Title 11.

33 (F) Nothing in this section creates a private right of action or an
34 expenditure of funds.”

35
36 B. Article 9, Chapter 6, Title 12 of the 1976 Code is amended by
37 adding:

38
39 “Section 12-6-1141. (A) In addition to the deductions allowed
40 in Section 12-6-1140, there is allowed a deduction in computing
41 South Carolina taxable income of an individual the actual costs,
42 but not exceeding three hundred dollars for an individual taxpayer,
43 and not exceeding one thousand dollars for a joint return or a

1 return claiming dependents, incurred by a taxpayer in the taxable
2 year to purchase a monthly or annual contract or subscription for
3 identity theft protection and identity theft resolution services. The
4 deduction allowed by this item may not be claimed by an
5 individual if the individual deducted the same actual costs as a
6 business expense or if the taxpayer is enrolled in the identity theft
7 protection and identity theft resolution services program pursuant
8 to Section 12-4-352(B)(1). For purposes of this item, 'identity theft
9 protection' and 'identity theft resolution services' have the same
10 meaning as provided in Section 12-4-352.

11 (B) By March fifteenth of each year, the department shall issue
12 a report to the Governor and the General Assembly detailing the
13 number of taxpayers claiming the deduction allowed by this item
14 in the most recent tax year for which there is an accurate figure,
15 and the total monetary value of the deductions claimed pursuant to
16 this item in that same year.

17 (C) The department shall prescribe the necessary forms to
18 claim the deduction allowed by this section. The department may
19 require the taxpayer to provide proof of the actual costs and the
20 taxpayer's eligibility."

21
22 C. Unless reauthorized by the General Assembly, SECTION 1B,
23 as contained in this act, is repealed on January 1, 2018, and only
24 applies to tax years beginning after 2012 and ending before 2018.
25

26 SECTION 2. A. Chapter 6, Title 37 of the 1976 Code is amended
27 by adding:

28
29 "Part 7
30 Identity Theft Unit
31

32 Section 37-6-701. There is created within the Department of
33 Consumer Affairs the Identity Theft Unit with duties and
34 organizations as provided in this part.
35

36 Section 37-6-702. The Identity Theft Unit must be staffed and
37 equipped to perform the functions prescribed in Section 37-6-703.
38

39 Section 37-6-703. The purpose of the Identity Theft Unit is to
40 promote the protection of individuals' personal information,
41 establish programs to inform the public with respect to identity
42 theft, identity fraud and related unlawful conduct or practices, and

1 provide identity theft and fraud resolution services to victims. The
2 unit shall:

3 (1) receive complaints concerning identity theft, identity fraud,
4 and related crimes;

5 (2) provide information and advice to the public on effective
6 ways of handling complaints that involve identity theft, identity
7 fraud, and related crimes;

8 (3) assist victims of identity theft, identity fraud, and related
9 crimes in rectifying the effects of the theft or fraud through
10 personalized assistance;

11 (4) refer complaints where appropriate to local, state, or federal
12 agencies that are available to assist the public with identity theft,
13 identity fraud, and related crimes;

14 (5) develop information and educational programs and
15 materials to foster public understanding and recognition of the
16 issues related to identity theft, identity fraud, and other unlawful
17 conduct or practices;

18 (6) identify consumer problems in, and promote and facilitate
19 the development and use of best practices in the protection of the
20 privacy of personal information;

21 (7) promote voluntary and mutually agreed upon non-binding
22 mediation of identity theft and identity fraud disputes where
23 appropriate;

24 (8) cooperate and assist local, state, and federal law
25 enforcement agencies in carrying out their legal enforcement
26 responsibilities related to identity theft and identity fraud;

27 (9) assist and coordinate in the training of local, state, and
28 federal law enforcement agencies regarding identity theft, identity
29 fraud, and other privacy related crimes; and

30 (10) provide a centralized location where information related to
31 incidents of identity theft may be securely stored and accessed for
32 the benefit of victims of identity theft.

33
34 Section 37-6-704. By March fifteenth of each year, the division
35 shall issue a report to the Governor, the General Assembly, and the
36 Joint Information Security Oversight Committee with
37 recommendations, including the text of an amendment effectuating
38 the recommendations, to state and federal law, including the
39 Consumer Protection Code, regarding identity theft that would
40 reduce the occurrence of identity theft and the costs, monetary and
41 otherwise, of identity theft.”

42

1 B. Notwithstanding the general effective date of this act, this
2 SECTION takes effect October 1, 2013.

3
4 SECTION 3. A. Title 1 of the 1976 Code is amended by adding:

5
6 "CHAPTER 36

7
8 Information Security

9
10 Article 1

11
12 Division of Information Security

13
14 Section 1-36-10. (A) There is hereby established within the
15 Budget and Control Board the Division of Information Security
16 that is dedicated to the protection of the state's information and
17 cyber security infrastructure, including, but not limited to, the
18 identification and mitigation of vulnerabilities, deterring and
19 responding to cyber events, and promoting cyber security
20 awareness within the State. The division also shall be responsible
21 for statewide policies, standards, programs, and services relating to
22 cyber security and information systems, including the statewide
23 coordination of critical infrastructure information. The division
24 shall consist of the Chief Information Security Officer, who is the
25 director of the division, and a staff employed by the Chief
26 Information Security Officer as necessary to carry out the duties of
27 the division and as are authorized by law. The Chief Information
28 Security Officer, with advice and assistance of the Office of
29 Human Resources of the Budget and Control Board, shall fix the
30 salaries of all staff subject to the funds authorized in the annual
31 general appropriations act. Subject to funding, the salaries of the
32 staff involved with information technology must be competitive
33 with the private sector. The compensation plan must be unique to
34 information technology employees working at the Division of
35 Information Security and consider all factors including areas
36 requiring specialized skill sets, and should include components
37 necessary to recruit and retain highly qualified information
38 technology professionals to the State.

39 (B) After consulting with the Division of State Information
40 Technology of the Budget and Control Board, the Governor shall
41 appoint the Chief Information Security Officer with the advice and
42 consent of the Senate for a term of four years, except that the
43 initial appointment shall expire June 30, 2017. The Governor may

1 reappoint the Chief Information Security Officer for additional
2 terms. The Chief Information Security Officer's compensation
3 must not be reduced during the Chief Information Security
4 Officer's uninterrupted continued tenure in office.

5 (C) The Chief Information Security Officer may be removed
6 from office only by the Governor as provided in Section
7 1-3-240(C).

8

9 Section 1-36-20.(A) In consultation with appropriate agency
10 heads, the Chief Information Security Officer shall develop cyber
11 security policies, guidelines, and standards. The Chief Information
12 Security Officer shall oversee the implementation of and
13 compliance with established standards. Each agency or agency
14 head shall, under the management of the Division of State
15 Information Technology, install and administer state data security
16 systems on its computer facilities consistent with these policies,
17 guidelines, standards, and state law to ensure the integrity of
18 computer-based and other data and to ensure applicable limitations
19 on access to data. In furtherance of and in addition to these duties,
20 the Chief Information Security Officer shall:

21 (1) include the identification and routine assessment of
22 security risks at the agency level in the information security plan
23 developed;

24 (2) regularly audit agencies to monitor compliance with
25 established standards;

26 (3) require in the information security plan developed that
27 agencies ensure service contractors follow established procedures
28 when providing contracted services;

29 (4) coordinate all incident responses to agency cyber
30 security breaches; and

31 (5) offer security services to agencies.

32 (B) The Chief Information Security Officer is responsible for
33 overall security of state agency networks connected to the Internet
34 as a component of the overall information technology function.
35 Information technology remains the responsibility of the Director
36 of the Division of State Information Technology. Each agency or
37 agency head is responsible for the security of the agency's data
38 within the guidelines of the policy established by the Chief
39 Information Security Officer.

40 Section 1-36-30.(A) In developing policies, guidelines, and
41 standards, the Chief Information Security Officer must consider:

42 (1) developing an information technology security
43 governance structure that is inclusive of all agencies;

1 (2) adopting control objectives to manage, implement, and
2 maintain information technology security;

3 (3) developing security metrics that accurately measure
4 unwanted intrusions, security breaches, penetrations, and
5 vulnerabilities;

6 (4) developing security standards based on a full risk
7 assessment of critical infrastructure vulnerabilities; and

8 (5) developing a method for the sharing of security
9 information sharing and analysis.

10 (B) The Chief Information Security Officer and the Director of
11 the Division of State Information Technology shall collaborate
12 with each other in developing policies, guidelines, and standards
13 required by each office.

14
15 Section 1-36-40. (A) All agencies must adopt and implement
16 the policies, guidelines, and standards developed by the Chief
17 Information Security Officer.

18 (B) Upon request of the Chief Information Security Officer for
19 information or data, all agencies must fully cooperate with and
20 furnish the Chief Information Security Officer with all documents,
21 reports, answers, records, accounts, papers, and other necessary
22 data and documentary information to perform the division's
23 mission and to exercise the division's functions, powers, and
24 duties.

25 (C) The Chief Information Security Officer shall coordinate at
26 least one training conference annually for state agency information
27 security officers and shall receive an appropriation for the
28 conference in an amount sufficient to attract the top cyber security
29 professionals in the country to speak and to produce training
30 materials for attendees.

31
32 Section 1-36-50. For purposes of this chapter, 'agency' means
33 all state agencies, departments, boards, commissions, institutions,
34 and authorities, except the legislative and judicial departments of
35 state government, that collect or maintain personally identifiable
36 information as defined in Section 12-4-352. 'Agency' also
37 includes all political subdivisions of this State, including school
38 districts, and public authorities that collect or maintain personally
39 identifiable information as defined in Section 12-4-352.

40
41 Section 1-36-60. The Division of Information Security may
42 promulgate regulations necessary to implement the provisions of
43 this chapter and to accomplish the objectives set forth in Section

1 1-36-20. The regulations may include penalties for any agency in
2 violation of Section 1-36-40.

3
4 Article 3

5
6 Technology Investment Council

7
8 Section 1-36-310. There is hereby established a Technology
9 Investment Council. The council shall consist of seven members,
10 appointed as follows:

11 (1) the Director of the Budget and Control Board, Division of
12 State Information Technology, who shall serve as chairman;

13 (2) the Chief Information Security Officer;

14 (3) five members, with one appointment made by each: the
15 Governor, President Pro Tempore of the Senate, Speaker of the
16 House of Representatives, Chairman of the Senate Finance
17 Committee, and Chairman of the House Ways and Means
18 Committee.

19
20 Section 1-36-320. The duties of the council are as follows:

21 (1) adopt policies and procedures used to develop, review, and
22 annually update a statewide technology plan and provide it to the
23 Governor, Office of State Budget, and the General Assembly;

24 (2) by October 1, 2013, and each October first thereafter, the
25 council shall provide the Governor, the Legislative Fiscal Office,
26 the Executive Budget and Strategic Planning Office, and the
27 General Assembly with a statewide technology plan. The plan
28 shall discuss the state's overall technology needs over a multiyear
29 period and the potential budgetary implications of meeting those
30 needs;

31 (3) by November fifteenth of each year, the council shall make
32 recommendations to the Governor and General Assembly
33 regarding the funding of technology for the next fiscal year;

34 (4) enforce active project management, review the progress of
35 current projects to determine if they are on budget and have met
36 their project milestones, and when necessary, recommend the
37 termination of projects; and

38 (5) develop minimum technical standards, guidelines, and
39 architectures as required for state technology projects.

40
41 Section 1-36-330. To assist the council and Division of
42 Information Security in fulfilling its duties, each agency shall
43 name an individual to act as that agency's 'information security

1 officer'. It is the intent of this section that such information
2 security officers will act as the primary points of contact for
3 appropriate communications between the council and the Division
4 of Information Security.”

5
6 B. Section 1-3-240(C)(1) of the 1976 Code, as last amended by
7 Act 105 of 2012, is further amended by adding an appropriately
8 numbered subitem at the end to read:

9
10 “() Chief Information Security Officer.”

11
12 C. Notwithstanding the general effective date of this act, this
13 SECTION takes effect July 1, 2013.

14
15 SECTION 4. Title 2 of the 1976 Code is amended by adding:

16
17 “CHAPTER 79

18
19 Joint Information Security Oversight Committee

20
21 Section 2-79-10. The General Assembly finds that:

22 (1) a need exists for the protection of the state’s information
23 and cyber security infrastructure;

24 (2) a need exists for statewide policies, standards, programs,
25 and services relating to cyber security and information systems;
26 and

27 (3) it is necessary that the General Assembly be kept apprised
28 of statewide efforts to improve cyber security, including any
29 barriers to improved cyber security.

30
31 Section 2-79-20. There is created the Joint Information Security
32 Oversight Committee to conduct a continuing study of the laws of
33 this State affecting cyber security, including the receipt of
34 information from the Division of Information Security regarding
35 impediments to improved cyber security. The committee is
36 composed of nine members appointed as follows:

37 (1) two members appointed by the Chairman of the Senate
38 Finance Committee;

39 (2) two members appointed by the Chairman of the House
40 Ways and Means Committee;

41 (3) one member appointed by the President Pro Tempore of the
42 Senate;

1 (4) one member appointed by the Speaker of the House of
2 Representatives;

3 (5) two members appointed by the Governor; and

4 (6) the Chief Information Security Officer who shall serve ex
5 officio.

6 At its first meeting the committee shall organize by selecting
7 from its membership a chairman, vice chairman, secretary, and
8 other officers the committee may determine. The committee shall
9 meet on the call of the chairman or a majority of the members. A
10 quorum consists of five members. Terms of appointed committee
11 members are coterminous with that of the appointing authority.
12 The committee shall report its initial findings and
13 recommendations to the General Assembly on March 15, 2014,
14 and shall make a report to the General Assembly each year
15 thereafter. The report shall include the text of an amendment that
16 effectuates the recommendations.

17
18 Section 2-79-30. The committee shall make a continuous study
19 and investigation of all facets of the laws and practices relating to
20 cyber security, so as to recommend appropriate modifications. The
21 committee and its subcommittees may hold hearings and act at the
22 times and places within the State the chairman designates and
23 require the appearance of witnesses and the production of
24 documents as provided for in Chapter 69, Title 2.

25
26 Section 2-79-40. (A) The members of the committee are
27 ineligible for compensation but shall receive the usual mileage, per
28 diem, and subsistence as is provided by law for members of state
29 boards, commissions, and committees. The allowed mileage, per
30 diem, and subsistence must be paid from approved accounts of the
31 Senate for the Senate appointees, from approved accounts of the
32 House for the House appointees, from funds appropriated to the
33 Office of the Governor for gubernatorial appointees, and from
34 funds appropriated to the Division of Information Security for the
35 Chief Information Security Officer.

36 (B) Upon funding from the General Assembly, the committee
37 may engage or employ staff or consultants as may be necessary
38 and prudent to assist the commission in the performance of its
39 duties and responsibilities.

40 (C) Staffs of the Senate, the House of Representatives, and the
41 Division of Information Security must be available to assist the
42 commission in its work. Any other expenses incurred by the
43 commission shall be paid equally from each respective house's

1 approved account subject to the approval of the Senate Operations
2 and Management Committee and the Speaker of the House.”

3

4 SECTION 5. Article 3, Chapter 4, Title 12 of the 1976 Code is
5 amended by adding:

6

7 “Section 12-4-355. (A) For the purposes of this section:

8 (1) ‘Eligible person’ shall mean a person whose personally
9 identifiable information was obtained by a third party from a
10 compromised computer system maintained by a state agency,
11 board, committee, or commission.

12 (2) ‘Eligible expenses’ shall mean financial losses incurred
13 by an eligible person directly related to the misappropriation of the
14 eligible person’s personally identifiable information that was
15 obtained by a third party from a compromised computer system
16 maintained by a state agency, board, committee, or commission.
17 Expenses for services provided by private entities to assist eligible
18 persons with financial losses are not eligible expenses to the extent
19 such services are offered through the State or a state-supported
20 program free of charge.

21 (3) ‘Financial losses’ shall mean actual losses, including, but
22 not limited to, lost wages, attorneys’ fees, and other costs incurred
23 by an eligible person related to correcting his credit history or
24 credit rating, or costs or judgments related to any criminal, civil, or
25 administrative proceeding brought against the eligible person
26 resulting from the misappropriation of the victim’s personally
27 identifiable information not recovered from any other source.
28 Costs associated with the purchase of identity theft protection and
29 identity theft resolution services as defined in Section
30 12-4-352(A)(2) and Section 12-4-352(A)(3) are not financial
31 losses.

32 (4) ‘Person’ shall mean an individual, corporation, firm,
33 association, joint venture, partnership, limited liability corporation,
34 or any other business entity.

35 (5) ‘Personally identifiable information’ means information
36 that can be used to uniquely identify, contact, or locate a single
37 person or can be used with other sources to uniquely identify a
38 single individual, including, but not limited to, social security
39 numbers, debit card numbers, and credit card numbers.

40 (B) There is established in the State Treasury the Department of
41 Revenue Identity Theft Reimbursement Fund which must be
42 maintained separately from the general fund of the State and all
43 other funds. The proceeds of the fund must be utilized to

1 reimburse eligible expenses incurred by an eligible person. The
2 obligation to reimburse claims pursuant to this section does not
3 arise until monies are credited to the fund, and only to the extent
4 that monies are credited to the fund.

5 (C) A person seeking reimbursement from the fund must file
6 with the Treasurer a claim on a form prescribed by him and
7 verified by the claimant. The Treasurer shall consider each claim
8 within ninety days after it is filed and give written notice to the
9 claimant if the claim is denied in whole or in part. If a claim is
10 allowed, the Treasurer shall reimburse the eligible person in an
11 amount equal to his eligible expenses subject to availability of
12 monies in the fund. The decision by the Treasurer regarding a
13 claim is a final agency decision that may be appealed to the
14 Administrative Law Court pursuant to the Administrative
15 Procedures Act naming the Treasurer as the defendant. The action
16 must be brought within ninety days after the Treasurer's decision
17 or within one hundred eighty days after the filing of the claim if he
18 has failed to act on it.

19 (D) The State Treasurer may promulgate regulations necessary
20 to implement the provisions of this section, including the disbursal
21 of proceeds of the fund.”

22

23 SECTION 6. Article 3, Chapter 4, Title 12 of the 1976 Code is
24 amended by adding:

25

26 “Section 12-4-356. (A) There is created in the State Treasury
27 the Spartanburg County Amusement Train Disaster Relief Fund.
28 This fund is separate and distinct from the general fund of the State
29 and all other funds. Earnings and interest on this fund must be
30 credited to it and any balance in this fund at the end of a fiscal year
31 carries forward in the fund in the succeeding fiscal year. The
32 purpose of the fund is to compensate victims of the amusement
33 train derailment in Cleveland Park in Spartanburg County on
34 March 19, 2011, for medical costs not covered by insurance or
35 other means which exceed the individual victim's share of the
36 maximum amount recoverable from a governmental entity for a
37 single occurrence pursuant to Section 15-78-120 of the Tort
38 Claims Act. The obligation to compensate victims pursuant to this
39 section does not arise until monies are credited to the fund, and
40 only to the extent that monies are credited to the fund.

41 (B) The Department of Revenue shall serve as the administrator
42 for the fund. The department shall establish a sixty day period to
43 receive claims to the fund. For two weeks prior to the opening of

1 the claims period, the department must publish a notice in a
2 newspaper of general circulation in Spartanburg County the
3 procedure by which claims may be submitted. The State Office of
4 Victim Assistance shall provide administrative and logistical
5 assistance to the department. The department may use up to fifty
6 thousand dollars from the fund to defray the costs associated with
7 managing the fund and to reimburse the State Office of Victim
8 Assistance for any costs associated with providing support.

9 (C) At the close of the claims period, the department shall pay
10 to each claimant the actual amount of their verifiable medical
11 expenses if the aggregate amount of claims to the fund does not
12 exceed the amount available in the fund. If the aggregate amount
13 of claims exceeds the amount in the fund, the department shall pay
14 each claimant a percentage of the fund equal to the percentage of
15 the uncompensated medical expenses incurred by the claimant in
16 relation to the total amount of uncompensated medical expenses
17 incurred by all claimants to the fund. Funds may only be used to
18 pay victims directly for uncompensated medical expenses and
19 must not be used to pay subrogation claims or attorneys' fees. Any
20 monies remaining in the fund after full payment is made to all
21 claimants must be transferred to the Insurance Reserve Fund.

22 (D) Notwithstanding any other provision of law, any amount
23 paid to a claimant pursuant to this section is not subject to any tax
24 imposed by this title.”

25

26 SECTION 7. Except as otherwise provided, this act takes effect
27 upon approval by the Governor

28

29

----XX----

30