

## What is the Minnesota Security Breach Disclosure Act?

*The Minnesota Security Breach Disclosure Act (H.F. No. 2121) requires businesses to notify individuals when a security breach causes their personal information to be released to unauthorized parties. The Act specifies the notification steps businesses must follow in the event of a security breach. The Act came into effect January 1, 2006.*

### **Who is affected?**

*This Act affects all businesses that conduct business in Minnesota and that store personal information of state residents. Personal Information is defined as the first name or initial and last name in combination with one or more of the following nonpublic unencrypted pieces of information: a social security number, a driver's license or identification card number, or a bank account, credit card or debit card number accompanied by the applicable passwords or security codes.*

### **What does the Security Breach Disclosure Act have to do with information management?**

*According to the Act, Minnesota businesses are responsible for the security of their computerized customer records. If companies experience a security breach and disclose personal information to unauthorized parties, they are responsible for notifying the affected individuals.*

*By monitoring and controlling the amount of customer data held on site in computerized form, businesses can reduce the risk of losing or otherwise releasing data to unauthorized parties. Computer backups containing personal information that are no longer needed should be disposed of securely. Similarly, other computerized mediums containing personal information, such as CDs, computer disks and hard drives, should be destroyed once no longer needed.*

### **What do companies have to do to comply with the Act?**

*Businesses must alert affected customers when personal information which is not publicly available is disclosed to unauthorized parties. Methods for notifying affected individuals are outlined in the Act. If the cost of notifying affected individuals is more than \$250,000, or if the number of affected individuals exceeds \$500,000, substitute notification methods may be followed. Additionally, businesses that experience a security breach of more than 500 persons at one time must contact all consumer reporting agencies that compile and maintain consumer records on a nationwide basis within 48 hours to notify them of the breach.*

### **How can we help?**

*As you develop your document disposal program in accordance with Minnesota House File 2121, consider contracting Securit to handle your document destruction needs. Securit destroys all of your confidential materials, including computerized data such as CD-ROMs/CD-Rs/DVDs and computer backups. By providing locked consoles for your office, Securit makes it easy and efficient to destroy unnecessary copies of your customers' personal information. Securit destroys documents on site in our mobile shredding truck. For peace of mind, contact Securit today at 1 800 697-4733.*

For more information:

Minnesota Legislature - <http://www.revisor.leg.state.mn.us>

This document does not constitute a legal opinion or legal advice. Do not rely on any of the information in this document without first obtaining legal advice.

© Copyright 2006