Minnesota Annotated Statutes
Chapter 325E – Trade Practices

§ 325E.61 Data Warehouses; Notice Required For Certain Disclosures

Subdivision 1. Disclosure of personal information; notice required.

(a) Any person or business that conducts business in this state, and that owns or licenses data that includes personal information, shall disclose 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 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 paragraph (c), or with any measures necessary to determine the scope of the breach, identify the individuals affected, and restore the reasonable integrity of the data system.

(b) Any person or business that maintains data that includes personal information that the person or business does not own 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) The notification required by this section and section 13.055, subdivision 6, may be delayed to a date certain if a law enforcement agency affirmatively determines that the notification will impede a criminal investigation.

(d) For purposes of this section and section 13.055, subdivision 6, "breach of the security of the system" means unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by the person or business. Good faith acquisition of personal information by an employee or agent of the person or business for the purposes of the person or business is not a breach of the security system, provided that the personal information is not used or subject to further unauthorized disclosure.

(e) For purposes of this section and section 13.055, subdivision 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 the data element is not secured by encryption or another method of technology that makes electronic data unreadable or unusable, or was secured and the encryption key, password, or other means necessary for reading or using the data was also acquired:

(1) Social Security number;

(2) driver's license number or Minnesota identification card number; or

(3) account number or credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account.

(f) For purposes of this section and section 13.055, subdivision 6, "personal information" does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records.

(g) For purposes of this section and section 13.055, subdivision 6, "notice" may be provided by one of the following methods:

(1) written notice to the most recent available address the person or business has in its records;

(2) electronic notice, if the person's primary method of communication with the individual is by electronic means, or if the notice provided is consistent with the provisions regarding electronic records and signatures in United States Code, title 15, section 7001; or

(3) substitute notice, if the person or business 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 person or business does not have sufficient contact information. Substitute notice must consist of all of the following:

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

(ii) conspicuous posting of the notice on the Web site page of the person or business, if the person or business maintains one; and

(iii) notification to major statewide media.

(h) Notwithstanding paragraph (g), a person or business 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 section and section 13.055, subdivision 6, shall be deemed to be in compliance with the notification requirements of this section and section 13.055, subdivision 6, if the person or business notifies subject persons in accordance with its policies in the event of a breach of security of the system.

Subd. 2. Coordination with consumer reporting agencies.

If a person discovers circumstances requiring notification under this section and section 13.055, subdivision 6, of more than 500 persons at one time, the person shall also notify, within 48 hours, all consumer reporting agencies that compile and maintain files on consumers on a nationwide basis, as defined by United States Code, title 15, section 1681a, of the timing, distribution, and content of the notices.

Subd. 3. Waiver prohibited.

Any waiver of the provisions of this section and section 13.055, subdivision 6, is contrary to public policy and is void and unenforceable.

Subd. 4. Exemption.

This section and section 13.055, subdivision 6, do not apply to any "financial institution" as defined by United States Code, title 15, section 6809(3).

Subd. 5.

[Renumbered 13.055, subd 6]

Subd. 6. Remedies and enforcement.

The attorney general shall enforce this section and section 13.055, subdivision 6, under section 8.31.

§ 325E.64 Access Devices; Breach Of Security

Subdivision 1. Definitions.

(a) For purposes of this section, the terms defined in this subdivision have the meanings given them.

(b) "Access device" means a card issued by a financial institution that contains a magnetic stripe, microprocessor chip, or other means for storage of information which includes, but is not limited to, a credit card, debit card, or stored value card.

(c) "Breach of the security of the system" has the meaning given in section 325E.61, subdivision 1, paragraph (d).

(d) "Card security code" means the three-digit or four-digit value printed on an access device or contained in the microprocessor chip or magnetic stripe of an access device which is used to validate access device information during the authorization process.

(e) "Financial institution" means any office of a bank, bank and trust, trust company with banking powers, savings bank, industrial loan company, savings association, credit union, or regulated lender.

(f) "Microprocessor chip data" means the data contained in the microprocessor chip of an access device.

(g) "Magnetic stripe data" means the data contained in the magnetic stripe of an access device.

(h) "PIN" means a personal identification code that identifies the cardholder.

(i) "PIN verification code number" means the data used to verify cardholder identity when a PIN is used in a transaction.

(j) "Service provider" means a person or entity that stores, processes, or transmits access device data on behalf of another person or entity.

Subd. 2. Security or identification information; retention prohibited.

No person or entity conducting business in Minnesota that accepts an access device in connection with a transaction shall retain the card security code data, the PIN verification code number, or the full contents of any track of magnetic stripe data, subsequent to the authorization of the transaction or in the case of a PIN debit transaction, subsequent to 48 hours after authorization of the transaction. A person or entity is in violation of this section if its service provider retains such data subsequent to the authorization of the transaction or in the case of a PIN debit transaction, subsequent to 48 hours after authorization of the transaction.

Subd. 3. Liability.

Whenever there is a breach of the security of the system of a person or entity that has violated this section, or that person's or entity's service provider, that person or entity shall reimburse the financial institution that issued any access devices affected by the breach for the costs of reasonable actions undertaken by the financial institution as a result of the breach in order to protect the information of its cardholders or to continue to provide services to cardholders, including but not limited to, any cost incurred in connection with:

(1) the cancellation or reissuance of any access device affected by the breach;

(2) the closure of any deposit, transaction, share draft, or other accounts affected by the breach and any action to stop payments or block transactions with respect to the accounts;

(3) the opening or reopening of any deposit, transaction, share draft, or other accounts affected by the breach;

(4) any refund or credit made to a cardholder to cover the cost of any unauthorized transaction relating to the breach; and

(5) the notification of cardholders affected by the breach.

The financial institution is also entitled to recover costs for damages paid by the financial institution to cardholders injured by a breach of the security of the system of a person or entity that has violated this section. Costs do not include any amounts recovered from a credit card company by a financial institution. The remedies under this subdivision are cumulative and do not restrict any other right or remedy otherwise available to the financial institution.