CHAPTER 108–H.F.No. 1758

An act relating to commerce; regulating access devices; establishing liability for security breaches; providing enforcement powers; proposing coding for new law in Minnesota Statutes, chapter 325E.

BE IT ENACTED BY THE LEGISLATURE OF THE STATE OF MINNESOTA:

Section 1. **[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.

EFFECTIVE DATES; APPLICATION. Subdivisions 1 and 2 are effective August 1, 2007. Subdivision 3 is effective August 1, 2008, and applies to breaches of the security of a system occurring on or after that date.

Presented to the governor May 18, 2007

Signed by the governor May 21, 2007, 2:58 p.m.