BOARD OF TRUSTEES
THE UNIVERSITY OF TENNESSEE

ACTION ITEM

DATE:	October 24,2008
COMMITTEE:	Finance and Administration
CAMPUS/UNIT:	The University of Tennessee System
ITEM:	**Establishment of an Identity Theft Prevention Program**
RECOMMENDATION:	Approval of the Resolution
PRESENTED BY:	Charles M. Peccolo, Vice President and Treasurer

Federal regulations promulgated under the Fair and Accurate Credit Transactions Act of 2003 (which amended the Fair Credit Reporting Act) will become effective on November 1, 2008. These regulations require certain financial institutions and creditors to establish an identity theft prevention program. Although some uncertainty exists in the higher education community concerning the application of these regulations to colleges and universities, the following and similar activities appear to bring The University of Tennessee within the statutory definition of a "creditor" required to establish an identity theft prevention program:

1. Participating in the Perkins Loan Program;
2. Being a school lender in the Federal Family Education Loan Program;
3. Offering institutional student loans;
4. Offering a plan for payment of tuition on a deferred basis; and
5. Offering debit cards to students, faculty, and staff for the purchase of meals.

The federal regulations require that the initial plan for identity theft prevention be approved by the institutional governing board. The governing board may delegate to a senior administrative official responsibility for oversight, development, implementation, and administration of the program and any needed changes in the program to keep it up-to-date. The proposed Identity Theft Prevention Program delegates this responsibility to the Chief Financial Officer or a designee of the Chief Financial Officer.

A Resolution establishing an Identity Theft Prevention Program follows this memorandum.

RESOLUTION
OF THE
THE UNIVERSITY OF TENNESSEE
BOARD OF TRUSTEES

ESTABLISHING AN IDENTITY THEFT PREVENTION PROGRAM
FOR THE UNIVERSITY OF TENNESSEE

WHEREAS, the Fair and Accurate Credit Transactions Act of 2003, an amendment to the Fair Credit Reporting Act, requires rules regarding identity theft protection to be promulgated and adopted jointly by the Office of the Comptroller of the Currency, Treasury; the Board of Governors of the Federal Reserve System; the Federal Deposit Insurance Corporation; the Office of Thrift Supervision, Treasury; the National Credit Union Administration; and the Federal Trade Commission; and

WHEREAS, the various federal agencies and offices have jointly promulgated and adopted rules that become effective November 1, 2008 and require certain financial institutions and creditors to implement an identity theft prevention program; and

WHEREAS, certain financial operations of The University of Tennessee appear to bring the University within the definition of a creditor for the purpose of these federal rules; and

WHEREAS, the risk to the University, and its students, faculty, staff, and other constituents from data loss and identity theft is of significant concern to the University, and the Board of Trustees has determined that the University should make reasonable efforts to detect, prevent, and mitigate identify theft; and

WHEREAS, the Board of Trustees has determined that the proposed Identity Theft Prevention Program is in the best interest of the University and its students, faculty, staff, and other constituents.

NOW THEREFORE BE IT RESOLVED by the Board of Trustees for The University of Tennessee meeting in Knoxville, Tennessee on October 24, 2008 that:

1. the Identity Theft Prevention Program attached hereto as Exhibit A is hereby approved; and

2. the Chief Financial Officer of the University is hereby delegated operational responsibility of the Identity Theft Prevention Program, including but not limited to oversight, development, implementation, and administration of the Program; approval of needed changes to the Program; and implementation of needed changes to the Program.

EXHIBIT A

IDENTITY THEFT PREVENTION PROGRAM

SECTION 1: BACKGROUND

The risk to the University, and its students, faculty, staff, and other constituents from data loss and identity theft is of significant concern to the University and the University should make reasonable efforts to detect, prevent, and mitigate identify theft.

SECTION 2: PURPOSE

The University adopts this Identity Theft Prevention Program (the "Program") in an effort to detect, prevent, and mitigate identify theft in connection with the opening of a "covered account" or any existing "covered account," as defined in Section 5 A. The Program is further intended to help protect students, faculty, staff, and other constituents and the University from damages related to the fraudulent activity of identity theft.

This Program will:

1. Identify patterns, practices, or specific activities ("Red Flags") that indicate the possible existence of identity theft with regard to new or existing covered accounts;

2. Detect Red Flags that have been incorporated into the Program;

3. Respond appropriately to any Red Flags that are detected under the Program;

4. Ensure periodic updating of the Program, including reviewing the accounts that are covered and the identified Red Flags that are part of the Program; and

5. Promote compliance with state and federal laws and regulations regarding identity theft protection.

SECTION 3: SCOPE

This Identity Theft Prevention Program applies to students, faculty, staff, and other constituents at the University.

SECTION 4: IDENTITY THEFT PREVENTION

4.A: Confidential Information for the Purpose of the University's Identity Theft Protection Program

4.A.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.A.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.A.1.b: Tax identification numbers, including:

1. Social Security number
2. Business identification number
3. Employer identification number

4.B.: Other Information Commonly Used in Identity Theft

4.B.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.B.1.a: Payroll information, including among other information:

1. Paychecks
2. Pay stubs

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

4.B.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.B.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.C.: Hard Copy Distribution

All University employees shall comply with the following requirements:

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.D.: 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.E.: Application of Other Laws and University Policies

University employees 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.

SECTION 5: ADDITIONAL IDENTITY THEFT PREVENTION EFFORTS

5.A.: Covered Accounts

For the purpose of the University's Identity Theft Prevention Program, a "covered account" includes:

1. any account that involves or is designed to permit multiple payments or transactions; and

2. any other account maintained by the University for which there is a reasonably foreseeable risk of identity theft to students, faculty, staff, and other constituents, or 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.

5.B.: Red Flags

5.B.1: 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.

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

    a. A fraud or active duty alert included with a consumer report;

    b. A notice of credit freeze from a consumer reporting agency in response to a request for a consumer report;

    c. 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

    d. 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:

        i. A recent and significant increase in the volume of inquiries;

        ii. An unusual number of recently established credit relationships;

        iii. A material change in the use of credit, especially with respect to recently established credit relationships; or

        iv. An account that was closed for cause or identified for abuse of account privileges by a financial institution or creditor.

2. **Suspicious documents.** Examples of these Red Flags include the following:

   a. Documents provided for identification that appear to have been altered or forged;

   b. 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;

   c. 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;

   d. Other information on the identification is not consistent with readily accessible information that is on file with the University; and

   e. An application appears to have been altered or forged, or gives the appearance of having been destroyed and reassembled.

3. **Suspicious personally identifying information.** Examples of these Red Flags include the following:

   a. Personally identifying information provided is inconsistent when compared against external information sources used by the University;

   b. Personally identifying information provided is associated with known fraudulent activity as indicated by internal or third-party sources used by the University;

   c. 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;

   d. The SSN provided is the same as that submitted by another student, faculty, staff, or constituent;

   e. 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;

   f. Personally identifying information provided is not consistent with personal identifying information that is on file with the University; and

   g. 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.

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

   a. 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;

   b. A covered account is used in a manner that is not consistent with established patterns of activity on the account;

   c. 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);

   d. 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;

   e. The University is notified that the student, faculty, staff, or other constituent is not receiving paper account statements;

   f. The University is notified of unauthorized charges or transactions in connection with a covered account;

   g. 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

   h. 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.

SECTION 6: RESPONDING TO RED FLAGS

6.A.: Once a Red Flag, or potential Red Flag, is detected, the University should endeavor to act quickly as a rapid appropriate response can protect students, faculty, staff, and other constituents and the University from damages and loss.

6.A.1: The University should quickly gather all related documentation, write a description of the situation, and present this information to the University's Chief Financial Officer, or a designee of the Chief Financial Officer, as set forth in Section 8.A.2, for determination.

6.A.2: The University's Chief Financial Officer, or a designee of the Chief Financial Officer, shall complete additional authentication to determine whether the attempted transaction was fraudulent or authentic.

6.B.: If a transaction is determined to be fraudulent, appropriate actions should be taken immediately. Actions may include:

1. Canceling the transaction;

2. Notifying and cooperating with appropriate law enforcement;

3. Determining the extent of liability of the University; and

4. Notifying the student, faculty, staff, or other constituent that fraud has been attempted.

SECTION 7: PERIODIC UPDATES TO THE IDENTITY THEFT PREVENTION PROGRAM

7.A.: At periodic intervals as deemed necessary by the University, the Program should be re-evaluated to determine whether all aspects of the Program are up to date and applicable in the current operational environment.

7.B.: Periodic reviews will include an assessment of which accounts are covered by the Program.

7.C.: As part of the review, red flags may be revised, replaced or eliminated. Defining new Red Flags may also be appropriate.

7.D.: Actions to take in the event that fraudulent activity is discovered may also require revision to reduce damage to the University and its students, faculty, staff, and other constituents.

SECTION 8: PROGRAM ADMINISTRATION

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. The Board's approval of the initial plan must be appropriately documented and maintained.

8.A.2: Operational responsibility of the Program, including but not limited to the oversight, development, implementation, and administration of the Program, approval of needed changes to the Program, and implementation of needed changes to the Program, is delegated to the University's Chief Financial Officer, or a designee of the Chief Financial Officer.

8.B.: Employee Training

8.B.1: Training shall be conducted for all employees for whom it is reasonably foreseeable, as determined by the University's Chief Financial Officer, or a designee of the Chief Financial Officer, that the employee 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.B.2: The University'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: The University 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.3: Any specific requirements should be specifically addressed in the appropriate contract arrangements.