



Senate

General Assembly

File No. 95

January Session, 2007

Substitute Senate Bill No. 1089

Senate, March 21, 2007

The Committee on Banks reported through SEN. DUFF of the 25th Dist., Chairperson of the Committee on the part of the Senate, that the substitute bill ought to pass.

AN ACT ENCOURAGING THE SAFEKEEPING OF CONSUMER INFORMATION.

Be it enacted by the Senate and House of Representatives in General Assembly convened:

1 Section 1. Section 36a-701b of the general statutes is repealed and
2 the following is substituted in lieu thereof (*Effective October 1, 2007*):

3 (a) For purposes of this section, "breach of security" means
4 unauthorized access to or acquisition of electronic files, media,
5 databases or computerized data containing personal information when
6 access to the personal information has not been secured by encryption
7 or by any other method or technology that renders the personal
8 information unreadable or unusable; "personal information" means an
9 individual's first name or first initial and last name in combination
10 with any one, or more, of the following data: (1) Social Security
11 number; (2) driver's license number or state identification card
12 number; or (3) account number, credit or debit card number, in
13 combination with any required security code, access code or password
14 that would permit access to an individual's financial account. "Personal

15 information" does not include publicly available information that is
16 lawfully made available to the general public from federal, state or
17 local government records or widely distributed media.

18 (b) Any person who conducts business in this state, and who, in the
19 ordinary course of such person's business, owns, licenses or maintains
20 computerized data that includes personal information, shall disclose
21 any breach of security following the discovery of the breach to any
22 resident of this state whose personal information was, or is reasonably
23 believed to have been, accessed by an unauthorized person through
24 such breach of security. Such disclosure shall be made without
25 unreasonable delay, subject to the provisions of subsection (d) of this
26 section and the completion of an investigation by such person to
27 determine the nature and scope of the incident, to identify the
28 individuals affected, or to restore the reasonable integrity of the data
29 system. Such notification shall not be required if, after an appropriate
30 investigation and consultation with relevant federal, state and local
31 agencies responsible for law enforcement, the person reasonably
32 determines that the breach will not likely result in harm to the
33 individuals whose personal information has been acquired and
34 accessed.

35 (c) Any person that maintains computerized data that includes
36 personal information that the person does not own shall notify the
37 owner or licensee of the information of any breach of the security of
38 the data immediately following its discovery, if the personal
39 information was, or is reasonably believed to have been accessed by an
40 unauthorized person.

41 (d) Any notification required by this section shall be delayed for a
42 reasonable period of time if a law enforcement agency determines that
43 the notification will impede a criminal investigation and such law
44 enforcement agency has made a request that the notification be
45 delayed. Any such delayed notification shall be made after such law
46 enforcement agency determines that notification will not compromise
47 the criminal investigation and so notifies the person of such

48 determination.

49 (e) Any notice required by the provisions of this section may be
50 provided by one of the following methods: (1) Written notice; (2)
51 telephone notice; (3) electronic notice, provided such notice is
52 consistent with the provisions regarding electronic records and
53 signatures set forth in 15 USC 7001; (4) substitute notice, provided such
54 person demonstrates that the cost of providing notice in accordance
55 with subdivision (1), (2) or (3) of this subsection would exceed two
56 hundred fifty thousand dollars, that the affected class of subject
57 persons to be notified exceeds five hundred thousand persons or the
58 person does not have sufficient contact information. Substitute notice
59 shall consist of the following: (A) Electronic mail notice when the
60 person, business or agency has an electronic mail address for the
61 affected persons; (B) conspicuous posting of the notice on the web site
62 of the person, business or agency if the person maintains one; and (C)
63 notification to major state-wide media, including newspapers, radio
64 and television.

65 (f) Any person that maintains such person's own security breach
66 procedures as part of an information security policy for the treatment
67 of personal information and otherwise complies with the timing
68 requirements of this section, shall be deemed to be in compliance with
69 the security breach notification requirements of this section, provided
70 such person notifies subject persons in accordance with such person's
71 policies in the event of a breach of security. Any person that maintains
72 such a security breach procedure pursuant to the rules, regulations,
73 procedures or guidelines established by the primary or functional
74 regulator, as defined in 15 USC 6809(2), shall be deemed to be in
75 compliance with the security breach notification requirements of this
76 section, provided such person notifies subject persons in accordance
77 with the policies or the rules, regulations, procedures or guidelines
78 established by the primary or functional regulator in the event of a
79 breach of security of the system.

80 (g) Failure to comply with the requirements of this section shall

81 constitute an unfair trade practice for purposes of section 42-110b and
82 shall be enforced by the Attorney General.

83 (h) Notwithstanding any provision of the general statutes, and in
84 addition to any other liability of a person to a bank or an out-of-state
85 bank, any person required to provide notice under subsection (b) or (c)
86 of this section shall be liable to a bank or an out-of-state bank that has
87 customers whose personal information was, or is reasonably believed
88 to have been, accessed by an unauthorized person through a breach of
89 security, for the costs of any reasonable action undertaken by the bank
90 or out-of-state bank on behalf of its customers as a direct result of the
91 breach of security in order to protect the sensitive information or
92 financial interests of such customers or to continue to provide financial
93 services to such customers, including any costs incurred in connection
94 with: (1) The cancellation or reissuance of any credit card, debit card or
95 other account access device issued by any such bank or out-of-state
96 bank; (2) the closure of any deposit, transaction or other account and
97 any other actions to stop payments or block transactions with respect
98 to any such account; (3) the opening or reopening of any deposit,
99 transaction or other account for any customer of the bank or out-of-
100 state bank; (4) any refund or credit made to any customer of the bank
101 or out-of-state bank as a result of unauthorized transactions; and (5)
102 any assistance provided to customers to help mitigate loss or
103 inconvenience or to prevent further loss or inconvenience.

This act shall take effect as follows and shall amend the following sections:		
Section 1	October 1, 2007	36a-701b

BA *Joint Favorable Subst.*

The following fiscal impact statement and bill analysis are prepared for the benefit of members of the General Assembly, solely for the purpose of information, summarization, and explanation, and do not represent the intent of the General Assembly or either chamber thereof for any purpose:

OFA Fiscal Note

State Impact: None

Municipal Impact: None

Explanation

This bill makes banks liable for costs incurred when a customer's personal information is violated, and there is no fiscal impact.

The Out Years

State Impact: None

Municipal Impact: None

OLR Bill Analysis**sSB 1089*****AN ACT ENCOURAGING THE SAFEKEEPING OF CONSUMER INFORMATION.*****SUMMARY:**

Under current law, anyone who conducts business in Connecticut and who, in the ordinary course of his business, owns, licenses, or maintains computerized data that includes personal information must disclose any security breach either to Connecticut residents whose personal information was, or is reasonably believed to have been, accessed by an unauthorized person. Anyone who maintains computerized data that includes personal information that the person does not own, must notify the owner or licensee of any such breach.

This bill makes these businesses, in addition to any other liability, liable to a Connecticut, federal, or out-of-state bank whose customers' personal information was, or is reasonably believed to have been, accessed by an unauthorized person. They are liable for the costs of any reasonable action the bank undertakes on behalf of its customers as a direct result of the breach in order to protect sensitive information or financial interests of, or to continue to provide financial services to, such customers. Liability includes costs incurred in connection with:

1. cancelling or reissuing any credit card, debit card, other account access device used by the bank;
2. closing any account and any other actions to stop payments or block transactions on the account;
3. opening or reopening an account for any customer of the bank;
4. any refund or credit made to any customer of the bank as a

result of unauthorized transactions; and

5. any assistance provided to customers to help mitigate or prevent loss or inconvenience.

EFFECTIVE DATE: October 1, 2007

COMMITTEE ACTION

Banks Committee

Joint Favorable Substitute

Yea 18 Nay 0 (03/06/2007)