

# Identity Theft and the Human Resources Professional

Eric Suter  
Barley Snyder LLC  
February 13, 2007

# Overview

Part 1: Introduction to Identity Theft

Part 2: Identity Theft from an HR Perspective

Part 3: Pennsylvania Law – SSNs & Breach Disclosure

Part 4: Federal Law – The “Shredder Law”

Part 5: A Cautionary Tale – *Bell v. AFL-CIO Local 1023*

# Identity Theft: A General Definition

- Identity theft, in its garden variety, occurs when an individual uses another person's name and personal information for financial gain.
- Other types of ID theft:
  - Criminal Identity Theft
  - Medical Identity Theft
  - Job-Related Identity Theft

# Pennsylvania Law

- Pennsylvania defines criminal identity theft as the:

“possess[ion] or use[], through any means, [of] **identifying information** of another person without the consent of that other person to further any unlawful purpose.”

18 P.S. § 4120

# “Identifying Information”

- Broadly inclusive definition:

“Any document, photographic, pictorial or computer image of another person, or any fact used to establish identity, including, but not limited to, a name, birth date, Social Security Number, driver’s license number, nondriver governmental identification number, telephone number, checking account number, savings account number, student identification number, employee or payroll number or electronic signature”

# The Scope of the Problem (1)

- US Adult Victims of Identity Theft/Fraud
  - 2003: 10.1 million
  - 2005: 9.3 million
  - 2006: 8.9 million

**Javelin/Better Business Bureau Survey**

# The Scope of the Problem (2)

- Total One-Year Fraud Amount:
  - 2003: \$53.2 billion
  - 2005: \$54.4 billion
  - 2006: \$56.6 billion

**Javelin/Better Business Bureau Survey**

# The Scope of the Problem (3)

- Average Fraud Amount per Victim
  - 2003: \$5,249
  - 2005: \$5,885
  - 2006: \$6,383
- The average resolution time is at a high of 40 hours per victim in 2006 compared to 28 hours in 2005 and 33 hours in 2003.

**Javelin/Better Business Bureau Survey**

But what does it mean for an  
HR professional?

# ID Theft from the HR Perspective

- Three Principal Risks
  - The Dishonest Insider
  - The Negligent Employee
  - Compromised Employee Data

# Dishonest Insider: Examples

- Atlantis Hotel - Kerzner Int'l (55,000 Records)
- University of Hawaii (150,000 Records)
- Westboro Bank (750 Records)
- Wachovia, BoA, PNC, Commerce (676,000 Records)
- California Fastrack (4,500 Records)
- Georgia DMV (465,000 Records)
- Progressive Casualty Insurance (13 Records)
- General Motors (100 Records)

*Source:* [PrivacyRights.org](http://PrivacyRights.org)

# Negligent Employee: Examples

- **Wisconsin Assembly:** Document containing 109 records stolen from employee's car
- **Univ. of Nebraska:** 72 employee records inadvertently posted to public website
- **WA Employment Security Dept.:** Stolen laptop containing 530 employee records
- **Ford Motor Co.:** Stolen computer containing 70,000 employee records
- **Boeing:** Stolen laptop containing 3600 employee records
- **Deloitte & Touche:** Lost CD containing 9,290 records

*Source:* PrivacyRights.org

# Compromised Employee Data: Examples

- **Univ. of San Diego:** Hackers gain access to 7,800 student/employee records
- **Department of Defense:** Hackers gain access to undisclosed number of DoD employee records
- **Department of Energy:** Hackers gain access to 1,502 DoE employee records
- **Department of Agriculture:** Hackers gain access to 26,000 DoA employee records
- **State of Indiana:** Hackers gain access to 5,600 records (2.10)

**Nearly 100,000,000 records exposed since Feb. 2005**

*Source:* PrivacyRights.org

# Legislative Responses

- Two principal Pennsylvania laws address the responsibilities of persons collecting identifying information
  - Act Relating to the Confidentiality of Social Security Numbers (74 P.S. § 201)
  - Breach of Personal Information Notification Act (73 P.S. § 2302, et seq.)

# Privacy of SSNs

In Pennsylvania, it is unlawful to:

- “Publicly post or publicly display” an individual’s SSN, i.e., “intentionally communicate or otherwise make available to the general public.”
- “Print an individual’s SSN on any card required for the individual to access products or services provided by the person [or] entity.”
- Require transmission of an SSN over an unsecured internet connection

# Privacy of SSNs, Cont'd

In Pennsylvania, it is unlawful to:

- Require an SSN to access an internet website unless a password, PIN or other authentication device is also required
- Print an individual's SSN on materials mailed to the individual unless so required by state or federal law (e.g., W-2)

# Exceptions to SSN Privacy Law

- A person or entity is exempted from the foregoing restrictions provided:
  - SSN was being used prior to Act
  - SSN use has been continuous ever since
  - Individual is provided annual disclosure informing the individual of his/her right to stop use of SSN number in prohibited manner
  - Individual does not opt out in writing
- If an opt out is received, must stop using SSN within 30 days
- Does not apply to any document that must be open to public by law, e.g., titles, deeds, etc.

# SSN Privacy: Governor's Message

- Any person or entity . . . that has used social security numbers prior to the effective date of this act, in a manner that may be inconsistent with the above guidelines, may continue to do so **as long as** the individual is provided proper disclosure of his rights regarding the use of his social security number. Upon receipt of the disclosure, the individual may submit a written request to the entity asking them to no longer utilize his social security number.

Governor Rendell's Signing Statement (June 29, 2006)

# Penalties for Violation of SSN Privacy Law

- First Violation: Punishable by fine not less than \$50 and not more than \$500
- Subsequent Violations: Punishable by fine of not less than \$500 and not more than \$5,000
- No statutory private right of action but violation would likely be considered evidence of negligence and, perhaps, negligence per se

# The BPINA

- BPINA: Breach of Personal Information Notification Act (2006)
- In Pennsylvania, a business must provide **notice** to affected Pennsylvania residents of any “**breach of the security of the system**” that **materially** compromises the security or confidentiality of **personal information**

# BPINA Applicability

- For our purposes, the BPINA covers any business that does business in Pennsylvania and that “maintains, stores or manages computerized data that includes personal information.”

# What Is “Personal Information”

- The BPINA defines personal information as:

an “individual’s first name or first initial and last name . . . linked [with] one or more of the following data elements” that are “not encrypted or redacted”: (1) SSN, (2) driver’s license number, or (3) credit or debit card account number in combination with any required access code (e.g., PIN).

# What Constitutes a Breach?

- The BPINA defines a breach of the security of the system as:

“The unauthorized access and acquisition of computerized data that **materially** compromises the security or confidentiality of personal information maintained by the entity as part of a database of personal information regarding multiple individuals and **that causes** or the entity **reasonably believes** has caused or will cause loss or injury to any resident.”

# Notice of Breach

Notice must be given “without unreasonable delay.”

- (1) Written notice to the last known home address.
- (2) Telephonic notice, if the [individual] can be reasonably expected to receive [telephone notice] and the notice is given in a clear and conspicuous manner, describes the incident in general terms and verifies personal information but does not require the customer to provide personal information and the customer is provided with a telephone number to call or Internet website to visit for further information or assistance.
- (3) E-mail notice, if a prior business relationship exists and the person or entity has a valid e-mail address for the individual.

# Substitute Notice

“Substitute notice” may be given if:

- The cost of providing notice would exceed \$100,000;
- The affected class of subject persons to be notified exceeds 175,000; **OR**
- The entity does not have sufficient contact information.

Substitute notice shall consist of all of the following:

- E-mail notice when the entity has an e-mail address for the subject persons;
- Conspicuous posting of the notice on the entity's Internet website if the entity maintains one; **AND**
- **Notification to major Statewide media.**

# Delayed Notice

Notice may be delayed only:

- To determine the scope of the breach,
- To restore “reasonable integrity of the data system,” or
- “if a law enforcement agency determines and advises in writing . . . that the notification [required by the BPINA] will impede a criminal or civil investigation”
  - Always consult law enforcement first?

# BPINA Exceptions

1. A business that “maintains its own notification procedures as part of an information privacy or security policy for the treatment of personal information” if those procedures are “consistent with [BPINA] notice requirements.”
2. Financial institutions that comply with the specific federal guidelines
3. Other businesses governed by guidelines established by a primary federal regulator

# Violations

- Any BPINA violation is, per se, an “unfair or deceptive act or practice” under Pennsylvania’s Unfair Trade Practices and Consumer Protection Law
- Enforcement by Attorney General
- Private enforcement unclear but unlikely
- Even negligent violation may trigger liability, but civil penalties under UTPCP limited to “willful” violation

# Federal “Shredder Law”

- Fair and Accurate Credit Transaction Act (2003) (amendment to Fair Credit Reporting Act)
- FTC regulations promulgated (16 CFR 682, *et seq.*)
- Regulates disposal of consumer information

# FACTA: Who Is Covered?

FACTA applies to just about every business:

“This rule applies to any person over which the Federal Trade Commission has jurisdiction, that, for a business purpose, maintains or otherwise possesses consumer information”

16 CFR 682.2(b)

# FACTA: What Is Covered?

FACTA applies to “consumer information” maintained or otherwise possessed for a “business purpose”

Consumer Information: “any record about an individual, whether in paper, electronic, or other form, that is a consumer report or derived from a consumer report. Consumer information also means a compilation of such records.”

# Examples of Consumer Information Covered by FACTA

- Credit Reports
- Employment background checks
- Check writing history
- Insurance claims
- Residential or tenant history
- Medical history
- Memos and Emails discussing any of the above as in the case of prospective hires

# FACTA: What Is Required?

- “Any person who maintains or otherwise possesses consumer information for a business purpose must properly dispose of such information by taking **reasonable measures** to protect against unauthorized access to or use of the information in connection with its disposal”

# What Is Reasonable?

- Implementing and monitoring compliance with policies and procedures for:
  - Burning, pulverizing or shredding of printed consumer information so information cannot **practicably** be read or reconstructed
  - Destruction or erasure of electronic media containing consumer information so information cannot **practicably** be read or reconstructed
- After **due diligence**, entering into and monitoring compliance with a contract another party engaged in the business of record destruction

# FACTA: Remedies

- Willful Non-Compliance
  - Actual damages sustained by a consumer or \$1000, whichever is greater
  - Punitive damages
  - Costs and attorneys fees
- Negligent Non-Compliance
  - Actual damages sustained by a consumer
  - Costs and attorneys fees
- Class Action Risk
- Potential for Federal & State Fines (up to \$2,500 per violation, *i.e.*, per record)

# Handling Confidential Information: Basic Mistakes

- Accessible and unsecured files
- Documents left in all-access copiers
- Placing SSNs on documents, including timecards, membership cards, paychecks, etc.
- Using SSNs as health plan policy/benefit reference numbers

# Handling Confidential Information: Best Practices

- **Do not use SSNs as reference numbers**
- Carefully screen and limit the number of employees who have access to personal information
- Train employees with regard to handling and destruction of appropriate data
- Secure all personal data (e.g., locked cabinets, encrypted files)
- Create and maintain ID Theft reporting policy

# A Cautionary Tale

- Bell v. AFL-CIO Local 1023 (Mich. 2005)
  - Mrs. Berry works for Union; matches union lists of 911 operators with City employee lists
  - Berry often takes work home
  - In 2000, Berry's daughter is arrested in connection with appropriation of 991 operators' identities
  - Notebook containing names, SSNs and DLNs of operators as well as lists of goods and services procured in their names recovered in daughter's bedroom
  - 911 operators sue union in negligence for disclosure of personal information and associated damages

# Societal Expectations

- “[S]ociety has a right to expect that personal information divulged in confidence to an organization . . . will be guarded with the utmost care. [D]efendant is in the best position to protect plaintiffs because it controls who has access to [personal information it collects].”

# Nature of the Risk

- “[W]ith advancements in technology, holders of [personal] information have had to become increasingly vigilant in protecting such information[.] [T]he severity of the risk of harm in allowing personal information to be taken to an unsecured environment is high.”

# The Bottom Line

- The Union “did owe plaintiffs a duty to protect them from identity theft by providing some safeguards to ensure the security of their most essential confidential information, information which could be easily used to appropriate a person’s identity.”
- \$275,000 damages award affirmed, including mental/emotional distress

# Pennsylvania Common Law

- No cases have yet been decided.
- Two recent statements on identity theft:
  - Certain records not available under FOIA-like request in view of “personal security interest in this era when identity theft is a national concern.” (Super. Ct. 2006)
  - Post-employment background check okay for employee handling “sensitive information [that] included credit card information, social security numbers, residential addresses, loan information, and other similar information. There was a specific concern about identity theft.” (Super. Ct. 2006)