House Bill 499

By: Representative Gilligan of the 24th

A BILL TO BE ENTITLED

AN ACT

To amend Article 34 of Chapter 1 of Title 10 of the Official Code of Georgia Annotated, relating to identity theft, so as to enact the "Georgia Personal Data Security Act"; to improve systems and procedures for providing and regulating notifications of data beaches affecting Georgia residents; to revise legislative findings and declarations; to modify definitions; to modify when notices of certain security breaches are required and to provide for the contents of such notices; to require certain entities to maintain certain data security procedures; to require that certain notices of a data breach be sent to certain officials of this state; to provide for enforcement by the Attorney General; to provide for civil penalties; to provide for designations; to provide for related matters; to repeal conflicting laws; and for other purposes.

BE IT ENACTED BY THE GENERAL ASSEMBLY OF GEORGIA:

SECTION 1.

Article 34 of Chapter 1 of Title 10 of the Official Code of Georgia Annotated, relating to identity theft, is amended by revising Code Sections 10-1-910 through 10-1-912 and designating the same as Part 1 of said article and by adding new Code Sections 10-1-912.1 through 10-1-912.4 at the end of said part to read as follows:

"Part 1

10-1-910.

This part shall be known and may be cited as the 'Georgia Personal Data Security Act.'

10-1-910.1.

The General Assembly finds and declares as follows:

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

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

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

(4) Implementation of technology security plans and security software as part of an information security policy may provide protection to consumers and the general public from identity thieves;

(5) Information brokers should clearly define the standards for authorized users of its data so that a breach by an unauthorized user is easily identifiable;

(6) Identity theft is costly to the marketplace and to consumers; and

(7) Victims of identity theft must act quickly to minimize the damage; therefore, expeditious notification of unauthorized acquisition and possible misuse of ~~a person's~~ an individual's personal information is imperative.

10-1-911.

As used in this ~~article~~ part, the term:

(1) 'Breach of the security of the system' means unauthorized acquisition of ~~an individual's electronic~~ data that compromises the security, confidentiality, or integrity of personal information of ~~such~~ an individual maintained by ~~an information broker or data collector~~ a covered entity. Good faith acquisition ~~or use~~ of personal information by an employee or agent of ~~an information broker or data collector for the purposes of such information broker or data collector~~ a covered entity for a legitimate purpose of the covered entity is not a breach of the security of the system, provided that the personal information is not used for a purpose unrelated to the business or subject to further unauthorized disclosure.

(2) 'Covered entity' means a data collector, sole proprietorship, partnership, corporation, trust, estate, cooperative, association, or other commercial entity that acquires, maintains, stores, or uses personal information; provided, however, that an entity's status as public, private, for profit, or nonprofit shall not affect its designation as a covered entity.

~~(2)~~(3) 'Data collector' means any state or local agency or subdivision thereof, including any department, bureau, authority, public university or college, academy, commission, or other government entity~~; provided, however, that the term 'data collector' shall not include any governmental agency whose records are maintained primarily for traffic safety, law enforcement, or licensing purposes or for purposes of providing public access to court records or to real or personal property information~~.

~~(3) 'Information broker' means any person or entity who, for monetary fees or dues, engages in whole or in part in the business of collecting, assembling, evaluating, compiling, reporting, transmitting, transferring, or communicating information concerning individuals for the primary purpose of furnishing personal information to nonaffiliated third parties, but does not include any governmental agency whose records are maintained primarily for traffic safety, law enforcement, or licensing purposes.~~

(4) 'Encrypted' means transformed as data through the use of an algorithmic process into a form in which there is a low probability of assigning meaning without use of a confidential process or key or secured by another method that renders the data unreadable or unusable.

~~(4)~~(5) 'Notice' means:

(A) Written notice to an individual's mailing address listed in the records of the covered entity;

(B) Telephone notice;

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

(D) Substitute notice, if the ~~information broker or data collector~~ covered entity demonstrates that the cost of providing notice would exceed ~~$50,000.00~~ $250,000.00, that the affected class of individuals to be notified exceeds ~~100,000~~ 500,000, or that the ~~information broker or data collector~~ covered entity does not have sufficient contact information to provide written or electronic notice to such individuals. Substitute notice shall consist of all of the following:

(i) E-mail notice~~, if the information broker or data collector~~ to each individual for whom the covered entity has an e-mail address ~~for the individuals to be notified~~;

(ii) Conspicuous posting of the notice on the ~~information broker's or data collector's~~ covered entity's website ~~page~~, if the ~~information broker or data collector~~ covered entity maintains one; and

(iii) Notification to major state-wide media;

provided, however, that in cases involving personal information of a minor, notice shall be made to the minor's parents or legal guardian. ~~Notwithstanding any provision of this~~

~~paragraph to the contrary, an information broker or data collector that maintains its own notification procedures as part of an information security policy for the treatment of personal information and is otherwise consistent with the timing requirements of this article shall be deemed to be in compliance with the notification requirements of this article if it notifies the individuals who are the subjects of the notice in accordance with its policies in the event of a breach of the security of the system.~~

~~(5) 'Person' means any individual, partnership, corporation, limited liability company, trust, estate, cooperative, association, or other entity. The term 'person' as used in this article shall not be construed to require duplicative reporting by any individual, corporation, trust, estate, cooperative, association, or other entity involved in the same transaction.~~

(6) 'Personal information' means ~~an individual's first name or first initial and last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted or redacted~~:

(A) ~~Social~~ A social security number that is not encrypted or redacted; or

(B) An individual's first and last name or first initial and last name in combination with one or more of the following data elements that are not encrypted or redacted:

~~(B)~~(i) Driver's license number, ~~or~~ state identification card number, passport number, military identification number, or other similar number issued on a government document used to verify identity;

~~(C)~~(ii) Account number, credit card number, or debit card number, if circumstances exist wherein such a number could be used without additional identifying information, access codes, or passwords;

~~(D)~~(iii) Account passwords or personal identification numbers or other access codes; ~~or~~

(iv) Student information, including grades, disciplinary history, and standardized test scores;

(v) Information related to medical treatment, diagnosis, or history;

(vi) An individual's health insurance policy number or subscriber identification number and any unique identifier used by a health insurer to identify the individual; or

~~(E)~~(vii) Any of the items contained in ~~subparagraphs (A) through (D) of this paragraph~~ divisions (i) through (vi) of this subparagraph when not in connection with the individual's first and last name or first initial and last name, if the information compromised would be sufficient to perform or attempt to perform identity theft against the ~~person~~ individual whose information was compromised.

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

(7) 'Redacted' means rendered as data to be unreadable or truncated so that no more than the last four digits of an identification number are accessible as part of the data.

(8) 'Third-party agent' means an individual or entity that has been contracted to maintain, store, or process personal information for or on behalf of a covered entity.

10-1-912.

(a) ~~Any information broker or data collector that maintains computerized data that includes personal information of individuals shall give notice of any breach of the security of the system following discovery or notification of the breach in the security of the data to any resident of this state whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person. The notice shall 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) of this Code section, or with any measures necessary to determine the scope of the breach and restore the reasonable integrity, security, and confidentiality of the data system.~~ A covered entity that maintains physical or computerized data that include personal information of individuals shall give notice of a breach of the security of the system to any resident of this state whose personal information was, or is reasonably believed to have been, accessed as a result of such breach. Such notice shall be made as expeditiously as practicable and without unreasonable delay, taking into account the time necessary to allow the covered entity to determine the scope of such breach, to identify individuals affected by such breach, and to restore the reasonable integrity of the data system that was breached, but no later than 45 days after the determination of such breach or reason to believe such breach occurred, unless subject to a delay authorized under subsection (c) of this Code section.

(b) ~~Any person or business that maintains computerized data on behalf of an information broker or data collector that includes personal information of individuals that the person or business does not own shall notify the information broker or data collector of any breach of the security of the system within 24 hours following discovery, if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person.~~ In the event of a breach of the security of the system, which system is maintained by a third-party agent for a covered entity, the third-party agent shall notify the covered entity of such breach as expeditiously as practicable but no later than 72 hours after the determination of such breach or reason to believe such breach has occurred. The third-party agent shall provide the covered entity with all information that the covered

entity needs to comply with its notice requirements under this Code section and Code Section 10-1-912.2.

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

(d)(1) Notwithstanding any provision of this part to the contrary, a covered entity that maintains its own notification procedures as part of an information security policy for the treatment of personal information shall be deemed to be in compliance with the notification requirements of this part if such covered entity notifies the individuals who are the subjects of the notice in accordance with its policies in the event of a breach of the security of the system.

(2) A covered entity that is regulated pursuant to a state or federal law and that maintains and follows procedures for a breach of the security of the system pursuant to the laws, rules, regulations, guidance, or guidelines established by a state or federal regulator is deemed to be in compliance with this part.

(3) Notwithstanding subsection (a) of this Code section, notice to individuals whose personal information has been accessed is not required if, after an appropriate investigation and consultation with relevant federal, state, or local law enforcement agencies, the covered entity reasonably determines that a breach of the security of the system has not and will not likely result in identity theft or any other financial harm to such individuals. Such a determination must be documented in writing and maintained for at least five years. The covered entity shall provide the written determination to the Attorney General within 30 days after the determination not to notify has been made.

~~(d)~~(4) In the event that ~~an information broker or data collector~~ a covered entity discovers circumstances requiring notification pursuant to this Code section of more than ~~10,000~~ 1,000 residents of this state at one time, the ~~information broker or data collector~~ covered entity shall also notify, without unreasonable delay, all consumer reporting agencies that compile and maintain files on consumers on a nation-wide basis, as defined by 15 U.S.C. Section 1681a, of the timing, distribution, and content of the notices.

10-1-912.1.

Each notice to an individual shall be titled 'Notice of Data Breach' and shall include the following:

(1) The date, estimated date, or estimated date range of the breach of the security of the system, if such information is possible to determine at the time the notice is provided;

(2) How data were accessed, if such information is possible to determine at the time the notice is provided;

(3) What data were or are reasonably believed to have been accessed;

(4) What potential harm may arise;

(5) Ways in which the individual may seek to reduce or eliminate harm;

(6) A telephone number where the individual may obtain additional information related to such breach; and

(7) The toll-free telephone numbers and addresses of the major credit reporting agencies.

10-1-912.2.

(a) For any breach of the security of the system for which notice to an individual is required under this part, a covered entity shall provide written notice to the Attorney General and the Governor that shall include:

(1) A copy of each notice to an individual required under this part;

(2) The number of individuals who are residents of this state and were or potentially have been affected by such breach;

(3) Any services related to such breach being offered or scheduled to be offered, without charge, by the covered entity to individuals; and

(4) The name, address, telephone number, and e-mail address of the employee or agent of the covered entity from whom additional information may be obtained about such breach.

(b) As provided for under subsection (a) of this Code section, a covered entity shall, upon request, provide the following information to the Attorney General or Governor:

(1) A police report, incident report, or computer forensics report;

(2) A copy of the policies in place regarding a breach of the security of the system; and

(3) Steps that have been taken to remedy the breach of the security of the system.

10-1-912.3.

Each covered entity shall maintain reasonable safeguards to protect and secure personal information.

10-1-912.4.

(a) The Attorney General shall be authorized to enforce the provisions of this part.

(b) The Attorney General shall have the authority to investigate alleged violations of this part, including all investigative powers available under Part 2 of Article 15 of this chapter, the 'Fair Business Practices Act of 1975,' including, but not limited to, the power to issue investigative demands and subpoenas as provided in Code Sections 10-1-403 and 10-1-404.

(c) If the Attorney General determines, after notice and hearing, that a covered entity has violated this part, the Attorney General may take any or all of the following actions:

(1) Issue an administrative order imposing a civil penalty not to exceed $500.00 for each resident of this state who did not receive the required notice, provided that the total civil penalty shall not exceed $250,000.00 per each breach of the security of the system;

(2) Issue an order compelling the covered entity to provide any notice required under this part; or

(3) Issue an order providing for the recovery of the Attorney General's reasonable costs in maintaining the action.

(d) Any hearing and administrative review in connection with alleged violations of this part shall be conducted in accordance with the procedure for contested cases pursuant to Chapter 13 of Title 50, the 'Georgia Administrative Procedure Act.' Any covered entity that has exhausted all administrative remedies available and is aggrieved or adversely affected by a final order or action of the Attorney General shall have the right of judicial review in accordance with such chapter.

(e) The Attorney General may file in the superior court of the county in which the covered entity maintains its principal place of business a certified copy of or the final order of the Attorney General, whether or not the order was appealed. Thereafter, the court shall render a judgment in accordance with the order and notify the parties. The judgment shall have the same effect as a judgment rendered by the court.

(f) Without regard as to whether the Attorney General has issued any orders under this Code section, upon a showing by the Attorney General in any superior court of competent jurisdiction that a covered entity has violated or is about to violate this part, a rule promulgated under this part, or an order of the Attorney General, the court may enter or grant any or all of the following relief:

(1) A civil penalty not to exceed $500.00 for each resident of this state who did not receive the required notice, provided that the total civil penalty shall not exceed $250,000.00 per each breach of the security of the system;

(2) An order compelling the covered entity to provide any notice required under this part;

(3) An order providing for the recovery of the Attorney General's reasonable costs in maintaining the action; and

(4) Other relief the court deems just and reasonable.

(g) Except as otherwise expressly provided in this Code section, nothing in this Code section shall be construed to restrict or expand any other authority or jurisdiction of the Attorney General.

(h) Nothing in this part either creates a private right of action or affects any private right of action existing under other law, including, but not limited to, under contract or tort.

(i) No provision of this part shall constitute a waiver of sovereign immunity.

(j) The provisions of this part are not exclusive and do not relieve a covered entity from compliance with all other applicable provisions of law."

SECTION 2.

Said article is further amended by designating Code Sections 10-1-913 through 10-1-915 as Part 2 of said article.

SECTION 3.

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