REPORTING BREACHES OF DATABASES

Thomas P. Brady
313.965.8291
tbrady@clarkhill.com

Brian D. Shekell
313.965.8803
bshekell@clarkhill.com

CLARK HILL

OBJECTIVES

- When does a security breach occur?
- When is notice required?
- Who is entitled to notice?
- What notice is required?
- What are the penalties for failing to give notice?
- What preventive measures should human resources take now?

WHAT IS A SECURITY BREACH?

Security breach means:

- 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.

WHAT IS PERSONAL INFORMATION?

"Personal information" means the **first name or first initial and last name** linked to one or more of the following data elements of a resident of this state:

- Social security number
- Driver license number or state personal identification card number
- Demand deposit or other financial account number, or credit card or debit card number, in combination with any required security code, access code, or password that would permit access to any of the resident's financial accounts

WHAT IS A DATABASE?

- The Act does not define database
- The Act defines data as “computerized personal information”
- The dictionary defines data base as “a collection of data arranged for ease and speed of retrieval, as by a computer”

EXAMPLES OF DATABASES

- Computerized personnel files
- Computerized medical or workers' compensation files
- Payroll Records

IS A BREACH BY AN EMPLOYEE A VIOLATION OF THE ACT?

A security breach does not include unauthorized access to data by an employee or other individual if the access meets all of the following:

- The employee or other individual acted in good faith in accessing the data
- The access was related to the activities of the agency or person
- The employee or other individual did not misuse any personal information or disclose any personal information to an unauthorized person

WHEN IS NOTICE OF A SECURITY BREACH REQUIRED?

Notice is required if:

- There was a security breach
- The security breach is likely to cause:
  - substantial loss or injury to, or
  - result in identity theft
  - with respect to, 1 or more residents of this state; and either
- The resident's unencrypted and un-redacted personal information was accessed and acquired by an unauthorized person; or
- The resident's personal information was accessed and acquired in encrypted form by a person with unauthorized access to the encryption key

HOW IS “SUBSTANTIAL LOSS OR INJURY” OR IDENTITY THEFT DETERMINED?

When determining whether a substantial loss, injury or identity theft is likely, a person or agency must act with the care an ordinarily prudent person or agency in like position would exercise under similar circumstances

WHAT IS IDENTITY THEFT?

With intent to defraud or violate the law, use or attempt to use the personal identifying information of another person to do either of the following:

- Obtain credit, goods, services, money, property, a vital record, a confidential telephone record, medical records or information, or employment
- Commit another unlawful act
- By concealing, withholding, or misrepresenting the person's identity, use or attempt to use the personal identifying information of another person to do either of the following:
  - obtain credit, goods, services, money, property, a vital record, a confidential telephone record, medical records or information, or employment
  - commit another unlawful act

WHAT IS PERSONAL IDENTIFYING INFORMATION?

"Personal identifying information" means 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

EXAMPLES OF PERSONAL IDENTIFYING INFORMATION

Persons name

Address

Telephone number

Diver license or State Id

SSN

Place of employment

Employee Id number

Passport number

Health insurance number

Mother’s maiden name

Bank account number

Account password

Stock account number

Credit card number

Vital record

Medical record or information

WHO MUST GIVE NOTICE?

- Notice must be given by the “person or agency that owns or licenses data that are included in a database that discovers a security breach, or receives notice of a security breach”
- Unless the person or agency determines that the security breach has not or 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 that maintains a database that includes data that the person or agency does not own or license that discovers a breach of the security of the database shall provide a notice to the owner or licensor of the information of the security breach

WHEN MUST THE NOTICE BE SENT?

- The notice must be given without unreasonable delay
- Delay is allowed if:
  - The person or agency needs to investigate if a security breach occurred
  - A law enforcement agency has told the person or agency responsible for giving notice that the notice will impede a criminal or civil investigation or jeopardize homeland security or national security

WHAT MUST THE NOTICE CONTAIN?

The notice must:

- Be written in a clear and conspicuous manner
- Describe the security breach in general terms
- Describe the type of personal information that is the subject of the unauthorized access or use
- If applicable, generally describe what the agency or person providing the notice has done to protect data from further security breaches
- Include a telephone number where a notice recipient may obtain assistance or additional information
- Remind notice recipients of the need to remain vigilant for incidents of fraud and identity theft

HOW MUST THE NOTICE BE GIVEN?

- Written notice sent to the recipient at the recipient's postal address in the records of the agency or person
- Written notice sent electronically to the recipient
- If not otherwise prohibited by state or federal law, notice given by telephone and/or
- Substitute notice

MODEL LETTER

MODEL LETTER FOR THE
COMPROMISE OF SOCIAL SECURITY NUMBERS

Dear _____:

We are contacting you about a potential problem involving identity theft. [Describe the information compromise and how you are responding to it.]

We recommend that you place a fraud alert on your credit file. A fraud alert tells creditors to contact you before they open any new accounts or change your existing accounts. Call any one of the three major credit bureaus. As soon as one credit bureau confirms your fraud alert, the others are notified to place fraud alerts. All three credit reports will be sent to you, free of charge, for your review. The numbers of the credit bureaus are:

Equifax, 800-685-1111, Experian, 888-397-3742, TransUnionCorp, 800-680-7289

Even if you do not find any suspicious activity on your initial credit reports, the Federal Trade Commission (FTC) recommends that you check your credit reports periodically. Victim information sometimes is held for use or shared among a group of thieves at different times. Checking your credit reports periodically can help you spot problems and address them quickly.

If you find suspicious activity on your credit reports or have reason to believe your information is being misused, call [insert contact information for law enforcement] and file a police report. Get a copy of the report; many creditors want the information it contains to absolve you of the fraudulent debts. You also should file a complaint with the FTC at www.consumer.gov/idtheft or at 1-877-ID-THEFT (877-438-4338). Your complaint will be added to the FTC's Identity Theft Data Clearinghouse, where it will be accessible to law enforcers for their investigations.

We have enclosed a copy of *Take Charge: Fighting Back Against Identity Theft*, a comprehensive guide from the FTC to help you guard against and deal with identity theft.

[Insert closing]
Your Name

WHEN MAY THE NOTICE BE SENT ELECTRONICALLY?

The notice can be sent electronically if any of the following conditions are met:

- The recipient has expressly consented to receive electronic notice
- 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
- The person or agency conducts its business primarily through internet account transactions or on the internet

WHEN MAY THE NOTICE BE GIVEN BY TELEPHONE?

The notice can be given by telephone if all of the following conditions are met:

- The notice is not given in whole or in part by use of a recorded message; **and**
- 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 in writing or electronically if the notice by telephone does not result in a live conversation between the individual representing the person or agency and the recipient within 3 business days after the initial attempt to provide telephonic notice

WHEN MAY SUBSTITUTE NOTICE BE GIVEN?

Substitute service may be given if the cost of providing written, electronic or telephone notice exceeds $250,000 or the notice must be provided to more than 500,000 Michigan residents

HOW MAY SUBSTITUTE SERVICE BE GIVEN?

- 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
- If the person or agency maintains a website, conspicuously posting the notice on that website
- 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

HOW ARE CONSUMER REPORTING AGENCIES NOTIFIED?

- After a person or agency provides a notice under this section, the person or agency shall notify each consumer reporting agency that compiles and maintains files on consumers on a nationwide basis of the security breach without unreasonable delay
- A notification under this subsection shall include the number of notices that the person or agency provided to residents of this state and the timing of those notices

CREDIT REPORTING AGENCIES

- Equifax, PO Box 105873, Atlanta, GA 30348, (800) 685-1111
- Experian, PO Box 2002, Allen, TX 75013, (888) 397-3742
- TransUnion, POBox 2000, Chester, PA 19022, (800) 888-4213

EXCEPTIONS TO NOTIFYING CONSUMER REPORTING AGENCIES

Notice to a consumer reporting agency is not necessary if either of the following is met:

- The person or agency is required under this section to provide notice of a security breach to 1,000 or fewer residents of this state
- The person or agency is subject to Title V of the Gramm-Leach-Bliley Act, *15 USC 6801* to 6809

SPECIAL INDUSTRY EXCEPTIONS

- Financial Institutions
- Persons or Agencies subject to and complying with HIPAA
- Public Utilities

WHAT ARE THE PENALTIES FOR NON-COMPLIANCE?

- A person who knowingly fails to provide the notice may be ordered to pay a civil fine of not more than $ 250.00 for each failure to provide notice
- The aggregate liability for civil fines under subsection (13) for multiple violations of subsection (13) that arise from the same security breach shall not exceed $ 750,000.00
- The attorney general or a prosecuting attorney may bring an action to recover a civil fine

CAN SOMEONE SUE FOR FAILURE TO GIVE NOTICE?

- Civil remedy for a violation of state or federal law are available

DOES THE ACT REQUIRE DESTRUCTION OF DATA

- A person or agency that maintains a database that includes personal information regarding multiple individuals shall destroy any data that contain personal information concerning an individual 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
- This does not prohibit a person or agency from retaining data that contain personal information for purposes of an investigation, audit, or internal review

HOW MUST THE DATA BE DESTROYED?

“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

ARE THERE EXCEPTIONS TO THE DESTRUCTION OF DATA?

A person or agency is considered to be in compliance with this section if:

- The person or agency is subject to federal law concerning the disposal of records containing personal identifying information and
- The person or agency is in compliance with that federal law

WHAT IS THE PENALTY FOR FAILING TO DESTROY DATA?

- A person who knowingly violates this section of the Act is guilty of a misdemeanor punishable by a fine of not more than $ 250.00 for each violation
- This subsection of the Act does not affect the availability of any civil remedy for a violation of state or federal law

ARE THERE PENALTIES FOR SENDING OUT FALSE NOTICES?

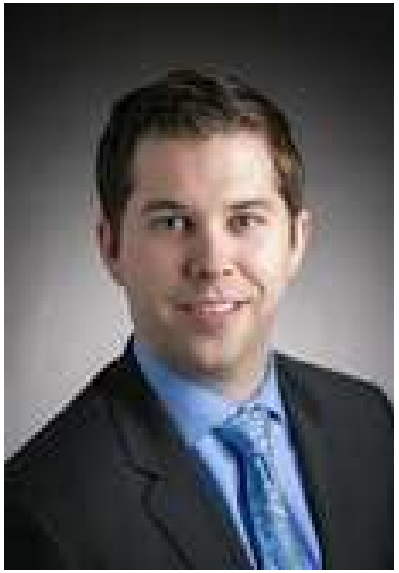
- A person that provides notice of a security breach when a security breach has not occurred, with the intent to defraud, is guilty of a misdemeanor punishable by imprisonment for not more than 93 days or a fine of not more than $ 250.00 for each violation, or both
- For a second violation, by imprisonment for not more than 93 days or a fine of not more than $ 500.00 for each violation, or both
- For a third or subsequent violation, by imprisonment for not more than 93 days or a fine of not more than $ 750.00 for each violation, or both

WHAT PREVENTIVE MEASURES SHOULD YOU TAKE?

- Have a plan
- Have a computer, e-mail and voice mail policy
- Review your data security measures
- Train your employees in proper data security

QUESTIONS?

Thomas P. Brady
313.965.8291
tbrady@clarkhill.com



Brian D. Shekell
313.965.8803
bshekell@clarkhill.com

Note: This document is not intended to give legal advice. It is comprised of general information. Employees facing specific issues should seek the assistance of an attorney.

CLARK HILL

ARIZONA | DELAWARE | ILLINOIS | MICHIGAN | NEW JERSEY | PENNSYLVANIA | WASHINGTON, DC | WEST VIRGINIA