S.C. Code Ann. § 39-1-90

This document is current through 2024 Regular Session Act No. 120, not including changes and corrections made by the Code Commissioner.

§ 39-1-90. Breach of security of business data; notification; definitions; penalties; exception as to certain banks and financial institutions; notice to Consumer Protection Division.

(A) A person conducting business in this State, and owning or licensing computerized data or other data that includes personal identifying information, shall disclose a breach of the security of the system following discovery or notification of the breach in the security of the data to a resident of this State whose personal identifying information that was not rendered unusable through encryption, redaction, or other methods was, or is reasonably believed to have been, acquired by an unauthorized person when the illegal use of the information has occurred or is reasonably likely to occur or use of the information creates a material risk of harm to the resident. The disclosure must be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement, as provided in subsection (C), or with measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system.

(B) A person conducting business in this State and maintaining computerized data or other data that includes personal identifying information that the person does not own shall notify the owner or licensee of the information of a breach of the security of the data immediately following discovery, if the personal identifying information was, or is reasonably believed to have been, acquired by an unauthorized person.

(C) The notification required by this section may be delayed if a law enforcement agency determines that the notification impedes a criminal investigation. The notification required by this section must be made after the law enforcement agency determines that it no longer compromises the investigation.

(D) For purposes of this section:

(1) "Breach of the security of the system" means unauthorized access to and acquisition of computerized data that was not rendered unusable through encryption, redaction, or other methods that compromises the security, confidentiality, or integrity of personal identifying information maintained by the person, when illegal use of the information has occurred or is reasonably likely to occur or use of the information creates a material risk of harm to a resident. Good faith acquisition of personal identifying information by an employee or agent of

the person for the purposes of its business is not a breach of the security of the system if the personal identifying information is not used or subject to further unauthorized disclosure.

(2) "Person" has the same meaning as in Section 37-20-110(10).

(3) "Personal identifying information" means the first name or first initial and last name in combination with and linked to any one or more of the following data elements that relate to a resident of this State, when the data elements are neither encrypted nor redacted:

(a) social security number;

(b) driver's license number or state identification card number issued instead of a driver's license;

(c) financial account number, or credit card or debit card number in combination with any required security code, access code, or password that would permit access to a resident's financial account; or

(d) other numbers or information which may be used to access a person's financial accounts or numbers or information issued by a governmental or regulatory entity that uniquely will identify an individual.

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

(E) The notice required by this section may be provided by:

(1) written notice;

(2) electronic notice, if the person's primary method of communication with the individual is by electronic means or is consistent with the provisions regarding electronic records and signatures in Section 7001 of Title 15 USC and Chapter 6, Title 11 of the 1976 Code;

(3) telephonic notice; or

(4) substitute notice, if the person demonstrates that the cost of providing notice exceeds two hundred fifty thousand dollars or that the affected class of subject persons to be notified exceeds five hundred thousand or the person has insufficient contact information. Substitute notice consists of:

(a) e-mail notice when the person has an e-mail address for the subject persons;

(b) conspicuous posting of the notice on the web site page of the person, if the person maintains one; or

(c) notification to major statewide media.

(F) Notwithstanding subsection (E), a person that maintains its own notification procedures as part of an information security policy for the treatment of personal identifying information and is otherwise consistent with the timing requirements of this section is considered to be in compliance with the notification requirements of this section if the person notifies subject persons in accordance with its policies in the event of a breach of security of the system.

(G) A resident of this State who is injured by a violation of this section, in addition to and cumulative of all other rights and remedies available at law, may:

(1) institute a civil action to recover damages in case of a wilful and knowing violation;

(2) institute a civil action that must be limited to actual damages resulting from a violation in case of a negligent violation of this section;

(3) seek an injunction to enforce compliance; and

(4) recover attorney's fees and court costs, if successful.

(H) A person who knowingly and wilfully violates this section is subject to an administrative fine in the amount of one thousand dollars for each resident whose information was accessible by reason of the breach, the amount to be decided by the Department of Consumer Affairs.

(I) This section does not apply to a bank or financial institution that is subject to and in compliance with the privacy and security provision of the Gramm-Leach-Bliley Act.

(J) A financial institution that is subject to and in compliance with the federal Interagency Guidance Response Programs for Unauthorized Access to Consumer Information and Customer Notice, issued March 7, 2005, by the Board of Governors of the Federal Reserve System, the Federal Deposit Insurance Corporation, the Office of the Comptroller of the Currency, and the Office of Thrift Supervision, as amended, is considered to be in compliance with this section.

(K) If a business provides notice to more than one thousand persons at one time pursuant to this section, the business shall notify, without unreasonable delay, the Consumer Protection Division of the Department of Consumer Affairs and all consumer reporting agencies that compile and maintain files on a nationwide basis, as defined in 15 USC Section 1681a(p), of the timing, distribution, and content of the notice.

History

2008 Act No. 190, § 7.A, eff July 1, 2009; 2013 Act No. 15, § 3, eff April 23, 2013.

End of Document