

Senate Bill 251

By: Senators Shafer of the 48th, Hamrick of the 30th, Heath of the 31st, Zamarripa of the 36th, Staton of the 18th and others

A BILL TO BE ENTITLED
AN ACT

1 To amend Chapter 1 of Title 10 of the Official Code of Georgia Annotated, relating to selling
2 and other trade practices, so as to provide a short title; to provide legislative findings; to
3 provide definitions; to require certain business entities to give notice to consumers of certain
4 security breaches; to provide for causes of actions and damages for unauthorized or improper
5 access of personal information of consumers; to provide for certain criminal penalties; to
6 provide for related matters; to provide an effective date; to repeal conflicting laws; and for
7 other purposes.

8 **BE IT ENACTED BY THE GENERAL ASSEMBLY OF GEORGIA:**

9 **SECTION 1.**

10 Chapter 1 of Title 10 of the Official Code of Georgia Annotated, relating to selling and other
11 trade practices, is amended by adding a new Article 34 to read as follows:

12 **"ARTICLE 34**

13 10-1-910.

14 This article shall be known and may be cited as the 'Data Base Privacy and Anti-identity
15 Theft Act.'

16 10-1-911.

17 The General Assembly finds that:

18 (1) The privacy and financial security of individuals is increasingly at risk due to the ever
19 more widespread collection of personal information by both the public and private sectors.

20 (2) Credit card transactions, magazine subscriptions, telephone numbers, real estate
21 records, automobile registrations, consumer surveys, warranty registrations, credit reports,
22 and Internet websites are all sources of personal information and form the source material
23 for identity thieves.

1 (3) Identity theft is one of the fastest growing crimes committed in Georgia. Criminals
2 who steal personal information, such as social security numbers, use the information to
3 open credit card accounts, write bad checks, buy cars, and commit other financial crimes
4 with other people's identities.

5 (4) Identity theft is costly to the marketplace and to consumers.

6 (5) Victims of identity theft must act quickly to minimize the damage. Therefore,
7 expeditious notification of possible misuse of a person's personal information is
8 imperative.

9 10-1-912.

10 As used in this article, the term:

11 (1) 'Breach of the security of the system' means unauthorized acquisition of a consumer's
12 file or computerized data that compromises the security, confidentiality, or integrity of
13 personal information of such consumer maintained by a business entity. Good faith
14 acquisition of personal information by an employee or agent of the business entity for the
15 purposes of the business entity is not a breach of the security of the system, provided that
16 the personal information is not used or subject to further unauthorized disclosure.

17 (2) 'Business entity' means any person or entity who, for profit, engages in a trade or
18 business but does not include any governmental agency whose records are maintained
19 primarily for traffic safety, law enforcement, or licensing purposes.

20 (3) 'Consumer' means a natural individual.

21 (4) 'File,' when used in connection with information on any consumer, means all of the
22 information on that consumer recorded, retained, or maintained by a business entity
23 regardless of how the information is stored.

24 (5) 'Notice' means:

25 (A) Written notice;

26 (B) Electronic notice, if the notice provided is consistent with the provisions regarding
27 electronic records and signatures set forth in Section 7001 of Title 15 of the United
28 States Code; or

29 (C) Substitute notice, if the business entity demonstrates that the cost of providing
30 notice would exceed \$250,000.00, that the affected class of persons to be notified
31 exceeds 500,000, or that the business entity does not have sufficient contact information
32 to provide written or electronic notice to such persons. Substitute notice shall consist
33 of all of the following:

34 (i) E-mail notice when the business entity has an e-mail address for the persons to be
35 notified;

1 (ii) Conspicuous posting of the notice on the business entity's website page, if the
2 business entity maintains one; and

3 (iii) Notification to major state-wide media.

4 Notwithstanding any provision of this paragraph to the contrary, a business entity that
5 maintains its own notification procedures as part of an information security policy for the
6 treatment of personal information and is otherwise consistent with the timing
7 requirements of this article shall be deemed to be in compliance with the notification
8 requirements of this article if it notifies the persons who are the subjects of the notice in
9 accordance with its policies in the event of a breach of the security of the system.

10 (6) 'Person' means any individual, partnership, corporation, limited liability company,
11 trust, estate, cooperative, association, or other entity. The term 'person' as used in this
12 article shall not be construed to require duplicative reporting by any individual,
13 corporation, trust, estate, cooperative, association, or other entity involved in the same
14 transaction.

15 (7) 'Personal information' means a consumer's first name or first initial and last name in
16 combination with any one or more of the following data elements, when either the name
17 or the data elements are not encrypted:

18 (A) Social security number;

19 (B) Driver's license number of a consumer or number of a consumer's identification
20 card issued pursuant to Article 5 of Chapter 5 of Title 40; or

21 (C) Account number or credit or debit card number, in combination with any required
22 security code, access code, or password that would permit access to a consumer's
23 financial account.

24 The term 'personal information' does not include publicly available information that is
25 lawfully made available to the general public from federal, state, or local government
26 records.

27 (8) 'Unauthorized electronic access' means the accessing of personal information on
28 consumers maintained by a business entity by any electronic means without the express
29 permission or authorization of the business entity.

30 (9) 'Unauthorized person' means any person who does not have authority or permission
31 of a business entity to access personal information on consumers maintained by such
32 business entity or who obtains access to such information by fraud, misrepresentation,
33 subterfuge, or similar deceptive practices.

34 10-1-913.

35 (a) Any business entity that collects, assembles, maintains, or compiles files or
36 computerized data that include personal information of consumers shall disclose any breach

1 of the security of the system following discovery or notification of the breach in the
2 security of the data to any resident of this state whose unencrypted personal information
3 or file was, or is reasonably believed to have been, acquired by an unauthorized person.
4 The disclosure shall be made in the most expedient time possible and without unreasonable
5 delay, consistent with the legitimate needs of law enforcement, as provided in subsection
6 (c) of this Code section, or any measures necessary to determine the scope of the breach
7 and restore the reasonable integrity of the data system.

8 (b) Any business entity that maintains computerized data that includes personal
9 information that the business entity does not own shall notify the owner or licensee of the
10 information of any breach of the security of the data immediately following discovery, if
11 the personal information was, or is reasonably believed to have been, acquired by an
12 unauthorized person.

13 (c) The notification required by this Code section may be delayed if a law enforcement
14 agency determines that the notification will impede a criminal investigation. The
15 notification required by this Code section shall be made after the law enforcement agency
16 determines that it will not compromise the investigation.

17 10-1-914.

18 A business entity shall have a cause of action against any person that gains access to such
19 business entity's files or computerized data containing personal information on consumers
20 through fraud, misrepresentation, subterfuge, or similar deceptive practices or by
21 unauthorized electronic access. Such business entity shall be authorized to recover all
22 damages incurred by such business entity as a result of such improper access, including all
23 costs of making the notifications required by Code Section 10-1-911, and reasonable
24 attorney's fees.

25 10-1-915.

26 It shall be unlawful for any person to access or attempt to access personal information of
27 consumers maintained by a business entity through fraud, misrepresentation, subterfuge,
28 or similar deceptive practices or by unauthorized electronic access. Upon conviction, a
29 person who violates this Code section shall be imprisoned for not less than one nor more
30 than ten years, pay a fine not to exceed \$100,000.00, or both."

31 **SECTION 2.**

32 This Act shall become effective upon its approval by the Governor or upon its becoming law
33 without such approval.

1

SECTION 3.

2 All laws and parts of laws in conflict with this Act are repealed.