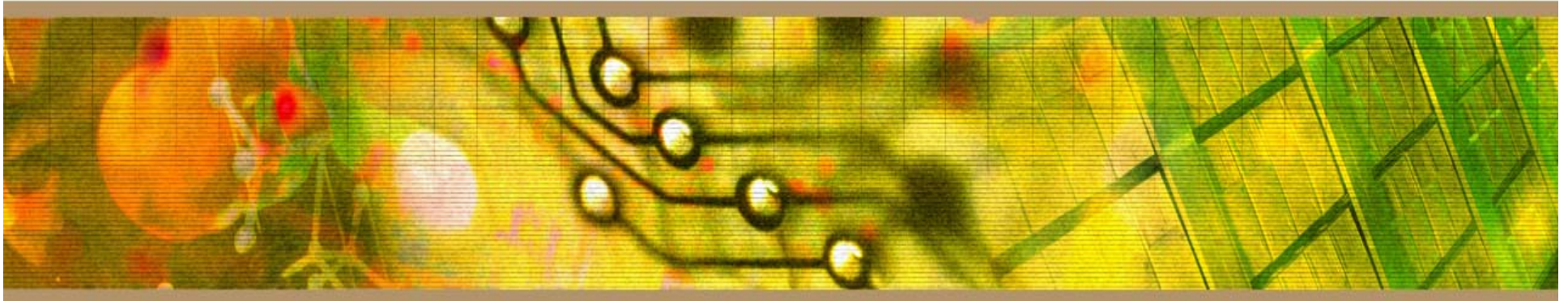




*Indiana Social Security Number
Disclosure and Security Breach
Legislation*



Presented by:
Joanna Lyn Grama, J.D., Information Security Project Manager
Scott Ksander, Senior Inforensics Analyst/Engineer



■ Outline

- Identity Theft and Existing Legislation
- New Indiana Legislation
- Purdue Policies
- Frequently Asked Questions
- References

- Identity theft is an increasing concern:
 - 685,000 fraud and identity theft complaints to FTC in 2005;
 - Indianapolis ranked 26th in a major metropolitan ranking list of identity theft related consumer complaints.

- Identity Theft Assumption Deterrence Act of 1998
 - Criminalizes the act of identity theft, before other crimes are committed.
 - Under the law, identity theft occurs when a person uses the identification of another, without permission, with intent to commit a crime.

- In Indiana:
 - a person who “knowingly or intentionally obtains, possesses, transfers, or uses the identifying information of another person” without consent and with intent to harm, defraud, or assume another’s identity commits identity deception.
Ind.Code § 35-43-5-3.5.

- Indiana has a long history of recognizing the importance of SSN.
- 1978 law states: “no individual may be compelled by any state agency, board, commission, department, bureau, or other entity of state government ... to provide the individual’s Social Security number to the state agency against the individual’s will.”

Ind. Code § 4-1-8

- Two new Indiana laws dealing with disclosures of personal information
 1. “Release of Social Security Number” (Ind. Code § 4-1-10)
 2. “Notice of Security Breach” (Ind. Code § 4-1-11)

- Ind. Code § 4-1-10 (effective July 1, 2006)
- Law states that, except where otherwise permitted, “a state agency may not disclose an individual’s Social Security number.”

Ind. Code § 4-1-10-3(b).

- A disclosure is permitted when:
 - The underlying individual gives written consent;
 - Where required by federal or state law;
 - Where required by court order;
 - When administering health benefits plan; and
 - Various other federal law requires (e.g., U.S. Patriot Act).

- **Additional Disclosure Exceptions:**
 - A state agency may disclose the Social Security Number of an individual to a state, local, or federal agency.
Ind. Code § 4-1-10-4(1)

- Where a disclosure is impermissibly made, penalties apply to the individual state agency employee making the disclosure.
 - “Knowing, intentional, or reckless” disclosure = Class D felony
 - “Negligent” disclosure = Class A infraction.

- Notification:
 - If a disclosure is impermissibly made, the University must give notice to the affected individuals.
- Ind. Code § 4-1-10-7

- Ind. Code § 4-1-11 (effective July 1, 2006)
- “Any state agency that owns or licenses computerized data that includes *personal information* shall disclose a *breach of the security of the system* following discovery or notification of the breach to any state resident whose *unencrypted personal information* was or is reasonably believed to have been acquired by an unauthorized person.”

Ind. Code § 4-1-11-5(a)

- “Personal Information” is defined as:
 - A person’s first and last name OR first initial and last name, *and at least one* of the following:
 1. Social Security Number
 2. Driver’s license or identification card number
 3. Account number, credit card number, debit card number, security code, access code, or password of an individual’s financial account.

- A “breach of the security of the system” is specifically defined as:
 - “unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by a state or local agency.”

Ind. Code § 4-1-11-2

- Notification:
 - If a security breach takes place, the state agency must give notice of the breach to the affected individuals.
Ind. Code § 4-1-11-5

- Must be made without unreasonable delay.
- Notification must be in writing or by electronic mail (if the individual has provided the state agency with the individual’s email address).

Ind. Code § 4-1-11-8

- Purdue's Social Security Number Policy
 - http://www.purdue.edu/policies/pages/information_technology/v_5_1.html

- Important specifications in Purdue SSN policy:
 - SSN may not be used as a common identifier or used as a database key in any electronic information system.
- SSN may be collected and used when necessary for employment records, financial aid records, and a limited number of other business and governmental transactions, as required by law.

- Important specifications in Purdue SSN policy (continued):
 - SSNs will be released by the University to external entities only:
 - » As allowed or required by law; OR
 - » When permission is granted by the individual; OR
 - » When the external entity is acting as the University's contractor or agent and adequate security measures and agreements are in place to prevent unauthorized dissemination to third parties.

- Data Classification Requirements
 - <http://www.itap.purdue.edu/security/policies/dataConfident/restrictions.cfm>
- Data Handling Requirements
 - <http://www.itap.purdue.edu/security/procedures/dataHandling.cfm>

PURDUE Data Handling Requirements

UNIVERSITY

- Includes handling requirements for:
 - Handling of Printed Information (paper, microfiche, microfilm)
 - Electronically Stored (Computer-based) Information
 - Electronically Transmitted Information

- SSNs are considered “Restricted” information and the handling practices for restricted information apply to University use of SSN.

- For instance:
 - Documents containing restricted information must not be further distributed or copied without permission.
 - Encryption is required in electronic communications such as email, FTP, connections to administrative applications, etc.

- Q: The normal business of my department requires that we exchange information containing SSNs within the department or with other Purdue departments such as the Registrar or Admissions. Is this still permitted under the new laws?
- A: Yes, internal use of SSN information within the Purdue system for the purpose of conducting normal business is still permitted under that law. However, it is important to remember that Purdue data handling guidelines address the usage and methods of exchanging sensitive and restricted data, in addition to just SSN information.

- Q: We need to exchange data containing SSN information with other Purdue campuses for business or academic purposes. Is this still permitted?
- A: Yes, internal use of SSN information within the Purdue system is permitted and, additionally, the new law also specifically permits the exchange of information between state agencies. Purdue data handling guidelines need to always be followed when determining the method and technology of these exchanges.

- Q: Is it permissible to disclose SSN information when required by a contractual relationship with a private business or a third-party not part of a state or federal agency?
- A: Generally, this type of disclosure would be prohibited under the new law but the individual circumstances of these situations need to be reviewed in consultations with University legal counsel. If you need to contact University counsel, consult with your Dean or department head.

- Q: We use SSN information as search criteria with external sources such as search engines and databases. Is this still permitted?
- A: In general, disclosing SSN information in this manner would not be permitted under the new laws if the external entity (search engine or database provider) is not a state or federal agency. Purdue data handling requirements may also affect the technology and manner of transmitting this information even if the use is permitted.

- “Release of Social Security Number” (Ind. Code § 4-1-10)
 - <http://www.in.gov/legislative/ic/code/title4/ar1/ch10.html>

- “Notice of Security Breach” (Ind. Code § 4-1-11)
 - <http://www.in.gov/legislative/ic/code/title4/ar1/ch11.html>

- Purdue's Social Security Number Policy
 - http://www.purdue.edu/policies/pages/information_technology/v_5_1.html
- Purdue Data Classification Requirements
 - <http://www.itap.purdue.edu/security/policies/dataConfident/restrictions.cfm>
- Purdue Data Handling Requirements
 - <http://www.itap.purdue.edu/security/procedures/dataHandling.cfm>