MIKE DEWINE
OHIO ATTORNEY GENERAL

SECURITY BREACHES AND COMPROMISE OF PERSONAL INFORMATION - FOR STATE AND LOCAL AGENCIES IN OHIO -

According to the Privacy Rights Clearinghouse, more than 165 million records containing sensitive personal information have been involved in United States data security breaches since 2005. Some of the ways that security breaches have occurred include: thieves hacking into computer files; back-up tapes lost during shipping; information sold to criminals by dishonest employees; and stolen computer equipment. While some security breaches may not be preventable, most can be planned for. This publication will guide state and local agencies on the steps to take – required and recommended – when involved in a security breach where individuals' personal information is compromised.

APPLICABLE LAW ON PERSONAL INFORMATION – PROTECTION AND NOTIFICATION WHEN COMPROMISED

Federal[1]

The Health Insurance Portability And Accountability Act of 1996 (HIPAA) Security Standards Rule, 45 C.F.R. Part 164 - health-care-covered entities.

The Children's Online Privacy Protection Act of 1998 (COPPA), 15 U.S.C. Section 6501 - owner or operator of a website or online service directed to children, or any operator that collects or maintains personal information from a child.

Financial Modernization Act of 1999 / Gramm-Leach-Blilely Act (GLBA) – financial institutions, including banks, securities firms, insurance companies, and companies providing other types of financial products and services to consumers. including lending, brokering or servicing any type of consumer loan, transferring or safeguarding money, preparing individual tax returns, providing financial advice or credit counseling, providing residential real estate settlement services, collecting consumer debts and an array of other activities.

The Federal Information Security Management Act of 2002, 44 U.S.C. Section 3541 - federal government agencies.

The FTC's Disposal Rule, 69 Fed. Reg. 68, 690 – all persons and groups that use consumer reports.

[1] Congressional Research Service Report for Congress, 2/3/06, *Data Security: Federal and State Laws;* Federal Trade Commission, *The Gramm-Leach-Bliley Act*.

Ohio

Ohio Revised Code Sections 1347.01, 1347.04, 1347.06, 1347.10, 1347.12

Highlights of these ORC sections include:[2]

Exempts from these requirements any state or local agency that performs as its principal function any activity relating to the enforcement of criminal laws, including the police, criminal courts, prosecutors, and authority of probation, pardon and parole.

Specifies that a state or local agency or officer or employee of such who complies in good faith with a rule applicable to the agency is not subject to criminal prosecution under these requirements.

Requires that a state or local agency shall only use the personal information in a personal information system in a manner that is consistent with the purposes of the system.

Permits any person harmed by the use of personal information maintained in a personal information system to recover damages in a civil action from any person who directly and proximately caused the harm; permits a court of competent jurisdiction to enjoin any person, or state or local agency, who violates or proposes to violate these requirements.

Requires any state agency or agency of a political subdivision that owns or licenses computerized data that includes personal information of a specified nature to disclose, in the most expedient time possible but generally not later than 45 days following its discovery or notification of the security breach, any breach of the security of the system to any Ohio resident whose personal information was, or reasonably is believed to have been, accessed and acquired by an unauthorized person if the access and acquisition by the unauthorized person causes or reasonably is believed will cause a material risk of identity theft or other fraud to the resident.

Requires any state agency or agency of a political subdivision that, on behalf of or at the direction of another state agency or agency of a political subdivision, is the custodian of or stores computerized data that includes personal information of a specified nature to notify that other state agency or agency of a political subdivision of any breach of the security of the system in an expeditious manner, if the personal information was, or reasonably is believed to have been, accessed and acquired by an unauthorized person and if the access and acquisition by the unauthorized person causes or reasonably is believed will cause a material risk of identity theft or other fraud to a resident of Ohio.

Permits a state agency or agency of a political subdivision to delay the required disclosure or notification if a law enforcement agency determines that the disclosure or notification will impede a criminal investigation or jeopardize homeland or national security.

[2] Legislative Service Commission, Bill Analysis – in part.

Specifies the methods by which a state agency or agency of a political subdivision may disclose or make a notification as required by the act.

Requires a state agency or agency of a political subdivision that discovers circumstances requiring disclosure to more than 1,000 Ohio residents involved in a single occurrence of a breach of the security of the system to notify without unreasonable delay all consumer reporting agencies that compile and maintain files on consumers on a nationwide basis of the timing, distribution, and content of the disclosure given to Ohio residents pursuant to the act; provides that, in no case may a state agency or agency of a political subdivision delay any disclosure or notification required under the provisions described in the preceding dot points in order to make the notification to consumer reporting agencies.

Authorizes the Attorney General to conduct an investigation and grants the Attorney General subpoena authority if the Attorney General has reason to believe that a state agency or agency of a political subdivision has failed or is failing to comply with the act's requirements, and prescribes procedures upon issuance of a subpoena by a court.

Grants the Attorney General the exclusive authority to bring a civil action in a court of common pleas if it appears that a state agency or agency of a political subdivision has failed or is failing to comply with the act's requirements and requires the court, upon a finding of such failure, to impose a civil penalty of a specified amount per day for each day the state agency or agency of a political subdivision fails to comply with the act.

Specifies that a public official, public employee, or person who maintains or is employed by a person who maintains a personal information system for a state or local agency, who purposefully refuses to comply with these requirements is guilty of a minor misdemeanor.

PRECAUTIONARY STEPS FOR STATE AND LOCAL AGENCIES TO PROTECT INFORMATION

The Federal Trade Commission offers a free guide for businesses on protecting personal information: *Protecting Personal Information, A Guide for Business* – parts of which may be relevant to state and local agencies. It can be downloaded at: http://www.ftc.gov/infosecurity/. According to the FTC, the 5 Key Principles of a sound data security plan are:

1. Take stock – Know what personal information you have in your files and on your computers.
    a. Inventory all places where sensitive data is stored, including electronic equipment and hard-copy storage.
    b. Track personal information through the business by talking with the various departments of the company, including sales, information technology, human resources, accounting, and any outside service providers.

    c. Recognize that different types of information – e.g., social security numbers, credit cards or financial information, and home addresses – present varying types of risk.
2. Scale down – Keep only what you need for your business.
    a. Use social security numbers only for required and lawful purposes.
    b. Don't keep customer credit card information unless there is a business need for it.
    c. Check the default settings on company software to make sure unnecessary information is not being kept inadvertently.
    d. Develop a written records retention policy to identify what information must be kept, how it will be secured, how long to keep it, and how to properly dispose of it.
3. Lock it – Protect the Information that you keep.
    a. Store anything that contains personal information – paper documents or files, cds, zip drives, and backup tapes – in a locked room or locked file cabinet. Limit and control employee access to that location.
    b. Require employees, at the end of their work day, to put away files, log off their computers, and lock their file cabinets and office doors.
    c. Implement appropriate access control for the building.
    d. If personal information is shipped off-site, encrypt the information and inventory the information being shipped.
    e. Regarding electronic security – general network security, password management, laptop security, firewalls, wireless and remote access, and detecting breaches - understand the vulnerabilities of the business' computer system and follow the advice of experts in the field.
    f. Explain the data security plan to the staff and train them to spot security vulnerabilities. Also consider reference or background checks, confidentiality agreements, limited access to information, procedures for employees who leave or transfer, regular training schedules, and discipline for security policy violations.
4. Pitch it – Properly dispose of what you no longer need.
    a. Dispose of paper records by shredding, burning or pulverizing before discarding. Make shredders available throughout the workplace.
    b. When disposing of old electronic equipment, use wipe utility programs.
    c. Make sure employees who work from home follow all security procedures.
5. Plan ahead – Create a plan to respond to security incidents.
    a. If a computer is compromised, disconnect it immediately from the Internet.
    b. Investigate security incidents immediately.
    c. Consider who must and should be notified, inside and outside the organization, when a security incident occurs.

STEPS FOR STATE AND LOCAL AGENICES IF INFORMATION COMPROMISED

The Federal Trade Commission offers a free guide for businesses in responding to personal information compromises: *FTC Facts for Business – Information Compromise and the Risk of Identity Theft: Guidance for Your Business* – parts of which may be relevant to state and local agencies. It can be downloaded at http://www.ftc.gov/bcp/edu/pubs/business/idtheft/bus59.shtm. The general areas highlighted include:

1. Notifying Law Enforcement – When the compromise could result in harm to a person or business, call your local police department immediately.
    a. If the local police are not familiar with investigation information compromises, contact the local office of the FBI or Secret Service.
2. Notifying Affected Businesses – Information compromises can have an impact on businesses other than yours.
    a. If another institution maintains accounts for you or you collect or store personal information on behalf of another business, notify them of any information compromise.
    b. If social security numbers have been stolen, you can contact the major credit bureaus for advice.
        i. TransUnion www.transunion.com 1-800-680-7289
        ii. Equifax www.equifax.com 1-888-766-0008
        iii. Experian www.experian.com 1-888-397-3742
3. Notifying Individuals – Generally, early notification to individuals whose personal information has been compromised allows them to take steps to mitigate the misuse of their information.
    a. Consult with law enforcement about timing of notification so it does not impede their investigation.
    b. Designate a contact person within your organization for releasing information.
    c. Your notice to individuals should:
        i. Describe clearly what you know about the compromise
        ii. Explain what responses may be appropriate for the type of information taken.
        iii. Includes current information about responding to potential cases of identity theft.
4. Model Letter – A model letter for notifying people whose names and Social Security numbers have been stolen is included in the FTC guide.