

Introduction

MCL 445.72 requires the Department to provide prompt notification to Michigan residents if a security breach of personal information from any Department database or system occurs. (The link to the full text of this law is included in Appendix A, which includes specific definitions of key terms.)

DTMB Technical Procedure 1340.00.01.02 Information Technology Information Security establishes a formal statewide Notification of Breach procedure in the event of a security breach. Information covered by this procedure may be in written or printed form or may reside electronically on traditional devices such as mainframes, servers and personal computers (desktop and laptop), on newer devices such as USB keys, PDAs, BlackBerrys and cell phones, or other state-of-the-art devices that may be developed. These devices may be state owned or may be owned by an employee or vendor. (The link to the full text of this procedure is included in Appendix B.)

The Michigan Department of State (MDOS) will institute the Security Breach Notification Strategy (SBNS), to notify all persons affected whenever a security breach causes unauthorized access and acquisition of data that compromises the security or confidentiality of MDOS personal information. MDOS will respond in a manner deemed appropriate based on legal requirements, the sensitivity of the personal information compromised, and the level of criticality concerning who and what data is involved.

NOTE: Notification is not required if the security breach has not or is not likely to cause substantial loss or injury to, or result in identity theft to one or more Michigan residents.

Action Plan

Upon notification from any source (DTMB, public, other) of a known or potential security breach of personal information, all known details, including the cause, scope and corrective action to be taken shall be forwarded to the appropriate Administration Director, who will then inform the Chief Of Staff (COS) and other Administration Directors and the Director of the Bureau of Information Security (BIS). The BIS Director will propose an Incident Response Team and corrective action related to the reported breach. The COS will make a final determination as to when the SBNS process must be invoked. If the SBNS process is invoked, notification must be made to the DTMB Liaison(s) as defined in DTMB Technical Procedure 1340.00.01.02. Personnel identified above are available 24/7 in the event of incident requiring immediate attention.

If the SBNS is invoked, the BIS Director will take a coordinating role with respect to this process, and (working with other MDOS areas and other agencies as appropriate) will immediately initiate appropriate actions as outlined below as soon as possible upon notification of a security breach incident. A reasonable delay may occur to allow the Department to determine the scope of the breach, restore integrity to the system(s), identify the needs of law enforcement, and determine if notification will impede a criminal investigation. The law allows law enforcement to delay notification if providing notice will impede a criminal or civil investigation or jeopardize homeland security. If a notification delay is requested by law enforcement, the following steps will take place once approval has been granted by that law enforcement agency.

The following actions will be instituted in the event that a security breach has occurred involving personal information maintained by the MDOS:

- 1) Determine the scope of the problem and implement corrective action.
- 2) Inform law enforcement and other officials/agencies as appropriate.
- 3) Finalize the Communication Plan.
- 4) Implement phone line changes as appropriate.
- 5) Inform individuals affected by the security breach.
- 6) Notify appropriate consumer reporting agencies. [15 USC §1681a (p)]
- 7) Coordinate appropriate follow-up action with other Michigan agencies as needed.

NOTE: Completing steps 1-4 will become a top Departmental priority, to ensure every effort is made to inform customers of the situation as soon as reasonably possible once the breach is discovered.

Detailed Process Steps

- 1) Determine the Scope of the Problem and Implement Corrective Action (DSA; BIS; DTMB)

The Department Services Administration (DSA) Director will work with the BIS Director, the MDOS work area responsible for the affected data and the MDOS-DTMB Liaison(s) to immediately determine the full scope of the data breach, determine needed fixes and implement corrective action to ensure the breach has been contained and all data files are secure. The DSA Director and/or MDOS-DTMB Liaison(s) will coordinate and communicate planned follow-up action to DTMB personnel as outlined in the DTMB Technical Procedure 1340.00.01.02.

- 2) Inform Law Enforcement / Other Officials and Agencies (Executive Office; Legal Services Administration (LSA) Director, BIS)

The COS and LSA Director will determine whether notification is needed to outside parties, including the Attorney General, Michigan State Police, other law enforcement agencies and other officials or agencies. LSA will coordinate notification with the Attorney General, BIS will coordinate notification to law enforcement, DSA will coordinate with the Department of Treasury, and the COS will coordinate communications with the Governor's office, other officials and agencies.

*SSA Compliance: A breach which includes SSA-provided data requires the Department to notify the SSA Regional Office Contact and the SSA Systems Security Contact. If the EIEP (Department) experiences or suspects a breach or loss of PII or a security incident, which includes SSA-provided information, they must notify the State official responsible for Systems Security designated in the agreement. That State official or delegate must then notify the SSA Regional Office Contact and the SSA Systems Security Contact **within one hour**, the responsible State Agency Official or delegate must report the incident by contacting **SSA's National Network Service Center (NNSC) toll free at 877-697-4889** (select "Security and PII Reporting" from the options list). The EIEP will provide updates as they become available to the SSA contact, as appropriate. Refer to the worksheet provided in the agreement to facilitate gathering and organizing information about an incident.*

3) Finalize the Communication Plan (Communications; CSA; DSA; LSA)

The Office of Communications will work with other MDOS areas to finalize the communication strategy. Message documents for the general public's consumption may include talking points, e-mail responses, columns, correspondence, web alerts and media advisories as appropriate. Final decisions on a Departmental point of contact will be made on a case-by-case basis. A sample notification, the content of which may be used for all communication channels, is included in Appendix C.

4) Implement Phone Line Changes as Appropriate (Executive Office; CSA; DSA)

By law, a toll-free number must be available to customers affected by a security breach. The existing toll-free number (888-767-6424) in use by the Department of State Information Center (DSIC) will be used in the case of a security breach. A separate menu item on the existing line will be utilized to provide information to customers. Departmental staff can implement the change to the phone system menu item. If necessary, specially-trained staff can be used to handle calls in the case of a wide-scale data breach.

5) Inform Affected Individuals (CSA; DSA; Communications)

The scope of the security breach must be assessed to determine if individual correspondence must be sent to each individual affected by the breach. By law, if the cost of providing individual notices is more than \$250,000, more than 500,000 notices are needed, or if the Department does not have sufficient contact information for those affected, then a substitute notification process may be used. A substitute notification process would entail sending e-mail notification to affected customers for whom we have an e-mail address, posting a security alert on the MDOS website, and/or a statewide or regional press release (depending on the scope/range of the breach).

If a mailing is required, DSA, CSA and the work area responsible for the affected data will work with DTMB and the Consolidated Print Center as needed. If a web alert and/or press release is used, the Office of Communications will coordinate posting and release of this information, as well as draft talking points and e-mail responses for use by internal staff responding to inquiries.

Note: by law, the notice must be clearly written or communicated, and must contain the following information:

- A description of the security breach in general terms.
- A description of the type(s) of personal information that was compromised.
- A description of actions taken, if any, to protect data from additional security breaches.
- A toll-free phone number for recipients to contact for additional assistance.
- A reminder to recipients to exercise vigilance to detect fraud or identity theft.

The Office of Communications will take the lead in drafting all needed notifications. Sample information that can be used in preparing these notifications is included in Appendix C.

6) Notify Appropriate Consumer Reporting Agencies (CSA; DSA; Communications)

If the security breach affects 1,000 or more individuals, the Department must also notify several consumer reporting agencies. These agencies are listed in Appendix D. The Office of Communications will take the lead in drafting this notification.

7) Coordinate Additional Follow-up with Other State Agencies (Executive Office; LSA; BIS; DSA)

Any additional follow-up needed with outside agencies (e.g., DTMB, MSP, Attorney General, Governor, Federal authorities or other law enforcement agencies) will be determined by the COS. Follow-up contact with these agencies will be coordinated by the MDOS area that is typically responsible (e.g., COS-liaison with Governor's office; LSA-liaison with Attorney General; BIS-liaison with law enforcement; DSA-liaison with DTMB, DSA-liaison with Treasury).

Other Related Issues

Documentation Package

BIS will create and maintain a full documentation package each time they are notified of a security breach incident. At a minimum, the following information should be retained in this package:

- Date and time of Incident
- Description of Incident
- Scope of Incident
- Corrective Action
- Internal and External notifications*
- Copy of data compromised **
- Delay justification ***

*Copies of the notice(s) sent to affected individuals (or at a minimum, a copy of the notice and a list of the people to whom the notice was given) should be retained, as well as notices sent to credit agencies (if any).

** If possible, a copy of the compromised data should be kept, as the scope of the breach may become an issue. These records should be kept for six years, which coincides with the general statute of limitations for civil actions. (MCL 600.5813)

***If a decision is made to delay providing customers with the required notification, information should be retained to identify or substantiate the reasons for the delay (i.e., a police report or other notification from a law enforcement agency advising us to delay the implementation of our notification procedures).

Outside Users of MDOS Data

Agreements with outside users/recipients of MDOS personal data will include a requirement that they immediately notify the Department in the case of a known or suspected security breach involving this data, and that it is the outside user's responsibility to take necessary steps to notify individuals as required by law (Appendix

E). Reports of this type of data breach should be communicated to the COS, Administration Directors and BIS Director as outlined above. However, in these situations the COS and LSA will consult and determine whether any action is necessary on the part of the Department.

Annual Review / Testing / Training

The SBNS should be reviewed on an annual basis (as well as following any breach) by the COS and Administration Directors, and should be updated as deemed necessary to incorporate lessons learned and industry best practices. When changes occur (and/or when deemed necessary by the COS), this policy should be re-sent to employees to reinforce the processes that must take place in the event of a data breach.

The data breach notification process should also be reviewed and revised as part of the annual review of the DTMB Partnership Agreement (PA) to ensure proper communication between MDOS and DTMB regarding the responsibilities of each agency.

Annual testing of the SBNS should occur during the annual review; testing is accomplished using a table-top exercise. Personnel responsible for confirming annual testing include the DSA Administration Director and the Director of the Bureau of Information Security.

All individuals that have a role in implementing this policy should be reminded of their roles and responsibilities on a regular basis, via the annual training session, and in conjunction with other procedural updates.

Appendix A

[Identity Theft Protection Act \(Act 452 of 2004\)](#)

APPENDIX B

[DTMB Technical Procedure 1340.00.01.02 Information Technology Information Security](#)

Appendix C



January XX, 20XX

Dear:

We are contacting you because you conducted business at the Secretary of State branch office located at 1234 Any Road, Any Town, MI.

The Michigan Department of State (MDOS) recently discovered thefts at this branch office involving documents from a limited number of MDOS customers who applied for a driver's license or personal identification card. According to our records, your Social Security number may have been included on these documents. Your credit card/financial information and your vehicle information were not included on these documents.

Once the thefts were discovered, we immediately began an internal investigation and an extensive, in-depth audit to determine which documents were affected. We will be closely monitoring future Michigan Department of State transactions to guard against potential fraud involving those records. In addition, we are working with federal officials who have agreed to use their records and computer resources to assist us in determining if any of the information has been misused. Our office also notified the Michigan State Police, which is conducting a criminal investigation into the thefts.

Protecting personal information is a department priority and we sincerely apologize for the situation. We wish to assure you that we are reviewing our security systems and immediately instituted additional precautions and new measures to prevent this from happening in the future.

Enclosed is information from the Michigan State Police on how to protect your identity and what to do if you become a victim of identity fraud.

If you need assistance or additional information, please contact the Department of State Information Center toll-free at 1-888-767-6424. If you would like to put a fraud alert on your driver license, simply call the toll-free number and from the main phone menu, select the Number 6 button, then select the Number 2 button and then the Number 4 button. The system will provide options of accessing the fraud alert form on-line. You may also have the form mailed to you or talk with a representative.

Sincerely,

Michigan Department of State

Appendix D

[Equifax](http://www.equifax.com) (www.equifax.com)

P.O. Box 740241

Atlanta, GA 30374-0241

1-800-685-1111

[Experian](http://www.experian.com) (www.experian.com)

P.O. Box 2104

Allen, TX 75013-0949

1-888-EXPERIAN (397-3742)

[Trans Union](http://www.transunion.com) (www.transunion.com)

P.O. Box 1000

Chester, PA 19022

1-800-916-8800

Department of the Attorney General

Consumer Protection Division

P.O. Box 30213

Lansing, Michigan 48909

Telephone: 1-877-765-8388 (toll free)

www.michigan.gov/ag

Visit www.OnGuardOnline.gov to learn how to avoid Internet fraud, secure your computer, and protect your personal information.

Michigan State Police [Identity Theft Unit](#)

Appendix E

LAW OFFICES OF
Attorney and Attorney, PC

1234 SUNNY SKIES BOULEVARD, SUITE 100, Any Town, USA
Phone: XXX-XXX-XXXX • Toll Free: XXX-XXX-XXXX • Fax: XXX-XXX-XXXX
Email: XXX@email.com • Web Site: www.website.com

Director of Operations

Collection Manager

[FULL NAME]
[ADDRESS]
[CITY, STATE] [ZIP CODE]

Dear XXXXXX:

I am writing to advise you that your personally identifiable information (“Information”) may have been viewed by a former employee of Attorney & Associates without permission. Specifically, the former employee *may* have viewed your name, address, date of birth, driver’s license number, and/or social security number. Although we cannot be sure that your Information was in fact used in an inappropriate manner, in an abundance of caution we are informing you that such viewing of your information *may* have occurred.

What Information May Have Been Viewed, When and By Whom?

One of our employees may have performed unauthorized searches on you. This information may have included your name, address, date of birth, driver’s license number, and social security number. We are advising you of this matter in an abundance of caution, but we stress that we cannot be sure that your Information was in fact used in an inappropriate manner. In fact, we cannot even be sure that your Information was actually viewed, but we are providing this notice out of an abundance of caution.

How Have We Responded to This Issue

Nonetheless, we certainly understand that this may be cause for concern. Attorney and Associates immediately terminated the employee who may have accessed the Information without permission. Attorney & Associates has also reviewed and reminded all of its employees about its policies and procedures regarding employee access to the subject information. Additional information and support resources are available through the non-profit Identity Theft Resource Center at www.idtheftcenter.org, by calling (858) 693-7935, or via e-mail at itrc@idtheftcenter.org.

Other Steps You Can Take:

Obtain and Review Your Credit Reports Carefully

You may receive a copy of your credit report from any of the following three credit bureaus: (1) Experian, P.O. Box 2002, Allen, TX, 75013, 1-800-397-3742, www.experian.com; (2) Equifax, P.O. Box 740241, Atlanta, GA, 30374, 1-800-685-1111, www.equifax.com; (3) TransUnion, 2 Baldwin Place, P.O. Box 1000, Chester, PA, 19022, 1-800-888-4213, www.transunion.com.

When you receive your credit reports, please review them carefully. While we do not believe that your Information was used to inappropriately obtain or use your credit, you should still look for inquiries you did not initiate, accounts you did not open and unexplained debts on the accounts you opened. If there are accounts or charges you did not authorize, immediately notify the appropriate credit bureau by telephone and in writing. Contact information for the three national credit bureaus will be included with your report.

For Inaccuracies and Notify Credit Bureaus of Them

While we do not believe that your Information was used to inappropriately obtain or use your credit, you also should check to see that information such as your most recent address(es), first and last names and middle initial are correct. Errors in this information can be warning signs of possible identity theft. You should notify the credit bureaus of all inaccuracies as soon as possible so the information can be investigated and, if found to be in error, corrected. Contact information for the three national credit bureaus will be included with your report.

Keep in mind, however, that inaccuracies in this information also may be due to simple mistakes. Nevertheless, if there are any inaccuracies in your reports, whether due to fraud or error, you should notify the credit bureaus as soon as possible so the information can be investigated and, if found to be in error, corrected.

Monitor Your Credit Report

While we do not believe that your Information was used to inappropriately obtain or use your credit, you should continue to check your credit reports frequently for the next year, to make sure no new fraudulent activity has occurred.

Report Errors and Suspicious Activity to Your Creditors As Soon As Possible.

While we do not believe that your Information was used to inappropriately obtain or use your credit, if you have discovered errors or suspicious activity on your credit report, you should consider immediately contacting any credit card companies with whom you have an account and tell them that you have received this letter. You should make sure the address they have on file is your current address and that any charges on the account were made by you. If you have not already done so, you should consider adding a personal identification number, or PIN, to your credit accounts. This will serve as an additional tool to protect your account and help the credit card company ensure they are only processing changes authorized by you.

Place a Security Alert on Your Credit Reports

We recommend before requesting a security alert that you review all items on your credit reports for inaccuracies. Although a security alert service will warn potential creditors to take additional precautions when reviewing your credit records or applications for additional credit, be aware that it could take longer for you to obtain new credit. If you want to renew the security alerts, the three national credit bureaus will require you to contact each organization separately.

We hope this information is helpful to you and we sincerely regret any inconvenience this may cause you. Should you have any questions please feel free to contact the Notice Department at Attorney and Associates at (xxx)-xxx-xxxx.

Sincerely,