

Article - Commercial Law

[Previous][Next]

§14–3504.

(a) In this section:

(1) “Breach of the security of a system” means the unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of the personal information maintained by a business; and

(2) “Breach of the security of a system” does not include the good faith acquisition of personal information by an employee or agent of a business for the purposes of the business, provided that the personal information is not used or subject to further unauthorized disclosure.

(b) (1) A business that owns or licenses computerized data that includes personal information of an individual residing in the State, when it discovers or is notified of a breach of the security of a system, shall conduct in good faith a reasonable and prompt investigation to determine the likelihood that personal information of the individual has been or will be misused as a result of the breach.

(2) If, after the investigation is concluded, the business determines that misuse of the individual’s personal information has occurred or is reasonably likely to occur as a result of a breach of the security of a system, the business shall notify the individual of the breach.

(3) Except as provided in subsection (d) of this section, the notification required under paragraph (2) of this subsection shall be given as soon as reasonably practicable after the business conducts the investigation required under paragraph (1) of this subsection.

(4) If after the investigation required under paragraph (1) of this subsection is concluded, the business determines that notification under paragraph (2) of this subsection is not required, the business shall maintain records that reflect its determination for 3 years after the determination is made.

(c) (1) A business that maintains computerized data that includes personal information that the business does not own or license shall notify the owner or licensee of the personal information of a breach of the security of a system if it is likely that the breach has resulted or will result in the misuse of personal information of an individual residing in the State.

(2) Except as provided in subsection (d) of this section, the notification required under paragraph (1) of this subsection shall be given as soon as reasonably practicable after the business discovers or is notified of the breach of the security of a system.

(3) A business that is required to notify an owner or licensee of personal information of a breach of the security of a system under paragraph (1) of this subsection shall share with the owner or licensee information relative to the breach.

(d) (1) The notification required under subsections (b) and (c) of this section may be delayed:

(i) If a law enforcement agency determines that the notification will impede a criminal investigation or jeopardize homeland or national security; or

(ii) To determine the scope of the breach of the security of a system, identify the individuals affected, or restore the integrity of the system.

(2) If notification is delayed under paragraph (1)(i) of this subsection, notification shall be given as soon as reasonably practicable after the law enforcement agency determines that it will not impede a criminal investigation and will not jeopardize homeland or national security.

(e) The notification required under subsections (b) and (c) of this section may be given:

(1) By written notice sent to the most recent address of the individual in the records of the business;

(2) By electronic mail to the most recent electronic mail address of the individual in the records of the business, if:

(i) The individual has expressly consented to receive electronic notice; or

(ii) The business conducts its business primarily through Internet account transactions or the Internet;

(3) By telephonic notice, to the most recent telephone number of the individual in the records of the business; or

(4) By substitute notice as provided in subsection (f) of this section, if:

(i) The business demonstrates that the cost of providing notice would exceed \$100,000 or that the affected class of individuals to be notified exceeds 175,000; or

(ii) The business does not have sufficient contact information to give notice in accordance with item (1), (2), or (3) of this subsection.

(f) Substitute notice under subsection (e)(4) of this section shall consist of:

(1) Electronically mailing the notice to an individual entitled to

notification under subsection (b) of this section, if the business has an electronic mail address for the individual to be notified;

(2) Conspicuous posting of the notice on the Web site of the business, if the business maintains a Web site; and

(3) Notification to statewide media.

(g) The notification required under subsection (b) of this section shall include:

(1) To the extent possible, a description of the categories of information that were, or are reasonably believed to have been, acquired by an unauthorized person, including which of the elements of personal information were, or are reasonably believed to have been, acquired;

(2) Contact information for the business making the notification, including the business' address, telephone number, and toll-free telephone number if one is maintained;

(3) The toll-free telephone numbers and addresses for the major consumer reporting agencies; and

(4) (i) The toll-free telephone numbers, addresses, and Web site addresses for:

1. The Federal Trade Commission; and
2. The Office of the Attorney General; and

(ii) A statement that an individual can obtain information from these sources about steps the individual can take to avoid identity theft.

(h) Prior to giving the notification required under subsection (b) of this section and subject to subsection (d) of this section, a business shall provide notice of a breach of the security of a system to the Office of the Attorney General.

(i) A waiver of any provision of this section is contrary to public policy and is void and unenforceable.

(j) Compliance with this section does not relieve a business from a duty to comply with any other requirements of federal law relating to the protection and privacy of personal information.

[Previous][Next]