

May 19, 2006

To: All Business Services Staff

Fr: Jim Almond, Vice President for Business Services

RE: Upcoming IN SSN Notification/Breach Laws

As a measure of heightened awareness and protection against IT data security breaches and unlawful use of social security numbers resulting in identity theft, the State of Indiana will be enacting two laws on July 1, 2006 that will affect state agencies (including Purdue University). Given the nature of our business, many of you within the Business Services organization work with data containing SSN numbers or work with outside organizations that may utilize the SSN as an identification number. Because of your required use of this data, it is imperative that you be familiar with the intent and impact of these laws. As a brief overview:

1) Law 1 Ind. Code § 4-1-10 - "Release of Social Security Number" - this law states that, except where otherwise permitted, "a state agency may not disclose an individual's SSN." A disclosure is only permitted when:

- a. The underlying person gives their written consent
- b. Where required by federal or state law (i.e. tax or employment requirements)
- c. Where required by a court order
- d. When administering employee health plan benefits
- e. Various other federal law requirements (US Patriot Act)
- f. A state agency discloses the SSN internally or to another state, local or federal agency

This law also states that when a disclosure is impermissibly made - criminal penalties apply to the individual state agency employee making the disclosure. Finally, the law also states that if a disclosure is impermissibly made, the agency (Purdue University) must give notice to the affected individuals.

2) Law 2 Ind. Code § 4-1-11 - "Notice of a Security Breach" - this law states that "any state agency that owns or licenses computerized data that includes personal information shall disclose a breach of the security of the system following a 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." Personal information under the law is defined as a person's first and last name or first initial and last name and at least one of the following:

- a. SSN
- b. Driver's license or state ID number
- c. Account number, credit card number, debit card number, security code, access code or password of an individual's financial account.

The notification that must occur to the affected individuals must be made without reasonable delay and, except in certain circumstances, must be made in writing.

As you can see, the enactment of these laws brings with it new responsibilities for insuring the protection of personal information as outlined in the Data Handling and Security Training that you have completed (or will soon complete). You will certainly read or hear more about these laws, but I

wanted to make you aware of them. There are a number of upcoming activities that will be made available to you to help you further understand the impacts of this legislation:

- * The Data Handling and Security Training will be updated to reflect this information
- * A "refresher" is being developed for the training
- * Presentations on these new laws will be scheduled to provide more information and answer questions. I encourage everyone to attend if you have not attended one yet. Announcements on these open sessions will be made soon.
- * ITaP Security and Privacy will be publishing a set of on-line frequently asked questions (FAQs) about these Laws. You will be notified of the web address when it is available.
- * An article will be published in your next issue of the Spotlight newsletter

Hopefully this message, the above upcoming activities and continued conversation will help you to be prepared for the enactment of these laws and to understand your responsibilities under them.

If you have any questions, please contact Terry Schroeder at tw@purdue.edu.

Sincerely,

Jim Almond
Vice President for
Business Services and
Assistant Treasurer