



Issued by the Labor and Employment Practice Group

January 10, 2007

DATABASE SECURITY BREACHES MAY RESULT IN SIGNIFICANT PERSONAL AND BUSINESS LIABILITY

Author:

Claudia D. Orr

Direct: (313) 983-4863

corr@plunkettcooney.com


Failing to protect personal information in your company's database could cost you more than just your customers—it could mean imprisonment and/or up to \$750,000 in penalties for violating the new senate bill recently signed into law.

On Jan. 3, Gov. Jennifer Granholm signed Senate Bill No. 309, which prohibits certain practices concerning identity theft, requires notification of a security breach of a database containing personal information and provides significant penalties for violations.

The new Michigan law, which takes effect on July 2, applies to the "breach of the security of a database" containing personal information such as the first name or first initial and last name of individuals linked to such information as social security numbers, driver's license or state personal identification card numbers, or to financial account information or credit/debit card numbers in combination with security access or password codes. The law requires very specific and prompt notices be provided to Michigan residents whose information has been exposed. Failure to provide the requisite notices may result in civil fines of \$250 for each failure, with a total aggregate liability of not more than \$750,000.

The law also prohibits providing notice of a security breach when a breach has not occurred, and where there is intent to defraud. The person providing the false notice of a security breach may be found guilty of a misdemeanor and face significant fines. Moreover, the law prohibits the distribution of an advertisement or making a solicitation that misrepresents that a security breach has occurred, and provides a misdemeanor penalty punishable by imprisonment of not more than 30 days or a fine of not more than \$1,000 for each violation.

In addition, where personal information is maintained in a database, the law requires the destruction of such data when it is removed from the database and it is no longer retained elsewhere for another purpose not prohibited by state or federal law. Lastly, the law requires the destruction of personal identifying information such as mother's maiden name, health insurance identification numbers,



passport numbers, vital records and medical records, among others. Failure to destroy the data may result in a misdemeanor conviction punishable by a fine of not more than \$250 for each violation.

Please note that the penalties discussed above do not affect the availability of a civil remedy for a violation of this or any other state or federal law, and there are now several laws protecting various kinds of personal information. If you or your company maintain personal information in a database, it is important to establish and follow procedures for destroying information as required under the act. If there is any reason to believe that a security breach has occurred, seek immediate legal advice.

If you need further information concerning the above or require assistance with other employment issues, please contact your Plunkett & Cooney attorney directly, or in the alternative, Plunkett & Cooney's Labor & Employment Law Practice Group Leader Theresa Smith Lloyd at (248) 901-4005.

Blmfield.PD.FIRM.832615-1