THE UNIVERSITY of TENNESSEE CHATTANOOGA

IDENTITY THEFT PREVENTION PROGRAM

1. BACKGROUND

The University of Tennessee (UT) developed this Identity Theft Prevention Program pursuant to the Federal Trade Commission's Red Flags Rule, Section 114 of the Fair and Accurate Credit Transactions Act, 2003. On October 24, 2008 the UT Board of Trustees met and approved Program and assigned operational responsibility of the Program to the University Chief Financial Officer of the University.

The risk to the University, its students, faculty, staff, and other constituents from data loss and identity theft is of significant concern, and University of Tennessee Chattanooga (UTC) shall make reasonable efforts to detect, prevent, and mitigate identify theft. UTC recognizes there are various requirements to make sensitive information available – e.g. Social Security numbers, credit card data, etc. – however, it can also lead to account holder vulnerability. In accordance with the University's Identity Theft Prevention Program, UTC will perform all reasonable administrative, organizational and technical steps to prevent unauthorized access and disclosure of identity information.

2. PURPOSE

The purpose of this Identity Theft Prevention Program ("Program") is to detect, prevent and mitigate identity theft in connection with the opening of a "covered account" or any existing "covered account," as defined in Section 4.A. The Program contains reasonable policies and procedures to:

- Identify relevant Red Flags (patterns, practices, or specific activities) that indicate the possible existence of identity theft with regard to new or existing Covered Accounts the University offers or maintains;
- Detect Red Flags that have been incorporated into the program;
- Respond appropriately to any Red Flags that are detected to prevent and mitigate identity theft;
- Ensure the Program is updated periodically; and
- Promote compliance with state and federal laws and regulations regarding identity theft protection.

3. SCOPE

This Identity Theft Prevention Program applies to students, faculty, staff, and other constituents at the University of Tennessee Chattanooga (UTC).

4. IDENTITY THEFT PREVENTION

4.A: General Definitions

4.A.1: Identify Theft means fraud committed or attempted using the identifying information of another person without their permission.

4.A.2: Red Flag means a pattern, practice or specific activity that indicates the possible existence of identity theft.

4.A.3: Covered Account For the purpose of the University's Identity Theft Prevention Program, a "covered account" means a consumer account offered or maintained by the University that involves or is designed to permit multiple payments or transactions. These include accounts where payments are deferred and made by a borrower periodically over time such as tuition or fee installment payment plans. Examples of Covered Accounts include student accounts, telephone/internet accounts, and loans. Every new and existing account maintained by the University for its students, faculty, staff, and other constituents that meets the following criteria is covered by this Program:

1. Accounts for which there is a reasonably foreseeable risk of identity theft; or
2. Accounts for which there is a reasonably foreseeable risk to the safety or soundness of the University from identity theft, including financial, operational, compliance, reputation, or litigation risks.

4.A.4: Identifying information is "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including: name, address, telephone number, social security number, date of birth, government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number, student identification number, computer's Internet Protocol address, or routing code.

4.B: Confidential Information for the Purpose of the University's Identify Theft Protection Program

4.B.1: Definition of Confidential Information

University Information Technology Policy No. IT0115, entitled "Information and Computer System Classification Policy," defines specific classifications of information and establishes the protection requirements for the confidentiality, integrity, and availability of information. Identity theft is often achieved through unauthorized access to or disclosure of confidential information as defined in Policy No. IT0115 (Confidential Information).

Confidential Information includes, but is not limited to, the following items whether stored in electronic or printed format (see Policy No. IT0115 for additional information):

4.B.1.a: Credit card information, including:
1. Credit card number (in part or whole)
2. Credit card expiration date
3. Cardholder name
4. Cardholder address

4.B.1.b: Tax identification numbers, including:
1. Social Security number
2. Business identification number
3. Employer identification number

4.C: Other Information Commonly Used in Identity Theft

4.C.1: The following information, even though it may otherwise be considered public or proprietary, is often used in conjunction with Confidential Information to commit fraudulent activity such as identity theft:

4.C.1.a: Payroll information, including among other information:
1. Paychecks

2. Pay stubs

4.C.1.b: Flexible benefits plan check requests and associated paperwork

4.C.1.c: Medical information for any employee or customer, including but not limited to:

1. Doctor names and claims
2. Insurance claims
3. Prescriptions
4. Any related personal medical information

4.C.1.d: Other personal information belonging to students, faculty, staff, and other constituents, examples of which include:

1. Date of birth
2. Address
3. Phone numbers
4. Maiden name
5. Names
6. Customer number

4.D: Hard Copy Distribution

1. File cabinets, desk drawers, overhead cabinets, and any other storage space containing documents with Confidential Information must be locked when not in use.
2. Storage rooms containing documents with Confidential Information and record retention areas must be locked at the end of each workday or when unsupervised.
3. Desks, workstations, work areas, printers and fax machines, and common shared work areas must be cleared of all documents containing Confidential Information when not in use.
4. Whiteboards, dry-erase boards, writing tablets, etc. in common shared work areas containing Confidential Information must be erased, removed, or shredded when not in use.
5. University records may only be destroyed in accordance with the University's records retention policy and applicable law.
6. Documents containing Confidential Information must be destroyed in a secure manner. The University's "Media Sanitization Best Practice," available at http://security.tennessee.edu/pdfs/MSBP.pdf, provides specific details on the proper method for discarding Confidential Information.

4.E: Electronic Distribution

All University employees are expected to be familiar with and follow the University's IT Security Best Practices for protecting information in an electronic format. The University's IT Security Best Practices are available at http://security.tennessee.edu/policies.shtml.

All University employees shall comply with the following policies:

1. Confidential Information may only be transmitted using approved methods, as set forth in the University's IT Security Best Practices.
2. Confidential Information in an electronic format must be protected from unauthorized access or disclosure at all times.
3. All e-mails containing Confidential Information should include the following statement:

"This message may contain confidential and/or proprietary information and is intended for the person/entity to whom it was originally addressed. Any use by others is strictly prohibited."

4.F.: Application of Other Laws and University Policies

University personnel should make reasonable efforts to secure Confidential Information to the proper extent. Furthermore, this section should be read and applied in conjunction with the Family Education Rights and Privacy Act ("FERPA"), the Tennessee Public Records Act, and other applicable laws and University policies. If an employee is uncertain of the confidentiality of a particular piece of information, he/she should contact the University's Chief Financial Officer, or a designee of the Chief Financial Officer, as set forth in Section 8.A.2, or the University's Office of Vice President and General Counsel.

5. IDENTIFICATION OF RED FLAGS

The following 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.

5.A: Alerts, notifications, or warnings from a consumer reporting agency. Examples of these Red Flags include the following:

1. A fraud or active duty alert included with a consumer report;
2. A notice of credit freeze from a consumer reporting agency in response to a request for a consumer report;
3. A notice of address discrepancy from a consumer reporting agency as defined in § 334.82(b) of the Fairness and Accuracy in Credit Transactions Act; and
4. A consumer report that indicates a pattern of activity inconsistent with the history and usual pattern of activity of an applicant or customer, such as:
    a. A recent and significant increase in the volume of inquiries;
    b. An unusual number of recently established credit relationships;
    c. A material change in the use of credit, especially with respect to recently established credit relationships; or
    d. An account that was closed for cause or identified for abuse of account privileges by a financial institution or creditor.

5.B: Suspicious documents. Examples of these Red Flags include the following:

1. Documents provided for identification that appear to have been altered or forged;
2. The photograph or physical description on the identification is not consistent with the appearance of the student, faculty, staff, and other constituent presenting the identification;
3. Other information on the identification is not consistent with information provided by the person opening a new covered account or student, faculty, staff, and other constituent presenting the identification;
4. Other information on the identification is not consistent with readily accessible information that is on file with the University; and
5. An application appears to have been altered or forged, or gives the appearance of having been destroyed and reassembled.

5.C: Suspicious personally identifying information. Examples of these Red Flags include the following:

1. Personally identifying information provided is inconsistent when compared against external information sources used by the University;
2. Personally identifying information provided is associated with known fraudulent activity as indicated by internal or third-party sources used by the University;
3. Personally identifying information provided is of a type commonly associated with fraudulent activity as indicated by internal or third-party sources used by the University;
4. The SSN provided is the same as that submitted by another student, faculty, staff, or constituent;
5. The person opening the covered account fails to provide all required personally identifying information on an application or in response to notification that the application is incomplete;
6. Personally identifying information provided is not consistent with personal identifying information that is on file with the University; and
7. When using security questions (mother's maiden name, pet's 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.

5.D: Unusual use of, or suspicious activity related to, the covered account. Examples of these Red Flags include the following:

1. Shortly following the notice of a change of address for a covered account, the University receives a request for new, additional, or replacement goods or services, or for the addition of authorized users on the account;
2. A covered account is used in a manner that is not consistent with established patterns of activity on the account;
3. A covered account that has been inactive for a reasonably lengthy period of time is used (taking into consideration the type of account, the expected pattern of usage and other relevant factors);
4. Mail sent to the student, faculty, staff, or other constituent is returned repeatedly as undeliverable although transactions continue to be conducted in connection with the covered account;
5. The University is notified that the student, faculty, staff, or other constituent is not receiving paper account statements;
6. The University is notified of unauthorized charges or transactions in connection with a covered account;
7. The University receives notice from students, faculty, staff, or other constituents, victims of identity theft, law enforcement authorities, or other persons regarding possible identity theft in connection with covered accounts held by the University; and

8. The University is notified by a student, faculty, staff, or other constituent, a victim of identity theft, a law enforcement authority, or any other person that it has opened a fraudulent account for a person engaged in identity theft.

5.E: Notice from Others Indicating Possible Identity Theft - such as the institution receiving notice from customers, victims of identity theft, law enforcement authorities, or other persons regarding possible identity theft in connection with Covered Accounts.

6. DETECTION OF RED FLAGS

Red Flags in connection with Covered Accounts may be detected through such methods as:

- Obtaining and verifying identity;
- Authenticating customers;
- Monitoring transactions;
- In connection with credit or background reports, identifying address discrepancies by verifying applicant's address at time the credit or background report is requested.

7. RESPONDING TO RED FLAGS

7.A: Once a Red Flag, or potential Red Flag, is detected, the University should act quickly so as to protect students, faculty, staff, and other constituents at UTC from damages and loss.

7.A.1: UTC should quickly gather all related documentation, write a description of the situation, and present this information to the UTC's Executive Vice Chancellor Finance & Operations, or designee(s).

7.A.2: UTC's Executive Vice Chancellor Finance & Operations, or designee(s), shall complete additional authentication to determine whether the attempted transaction was fraudulent or authentic.

7.B: If a transaction is determined to be fraudulent, appropriate actions should be taken immediately. Actions may include but not limited to:

1. Monitoring a Covered Account for evidence of identity theft;
2. Canceling the transaction;
3. Changing any passwords, security codes or other security devices that permit access to a Covered Account;
4. Closing an existing Covered Account;
5. Reopening a Covered Account with a new account number;
6. Notifying and cooperating with appropriate law enforcement;
7. Determining the extent of liability of the University; and
8. Notifying the student, faculty, staff, or other constituent that fraud has been attempted.
9. Determine no response is warranted under the particular circumstances.

8. PROGRAM ADMINISTRATION

The Program should be re-evaluated periodically by the University to determine whether all aspects of the Program are up to date and applicable in the current operational environment including, accounts, red flags, reactions to fraudulent activity.

8.A: Involvement of management

8.A.1: Establishment of the Identity Theft Prevention Program is the responsibility of the University's Board of Trustees.

8.A.2: The University's Chief Financial Officer, or designee of the Chief Financial Officer, shall have operational responsibility for the Program. The Chief Financial Officer shall update the Program periodically to reflect changes in risks to consumers or to the safety and soundness of the University from identity theft

8.A.3: UTC's Executive Vice Chancellor Finance & Operations, or designee(s), shall authorize all employees who may come into contact with accounts or personally identifiable information that may constitute a risk to the University or its students, faculty, staff, and other constituents.

8.A.4: Compliance shall include having reasonable policies and procedures in place designed to detect, prevent and mitigate the risk of identity theft whenever the University engages a service provider to perform an activity in connection with one or more Covered Accounts.

8.B: Employee training

8.B.1: Training shall be conducted for all employees for whom it is reasonably foreseeable, as determined by UTC's Executive Vice Chancellor Finance & Operations or a designee(s), that the employee may come into contact with accounts or personally identifiable information that may constitute a risk to UTC or its students, faculty, staff, and other constituents.

8.B.2: UTC's Human Resources offices are responsible for ensuring that identity theft training is conducted for all employees for whom it is required.

8.B.3: Employees shall receive annual training in all elements of the Identity Theft Prevention Program.

8.B.4: To ensure maximum effectiveness, employees shall continue to receive additional training as changes to the Program are made.

8.C: Oversight of service provider arrangements

8.C.1: UTC shall endeavor to ensure that the activities of all service providers are conducted in accordance with reasonable policies and procedures designed to detect, prevent, and mitigate the risk of identity theft.

8.C.2: A service provider that maintains its own identity theft prevention program, consistent with the guidance of the red flag rules and validated by appropriate due diligence, may be considered to be meeting these requirements.

8.C.2: Any specific requirements should be specifically addressed in the appropriate contract arrangements.