AN ACT concerning business.

Be it enacted by the People of the State of Illinois, represented in the General Assembly:

Section 1. Short title. This Act may be cited as the Personal Information Protection Act.

Section 5. Definitions. In this Act:

"Data Collector" may include, but is not limited to, government agencies, public and private universities, privately and publicly held corporations, financial institutions, retail operators, and any other entity that, for any purpose, handles, collects, disseminates, or otherwise deals with nonpublic personal information.

"Breach of the security of the system data" means unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by the data collector. "Breach of the security of the system data" does not include good faith acquisition of personal information by an employee or agent of the data collector for a legitimate purpose of the data collector, provided that the personal information is not used for a purpose unrelated to the data collector's business or subject to further unauthorized disclosure.

"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:

(1) Social Security number.

(2) Driver's license number or State identification card number.

(3) Account number or credit or debit card number, or an account number or credit card number in combination with any required security code, access code, or password that

would permit access to an individual's financial account. "Personal information" does not include publicly available information that is lawfully made available to the general public from federal, State, or local government records.

Section 10. Notice of Breach.

(a) Any data collector that owns or licenses personal information concerning an Illinois resident shall notify the resident that there has been a breach of the security of the system data following discovery or notification of the breach. The disclosure notification shall be made in the most expedient time possible and without unreasonable delay, consistent with any measures necessary to determine the scope of the breach and restore the reasonable integrity, security, and confidentiality of the data system.

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

(c) For purposes of this Section, notice to consumers may be provided by one of the following methods:

(1) written notice;

(2) electronic notice, if the notice provided is consistent with the provisions regarding electronic records and signatures for notices legally required to be in writing as set forth in Section 7001 of Title 15 of the United States Code; or

(3) substitute notice, if the data collector demonstrates that the cost of providing notice would exceed $250,000 or that the affected class of subject persons to be notified exceeds 500,000, or the data collector does not have sufficient contact information. Substitute notice shall consist of all of the following: (i) email notice if

the data collector has an email address for the subject persons; (ii) conspicuous posting of the notice on the data collector's web site page if the data collector maintains one; and (iii) notification to major statewide media.

(d) Notwithstanding subsection (c), a 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 Act, shall be deemed in compliance with the notification requirements of this Section if the data collector notifies subject persons in accordance with its policies in the event of a breach of the security of the system data.

Section 15. Waiver. Any waiver of the provisions of this Act is contrary to public policy and is void and unenforceable.

Section 20. Violation. A violation of this Act constitutes an unlawful practice under the Consumer Fraud and Deceptive Business Practices Act.

Section 900. The Consumer Fraud and Deceptive Business Practices Act is amended by changing Section 2Z as follows:

(815 ILCS 505/2Z) (from Ch. 121 1/2, par. 262Z)

Sec. 2Z. Violations of other Acts. Any person who knowingly violates the Automotive Repair Act, the Home Repair and Remodeling Act, the Dance Studio Act, the Physical Fitness Services Act, the Hearing Instrument Consumer Protection Act, the Illinois Union Label Act, the Job Referral and Job Listing Services Consumer Protection Act, the Travel Promotion Consumer Protection Act, the Credit Services Organizations Act, the Automatic Telephone Dialers Act, the Pay-Per-Call Services Consumer Protection Act, the Telephone Solicitations Act, the Illinois Funeral or Burial Funds Act, the Cemetery Care Act, the Safe and Hygienic Bed Act, the Pre-Need Cemetery

Sales Act, the High Risk Home Loan Act, subsection (a) or (b) of Section 3-10 of the Cigarette Tax Act, subsection (a) or (b) of Section 3-10 of the Cigarette Use Tax Act, the Electronic Mail Act, paragraph (6) of subsection (k) of Section 6-305 of the Illinois Vehicle Code, ~~or~~ the Automatic Contract Renewal Act, or the Personal Information Protection Act commits an unlawful practice within the meaning of this Act.

(Source: P.A. 92-426, eff. 1-1-02; 93-561, eff. 1-1-04; 93-950, eff. 1-1-05.)