STATE BAR OF MICHIGAN

MICHIGAN COMPUTER LAWYER

State Bar of Michigan Computer Law Section http://www.michbar.org/computer/ Volume 24, No. 2

Preventing Security Breaches:

Best Practices Under Michigan's New Notification Law

By Mark L. Kowalsky and Derek D. McLeod, Hertz Schram PC
Bloomfield Hills

Identity theft is so common today that it has been referred to as "the crime of the 21st century."[1] Numerous incidents demonstrate the breadth of identity thievery:

- Data broker CheckPoint Inc. recently paid $15 million to settle Federal Trade Commission charges that its lax procedures violated consumer protection laws when identity thieves posing as legitimate customers gathered personal records of 163,000 people from which at least 800 cases of identity theft arose;[2]
- TJX Cos.'s (parent of T.J. Maxx and Marshalls) customer database containing 45.7 million credit and debit card numbers was compromised;[3]
- DSW Retail Ventures Inc.'s database containing 14 million credit card numbers was penetrated by hackers;[4]
- Time Warner Inc. lost computer tapes containing personal information of 600,000 employees;[5]
- Lexis/Nexis reported in 2005 that an "unauthorized person" acquired personal information of approximately 280,000 individuals;[6]
- Although eventually found, ABN AMRO Mortgage Group, Inc. lost a tape containing residential mortgage information.[7]

A common misconception is that security breaches affect only Fortune 500 and other large companies. However, any size business maintaining electronically stored databases containing personal information such as So-

Continued on next page

Michigan Computer Lawyer is published bi-monthly. If you have an article you would like considered for publication, send a copy to:

Matthew M. Jakubowski
Brooks Kushman, P.C.
1000 Town Center
Floor 22, Suite 2200
Southfield, MI 48075-1183
e-mail: *mjakubowski@brookskushman.com*

cial Security numbers, credit card numbers, driver's license numbers, maiden names, and the like, are susceptible to security breaches. Indeed, a security breach at a gas station/convenience store chain based in Muskegon, Michigan, resulted in reissuance of debit cards after "thousands of credit and debit cards" were cancelled due to "fraud concerns …."[8]

In response to the increase in identity theft, the federal government and several states, including Michigan, have enacted laws to stem the incidents of such theft. One such aspect of these laws imposes notification procedures when a breach of security occurs. As a consequence, these laws should not be ignored, as security breaches can result in significant expenses, including the cost to notify all affected individuals of the breach, civil liability, civil fines up to $750,000 and criminal penalties. This article seeks to analyze the breadth and scope of Michigan's new security breach notification law, MCL 445.72, which goes into effect on July 2, 2007.[9] Further, this article recommends several "best practices" to prevent and respond to such breaches of security.

Laws Requiring Notification of Security Breaches

Congress, through the passage of Title V of the Gramm-Leach-Bliley Act ("GLB"),[10] now requires financial institutions[11] to disclose to consumers policies and practices concerning: (1) the disclosure of personal information to affiliates and non-affiliates; (2) the disclosure of personal information of persons who are no longer customers of the financial institution; and (3) the protection of consumers' personal information.[12] A federal breach of security notification requirement is not included in the GLB and, as a recent piece in *The Wall Street Journal* observed, "efforts to pass a federal notification law have stalled over disagreements between consumer and industry groups."[13]

State lawmakers, however, have acted to fill this void. The National Conference of State Legislatures reports that at least thirty-five (35) states have enacted legislation requiring private entities and/or governmental agencies to disclose security breaches concerning personal information.[14] Michigan recently became one such state.[15]

Michigan's New Security Breach Notification Law

In 2005, Michigan's Identity Theft Protection Act (or "Act") took effect.[16] In 2006, the Michigan Legislature amended the Identity Theft Protection Act as it relates to, among other things, the notification required when a security breach occurs.[17] On one hand, the new law is simple: It provides that when a person or agency discovers a security breach of "personal information," ***it must provide a notice of the security breach to each affected Michigan resident***.[18] On the other hand, the broad definitions and nuanced requirements underlying this new notification requirement are critical and warrant close examination.

What Personal Information Is Contemplated and Protected by the Act?

"Personal information" under Michigan's new notification law encompass first names or first initials and last names, Social Security numbers, driver's license (or state personal identification card) numbers, demand deposit or

other financial account numbers, credit card numbers,[19] and debit card numbers, in addition to any security codes, access codes, or passwords that would permit access to financial accounts.[20] A security breach is deemed to have occurred if the personal information was accessed or acquired in either unencrypted or encrypted form by an unauthorized person.[21]

When Does a Security Breach Occur?

The phrases "breach of the security of a database" and "security breach" are expansively defined to mean "the unauthorized access and acquisition of data that compromises the security or confidentiality of personal information maintained by a person or agency as part of a database of personal information regarding multiple individuals."[22] The notice requirement for a secuity breach is triggered if the personal information was accessed or acquired, in either unencrypted or encrypted form, by an unauthorized person.[23]

Preemption of Existing Michigan Laws

The new law expressly states that because the subject matter of identity theft and, correspondingly, notification of security breaches, is a matter of statewide concern, "any charter, ordinance, resolution, regulation, rule, or other action by a municipal corporation or other political subdivision of" Michigan "to regulate, directly or indirectly, any matter expressly set forth in [MCL 445.72] is preempted."[24]

Exception to Notification Obligations

The notification requirements prescribed in MCL 445.72(1) and (2) contain a significant exception: The new Michigan law provides that notice of a security breach is not required if that "person or agency determines that the security breach has not or is not likely to cause substantial loss or injury, or result in identity theft."[25] This exception may be illusory as the statute expressly provides that "[i]n determining whether a security breach is not likely to cause substantial loss or injury to, or result in identity theft with respect to[ ] 1 or more residents of this state … [ ] a person or agency shall act with the care an ordinary prudent person or agency in like position would exercise under similar circumstances."[26] It is foreseeable that litigation will arise under this section of Michigan's new notification for security breaches law.

Who Must Make the Notification?

The person or agency that owns or licenses the data must make the required notification. As stated, the Identity Theft Protection Act defines a "person" as "an individual partnership, corporation, limited liability company, association, or other legal entity."[27] Likewise, an "agency" is defined as "a department, board, commission, office, agency, authority, or other unit of state government," in addition to institutions of higher education of Michigan.[28] For purposes of the Act, however, an "agency" does not include "circuit, probate, district, or municipal court[s]."[29] The Act also requires persons or agencies that simply maintain, but do not own or license the databases, to provide notice to the owner or licensor of such information upon the discovery of a security breach.[30]

When Must the Notification Be Made?

Notification of a security breach under this new law must be made "without unreasonable delay."[31] A person or agency may delay giving notice without violating MCL 445.72 where "[a] delay is necessary in order for the person or agency to take any measures necessary to determine the scope of the security breach and restore the reasonable integrity of the database."[32] However, in the event a delay is necessary, the person or agency is required to provide notice "without reasonable delay after the person or agency completes the measures necessary to determine the scope of the security breach and restore the reasonable integrity of the database."[33]

Likewise, the "without unreasonable delay" requirement of Michigan's new notification law may be temporarily suspended where "[a] law enforcement agency determines and advises the agency or person that providing a notice will impede a criminal or civil investigation or jeopardize homeland or national security."[34] In this event, the agency

or person must provide notice of the security breach consistent with the new law "after the law enforcement agency determines that providing the notice will no longer impede the investigation or jeopardize homeland or national security."[35]

How Must the Notification Be Made?

The new law prescribes several different avenues to provide notification of the security breach:[36] (a) written notice sent to the recipient at his or her address contained in the records of the agency or person; or (b) electronic written notice subject to the following:

(i) The recipient has expressly consented to receive electronic notice.

(ii) The person or agency has an existing business relationship with the recipient that includes periodic electronic mail communications, and based on those communications, the person or agency reasonably believes that it has the recipient's current electronic mail address.

(iii) The person or agency conducts its business primarily through internet account transactions or on the internet.[37]

Written notice of a security breach made under MCL 445.72(5)(a) and (b) must be written in a "clear and conspicuous manner…."[38] Notice by telephone may be given by an agent of a person or agency if all of the following are met and such notification is not prohibited by state or federal law:

(i) The notice is not given in whole or in part by use of a recorded message.

(ii) The recipient has expressly consented to receive notice by telephone, or if the recipient has not expressly consented to receive notice by telephone, the person or agency also provides notice under [MCL 445.72(5)](a) or (b) if the notice by telephone does not result in a live conversation between the individual representing the person or agency and the recipient within three business days after the initial attempt to provide telephonic notice.[39]

A person or agency providing telephonic notice of security breaches must "clearly communicate the content required under" MCL 445.72(6)(c)-(g), discussed below, "to the recipient of the telephone call."[40]

Where a person or agency demonstrates that the cost of providing written or telephonic notice will exceed $250,000.00, or that the person or agency will have to provide notice to more than 500,000 Michigan residents, Michigan's new notification law provides for substitute notice.[41] Substitute notice is obtained by completion of ***each*** of the following:

(i) If the person or agency has electronic mail addresses for any of the residents of this state who are entitled to receive the notice, providing electronic notice to those residents.

(ii) If the person or agency maintains a website, conspicuously posting the notice on that website.

(iii) Notifying major statewide media. A notification under this subparagraph shall include a telephone number or a website address that a person may use to obtain additional assistance and information.[42]

Further, the new notification law permits some leeway by expressly providing that a person or agency may provide notice pursuant to agreement, provided however, that the "notice provided pursuant to the agreement does not conflict with any provision of" the Act.[43]

Pursuant to MCL 445.72(6)(a)-(g), ***all*** notices provided under Michigan's new security breach notification law must: (1) describe the security breach in general terms; (2) describe the type of personal information that is the subject of the security breach; (3) generally describe what the person or agency providing the notice has done to protect data from further security breaches (if applicable); (4) include a telephone number where a recipient of the notice may obtain assistance or additional information; and (5) remind recipients of the notice "to remain vigilant for incidents of fraud and identity theft."[44]

Additional Notification Requirements

After a person or agency provides notification of a security breach under the new Michigan law, the person or agency must also notify each consumer reporting agency that complies with and maintains files on consumers on a nationwide basis—as defined in 15 USC 1681a(p)—of the security breach without unreasonable delay.[45] Notification under this provision includes the number of notices that the person or agency provided to Michigan residents and the timing of those notices.[46] However, notification under this subsection does not apply where: (a) the person or agency is required by the new law to provide notice of a security breach to 1,000 or fewer Michigan residents; or (b) the person or agency is subject to Title V of the GBL.[47]

Notification Carve-Outs: Financial Institutions, Persons or Agencies Subject to HIPAA, and Public Information

Michigan's new security breach notification law carves out a special exception to the notice requirement for certain entities. For example, financial institutions or a person or agency that is subject to and complies with the Health Insurance Portability and Accountability Act of 1996 (HIPAA)[48] may under certain circumstances be "considered to be in compliance" with the Act.[49] Michigan's new notification law also does not apply where the access or acquisition of personal information by a person or agency of federal, state, or local government records or documents are lawfully available to the general public.[50]

Penalties for Violating Michigan's New Notification Law

A person—***but not an agency***—that knowingly fails to provide notice of a security breach as required by this new law "may be ordered to pay a civil fine of not more than $250 for each failure to provide notice."[51] The aggregate liability of a person for civil fines imposed by MCL 445.72(13) for multiple violations of that section arising from the same security breach, however, cannot exceed $750,000.[52] While this new law does not affect the availability of a private right of action for failures to provide notice of a security breach,[53] the attorney general or prosecuting attorneys are authorized to bring actions to recover civil fines under the Act.[54]

Further, Michigan's new notification law punishes not only a person who knowingly fails to provide notice of a security breach, but also a person who provides notice as prescribed by the Act when no security breach has occurred, if such notice is provided "with the intent to defraud[.]"[55] In this scenario, the person is guilty of a misdemeanor, an offense punishable by imprisonment for not more than thirty (30) days or a fine not to exceed $250.00 for each violation—or both.[56]

Amendments to the Identity Theft Protection Act Not Relating to Notification: Destroying Personal Information After Removal From Database

The amendments to Michigan's Identity Theft Protection Act affect not only security breach notification, but also concern the destruction of data containing personal information as well as prohibitions against misrepresentations by advertisements and solicitations. Thus, in addition to providing notification of security breaches, MCL 445.72a(1) prescribes that persons and agencies maintaining databases that include personal information must destroy any data that contains personal information concerning individuals "when that data is removed from the database and the person or agency is not retaining the data elsewhere for another purpose not prohibited by state or federal law." As used in MCL 445.72a, "'destroy' means to destroy or arrange for the destruction of data by shredding, erasing, or otherwise modifying the data so that they cannot be read, deciphered, or reconstructed through generally available means."[57] A person—but not agency—who knowingly violates MCL 445.72a is guilty of a misdemeanor, which is punishable by a fine not to exceed more $250.00 for each violation. Civil remedies are not, however, affected for such violations.[58]

MCL 445.72a(1), however, does not prohibit a person or agency from retaining data containing personal information for purposes of an investigation, an audit, or an internal review. Further, a person or agency is considered to be in compliance with MCL 445.72a if the person or agency is subject to and in compliance with federal law concerning the disposal of records containing personal identifying information.[59]

Finally, MCL 445.72b prohibits a person, but not an agency, from distributing an advertisement or "any other solicitation that misrepresents to a recipient that a security breach has occurred that may affect the recipient."[60] Further, a person may not distribute an advertisement or make any other solicitation that is substantially similar to a notice required under MCL 445.72(5) or one required by federal law if that notice is prescribed by state or federal law, or rule or regulation.[61] A person who knowingly or intentionally violates MCL 445.72b is guilty of a misdemeanor punishable by imprisonment of not more than thirty (30) days or a fine not to exceed $1,000.00 for each violation, or both.[62] Nevertheless, the penalties prescribed by MCL 445.72b(3) do not affect the availability of any civil remedy for violations of state or federal law.[63]

General Tips to Businesses

It is apparent that the implementation of an effective information security program not only makes for a good business practice, but is now also implied by this new law. The California Office of Privacy Protection has enumerated a myriad of "Recommended Practices." While these "Recommended Practices" are not exhaustive, they are relatable in avoiding penalties under Michigan's new notification law.

Therefore, a firm should consider the following safeguards in order to prevent the pilfering of personal information:

- Collect the minimum amount of personal information necessary to accomplish the person's or agency's purpose;
- Retain personal information only for the minimum time necessary;
- Inventory data to identify personal information;
- Classify personal information in data systems according to sensitivity;
- Use appropriate safeguards to protect personal information;
- Pay special attention to high-risk systems containing personal information (i.e., laptop computers);
- Apprise employees of privacy safeguard policies and procedures and train employees;
- Apprise service providers and business partners handling personal information of policies and procedures and require compliance;
- Institute and utilize technological safeguards to ensure swift detection and response to security breaches;
- Use data encryption in conjunction with host protection and access control;
- Securely dispose of records and equipment containing personal information; and
- Review and revise security plans regularly or whenever there is a material change in business practices that may affect the security of personal information.[64]

Preparing for Compliance With Michigan's New Notification Law

Taking a queue from the California Office of Privacy Protection, there are many ways to effectively prepare for the implementation of the Act:

- Prescribe written procedures for internal notification of security breaches that may involve unauthorized access to personal information;
- Designate one individual to be responsible for coordinating internal notification procedures;
- Train employees, including temporary and contract employees, in their responsibilities;
- Define relevant terms in the notification plan and designate responsible individuals;
- Plan for and utilize measures to contain, control, and correct any security breach;
- Require the data custodian (or others) who detect security breaches to immediately notify the person or agency who owns or licenses the data subject to the security breach;

- Identify and inform appropriate law enforcement that the security breach may involve unlawful conduct;
- Consider any recommendations of law enforcement and include such recommendations in the security breach response plan;
- Obtain consent for e-mail notification pursuant to MCL 445.72(5)(b)(i)-(iii);[65]
- Prescribe written procedures for notifying Michigan residents whose unencrypted personal information has been or is more likely than not caused substantial loss or injury;
- Document response actions taken on a security breach; and
- Review the security breach response plan regularly or whenever there is a material change in business practices affecting personal information.[66]

Possible Insurance Coverage

The insurance industry regularly offers new and expanded types of coverage in response to changing regulatory and legal obligations.[67] It is advisable to consult with your insurance agent to consider a policy that will cover the notification and other costs associated with a security breach.

Conclusion

Michigan's new notification law presents issues entities need to consider. The law is both broad and complex, and the consequences for non-compliance are significant. Therefore, entities should institute the best practices outlined above to prepare and be best positioned if a breach occurs.

About the Authors

Mark L. Kowalsky *is a partner of Hertz Schram PC, in Bloomfield Hills, specializing in civil litigation with concentrations in commercial disputes and securities law. He is routinely involved in handling disputes that involve contracts, non-competition agreements, trade secrets, employment, shareholders, partnerships, dissolutions, collections, and leasing for public and private businesses and individuals. He has extensive experience in federal and state courts, arbitration, mediation, and in securities law regulatory matters. He is certified and sits as an arbitrator for the National Association of Securities Dealers, New York Stock Exchange, American Arbitration Association, National Arbitration Forum, and is also a mediator for the Oakland County Circuit Court and District Courts. He has presented at a continuing education program on Advanced Litigation Skills, is a past lecturer on securities compliance and regulatory issues for a national securities firm, and has co-authored several publications. He is a former chair of Oakland County Bar Association Federal Courts Committee and is currently chair of the Greater West Bloomfield Cable Advisory Board, where he led the negotiations to refranchise the cable system. Mr. Kowalsky is a member of the State Bar of Michigan and is admitted to practice in the Eastern and Western Districts of Michigan and the U.S. Courts of Appeals for the Fourth, Sixth, and Seventh Circuits. He graduated with a bachelor of arts degree from the University of Michigan with highest honors and high distinction in 1980, and received his law degree from the University of Michigan Law School in 1983.*

Derek D. McLeod *is an associate of Hertz Schram PC, in Bloomfield Hills, where he practices in the firm's Commercial Litigation, Securities Litigation, and ERISA and Contractual Disability practice groups. Before entering private practice, Mr. McLeod served as a law clerk to the Honorable Victoria A. Roberts of the United States District Court for the Eastern District of Michigan. Mr. McLeod graduated cum laude and Phi Kappa Phi from The Citadel, The Military College of South Carolina in 2000, and received his J.D. in 2003 from Northeastern University School of Law. He is a member of both the State Bar of Michigan and The Florida Bar.*

Endnotes

1 Cal Dep't of Consumer Affairs, Office of Privacy Protection, *Recommended Practices on Notice of Security Breach Involving Personal Information* (Rev Feb 2007) (available at http://www.privacy.ca.gov/recommendations/recomend.htm).

2 Federal Trade Commission, *ChoicePoint Settles Data Security Breach Charges; to pay $10 Million in Civil Penalties, $5 Million for Consumer Redress* <http://www.ftc.gov/opa/2006/01/choicepoint.htm> (January 26, 2006).

3 Josh Pereira, "How Credit-Card Data Went Out Wireless Door," *The Wall Street Journal* A1 (May 4, 2007).

4 *Id.*

5 *The Washington Post*, "Time Warner Reports Loss of Personal Data on 600,000 Employees" <http://www.washingtonpost.com/wp-dyn/content/article/2005/05/02/AR2005050201528.html> (May 3, 2005).

6 Lexis Nexis Media Relations, *LexisNexis Concludes Review of Data Search Activity, Identifying Additional Instances of Illegal Data Access* <http://www.lexisnexis.com/about/releases/0789.asp> (April 12, 2005).

7 LaSalle Bank, *Press Room—12-19-2005 Mortgage Tape Found/A Message to Our Customers* <http://www.lasallebank.com/about/dec162005_chicago.html> (December 19, 2005).

8 *Computerworld*, "Retail Breach Forces Banks to Cancel Cards" <http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=274392&source=rss_topic82> (November 20, 2006).

9 MCL 445.72(16).

10 15 USC 6801, *et seq.*

11 GLB governs financial institutions defined in 15 USC 6805(a).

12 15 USC 6803(a)(1)-(3). Similarly, the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), and correspondingly, the Health Insurance Reform Security Standards, require that medical information be protected from unauthorized disclosure. Public Law 104-191; 45 CFR Parts 160, 162, and 164.

13 Michael Totty, "Warning! What kind of federal consumer-notification law is needed in case of data-security breach? It depends on whom you ask," *The Wall Street Journal* R5 (January 29, 2007). Title V of GLB expressly provides that the federal notification of security breach law does not supersede, alter, or affect any state statute, regulation, order, or interpretation, except to the extent that the state provision is inconsistent with GLB (and then, only to the extent that it is inconsistent). 15 USC 6807(a). However, preemption issues may arise if Congress enacts legislation introduced in February 2007. Jon Swartz, "Congress May Act on Data Security," *Detroit Free Press* 10A (Feb. 26, 2007).

14 Nat'l Conf of State Legislatures, *State Security Breach Notification Law* <http://www.ncsl.org/programs/lis/cip/breachlaws.htm> (January 9, 2007). Reuters reports that Massachusetts is considering legislation that goes further than notification. Under the proposed Massachusetts legislation, companies victimized by breaches of security would be liable for all fraud-related losses to the affected consumers. Reuters, "Mass. Bill Would Make Retailers Pay for Data Leaks" <http://today.reuters.com/news/articlenews.aspx?type=domesticNews&storyid=2007-02-22T072834Z_01_N22375241_RTRUKOC_0_US-MASSACHUSETTS-BILL.xml&src=rss> (February 22, 2007). In fact, the article states that Congressman Barney Frank of Massachusetts has drafted similar legislation to introduce before Congress.

15 *See* MCL 445.72.

16 MCL 445.61, *et seq.*

17 *See* 2006 PA 566. All citations to the Michigan Identity Theft Protection Act refer to the Act as it is effective July 2, 2007.

18 The terms "person" and "agency" will be discussed below. *See* MCL 445.63(a), (j).

19 MCL 445.63(d) incorporates the definition of "credit card" in MCL 750.157m.

20 MCL 445.63(p).

21 MCL 445.63(n).

22 MCL 445.63(b).

23 MCL 445.72(1)(a)-(b). Note, however, that a "breach of security of a database" or "security breach" do not include unauthorized access to data by an employee or other individual if the access meets ***each*** of the following: (1) the employee or other individual acted in good faith in accessing the data; (2) the access was related to the activities of the agency or person; and (3) the employee or other individual did not misuse any personal information or disclose any personal information to an unauthorized person. MCL 445.63(b)(i)-(iii). "Data" under the Identify Theft Protection Act "means computerized personal information." MCL 445.63(e).

24 MCL 445.72(18).

25 MCL 445.72(1)-(2).

26 MCL 445.72(3).

27 MCL 445.63(n).

28 MCL 445.63(a).

29 *Id.*

30 MCL 445.72(2).

31 MCL 445.72(4).

32 MCL 445.72(4)(a).

33 *Id.*

34 MCL 445.72(4)(b).

35 *Id.*

36 Observe, however, that MCL 445.72(5) is subject to MCL 445.72(11), which concerns public utilities.

37 MCL 445.72(5)(b)(i)-(iii).

38 MCL 445.72(6)(a).

39 MCL 445.72(5)(c)(i)-(ii).

40 MCL 445.72(6)(b).

41 MCL 445.72(5)(d).

42 MCL 445.72(5)(d)(i)-(iii).

43 MCL 445.72(7).

44 MCL 445.72(6)(g). Michigan's new notification law also provides that a public utility that sends monthly billing or account statements to the postal addresses of its customers may provide notice of a security breach to its customers in the manner prescribed in MCL 445.72(5) (that is, by written notice, written electronic notice, telephonic notice, or approved substituted notice), or, in the alternative, in the following manner: (a) as applicable, notice as described in MCL 445.72(5)(b) (written electronic notice); (b) notification of the security breach to the media reasonably calculated to inform the customers of the public utility; (c) conspicuous posting of the notice of the security breach on the public utility's website; and (d) written notice, sent in conjunction with the monthly billing or account statement, to the customer at the customer's postal address in the public utility's records. MCL 445.72(11)(a)-(d).

45 MCL 445.72(8). Section 1681a(p) of Title 15 of the United States Code provides:

> The term "consumer reporting agency that compiles and maintains files on consumers on a nationwide basis" means a consumer reporting agency that regularly engages in the practice of assembling or evaluating, and maintaining, for the purpose of furnishing consumer reports to third parties bearing on a consumer's credit worthiness, credit standing, or credit capacity, each of the following regarding consumers residing nationwide:
>
> (1) Public record information.
>
> (2) Credit account information from persons who furnish that information regularly and in the ordinary course of business.

46 MCL 445.72(8).

47 MCL 445.72(8)(a)-(b).

48 Public Law No 104-191.

49 MCL 445.72(9)-(10).

50 MCL 445.72(17).

51 MCL 445.72(13). Interestingly, the penalty provisions of the new law, MCL 445.72(12) and (13), invoke only the word "person," but not "agency."

52 MCL 445.72(14).

53 MCL 445.72(15).

54 MCL 445.72(13).

55 MCL 445.72(12).

56 *Id.*

57 MCL 445.72a(4).

58 MCL 445.72a(2).

59 MCL 445.72a(3). The Identity Theft Protection Act defines "[p]ersonal identifying information" as:

> [A] name, number, or other information that is used for the purpose of identifying a specific person or providing access to a person's financial accounts, including, but not limited to, a person's name, address, telephone number, driver's license or state personal identification card number, Social Security number, place of employment, employee identification number, employer or taxpayer identification number, government passport number, health insurance identification number, mother's maiden name, demand deposit account number, savings account number, financial transaction device account number or the person's account password, stock or other security certificate or account number, credit card number, vital record, or medical records or information.
>
> MCL 445.63(o).

60 MCL 445.72b(1).

61 MCL 445.72b(2).

62 MCL 445.72(3).

63 *Id.*

64 Note 1, *supra*, at pp 9-10

65 The California Office of Privacy Protection further recommends that a person or agency observe the consent procedures prescribed in the Electronic Signature Act. 15 USC 7001, *et seq.*

66 Note 1, *supra*, at pp 9-10.

67 *Id* at pp 10-11.

State Bar of Michigan
Michael Franck Building
306 Townsend Street
Lansing, MI 48933

**Presorted
First Class Mail
U.S. Postage Paid
Lansing, MI 48933
Permit No. 191**