

2008 MAR 27 PM 4:59

**WEST VIRGINIA LEGISLATURE**  
**SEVENTY-EIGHTH LEGISLATURE**  
**REGULAR SESSION, 2008**

---

COMMITTEE SUBSTITUTE  
FOR

**ENROLLED**  
**Senate Bill No. 340**

(SENATORS KESSLER, CHAFIN, OLIVERIO, BARNES, WHITE,  
FOSTER, HUNTER, GREEN, MINARD, WELLS, JENKINS, YODER,  
LOVE, GUILLS, UNGER AND MCKENZIE, *original sponsors*)

---

[Passed March 8, 2008; in effect ninety days from passage.]

2008 MAR 21 PM 4:59

SENATE CLERK  
STATE OF WEST VIRGINIA

**ENROLLED**

COMMITTEE SUBSTITUTE

FOR

**Senate Bill No. 340**

(SENATORS KESSLER, CHAFIN, OLIVERIO, BARNES, WHITE,  
FOSTER, HUNTER, GREEN, MINARD, WELLS, JENKINS, YODER,  
LOVE, GULLS, UNGER AND MCKENZIE, *original sponsors*)

[Passed March 8, 2008; in effect ninety days from passage.]

AN ACT to amend the Code of West Virginia, 1931, as amended, by adding thereto a new article, designated §46A-2A-101, §46A-2A-102, §46A-2A-103, §46A-2A-104 and §46A-2A-105, all relating to the unauthorized access or acquisition of certain computerized data which compromises the security, confidentiality or integrity of personal information; requiring notification of a breach of the security

of a system compromising personal information; permitting internal notification procedures; noncompliance; enforcement by the Attorney General; civil penalties; violations by a licensed financial institution; and applicability.

*Be it enacted by the Legislature of West Virginia:*

That the Code of West Virginia, 1931, as amended, be amended by adding thereto a new article, designated §46A-2A-101, §46A-2A-102, §46A-2A-103, §46A-2A-104 and §46A-2A-105, all to read as follows:

**ARTICLE 2A. BREACH OF SECURITY OF CONSUMER INFORMATION.**

**§46A-2A-101. Definitions.**

- 1 As used in this article:
- 2 (1) "Breach of the security of a system" means the  
3 unauthorized access and acquisition of unencrypted  
4 and unredacted computerized data that compromises  
5 the security or confidentiality of personal information  
6 maintained by an individual or entity as part of a  
7 database of personal information regarding multiple  
8 individuals and that causes the individual or entity to  
9 reasonably believe that the breach of security has  
10 caused or will cause identity theft or other fraud to any  
11 resident of this state. Good faith acquisition of personal  
12 information by an employee or agent of an individual or  
13 entity for the purposes of the individual or the entity is  
14 not a breach of the security of the system, provided that  
15 the personal information is not used for a purpose other  
16 than a lawful purpose of the individual or entity or  
17 subject to further unauthorized disclosure.

18       (2) “Entity” includes corporations, business trusts,  
19 estates, partnerships, limited partnerships, limited  
20 liability partnerships, limited liability companies,  
21 associations, organizations, joint ventures,  
22 governments, governmental subdivisions, agencies or  
23 instrumentalities, or any other legal entity, whether for  
24 profit or not for profit.

25       (3) “Encrypted” means transformation of data  
26 through the use of an algorithmic process to into a form  
27 in which there is a low probability of assigning meaning  
28 without use of a confidential process or key or securing  
29 the information by another method that renders the  
30 data elements unreadable or unusable.

31       (4) “Financial institution” has the meaning given  
32 that term in Section 6809(3), United States Code Title  
33 15, as amended.

34       (5) “Individual” means a natural person.

35       (6) “Personal information” means the first name or  
36 first initial and last name linked to any one or more of  
37 the following data elements that relate to a resident of  
38 this state, when the data elements are neither encrypted  
39 nor redacted:

40       (A) Social security number;

41       (B) Driver’s license number or state identification  
42 card number issued in lieu of a driver’s license; or

43       (C) Financial account number, or credit card, or  
44 debit card number in combination with any required  
45 security code, access code or password that would

46 permit access to a resident's financial accounts.

47 The term does not include information that is lawfully  
48 obtained from publicly available information, or from  
49 federal, state or local government records lawfully  
50 made available to the general public.

51 (7) "Notice" means:

52 (A) Written notice to the postal address in the  
53 records of the individual or entity;

54 (B) Telephonic notice;

55 (C) Electronic notice, if the notice provided is  
56 consistent with the provisions regarding electronic  
57 records and signatures, set forth in Section 7001,  
58 United States Code Title 15, Electronic Signatures in  
59 Global and National Commerce Act.

60 (D) Substitute notice, if the individual or the entity  
61 required to provide notice demonstrates that the cost of  
62 providing notice will exceed fifty thousand dollars or  
63 that the affected class of residents to be notified  
64 exceeds one hundred thousand persons or that the  
65 individual or the entity does not have sufficient contact  
66 information or to provide notice as described in  
67 paragraph (A), (B) or (C). Substitute notice consists of  
68 any two of the following:

69 (i) E-mail notice if the individual or the entity has  
70 e-mail addresses for the members of the affected class  
71 of residents;

72 (ii) Conspicuous posting of the notice on the website

73 of the individual or the entity if the individual or the  
74 entity maintains a website; or

75 (iii) Notice to major statewide media.

76 (8) "Redact" means alteration or truncation of data  
77 such that no more than the last four digits of a social  
78 security number, driver's license number, state  
79 identification card number or account number is  
80 accessible as part of the personal information.

**§46A-2A-102. Notice of breach of security of computerized  
personal information.**

1 (a) An individual or entity that owns or licenses  
2 computerized data that includes personal information  
3 shall give notice of any breach of the security of the  
4 system following discovery or notification of the breach  
5 of the security of the system to any resident of this state  
6 whose unencrypted and unredacted personal  
7 information was or is reasonably believed to have been  
8 accessed and acquired by an unauthorized person and  
9 that causes, or the individual or entity reasonably  
10 believes has caused or will cause, identity theft or other  
11 fraud to any resident of this state. Except as provided  
12 in subsection (e) of this section or in order to take any  
13 measures necessary to determine the scope of the  
14 breach and to restore the reasonable integrity of the  
15 system, the notice shall be made without unreasonable  
16 delay.

17 (b) An individual or entity must give notice of the  
18 breach of the security of the system if encrypted  
19 information is accessed and acquired in an unencrypted  
20 form or if the security breach involves a person with

21 access to the encryption key and the individual or  
22 entity reasonably believes that such breach has caused  
23 or will cause identity theft or other fraud to any  
24 resident of this state.

25 (c) An individual or entity that maintains  
26 computerized data that includes personal information  
27 that the individual or entity does not own or license  
28 shall give notice to the owner or licensee of the  
29 information of any breach of the security of the system  
30 as soon as practicable following discovery, if the  
31 personal information was or the entity reasonably  
32 believes was accessed and acquired by an unauthorized  
33 person.

34 (d) The notice shall include:

35 (1) To the extent possible, a description of the  
36 categories of information that were reasonably believed  
37 to have been accessed or acquired by an unauthorized  
38 person, including social security numbers, driver's  
39 licenses or state identification numbers and financial  
40 data;

41 (2) A telephone number or website address that the  
42 individual may use to contact the entity or the agent of  
43 the entity and from whom the individual may learn:

44 (A) What types of information the entity maintained  
45 about that individual or about individuals in general;  
46 and

47 (B) Whether or not the entity maintained  
48 information about that individual.

49 (3) The toll-free contact telephone numbers and  
50 addresses for the major credit reporting agencies and  
51 information on how to place a fraud alert or security  
52 freeze.

53 (e) Notice required by this section may be delayed  
54 if a law-enforcement agency determines and advises the  
55 individual or entity that the notice will impede a  
56 criminal or civil investigation or homeland or national  
57 security. Notice required by this section must be made  
58 without unreasonable delay after the law-enforcement  
59 agency determines that notification will no longer  
60 impede the investigation or jeopardize national or  
61 homeland security.

62 (f) If an entity is required to notify more than one  
63 thousand persons of a breach of security pursuant to  
64 this article, the entity shall also notify, without  
65 unreasonable delay, all consumer reporting agencies  
66 that compile and maintain files on a nationwide basis,  
67 as defined by 15 U. S. C. §1681a (p), of the timing,  
68 distribution and content of the notices. Nothing in this  
69 subsection shall be construed to require the entity to  
70 provide to the consumer reporting agency the names or  
71 other personal identifying information of breach notice  
72 recipients. This subsection shall not apply to an entity  
73 who is subject to Title V of the Gramm Leach Bliley  
74 Act, 15 U. S. C. §6801, *et seq.*

75 (g) The notice required by this section shall not be  
76 considered a debt communication as defined by the Fair  
77 Debt Collection Practice Act in 15 U. S. C. §1692a.

**§46A-2A-103. Procedures deemed in compliance with security  
breach notice requirements.**



1 (a) An entity that maintains its own notification  
2 procedures as part of an information privacy or security  
3 policy for the treatment of personal information and  
4 that are consistent with the timing requirements of this  
5 article shall be deemed to be in compliance with the  
6 notification requirements of this article if it notifies  
7 residents of this state in accordance with its procedures  
8 in the event of a breach of security of the system.

9 (b) A financial institution that responds in  
10 accordance with the notification guidelines prescribed  
11 by the Federal Interagency Guidance on Response  
12 Programs for Unauthorized Access to Customer  
13 Information and Customer Notice is deemed to be in  
14 compliance with this article.

15 (c) An entity that complies with the notification  
16 requirements or procedures pursuant to the rules,  
17 regulation, procedures or guidelines established by the  
18 entity's primary or functional regulator shall be in  
19 compliance with this article.

**§46-2A-104. Violations.**

1 (a) Except as provided by subsection (c) of this  
2 section, failure to comply with the notice provisions of  
3 this article constitutes an unfair or deceptive act of  
4 practice in violation of section one hundred four, article  
5 six, chapter forty-six-a of this code, which may be  
6 enforced by the Attorney General pursuant to the  
7 enforcement provisions of this chapter.

8 (b) Except as provided by subsection (c) of this  
9 section, the Attorney General shall have exclusive  
10 authority to bring action. No civil penalty may be

11 assessed in an action unless the court finds that the  
12 defendant has engaged in a course of repeated and  
13 willful violations of this article. No civil penalty shall  
14 exceed one hundred fifty thousand dollars per breach  
15 of security of the system or series of breaches of a  
16 similar nature that are discovered in a single  
17 investigation.

18 (c) A violation of this article by a licensed financial  
19 institution shall be enforceable exclusively by the  
20 financial institution's primary functional regulator.

**§46A-2A-105. Applicability.**

1 This article shall apply to the discovery or  
2 notification of a breach of the security of the system  
3 that occurs on or after the effective date of this article.



Enr. Com. Sub. for S. B. No. 340] 10

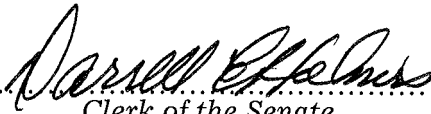
The Joint Committee on Enrolled Bills hereby certifies that the foregoing bill is correctly enrolled.

  
.....  
Chairman Senate Committee

  
.....  
Chairman House Committee

Originated in the Senate.

In effect ninety days from passage.

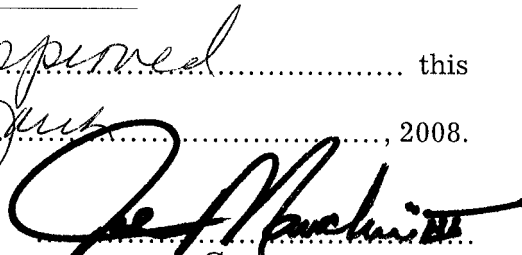
  
.....  
Clerk of the Senate

  
.....  
Clerk of the House of Delegates

  
.....  
President of the Senate

  
.....  
Speaker House of Delegates

The within *is approved* ..... this  
the *2<sup>th</sup>* Day of *June* ....., 2008.

  
.....  
Governor

PRESENTED TO THE  
GOVERNOR

MAR 18 2008

Time

3:05 p.