Trine University
Identity Prevention Program and Red Flag Policy
Approved 12/11

Background

Trine University ("University") desires to protect its employees, students, alumni, board members and other third parties from data loss and identity theft. The risk from data loss and identity theft is of significant concern to the University and can be reduced only through the diligent efforts of every employee. It is important to remember if we collect it, we have to protect it.

The University developed this Identity Theft Prevention Program ("Program") pursuant to the Federal Trade Commission's Red Flags Rule ("Rule"), which implements Section 114 of the Fair and Accurate Credit Transactions Act of 2003.

This Program was developed with oversight and approval of the Executive Committee of the Board of Trustees. The Board of Trustees determined that this Program was appropriate for the University, and therefore approved this Program on January 1, 2012.

Policy

The University adopts this Program to help protect employees, students, all other affected third parties and the University from damages related to the loss or misuse of sensitive information.

Sensitive/Identity theft information includes the following items whether stored in electronic or printed form:

- Social Security number
- Driver's license number
- State ID card number
- Credit or Debit card number, expiration date, security verification code
- Financial account number
- Trine University issued passwords
- Paychecks/Paystubs
- W2's
- Personal medical information
- Employee/Student date of birth, maiden name, phone numbers, addresses

Information classified as identity theft information should only be collected, used and retained if there is a clear organizational requirement. Access to identity theft information should be provided only to those individuals involved in the Trine University activity which requires access to our use of such information. Use of alternative data, such as Trine ID number, the last four digits of a credit card, or noting as "on file" should be used whenever possible. Identity theft information, whether in paper or electronic form, must be securely stored and disposed of in an approved and confidential manner.

University personnel are encouraged to use common sense judgment in securing confidential information. If an employee is uncertain of the sensitivity of a particular piece of information, they should contact their supervisor.

Paper records storage and disposal

File Cabinets, desk drawers, overhead cabinets, and any other storage space containing documents with sensitive information will be locked when not in use.

Desks, work areas, printers and fax machines will be cleared of all documents containing sensitive information when the documents are not in use or when one leaves the area unattended.

Storage rooms containing documents with sensitive information and record retention areas will be locked at the end of each day or when unsupervised.

When documents containing sensitive information are discarded, they will be placed in a locked shred bin or immediately shredded using a mechanical shredding device. Locked shred bins are labeled "Security Container." University records may only be destroyed in accordance with the University's records retention policy.

Electronic media storage and disposal

Internally, sensitive information may be transmitted using approved University email when communication via the telephone or administrative software systems is not possible. Email is not encrypted, so may not be used to transmit sensitive information external to the University. External submission of sensitive data may only be made using a secure, encrypted University endorsed service provider.

Identity theft information should only be stored on Trine central administrative software (Jenzabar, PowerFaids) or payroll (PayServ) software. If there is a need to store this information on Trine University managed servers, it should be done only with the approval of the VP and CIO.

Identity theft information should not be stored on mobile devices, including but not limited to, smart phones, laptops/tablets/netbooks, and USB attached storage devices, i.e. thumb drives.

Breach

Any breach or exposure of identity theft information must be reported and appropriate steps taken.

A breach includes:

- Improper disposal of any media containing identity theft information.
- Unauthorized acquisition or transfer of data that compromises the security, confidentiality, or integrity of identity theft information.
- Loss of electronic devices that includes identity theft information.

In the event of a breach, the party must inform their supervisor immediately. The supervisor will notify the vice-president in charge of that area and the Identity Protection Committee.

In the event of a breach, Trine will initiate the appropriate course of action per Trine policy and applicable laws. Actions may include:

- Determine extent of breach and what information has potentially been compromised
- Notifying appropriate individual affected by exposure
- Notify and cooperate with appropriate law enforcement and credit reporting agencies
- Determine extent of Trine's liability
- Change passwords, security codes, or other security devices that permit access to accounts involved in incident.

Indiana Code (IC 24-2-14) indicates breach has occurred per law whenever:

- Social Security number is disclosed when not encrypted and includes more than five digits OR
- Individual's first and last name or first initial and last name and one or more of the following are disclosed:
    - Driver's license number
    - State ID card number
    - Credit card number
    - Financial account/debit card number and security code/password or access code

Red Flags

Covered Accounts

A covered account includes any account that involves or is designed to permit multiple payments or transactions. Every new and existing employee or student account that meets the following criteria is also covered by this policy:

- Business, personal and household accounts for which there is a reasonably foreseeable risk of identity theft; or

- Business, personal and household accounts for which there are a reasonably foreseeable risk to the safety or soundness of the University from identity theft, including financial, operational, compliance, reputation, or litigation risks.

Red Flags

Red flags are potential indicators of fraud. Any time a red flag, or a situation closely resembling a red flag, is apparent, it should be investigated for verification.

Suspicious Documents

- Documents provided for identification that appears to have been altered or forged.

- The photograph or physical description on the identification is not consistent with the appearance of the person presenting the identification.
- Other information on the identification is not consistent with information provided by the person opening a new covered account or presenting the identification.
- Other information on the identification is not consistent with readily accessible information that is on file with the University.
- An application appears to have been altered or forged, or gives the appearance of having been destroyed and reassembled.

Suspicious Personal Identifying Information

- Personal identifying information provided is inconsistent when compared against external information sources used by the University. For example:
    - Personal identifying information provided by the employee or student is not consistent with other personal identifying information provided by the person. For example, there might be a lack of correlation between the SSN range and date of birth.
    - Personal identifying information provided is associated with known fraudulent activity as indicated by internal or third-party sources used by the University. For example
        - The address on a document is fictitious or a mail drop
        - The phone number is invalid or is associated with a pager or answering service
        - The request was made from a non-Trine issued e-mail account
    - The SSN provided is the same as that submitted by other employees, students or other affected parties
    - The address or telephone number provided is the same as or similar to the address or telephone number submitted by an unusually large number of other employees, students or other affected parties.
    - The person opening the covered account fails to provide all required personal identifying information.
    - Personal identifying information provided is not consistent with personal identifying information that is on file with the University.
    - When using security questions (mother's maiden name, etc.), the person opening the covered account cannot provide authenticating information beyond that which generally would be available from a wallet or consumer report.

Unusual Use of or Suspicious Activity Related to the Covered Account

.

Red flags may further include the following:

- Mail sent to the employee, student or other affected party is returned repeatedly as undeliverable although transactions continue to be conducted in connection with the covered account.
- The University is notified that the employee or student is not receiving paper or electronic account statements.
- The University is notified of unauthorized activity in connection with an employee’s or student's covered account.

- The University receives notice from employees, students, victims of identity theft, law enforcement authorities, or other persons regarding possible identity theft in connection with covered accounts held by the University.
- The University is notified by an employee, student, a victim of identity theft, a law enforcement authority, or any other person that the University has opened a fraudulent account for a person engaged in identity theft.

Responding to Red Flags

Once potentially fraudulent activity is detected, the University employee must act quickly as a rapid appropriate response can protect the University and any affected person from damages and loss.

- Once potentially fraudulent activity is detected, the employee must gather all related documentation, write a description of the situation and present this information to the designated authority for determination.
- The University's legal counsel will complete additional authentication to determine whether the attempted transaction was fraudulent or authentic.
- If a transaction is determined to be fraudulent, appropriate actions must be taken immediately. Actions may include:
  - Denying access to the covered account until other information is available to eliminate the red flag;
  - Canceling the transaction;
  - Notifying and cooperating with appropriate law enforcement;
  - Determining the extent of liability of the University;
  - Notifying the affected person that fraud has been attempted;
  - Changing any passwords, security codes, or other security devices that permit access to a covered account; and,
  - Determining that no response is warranted under the particular circumstances.

Periodic Updates to the Program

At periodic intervals or as required, this Program will be re-evaluated to determine whether all aspects of the Program are up to date and applicable in the current business environment. The following factors may lead to a re-evaluation or review:

- The experiences of the University with identity theft;
- Changes in methods of identity theft;
- Changes in methods to detect, prevent, and mitigate identity theft;
- Changes in the types of accounts that the University offers or maintains; and
- Changes in the business arrangements of the University, including service provider arrangements.

Periodic reviews will include an assessment of which accounts are covered by the Program. As part of the review, red flags may be revised, replaced or eliminated. Defining new red flags may also be appropriate. Actions to take in the event that fraudulent activity is discovered may also require revisions to the Program to reduce damage to the University and its customers.

Program Administration

Operational responsibility of this policy is delegated to the Identity Theft Prevention Committee which consists of the CFO, the CIO and the Director of Human Resources. This policy will be reviewed annually by the committee in ensure the policy is up-to-date.

The Board of Trustees will be made aware in the event any material breaches occur.

Annual staff training will be conducted for all employees for whom it is reasonably foreseeable that they may come into contact with red flag covered accounts or personally identifiable information that may constitute a risk to the University or its customers. The Identity Theft Prevention Committee is responsible for training. The Vice President and General Counsel will advise new employees of this policy.