



Unauthorized Disclosure of Personal Information –
What Should an Organization Do?

John C. Thomure, Jr.

Have You Encountered This Scenario?

- As a manager, it has just been brought to your attention that an assistant benefits clerk who was working on updating benefit and payroll information on her laptop computer at home had her car stolen with the laptop inside from the Company parking lot.
- As a manager, it has just been brought to your attention that an employee in the admissions department inadvertently e-mailed the names and social security numbers of hundreds of students to an outside vendor

2

Wisconsin Legal Requirements

- Wisconsin Statute § 134.98 – Notice of Unauthorized Acquisition of Personal Information
- Originally passed in 2005 and subsequently amended on two different occasions by the Legislature
- Wisconsin joins numerous other states who have similar statutory notice requirements
- Consider whether other state's laws may be implicated because of the residency of the person whose information was erroneously disseminated

3

I. Who Is Covered?

- Entity:
 - A person, other than an individual, that:
 - Conducts business in the state and maintains personal information in the ordinary course of business
 - Licenses personal information in this state
 - Maintains for a resident of the state a depository account
 - Lends money to a resident of this state

I. Who is Covered? (continued)

- Entity Also Includes:
 - Any office, department, independent agency, authority, institution, association, society or body in state government created or authorized to be created by any law
 - The legislature and the courts
 - A city, village, town or county

II. What Information is Covered?

- "Personal Information" means:
 - An individual's last name and first name or first initial +
 - The individual's social security number
 - The individual's driver's license number or state identification number
 - An individual's financial account number
 - The individual's DNA profile
 - An individual's otherwise unique biometric data

III. When Is Notice Required?

- An entity whose principal place of business is located in this state
- Or an entity that maintains or licenses personal information in this state
- Knows that personal information in the entity's possession has been acquired by someone who the entity has not authorized to acquire the information
- Shall make reasonable efforts to notify the subject of the personal information

When Is Notice Required? (continued)

- Also applies to entities whose principal place of business is not located in the state if the personal information pertains to a resident of the state
- Also applies to a person, other than an individual, that stores personal information pertaining to a resident of the state, but does not own or license the personal information

Special Rule for 1,000 or More

- If as a result of a single incident, you have to notify 1,000 or more individuals, the entity shall also without unreasonable delay notify all consumer reporting agencies

Exceptions to the Requirement of Notice

- The acquisition of personal information does not create a material risk of identity theft or fraud to the subject of the personal information
- The personal information was acquired in good faith by an employee or agent of an entity and used for a lawful purpose of the entity

Law Enforcement Exception

- In order to protect an investigation or homeland security, law enforcement may ask the entity not to provide the notice otherwise required

Timing and Manner of Notice

- Must provide notice to persons affected within a reasonable time, not to exceed 45 days, after the entity learns of the breach
- Notice should be provided by mail or by method that the entity previously communicated with the subject of the personal information
- If requested by the person who received a notice, the entity must provide the person with information regarding what was acquired

Affect on Civil Claim

- Failure to comply with the notice requirement is not negligence or a breach of any duty, **but may be evidence of negligence or a breach of a legal duty**
- Increase in litigation by persons whose information is leaked

13

Practical Considerations

- Who sends the notice?
 - Level of security
 - Publicity
- What should notice include?
 - Suggest taking steps at ftc.gov
 - Credit monitoring services
- Coordinated response contact for consistent messaging and release of information regarding breach

14

Federal Law Update

- Red Flags Rule
 - In November 2007, the Federal Trade Commission (FTC), the federal bank regulatory agencies, and the National Credit Union Administration (NCUA) issued regulations (***the Red Flags Rule***) requiring certain institutions and creditors to develop and implement written identity theft prevention programs

15

Red Flags Rule

- What is a Red Flag?
 - A Red Flag is an indicator of possible identity theft
- What is the Purpose of the Red Flags Rule?
 - To protect personal identifying information
 - Social Security Numbers
 - Credit Card Numbers
 - Insurance Enrollment or Coverage Data

Who Must Comply with the Red Flags Rule?

- Creditors
 - Any entity that regularly defers payments for goods or services or arranges for the extension of credit
- Financial Institutions
 - State or federal bank, state or federal savings and loan association, a mutual savings bank, state or federal credit union
- Transaction Account
 - Deposit or other account from which the owner makes payments or transfers: checking accounts, savings deposits subject to automatic transfers
- Covered Account
 - Account used for personal purposes involving multiple payments or transactions: credit card, mortgage loans, utility accounts, etc.

Red Flags Rule Requirements

- If you are covered by the Red Flags Rule you must:
 - Identify the kinds of red flags that are relevant to your business;
 - Explain your process for detecting them;
 - Describe how you'll respond to red flags to prevent and mitigate identity theft;
 - Provide for training of staff; and
 - Spell out how you'll keep your program current

Red Flags Rule and Insurance Companies

- Are Insurance Companies Covered by the Rule?
 - The Red Flags Rule should not apply to an insurer when engaged in activities related to insurance underwriting
 - HOWEVER** If an insurer extends credit, they may be covered
 - Finance premiums
 - Extend credit to vendor or agents
 - Extend credit to business partners
 - Extend credit with investment activities

Compliance with Red Flags Rule

- Compliance Date: June 1, 2010
 - Compliance date delayed at request of members of Congress
 - Previously set for May 1, 2009; Nov. 1, 2009; & Nov. 1, 2008
- Penalties for non-compliance
 - No criminal penalties
 - Financial penalties
 - Fines of up to \$2,500 per violation
 - Regulatory enforcement actions

Government Resources for Compliance

- <http://www.ftc.gov/redflagsrule>


