What Township Officials Need to Know About:

Complying with the Michigan Social Security Number Privacy Act

Public Act 454 of 2004, MCL 445.81, *et seq.*

MTA
Michigan Townships Association

P.O. Box 80078
Lansing, Michigan 48908-0078
(517) 321-6467
www.michigantownships.org

October 2005

[Intentionally left blank]

Table of Contents

The Sample Social Security Number Privacy Policy included in this handout was prepared by MTA Legal Counsel.

The compliance guidelines in this handout were prepared by MTA Staff using the language of the Social Security Number Privacy Act, other state and federal statutes, and the resources on Page 15.

[Intentionally left blank]

Introduction

Every township must comply
Beginning January 1, 2006, each township board must adopt a Social Security number privacy policy to protect the confidentiality of all Social Security numbers obtained by the township. It doesn't matter what your SEV, taxable value or population is, every township must comply.

The **Social Security Number Privacy Act**, Public Act 454 of 2004 (MCL 445.81, *et seq.*), which took effect March 1, 2005, prohibits many uses of entire Social Security numbers, restricts other uses, and requires that policies be adopted to ensure that all uses are lawful and confidential.

Avoid using Social Security numbers
The best approach is to stop using Social Security numbers for any purpose other than those required by state or federal law. Townships are encouraged to adopt a "unique identification number" (UIN) for persons, accounts and information currently identified by Social Security number.

Any township that uses Social Security numbers in the ordinary course of township business—including employee identification, payroll reporting, benefits accounts, medical records, voter registration, law enforcement, bank accounts or computer passwords—is required to comply with the act and adopt a privacy policy.

All 1,242 townships must implement a Social Security Privacy Policy beginning January 1, 2006.

In some cases, the township can limit its uses of a Social Security number to four sequential digits of the number or may continue to use entire Social Security numbers as a primary account number if that use began prior to March 1, 2005, and is ongoing, continuous and in the ordinary course of business.

The Act imposes criminal penalties
The criminal penalties for knowingly violating the Social Security Number Privacy Act include imprisonment for not more than 93 days or a fine of not more than $1,000, or both.

An individual who prevails in a civil action against a person who violates the act may recover actual damages. An individual who prevails in a civil action against a person who *knowingly* violated the act may recover actual damages or $1,000, whichever is greater, and may recover reasonable attorney fees.

Develop a Social Security number policy
A Social Security number privacy policy must provide methods to ensure the confidentiality of Social Security numbers, prohibit their unlawful disclosure, limit access to and provide for disposal of documents that include them, and establish penalties for violations of the privacy policy.

MTA staff prepared this implementation guide to assist township officials comply with the Act. **For more information, contact MTA Member Information Services at (517) 321-6467.**

SAMPLE SOCIAL SECURITY NUMBER PRIVACY POLICY

TOWNSHIP OF _____
_____ COUNTY, MICHIGAN
_____, 2005

1. Purpose.
The Township of _____ (the "Township") is required by the Michigan Social Security Number Privacy Act, Public Act 454 of 2004, MCL 445.81 *et seq*., (the "Act") to create a privacy policy concerning the Social Security numbers that it possesses or obtains.

Pursuant to the Act, the privacy policy must at least:

a. Ensure to the extent practicable the confidentiality of the Social Security numbers.

b. Prohibit unlawful disclosure of the Social Security numbers.

c. Limit who has access to information or documents that contain the Social Security numbers.

d. Describe how to properly dispose of documents that contain the Social Security numbers.

e. Establish penalties for violation of the privacy policy.

This Privacy Policy sets forth the Township's policies and procedures regarding how Social Security numbers are obtained, stored, transferred, used, disclosed and disposed.

2. Policy.
It is the policy of the Township to protect the confidentiality of Social Security numbers obtained in the ordinary course of township business from employees, vendors, contractors, customers or others. No person shall knowingly obtain, store, transfer, use, disclose, or dispose of a Social Security number that the Township obtains or possesses except in accordance with the Act and this Privacy Policy.

3. Procedure.
a. Obtaining Social Security Numbers. Social Security numbers should be collected only where required by federal and state law or as otherwise permitted by federal and state law for legitimate reasons consistent with this Privacy Policy.

Legitimate reasons for collecting a Social Security number include, but are not limited to:

- Applicants may be required to provide a Social Security number for purposes of a pre-employment background check.

- Copies of Social Security cards may be obtained for purposes of verifying employee eligibility for employment.

- Social Security numbers may be obtained from employees for tax reporting purposes, for new hire reporting or for purposes of enrollment in any Township employee benefit plans.

- Social Security numbers may be obtained from creditors or vendors for tax reporting purposes.

b. Public Display. All or more than four sequential digits of a Social Security number shall not be placed on identification cards, badges, time cards, employee rosters, bulletin boards, permits, licenses or any other materials or documents designed for public display. Documents, materials or computer screens that display all or more than four sequential digits of a Social Security number shall be kept out of public view at all times.

c. Account Numbers. All or more than four sequential digits of a Social Security number shall not be used as a primary account number for an individual.

d. Computer Transmission. All or more than four sequential digits of a Social Security number shall not be used or transmitted on the Internet or on a computer system or network unless the connection is secure or the transmission is encrypted.

e. Mailed Documents. Township documents containing all or more than four sequential digits of a Social Security number shall only be sent in cases where state or federal law, rule, regulation, or court order or rule authorizes, permits or requires that a Social Security number appear in the document. Documents containing all or more than four sequential digits of a Social Security number, that are sent through the mail, shall not reveal the number through the envelope window or otherwise be visible from outside the envelope or package.

f. Freedom of Information Act. Where all or more than four sequential digits of a Social Security number are contained within a document subject to release under the Freedom of Information Act, the Social Security number shall be redacted or otherwise rendered unreadable before the document or copy of a document is disclosed.

g. Storage. All documents containing Social Security numbers shall be stored in a physically secure manner. Social Security numbers shall not be stored on computers or other electronic devices that are not secured against unauthorized access.

h. Access to Social Security Numbers. Only personnel who have legitimate business reasons to know will have access to records containing Social Security numbers. The department heads having access to records containing Social Security numbers shall determine which other personnel within their departments have a legitimate reason in the Township's ordinary course of business to have access to such Social Security numbers. Personnel using records containing Social Security numbers must take appropriate steps to secure such records when not in immediate use.

i. Disposal. Documents containing Social Security numbers will be retained in accordance with the requirements of state and federal laws. At such time as documents containing Social Security numbers may be disposed of, such disposal shall be accomplished in a manner that protects the confidentiality of the Social Security numbers, such as shredding.

j. Unauthorized Use or Disclosure of Social Security Numbers. The Township shall take reasonable measures to enforce this Privacy Policy and to correct and prevent the reoccurrence of any known violations. Any employee, who knowingly obtains, uses or discloses Social Security numbers for unlawful purposes or contrary to the requirements of this privacy policy shall be subject to discipline up to and including discharge. Additionally, certain violations of the Act carry criminal and/or civil sanctions. The Township will cooperate with appropriate law enforcement or administrative agencies in the apprehension and prosecution of any person who knowingly obtains, uses or discloses Social Security numbers through the Township for unlawful purposes.

Prepared by MTA Legal Counsel, September 2005

The purpose of this sample policy is to provide a suggested guideline for the types of items that should be included. Certainly, no sample policy should be used unless, after careful review, it is the professional judgment of your legal counsel that using the sample will accomplish the particular objectives and intentions of your township. Although these sample policies are the result of much thought and effort, neither MTA Legal Counsel nor the Michigan Townships Association assumes any responsibility for the results of using these samples word-for-word in individual cases.

Using your township's privacy policy:

1. Adopt a Social Security Number Privacy Policy.

Beginning January 1, 2006, each township board must adopt a Social Security number (SSN) privacy policy to protect the confidentiality of all Social Security numbers obtained by the township.

Start an Employee Handbook
Although employers have not previously been required by law to have a personnel policy manual or employee handbook, the Michigan Social Security Number Privacy Act now requires **all** employers to have one:

"A person that creates a privacy policy under subsection (1) shall publish the privacy policy in an employee handbook, in a procedures manual, or in 1 or more similar documents, which may be made available electronically."
MCL 445.84(2)

MTA recommends that all townships, as employers, develop an employee handbook that contains:

- Job descriptions
- Personnel policies
- Administrative procedures
- Privacy policies (for Social Security numbers and other restricted information)

2. Limit the use of Social Security numbers.

Whenever possible, don't use SSNs to identify persons. Use a "unique identification number" (UIN) instead.

If you are required or authorized by federal or state law to use SSNs, use only four digits of a SSN (**XXX-XX-1234**) wherever possible.

Unless otherwise required by federal or state law, limit the uses of SSNs to:

- Pre-employment background checks
- Verifying employee eligibility for employment
- New hire reporting
- Enrollment in employee benefit plans
- Federal and state tax reporting and withholding purposes

For example, a township, or a vendor or contractor of a township, **MAY** use of all or more than four sequential digits of the SSN in the ordinary course of business for administrative purposes to:

- Verify an individual's identity related to a current or proposed account, transaction, product, service, or employment.

- Investigate an individual's claim history, credit history, criminal history, or driving history. (*Consult the township's attorney or human resources staff before proceeding*.)

- Detect, prevent or deter identity theft or another crime.

- Lawfully pursue or enforce a person's legal rights, including, but not limited to, an audit, collection, investigation, or transfer of a tax, employee benefit, debt, claim, receivable, account, or interest in a receivable or account.

- Lawfully investigate, collect, or enforce a child or spousal obligation or tax liability.

- Provide or administer employee or health insurance or membership benefits, claims, or retirement programs or to administer the ownership of stock or other investments.

Do **NOT** use Social Security numbers as a:

- Primary account number.
- Identification number for purposes not required by state or federal law, such as an ID card, access card, multi-purpose card or “smart” card.
- Computer, network or Internet password, user ID or key, unless the connection is secure or the transmission is encrypted. If you don’t know if the connection is secure or the transmission is encrypted, don’t use a Social Security number at all until you know.

Tip: A driver’s license number is also personal information limited to certain uses by law

You may use a driver's license number to check an employment applicant's driving record if that is relevant to the job duties.

MCL 257.208c authorizes an employer, or the employer’s agent or insurer to obtain or verify information relating either to the holder of a commercial driver license that is required under federal law or to the holder of a chauffeur's license that is required under Chapter 3 of the Michigan Vehicle Code. (MCL 257.208c)

Restrictions on using a driver's license number:

- Under the Freedom of Information Act, a driver's license number (or state personal identification number or Social Security number) must be redacted (edited out) before you release any portion of a voter registration record that contains the number, under the FOIA. (MCL 168.509gg) This includes any computer tape, disk or list of the names and addresses of the registered electors of the township requested by any person. (MCL 168.522)
- A township cannot use a driver's license number (or state personal identification number or Social Security number) on the outside of an envelope or package or on the inside of an envelope or package if the number is visible from the outside of the envelope or package in any way. (Disclosure of Personal Information on Documents Act, MCLs 37.251-37.252)

3. Inform each person of all uses of his or her Social Security number.

Right to refuse to disclose SSN
It is unlawful for a township to deny any individual any right, benefit, or privilege provided by law because that person refuses to disclose his or her SSN, unless:

1) the disclosure is required by federal law, or

2) is required to be made to a federal, state, or local agency operating a system of records that existed before January 1, 1975, to verify the identify of an individual, if that disclosure was required under statute or regulation adopted prior to that date. (Section 7(a) of the federal Privacy Act of 1974, 5 U.S.C. 552a, Note)

For example, when a township collects an employee's SSN for payroll purposes, language similar to the following could be attached to the form:

Mandated Use of
Social Security Number

As an employer, _____ Township is required by federal and state law to use Social Security numbers (SSNs) to report and withhold payroll taxes.

The township will use employee SSNs (including elected and appointed officials, employees, and volunteers to whom compensation is paid) for payroll functions, expense reimbursement, and federal and state income tax reporting purposes.

Similar language could be developed for other township uses of SSNs, including employment records and providing employee benefits.

Notice recommended
Any time a township requests that a person disclose his or her SSN, the township may wish to inform that person: 1) whether that disclosure is mandatory or voluntary, 2) by what statutory or other authority the SSN is solicited, and 3) what uses will be made of the SSN.

Note: This notice appears to be mandated for local government agencies by the text of Section 7(b) of the federal Privacy Act of 1974, 5 U.S.C. 552a, Note, but a subsequent opinion by the U.S. Court of Appeals for the 6th Circuit, which is binding in Michigan, ruled that Section 7(b) applies exclusively to federal agencies. See *Schmitt v City of Detroit*, 395 F.3d 327, January 2005. As a matter of public policy, a township may still wish to give notice of use of SSNs. Consider developing a disclosure statement that can be attached to any form that asks a person to submit a SSN. ***(See box)***

Do not disclose SSNs for any purposes NOT authorized by law without getting the consent of the person.

Right to inspect
An individual should be allowed to inspect and request corrections in his or her personal information. Each person should know that his or her SSN is being retained.

4. Keep Social Security numbers confidential.

Do **NOT display** complete SSNs or more than four digits of an SSN on:

- Materials **issued** to employees, volunteers, clients, vendors or other persons:
    - ID cards
    - Badges
    - Time cards
    - Attendance/absence sheets
    - Membership/participant cards (employee benefit programs)
    - Credit cards (township/business)
    - Password/access cards
    - ATM cards
    - Parking passes
    - Paycheck stubs

- Materials **posted** anywhere:
    - Employee rosters, lists or schedules
    - Bulletin board postings
    - Permits that must be posted
    - Exam/test results
    - Seniority lists

- **Identification** materials
    - Permits
    - Licenses
    - Certifications
    - Access cards
    - ID badges/cards

- **Any** materials or documents that may be on **public display**, including computer monitors, kiosks, shared files, email, Web sites, etc.

Tip: Social Security numbers are exempt from Freedom of Information Act disclosure

Michigan law prohibits disclosure of a Social Security number, and Social Security numbers are specifically exempt from FOIA disclosure (MCL 15.243(w). When records that are subject to disclosure under the FOIA contain SSNs, all SSNs must be "redacted" (covered prior to copying or viewing; "blacked" or "whited" out on copies).

Train all officials, employees, volunteers, student interns, independent contractors and other persons who might receive a FOIA request to know how they should get the request to the proper persons (FOIA coordinator and his/her designees) who can determine FOIA compliance AND ensure that SSNs are not disclosed.

Computers, Data, Digital Files and Network Security

Remember that SSNs must be protected even when they are in digital or electronic formats including floppy disks, ZIP disks, CDs, DVDs, flash drives/cards, external hard drives, tape backups, servers, workstation hard drives, laptops, personal digital assistants (PDAs) and wireless networks.

Modify databases and other programs so that no more than four digits of a SSN are displayed on a computer screen or in an onscreen or printed report.

If all or more than four digits of a SSN are displayed on a computer/PDA screen, arrange the monitor so that only authorized persons can see the screen. Set the computer's screen saver to activate within a short time if the program is not used and require a password to deactivate the screen saver.

Train staff to never leave a computer terminal unattended when SSNs are visible onscreen.

Require passwords to be changed often and have passwords expire at regular intervals. Train all staff to follow password and virus protection procedures.

If a database requires the use of all or more than four digits of a SSN, have the database modified so it automatically cross-references between the SSNs and other information using conversion tables.

Mail

Do not use all or more than four digits of a SSN on any mailing materials, including labels, envelopes, mailers, tracking/routing materials, etc.

If using windowed envelopes or mailers, ensure that a SSN will not be visible through the window, either directly or if the envelope or mailer is manipulated.

Email

Do not send or request SSNs by email or over the Internet unless the connection is secure or the SSN is encrypted.

5. Protect against unlawful disclosure of Social Security numbers.

Have a "clean desk" policy that requires all township personnel to return all documents and materials that contain SSNs to confidential locations when they are not at their workstations.

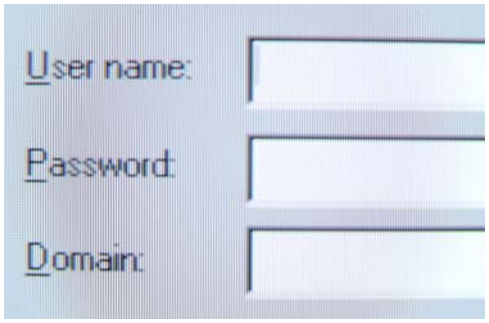
Do not take materials containing SSNs away from your office. If your office is in your home, never leave them where anyone else can see them, and take steps to adequately protect them by storing them in confidential locations that cannot be accessed by anyone not authorized to see them.

Have a **record retention schedule** and train all staff to use it (see General Schedule No. 10—Township Record Retention Schedule).

A record retention schedule identifies when a record may be destroyed. Records containing SSNs or confidential information should not be retained beyond their destruction date (unless a FOIA request has been received for a particular record or the township's legal counsel directs otherwise).

Destroy records that contain Social Security numbers by shredding or shredding and burning them. Store records awaiting disposal in a locked trash bin.

Have IT staff render SSNs in electronic files and databases irretrievable (by erasing and then physically destroying) before discarding the files, databases or the computer equipment. Limit the number of people capable of doing this.



Establish procedures to prevent former officials, employees, volunteers, student interns, and others from gaining access to SSNs or other confidential information. Have them turn over keys, badges, ID cards, access codes, etc., before they leave township service, and change any keys, locks, passwords, access codes, log-in codes, etc., that they had access to which would allow disclosure of SSNs or other confidential information.

Train all officials, employees, volunteers, student interns, and others who handle SSNs and other personal information to avoid disclosing that information to an unauthorized person who is trying to fraudulently access SSNs or other confidential information:

- Train staff to NOT give out SSNs to anyone
- Identify how SSNs may be used – and NOT used
- Identify who has authority to access SSNs and confidential information – and who does NOT (such as a person who calls or visits requesting SSNs or other confidential information on the fraudulent pretext of a family emergency, investigation, or banking matter)
- Adopt procedures for notifying all staff if an attempt is made by an unauthorized person to fraudulently access SSNs
- Consider using logs or electronic audit trails to monitor access to records with SSNs

6. Routinely train all personnel to properly handle Social Security numbers.

Train all officials, employees, volunteers, student interns, independent contractors and other persons who might come in contact with SSNs so that they understand that they must comply with the:

- Michigan Social Security Number Privacy Act
- Township's Social Security Number Privacy Policy
- Procedures and training regarding the use (or nonuse) of SSNs

Third Parties
If you use a third party company for anything that involves SSNs (payroll, medical benefits, etc.):

- Ensure they are aware of the township's SSN privacy policy
- Prohibit them from disclosing SSNs, except as required by state or federal law
- Monitor the third party's use of and safeguards for SSNs

Regularly audit the township's privacy practices
Privacy audits should be conducted to monitor the township's compliance.

7. Consider designating a chief privacy officer.

The township board may wish to consider designating at least one position as chief privacy officer, responsible for coordinating the township's privacy policies and compliance with those policies.

Depending on the number of township employees, any collective bargaining agreements/union contracts, programs and services provided, and whether the township is a charter township with a superintendent, a township board may want to consider designating any of several positions as chief privacy officer, such as (not in any order of preference):

- Superintendent
- Manager
- Human resources director
- FOIA coordinator
- Office manager
- Records specialist
- Information technology officer
- Township attorney

The Social Security Number Privacy Act does not require a township to have a chief privacy officer, but it is important to have at least one person who is familiar with the various statutes that require specific township information and records to be kept confidential.

8. Coordinate township privacy practices and policies.

The following are only some of the many state and federal statutes that impact the use and disclosure of township records. Consult your local legal counsel and human resource personnel to determine what statutes apply to your township.

- **Social Security Number Privacy Act**, MCL 445.81, *et seq*. (SSNPA)—Social Security numbers
- **Freedom of Information Act**, MCL 15.231, *et seq*. (FOIA)—information exempt from disclosure
- **Open Meetings Act**, MCL15.261, *et. seq*. (OMA)—closed session minutes
- **Michigan Vehicle Code** (MVC)—use of personal information, including driver's license and state personal identification numbers (MCL 257.208c)
- **Disclosure of Personal Information on Documents Act**, MCL 37.251, *et seq.*—mailing personal information
- **State Personal Identification Card Act**, MCL 28.291, *et seq*.—use of personal information
- **Bullard-Plawecki Employee Right-to-Know Act**, MCL 423.501, *et seq*.—access to and use of personnel records
- **Social Security Act**, 42 U.S.C. 405(c)(2)(C)(viii), (Social Security Act Amendments of 1990)
- **Social Security Administration Rules**, 20 C.F.R. Part 401 (use of Social Security numbers by Social Security Administration)
- **The Privacy Act of 1974**—disclosure of Social Security numbers and other information on individuals (5 U.S.C. 552a)
- **Health Insurance Portability and Accountability Act** (HIPAA)—medical information (Department of Health and Human Services HIPAA Web page)

9. Know what to do if Social Security numbers are improperly disclosed:

- Promptly consult the township's local legal counsel for specific guidance
- Promptly notify the individuals potentially affected
- Promptly notify the township's liability insurance carrier
- Take steps to determine how the SSNs were disclosed and prevent further disclosures

Resources and Links of Interest

Recommended Practices for Protecting the Confidentiality of Social Security Numbers, California Department of Consumer Affairs, June 2002, revised January 2003. http://www.privacy.ca.gov/ssn/ssn.htm

Social Security Numbers: Governments Could Do More to Reduce Display in Public Records and on Identity Cards, U.S. Governmental Accountability Office (GAO), November 2004. http://www.gao.gov/new.items/d0559.pdf

Social Security Numbers: SSNs Are Widely Used by Government and Could Be Better Protected, U.S. Governmental Accountability Office (GAO), April 2002, http://www.gao.gov/new.items/d02691t.pdf

University of Illinois Policy on Social Security Numbers, University of Illinois Web site: http://www.ssn.uillinois.edu/

Information Technology Policies and Guidelines at the University of Michigan, University of Michigan Web site: http://www.umich.edu/~policies/

Federal Trade Commission Privacy Initiatives Web pages: http://www.ftc.gov/privacy/index.html

SOCIAL SECURITY NUMBER PRIVACY ACT
Act 454 of 2004

AN ACT to establish the social security number privacy act in the state of Michigan; to prescribe penalties; and to provide remedies.

History: 2004, Act 454, Eff. Mar. 1, 2005.

The People of the State of Michigan enact:

445.81 Short title.

Sec. 1. This act shall be known and may be cited as the "social security number privacy act".

History: 2004, Act 454, Eff. Mar. 1, 2005.

445.82 Definitions.

Sec. 2. As used in this act:

(a) "Child or spousal support" means support for a child or spouse, paid or provided pursuant to state or federal law under a court order or judgment. Support includes, but is not limited to, any of the following:

(*i*) Expenses for day-to-day care.

(*ii*) Medical, dental, or other health care.

(*iii*) Child care expenses.

(*iv*) Educational expenses.

(*v*) Expenses in connection with pregnancy or confinement under the paternity act, 1956 PA 205, MCL 722.711 to 722.730.

(*vi*) Repayment of genetic testing expenses, under the paternity act, 1956 PA 205, MCL 722.711 to 722.730.

(*vii*) A surcharge paid under section 3a of the support and parenting time enforcement act, 1982 PA 295, MCL 552.603a.

(b) "Computer", "computer network", or "computer system" mean those terms as defined in section 2 of 1979 PA 53, MCL 752.792.

(c) "Internet" means that term as defined in 47 U.S.C. 230.

(d) "Mailed" means delivered by United States mail or other delivery service that does not require the signature of recipient indicating actual receipt.

(e) "Person" means an individual, partnership, limited liability company, association, corporation, public or nonpublic elementary or secondary school, trade school, vocational school, community or junior college, college, university, state or local governmental agency or department, or other legal entity.

(d) "Publicly display" means to exhibit, hold up, post, or make visible or set out for open view, including, but not limited to, open view on a computer device, computer network, website, or other electronic medium or device, to members of the public or in a public manner. The term does not include conduct described in section 3(1)(b), (c), or (f).

(e) "Title IV-D agency" means that term as defined in section 2 of the support and parenting time enforcement act, 1982 PA 295, MCL 552.602.

(f) "Vital record" means that term as defined in section 2805 of the public health code, 1978 PA 368, MCL 333.2805.

(g) "Website" means a collection of pages of the world wide web or internet, usually in HTML format, with clickable or hypertext links to enable navigation from 1 page or section to another, that often uses associated graphics files to provide illustration and may contain other clickable or hypertext links.

History: 2004, Act 454, Eff. Mar. 1, 2005.

Compiler's note: In subdivision (b), the phrase "mean those terms" evidently should read "means those terms."

Following the first occurrence of subdivision (e), subdivision (d) should evidently be designated subdivision (f), subdivision (e) should evidently be designated subdivison (g), subdivison (f) should evidently be designated (h), and subdivison (g) should evidently be designated (i).

445.83 Prohibited use of social security number of employee, student, or other individual; exceptions.

Sec. 3. (1) Except as provided in subsection (2), a person shall not intentionally do any of the following with the social security number of an employee, student, or other individual:

(a) Publicly display all or more than 4 sequential digits of the social security number.

(b) Subject to subsection (3), use all or more than 4 sequential digits of the social security number as the primary account number for an individual. However, if the person is using the social security number under

subdivision (c) and as the primary account number on the effective date of this act, this subdivision does not apply to that person until January 1, 2006.

(c) Visibly print all or more than 4 sequential digits of the social security number on any identification badge or card, membership card, or permit or license. However, if a person has implemented or implements a plan or schedule that establishes a specific date by which it will comply with this subdivision, this subdivision does not apply to that person until January 1, 2006, or the completion date specified in that plan or schedule, whichever is earlier.

(d) Require an individual to use or transmit all or more than 4 sequential digits of his or her social security number over the internet or a computer system or network unless the connection is secure or the transmission is encrypted.

(e) Require an individual to use or transmit all or more than 4 sequential digits of his or her social security number to gain access to an internet website or a computer system or network unless the connection is secure, the transmission is encrypted, or a password or other unique personal identification number or other authentication device is also required to gain access to the internet website or computer system or network.

(f) Include all or more than 4 sequential digits of the social security number in or on any document or information mailed or otherwise sent to an individual if it is visible on or, without manipulation, from outside of the envelope or packaging.

(g) Subject to subsection (3), beginning January 1, 2006, include all or more than 4 sequential digits of the social security number in any document or information mailed to a person, unless any of the following apply:

(*i*) State or federal law, rule, regulation, or court order or rule authorizes, permits, or requires that a social security number appear in the document.

(*ii*) The document is sent as part of an application or enrollment process initiated by the individual.

(*iii*) The document is sent to establish, confirm the status of, service, amend, or terminate an account, contract, policy, or employee or health insurance benefit or to confirm the accuracy of a social security number of an individual who has an account, contract, policy, or employee or health insurance benefit.

(*iv*) The document or information is mailed by a public body under any of the following circumstances:

(A) The document or information is a public record and is mailed in compliance with the freedom of information act, 1976 PA 442, MCL 15.231 to 15.246.

(B) The document or information is a copy of a public record filed or recorded with a county clerk or register of deeds office and is mailed by that office to a person entitled to receive that record.

(C) The document or information is a copy of a vital record recorded as provided by law and is mailed to a person entitled to receive that record.

(*v*) The document or information is mailed by or at the request of an individual whose social security number appears in the document or information or his or her parent or legal guardian.

(*vi*) The document or information is mailed in a manner or for a purpose consistent with subtitle A of title V of the Gramm-Leach-Bliley act, 15 USC 6801 to 6809; with the health insurance portability and accountability act of 1996, Public Law 104-191; or with section 537 or 539 of the insurance code of 1956, 1956 PA 218, MCL 500.537 and 500.539.

(2) Subsection (1) does not apply to any of the following:

(a) A use of all or more than 4 sequential digits of a social security number that is authorized or required by state or federal statute, rule, or regulation, by court order or rule, or pursuant to legal discovery or process.

(b) A use of all or more than 4 sequential digits of a social security number by a title IV-D agency, law enforcement agency, court, or prosecutor as part of a criminal investigation or prosecution, or providing all or more than 4 sequential digits of a social security number to a title IV-D agency, law enforcement agency, court, or prosecutor as part of a criminal investigation or prosecution.

(3) It is not a violation of subsection (1)(b) or (g) to use all or more than 4 sequential digits of a social security number if the use is any of the following:

(a) An administrative use of all or more than 4 sequential digits of the social security number in the ordinary course of business, by a person or a vendor or contractor of a person, to do any of the following:

(*i*) Verify an individual's identity, identify an individual, or do another similar administrative purpose related to an account, transaction, product, service, or employment or proposed account, transaction, product, service, or employment.

(*ii*) Investigate an individual's claim, credit, criminal, or driving history.

(*iii*) Detect, prevent, or deter identity theft or another crime.

(*iv*) Lawfully pursue or enforce a person's legal rights, including, but not limited to, an audit, collection, investigation, or transfer of a tax, employee benefit, debt, claim, receivable, or account or an interest in a receivable or account.

(*v*) Lawfully investigate, collect, or enforce a child or spousal support obligation or tax liability.

(*vi*) Provide or administer employee or health insurance or membership benefits, claims, or retirement programs or to administer the ownership of shares of stock or other investments.

(b) A use of all or more than 4 sequential digits of a social security number as a primary account number that meets both of the following:

(*i*) The use began before the effective date of this act.

(*ii*) The use is ongoing, continuous, and in the ordinary course of business. If the use is stopped for any reason, this subdivision no longer applies.

History: 2004, Act 454, Eff. Mar. 1, 2005.

445.84 Privacy policy.

Sec. 4. (1) Beginning January 1, 2006, a person who obtains 1 or more social security numbers in the ordinary course of business shall create a privacy policy that does at least all of the following concerning the social security numbers the person possesses or obtains:

(a) Ensures to the extent practicable the confidentiality of the social security numbers.

(b) Prohibits unlawful disclosure of the social security numbers.

(c) Limits who has access to information or documents that contain the social security numbers.

(d) Describes how to properly dispose of documents that contain the social security numbers.

(e) Establishes penalties for violation of the privacy policy.

(2) A person that creates a privacy policy under subsection (1) shall publish the privacy policy in an employee handbook, in a procedures manual, or in 1 or more similar documents, which may be made available electronically.

(3) This section does not apply to a person who possesses social security numbers in the ordinary course of business and in compliance with the fair credit reporting act, 15 USC 1681 to 1681v, or subtitle A of title V of the Gramm-Leach-Bliley act, 15 USC 6801 to 6809.

History: 2004, Act 454, Eff. Mar. 1, 2005.

445.85 Exemption from disclosure.

Sec. 5. All or more than 4 sequential digits of a social security number contained in a public record are exempt from disclosure under the freedom of information act, 1976 PA 442, MCL 15.231 to 15.246, pursuant to section 13(1)(d) of the freedom of information act, 1976 PA 442, MCL 15.243.

History: 2004, Act 454, Eff. Mar. 1, 2005.

445.86 Violation of MCL 445.83 as misdemeanor; penalty; recovery of damages in civil action.

Sec. 6. (1) A person who violates section 3 with knowledge that the person's conduct violates this act is guilty of a misdemeanor punishable by imprisonment for not more than 93 days or a fine of not more than $1,000.00, or both.

(2) An individual may bring a civil action against a person who violates section 3 and may recover actual damages. If the person knowingly violates section 3, an individual may recover actual damages or $1,000.00, whichever is greater. If the person knowingly violates section 3, an individual may also recover reasonable attorney fees. Except for good cause, not later than 60 days before filing a civil action, an individual must make a written demand to the person for a violation of section 3 for the amount of his or her actual damages with reasonable documentation of the violation and the actual damages caused by the violation. This subsection does not apply to a person for conduct by an employee or agent of the person in violation of a privacy policy created pursuant to section 4 or in compliance with the fair credit reporting act, 15 USC 1681 to 1681v, or subtitle A of title V of the Gramm-Leach-Bliley act, 15 USC 6801 to 6809, if the person has taken reasonable measures to enforce its policy and to correct and prevent the reoccurrence of any known violations.

History: 2004, Act 454, Eff. Mar. 1, 2005.

445.87 Effective date.

Sec. 7. This act takes effect March 1, 2005.

History: 2004, Act 454, Eff. Mar. 1, 2005.