

Michigan's New Data Breach Notification Act

The press has been filled with stories about stolen laptop computers containing personal information, lost computer hard drives or backup tapes, and situations where computer databases have been hacked. Two such events occurred in Michigan in 2006. One involved a stolen flash drive from an agency computer that contained the records of 4,000 Michigan residents; the other involved a stolen laptop computer with over 28,000 records. (For information about these and other events, look at the Identity Theft 911 Web site at www.identitytheft911.org.) In many of these cases, the potential for access to and the misuse of personal information (such as social security numbers and credit card data) has led to initiatives to require notification to potentially affected people. The federal government has been slow to respond to these problems, forcing businesses to deal with potentially inconsistent state legislation.

Without much fanfare, Michigan joined the growing list of states that have enacted legislation requiring companies or agencies to notify people of possible disclosures of personal and confidential information. Led by California, these states have enacted legislation that seeks to protect individuals whose personal information may have been accessed or compromised. The legislative initiatives are also providing guidance for businesses and governmental agencies facing the situation.

Michigan's new law came into existence at the end of the last legislative session without much publicity as Act No. 566, Public Acts of 2006. It amends the Identity Theft Protection Act ("Act") and follows the pattern established in a number of states by defining the nature of personal information and the type of potential breach that triggers a notification requirement. About the legislation, Governor Jennifer Granholm said the following:

Today's technology has taken commerce and communication to new heights, but it also puts citizens at additional risk of identity theft as ever-increasing amounts of personal information are stored and transmitted electronically. While I am pleased to sign legislation that provides critical information to consumers, we must do more to provide our citizens with the tools they need to truly protect themselves.¹

What Information Is Covered?

The new Michigan legislation² defines "personal information" as data that links a person's name to:

- Social Security number;
- Driver's license or identification number; or
- Financial institution information.

A separate and much broader definition of "personal identifying information"³ has a different application as discussed below.

What Triggers the Notification Requirement?

The notification requirement is triggered by a "breach of the security of a database" or a "security breach," which means unauthorized access and acquisition of personal information data.⁴ The two primary situations that the law seeks to address are the unauthorized access of a database containing personal information, and the loss or theft of computer or other equipment that contains unencrypted personal information. Notification must occur unless the person or agency determines that the security breach has not or is not likely to cause substantial loss or injury to one or more residents of the state.⁵ (Would you want to give that opinion?)

What Notification is Required and How Must It Be Done?

The legislation leaves some room for interpretation as to the form and manner of notification. One of the issues that a business must address is the timing of notification. Section 12(4) of the legislation requires that the notification to the person affected by the security breach must occur "without unreasonable delay."⁶ The effect of this is to put the burden on the business or agency to decide how soon the disclosure and notification must be made, which may be influenced by the severity of the breach. There is no safe harbor in the legislation to address this obligation, but there are provisions that provide for delays in order to conduct appropriate investigations, restore security and to notify the appropriate law enforcement agencies.⁷

The form of notification is also left to the affected business or agency and can include regular mail, facsimile, electronic mail, or telephonic notice in different situations.⁸ Mass media can be used for large scale breaches.⁹ The pattern established by companies that have faced the issue is to publicly disclose the breach with a follow-up direct notification to each affected person.

Are There Other Issues That a Business Must Address?

Businesses must also address the impact of the disclosure if the information is covered by the Health Insurance Portability and Accountability Act (HIPAA) or the Graham-Leach-Bliley Act (GLB). GLB relates to financial information.¹⁰ Additionally, to the extent that the personal information contained in the affected database includes information of persons outside of the state of Michigan, the business must comply with other state laws. The effect of this is to require a business to comply with

the most restrictive of the state laws, which is usually considered to be the California legislation.

At the end of the Act as amended is another interesting obligation that addresses the removal of unnecessary data from databases. Unless the person or agency maintaining the database is subject to federal law that governs the disposal of records containing the personal identifying information, Section 12a of the Act requires that all data that contains personal information must now be destroyed once the personal information is removed from the database.¹¹ This presumably means that the business or agency has to go back to all archives, back-up tapes and discs, and similar media to destroy or overwrite the data.

Planning Considerations

To the extent that businesses have not focused on the importance of information security and digital asset management, the new Michigan legislation gives them another reason to address the manner in which personal information is collected, stored, and protected. The Act provides for civil fines of up to \$250 for each failure to provide notice and each record not deleted.¹² This is mitigated somewhat by the fact that civil fines cannot exceed \$750,000 for multiple violations arising from the same security breach.¹³ Make sure you bring these potential liabilities to the attention of your company's board of directors.



Michael S. Khoury, of Jaffe Raitt Heuer & Weiss, PC, Ann Arbor and Southfield, practices in the areas of information technology, electronic commerce, intellectual property, and commercial and corporate law. He is the vice-chairperson of the State Bar of Michigan Business Law Section and past chairperson of the Computer Law Section. He is also a member of the American Bar Association Sections of Business Law, Science and Technology, and Intellectual Property.



Holli Hart Targan is a member of Jaffe, Raitt, Heuer, & Weiss and counsels financial institutions and businesses on contractual and regulatory matters dealing with credit and debit cards, electronic fund transfers, loyalty cards, and payment systems. As an advisor to companies in the credit card processing industry internationally, Holli counsels companies on strategic issues, handles merchant portfolio and card processing industry mergers and acquisitions, and keeps businesses apprised of legal and regulatory developments, including representing companies before Visa and MasterCard. She is a frequent author and speaker at industry forums and is a contributing author to The 1999 Guide to Smart Cards and Stored Value. Holli is a member of the Board of Directors of the Electronic Transactions Association

NOTES

1. Granholm, Jennifer, "2006 State of the State Address" (Lansing, MI, Jan. 25, 2006).

2. MCL 445.63(p).

3. MCL 445.63(o).

4. MCL 445.63(b).

5. MCL 445.72(1).

6. MCL 445.72(4).

7. *Id.*

8. MCL 445.72(5).

9. MCL 445.72((5)(d)(iii).

10. MCL 445.72(8)(b), (10).

11. MCL 445.72a.

12. MCL 445.72(12).

13. MCL 445.72(14).