TENNESSEE
STATE UNIVERSITY

Red Flags Identity Theft Prevention Program

Effective November 1, 2009

Dr. John Cade
Program Administrator

October 22, 2009

TABLE OF CONTENTS

PROGRAM ADOPTION

In response to the threat of identity theft primarily through financial transactions, the United States Congress passed the Fair and Accurate Credit Transactions Act of 2003 (FACTA), Public Law 108-159, an amendment to the Fair Credit Reporting Act. In accordance with sections 114 and 315 of FACTA, 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 jointly adopted and promulgated rules known as the "red flags rules" that require certain entities to enact certain policies and procedures by the November 1, 2009 effective date.

BACKGROUND

The Tennessee Board of Regents, on behalf of its institutions, has adopted an identity theft prevention policy and program, set forth in TBR Policy #4:01:05:60, in an effort to detect, prevent and mitigate identity theft, and to help protect institutions, faculty, staff, students and other applicable constituents from damages related to the loss of misuse of identifying information due to identify theft.

Tennessee State University (the "University") developed this policy pursuant to TBR Policy #4:01:05:60 and the red flags rules. This policy was developed in order to satisfy the requirements of the red flags rules and TBR Policy #4:01:05:60 in consideration of the University's size and the nature of its activities, with oversight by the program administrator.

PURPOSE AND DEFINITIONS

Purpose

The purpose of the program is to detect, prevent and mitigate Identity theft in connection with any covered account. This program envisions the creation of policies and procedures in order to achieve these goals. Under this policy the program will:

1. Identify relevant red flags for new and existing covered accounts and incorporate those red flags into the policy;
2. Detect red flags that have been incorporated into the policy;
3. Respond appropriately to any red flag that is detected to prevent and mitigate identify theft; and
4. Ensure the policy is updated periodically to reflect changes in risks to students and other University constituents from identity theft.
5. Promote compliance with state and federal laws and regulations regarding identity theft protections.

The program shall, as appropriate, incorporate existing TBR and institutional policies and guidelines, such as anti-fraud programs and information security programs that control reasonably foreseeable risks.

Definitions

"Confidential Data" includes information that the University is under legal or contractual obligation to protect.

"**Covered Account**" includes any account administered by the University that involves or is designed to permit multiple payments or transactions. New and existing accounts maintained by the University for its students, faculty, staff and other constituents for whom there exists a reasonably foreseeable risk: (1) to the students, faculty, staff, or other constituents related to identity theft, or (2) to the safety and soundness of University itself from the financial, operational, compliance, reputation or litigation risks resulting from identity theft.

"**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:

Personal information such as:

Name
Maiden name
Address
Date of birth
Telephone number
Student/Faculty/Staff identification number (e.g., the "T" number assigned by the University)
Computer internet protocol address

Credit card or other account information such as:

Credit card number, in whole or in part
Credit card expiration date

Tax identification numbers such as:

Social Security number
Business identification number
Employer identification number

Payroll information such as:

Paycheck
Paystub
Bank account/routing information

Medical information such as:

Doctor's name and claim
Insurance claim

Prescription
Any personal medical information

Government-issued identification numbers such as:
Driver’s license number
Alien registration number
Passport number

“**Identity Theft**” is a fraud committed or attempted using identifying information of another person without authorization.

"Need to Know" authorization is given to user for whom access to the information must be necessary for the conduct of one's official duties and job functions as approved by the employee's supervisor.

"Public Record" is a record or data item that any entity, either internal or external to the University, can access.

“**Red Flag**” is a pattern, practice, or specific activity that indicates the possible existence of identity theft.

COVERED ACCOUNTS

The University has identified the following types of accounts as covered accounts administered by the University or administered by a service provider:

A. University Covered Accounts:

1. Deferment of Tuition payments
2. Refunds of credit balances involving Plus Loans
3. Refunds of credit balances without Plus Loans
4. Background checks and credit reports in the employee hiring process and for students enrolled in certain programs
5. Meal plans
6. Fines or fees for parking or the Library

B. Service Provider Covered Accounts:

1. Federal Perkins Loan Program
2. Tuition payment plans

IDENTIFICATION OF RED FLAGS

In order to identify relevant red flags, the University considers the types of accounts that it offers and maintains, methods it provides to open its accounts, methods it provides to access its accounts, and its previous experiences with identity theft. The following red flags are potential indicators of fraud that the University has identified. Any time a red flag or a situation closely resembling a red flag is apparent, it should be investigated for verification.

A. Notifications and Warnings from Credit Reporting Agencies Red Flag Examples

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

B. Suspicious Document Red Flag Examples

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

C. Suspicious Personally Identifying Information Red Flag Examples

1. Personally identifying information provided is inconsistent when compared against other sources of information used by the University.

   For example:

   a. The address does not match any address in the consumer report; or
   b. The Social Security number (SSN) has not been issued or is listed on the Social Security Administration's Death Master File.

2. Personally identifying information provided by the individual is not consistent with other personally identifying information provided by that individual. For example, a lack of correlation between the SSN range and date of birth.
3. Personally identifying information provided is associated with known fraudulent activity. For example:
    a. The address on an application is the same as the address provided on a fraudulent application; or,
    b. The phone number on an application is the same as the number provided on a fraudulent application
4. Personally identifying information provided is of a type commonly associated with fraudulent activity. For example:
    a. The address on an application is fictitious, a mail drop, or a prison; or
    b. The phone number is invalid or is associated with a pager or answering service.
5. The social security number provided is the same as that submitted by another person opening an account.
6. The address or telephone number provided is the same as or similar to the address or telephone number submitted by that of another person.
7. The individual opening the covered account fails to provide all required personally identifiable information on an application or in response to notification that the application is incomplete.
8. Personally identifying information provided is not consistent with personally identifying information that is on file with the Institution.
9. When using security questions (mother's maiden name, pet's name, etc.), the person opening that covered account cannot provide authenticating information beyond that which generally would be available from a wallet or consumer report.

D. Suspicious Covered Account Activity or Unusual Use of Account Red Flag Examples

1. Change of address for an account followed by a request to change the student’s or other constituent’s name, or a request for new, additional or replacement goods or services, or for the addition of authorized users on the account;
2. Payments stopped on an otherwise consistently up-to-date account;
3. Account used in a way that is not consistent with an established pattern of activity on that account. For example:
    a. Nonpayment when there is no history of late or missed payments
    b. A material change in purchasing or usage patterns
4. Mail sent to the student, employee, or other constituent is repeatedly returned as undeliverable although transactions continue to be conducted in connection with the covered account;
5. Notice to the University that a student, employee, or other constituent is not receiving paper account statements sent by the University;
6. Notice to the University that a covered account has unauthorized activity; and
7. Awareness of a breach in the University’s computer system’s security or the security of paper files, resulting in unauthorized access to or use of account information of students, employees, or other constituents.

DETECTING RED FLAGS

A. Student Enrollment

In order to detect any of the red flags identified above associated with the enrollment of a student, University personnel will take the following steps to obtain and verify the identity of the person opening the covered account by:

1. Requiring certain identifying information such as name, date of birth, academic records, home address or other identification; and
2. Verifying the student's identity at the time of issuance of a student identification card (i.e., review of driver's license or other government-issued photo identification).

B. Existing Accounts

In order to detect any of the red flags identified above for an existing covered account, University personnel will take the following steps to monitor that account:

1. Verify the identification of the student, employee, or other covered account holder if he/she requests information (in person, via telephone, via facsimile, via email);
2. Verify the validity of requests to change billing addresses by mail or email and provide the student, employee or other covered account holder a reasonable means of promptly reporting incorrect billing address changes; and
3. Verify changes in banking information given for billing and payment purposes.

C. Consumer ("Credit") Report Requests

In order to detect any of the red flags identified above for an employment or volunteer position for which a credit or background report is sought, University personnel will take the following steps to assist in identifying address discrepancies:

1. Require written verification from any applicant that the address provided by the applicant is accurate at the time the request for the credit report is made to the consumer reporting agency; and
2. In the event that notice of an address discrepancy is received, verify that the credit report pertains to the applicant for whom the requested report was made and report to the consumer reporting agency an address for the applicant that the University has reasonably confirmed is accurate.

RESPONDING TO AND PREVENTING AND MITIGATING IDENTITY THEFT

Response to Red Flags

In the event University personnel detect any identified red flag, an employee must act quickly, as a rapid appropriate response can protect students, faculty, staff, other constituents and the University from damages and loss. If a potentially fraudulent activity is detected, all related documentation should be gathered and a description of the situation should be summarized and reported to the Program Administrator. The University will respond in a reasonable and timely manner to possible data breaches and indicators of identity theft. Depending on the degree of risk posed by the red flag, appropriate actions might include:

1. Determining that no response is warranted under the particular circumstances;
2. Canceling the transaction;
3. Continuing to monitor the covered account for evidence of identity theft;
4. Refusing to open a new covered account;
5. Contacting the student, faculty, employee, applicant (for which a credit report was run) or other applicable constituent;
6. Changing any password or other security device that permits access to Covered Account;
7. Providing the affected student, faculty or staff member with a new identification number ("T" number);
8. Notifying appropriate law enforcement;
9. Filing or assisting in filing a Suspicious Activities Report ("SAR"); and/or
10. Determining the extent of potential liability for the University.

Required Measure:

Data breach laws – Most states (currently 44 out of 50) have laws addressing accidental disclosure of SPI data. The State of Tennessee addresses this in Tenn. Code Ann. § 47-18-2101 et seq. (the *Tennessee Identity Theft Deterrence Act of 1999*). In addition, H.R. 2221, the Data Accountability and Trust Act, which protects consumers by requiring reasonable security policies and procedures to protect computerized data containing personal information, requires notification following discovery of a security breach of a system maintained by any person engaged in interstate commerce who owns or possesses data in electronic form containing personal information.

The bill requires notification to each individual whose personal information was acquired by an unauthorized person as a result of such a breach of security, and to the Federal Trade Commission. The bill includes special notification requirements for third party agents, telecommunications carriers, cable operators, information services, and interactive services, and for a breach involving health information.

Personal information, as defined in the bill, is an individual's first name or initial and last name, or address, or phone number, in combination with any one or more of the following: the individual's social security number, driver's license number or other State identification number, or a financial account number or credit card number and any security or access code needed to access the account. Breach notification would be exempted, however, where the person that owns or possesses the data determines that there is “no reasonable risk of identity theft, fraud or unlawful conduct” from the unauthorized data access. Breaches of encrypted data would presumptively be exempt.

Where notification is required, the bill specifies methods for and required content of notification. Written or in some circumstances email notification is required; the notice must include a description of the information acquired, notice of the right to receive free consumer credit reports, and certain relevant telephone contact numbers. Substitute notification, allowing notification to be posted on the entity’s website and in print and broadcast media, is allowed for those persons owning or possessing the data of fewer than 1,000 individuals.

Prevention and Mitigation of Identity Theft

In order to further prevent the likelihood of identity theft occurring with respect to covered accounts, the University will take the following steps with respect to its internal operating procedures to protect identifying information:

Prevent and Mitigate

1. Ensure that its website is secure or provide clear notice that the website is not secure;
2. Ensure that file cabinets, desk drawers, and any other storage space or room containing documents with Identifying Information be locked when not in use or unsupervised;
3. Ensure that desks, workstations, printers, copiers, fax machines, whiteboards, dry-erase boards in common shared work areas will be cleared of all Indentifying Information when not in use.
4. Ensure complete and secure destruction of paper documents and computer files containing Identifying Information when a decision has been made to no longer maintain such information;
5. Ensure that office computers with access to covered account information are password protected;
6. Ensure that all electronic storage and transmission of indentifying information follows guidelines established by the University’s Communication and Information Technology (CIT) department.
7. Avoid use of Social Security numbers;
8. Ensure computer virus protection is up to date;
9. Require and keep only the kinds of identifying information that is necessary for University purposes;
10. Continue to monitor a covered account for evidence of identity theft;
11. Contact the individual or applicant (for which a credit report was run);
12. Change any passwords or other security devices that permit access to covered accounts;
13. Refuse to open a new covered account;

14. Provide the individual with a new individual identification number;
15. Notify the Committee for determination of the appropriate steps taken or that need to be taken;
16. Notify law enforcement;
17. File or assist in filing a Suspicious Activity Report ("SAR") with the Financial Crimes Enforcement Network, United States Department of the Treasury or other relevant law enforcement agency; or
18. Determine that no response is warranted under the particular circumstances.

Protect Identifying Information

In order to further prevent the likelihood of Identity theft occurring with respect to covered accounts, the University will take the following steps with respect to its internal operating procedures to protect individual Identifying Information:

1. Ensure that websites providing access to covered accounts are secure;
2. Ensure complete and secure destruction of paper documents and computer files containing individual account information in accordance with the University's records retention guidelines;
3. Ensure that office computers with access to covered account information are password protected;
4. Ensure that laptops are password protected;
5. Avoid unnecessary use of Social Security numbers;
6. Ensure the security of the physical facility that contains covered account information;
7. Ensure that transmission of information is limited and encrypted when necessary;
8. Ensure computer virus protection is up-to-date;
9. Require and keep only the kinds of individual information that are necessary for University purposes in accordance with the University's records retention guidelines.
10. University policy requires that data that is classified as Restricted in the Data Classification policy be stored on CIT's network storage facilities, not on local hard drives or media.

ADDITIONAL PREVENTION MEASURES AND RESOURCES

Hard Copy Distribution

Each employee and contractor performing work for the University will comply with the following policies:

1. Physical security will be maintained over documents containing Identifying Information related to covered accounts. Examples include keeping offices locked after hours and locking rooms and files when staff is not present.
2. Desks, workstations, work areas, printers and fax machines, and common shared work areas will be cleared of all documents containing Identifying Information

when not in use.

3. Whiteboards, dry-erase boards, writing tablets, and other writing surfaces in common shared work areas, which contain identifying information, will be erased, removed, or shredded when not in use.
4. When documents containing Identifying Information are discarded, they will be shredded timely.

External and Internal Policies and Procedures

- **Internal**

  Policies by Department/Division: http://www.tnstate.edu/interior.asp?mid=6680&ptid=1

  Information Technology Services: http://www.tnstate.edu/interior.asp?ptid=1&mid=267

- **External**

  Tennessee Board of Regents: http://www.tbr.edu/policies/default.aspx?id=1166

POLICY ADMINISTRATION

A. Oversight

Operational responsibility for developing, implementing and updating this policy lies with the Program Administrator and members of the Committee representing key units of the University. The Program Administrator will be responsible for ensuring appropriate training of University staff on the Policy, for reviewing any staff reports regarding the detection of red flags and the steps for preventing and mitigating Identity theft in relation to covered accounts, determining which steps of prevention and mitigation should be taken in particular circumstances and considering periodic changes to the Policy.

The Program Administrator and head of the Committee is the Director of Banner Services and Protocol Officer. Responsibility for the *Identity Theft Prevention Program* is assigned to a Committee comprised of the following positions:

Department	Position
Communication and Information Technology	Associate Vice President
Budget and Fiscal Planning	Director
Finance and Accounting	Associate Vice President
Bursar's Office	Bursar
Financial Aid	Director
Campus Center	Director
Facilities Management	Assistant Vice President
Human Resources	Associate Vice President/Director
Records Office	Registrar

Residence Life	Director
Admissions	Director

The positions will work together and be responsible for coordinating the University's *Identity Theft Prevention Program*, including the following:

1. Identifying relevant patterns, practices, and specific forms of activity that are "red flags" signaling possible Identity theft and incorporate those red flags into the program;
2. Detecting red flags that have been incorporated into the program; and
3. Responding appropriately to any red flag that is detected to prevent and mitigate theft;
4. Reviewing and update the Identity theft Prevention Program regularly, with changes approved by the President of the University;
5. Identifying training and education relevant to the *Identity Theft Prevention Program*; and
6. Developing and review policies and procedures as appropriate to the *Identity Theft Prevention Program*.

B. Staff Training and Reports

Training shall be conducted for all University employees for whom it is reasonably foreseeable that the employees may come into contact with covered accounts or Identifying Information that may constitute a risk to the University, its student, faculty, employees or other constituents. Failure to complete such training will lead to discipline, up to and including termination.

University employees are expected to notify The Program Administrator once they become aware of an incident of identity theft or of the University's failure to comply with this policy. At least annually or as otherwise requested by the President, the Program Administrator shall prepare a report on compliance with this Policy. The report should address such issues as effectiveness of the policies and procedures in addressing the risk of Identity theft in connection with the opening and maintenance of covered accounts, service provider arrangements, and significant incidents involving identity theft and management's response, and recommendations for changes to the policy. Failure to do so will lead to discipline, up to and including termination. University employees who become aware of an incident of identity theft or of a failure by any University employee to comply with this policy must also notify the Department of Internal Audit.

C. Service Provider Arrangements

In the event the University engages a service provider to perform an activity in connection with one or more covered accounts, the University will take the following steps to ensure the service provider performs its activity in accordance with reasonable policies and procedures designed to detect, prevent and mitigate the risk of identity theft.

1. Require, by contract, that service providers have such policies and procedures in place; or

2. Require, by contract, that service providers review the University's policy and report any red flags to the Policy Administrator or the University employee with primary oversight of the service provider relationship.
3. Specific language for inclusion in contracts can be found in TBR Guideline G-030, Contracts and Agreements.

Whenever the University engages a third party or service to perform an activity that may include or expose SPI data, the University will review that the policies and procedures of the vendor are reasonable to detect, prevent and mitigate the risk of Identity theft.

Current known vendors:

A. Campus partners for student loan data
B. Collection agencies (past due student accounts)
C. Third-party credit card processors
E. National Student Clearinghouse

D. Non-disclosure of Specific Practices

For the effectiveness of this identity theft prevention policy, knowledge about specific red flag identification, detection, mitigation and prevention practices may need to be limited to the Program Administrator and to those employees with a need to know them. Any document that may have been produced or are produced in order to develop or implement this policy that lists or describes such specific practices and the information those documents contain are considered "confidential" and should not be shared with other University employees or the public. The Program Administrator shall inform those employees with a need to know the information of those documents or specific practices which should be maintained in a confidential manner.

E. Policy Updates

The Program Administrator will periodically review and update this policy to reflect changes in risks to students, employees and other constituents and the soundness of the University from identity theft related to covered accounts. In doing so, the Program Administrator will consider the University's experiences with identity theft situations, changes in identity theft methods, changes in identity theft detection and prevention methods, and changes in the University's business arrangements with other entities. After considering these factors, the *Identity Theft Prevention Program* Committee will determine whether changes to the Policy, including the listing of red flags, are warranted. If warranted, the Committee will update the policy.

STANDARD PRACTICES
REQUIRING SAFEGUARDS OF PERSONALLY IDENTIFIABLE INFORMATION

Many offices at the University maintain files, both electronic and paper, of student biographical, academic, health, financial, and admission records. These records may also include the following:

1. Student billing information
2. Federal Perkins Loan records
3. Personal correspondence with students and parents

Policies to insure compliance with Gramm-Leach-Bliley Act (GLB), Family Educational Rights and Privacy Act (FERPA), system and application security, and internal control procedures provide an environment where identify theft opportunities are mitigated. Records are safeguarded to ensure the privacy and confidentiality of student, parents, alumni and employees.

The Office of Human Resources performs credit and criminal background checks on some potential employees prior to their dates of hire. This population includes police services employees. Additionally, criminal background checks are performed during the admission process for undergraduate and graduate level nursing students. Many clinical placement sites also require background checks for students during clinical/practical training.

The University's controls over privileged information include:

1. Students are given the opportunity to set up an authorized payer that enables a third party (e.g., parents or grandparents) access to their student accounts, which includes information regarding their bills only.

2. Access to non-directory student data in the Banner system is restricted to those employees of the University with a need to properly perform their duties. These employees are trained to know FERPA and red flag regulations.

3. Social Security numbers are not used as primary student identification numbers and this data is classified as non-directory student data.

4. Student Financial Services employees managing covered accounts are trained to know FERPA and red flag regulations.

5. The University is sensitive to the personal data (unlisted telephone numbers, dates of birth, etc.) that it maintains in its personnel files and databases. The University will not disclose personal information, except by written request or signed permission of the employee (or unless there is a legitimate business "need-to-know", or if compelled by law.

6. Every effort is made to limit the access to private information to those employees on campus with a legitimate "need-to-know." University staff members who have approved access to the administrative information databases understand that they are restricted in using the information obtained only in the conduct of their official duties. The inappropriate use of such access and/or use of administrative data may result in disciplinary action up to, and including, dismissal from the University.

7. The University's official personnel files for all employees are retained in the Human Resources Office. Employees have the right to review the materials contained in their personnel files.

8. The University's School of Nursing and College of Health Sciences each has policies and procedures relating to obtaining and safeguarding information obtained through background checks of students.

9. The University has policies that address the safeguarding of various forms of confidential information. Those policies include:

    a. FERPA Rights
    b. Records Retention

10. Staff who have access to HR and payroll data have received training that non-directory information regarding employees is not to be provided unless approved in writing by the employee.

11. The student is required to give written authorization to the Registrar's Office if his/her information is permitted to be shared with another party. A FERPA disclosure statement is distributed to the students each year informing him/her of his/her rights under FERPA.

12. Social Security numbers are not used as identification numbers and this data is classified as confidential.

13. All paper files, when not in use, must be stored in locked filing cabinets. All offices must be secured during normal business hours and, when not occupied, are to be locked.

14. Access to confidential employee data in the University's human resources and payroll systems is restricted to only those employees who have a need to know and for proper execution of their job functions. These employees receive training related to FERPA and "red flag" regulations.

15. Employees and students are requested to report all changes in name, address, telephone number or marital status to the Office of Human Resources and/or the Registrar's Office as soon as possible.

16. Any information classified as confidential contained within the personnel file remains confidential. Employees have the right to review the information contained in their personnel files.

The Tennessee Public Records Act is found in Tenn. Code Ann. § 10-7-101 et seq. and the sections that follow it. For purposes of access to public records, the operative provision is found in Tenn. Code Ann. § 10-7-503, which reads: "All state, county, and municipal records ... shall at all times, during business hours, be open for public inspection by any citizen of Tennessee, and those in charge of such records shall not refuse such right of inspection to any citizen, unless provided by state law."

"Records" are defined in Tenn. Code Ann. § 10-7-301(6) as "all documents, papers, letters, maps, books, photographs, microfilms, electronic data processing files and output, films, sound recordings, or other material, regardless of physical form or characteristics made or received pursuant to law or ordinance or in connection with the transaction of official business of any governmental agency."

OTHER METHODS OF PREVENTING AND MITIGATING IDENTITY THEFT

Based the red flags rule guidelines, Tennessee State University has developed the following policies and procedures to prevent and mitigate identity theft. Each department may have a unique set of interactions, transactions, and activities to be performed with students or staff. Proper procedures and training must take place at the departmental level to protect sensitive information, detect the red flags that indicate identity theft, and guard against risks that might arise from that unit.

This policy covers electronic records of people in Banner and any other system that stores sensitive personal information that could be used for identity theft. This policy also applies to paper and hard copy records that contain sensitive information.

Verification of Identity

1. Review Sources of Personal Identification – Watch for documents provided that appear to have been forged or altered, a photograph or physical description that is not consistent with appearance, addresses or names that do not match other records or information on file, documents that appear to have been destroyed and reassembled, and documents provided that are not consistent when compared against external information sources.

2. Review Official Documents – Verify names, nicknames or full names that do not match other records, Social Security numbers that are duplicate or do not match information already on file, incomplete addresses or mail drops, incomplete personally identifying information submitted, and inability of an account holder to provide authenticating information when asked.

3. New Records - When students or employees are added or modified in Banner or other systems, as much personally identifying information as possible should be gathered, verified and recorded. This information can be used in later steps to reduce the chance of fraud and increase the detection of suspicious activity.

4. Persons conducting identity verification should ask for both internal identification (University ID Card or ID number) and an additional outside ID that is not already recorded in Banner (e.g., driver's license, other photo ID, passport) for proof of identity.

5. Identification Card (Campus ID) Issuance – Campus ID Cards are used for a wide range of identification. When issuing cards, the person must already exist in Banner and at least one additional outside picture identification will be provided.

6. Manage Release of Information – Strengthen verification of the identity of people who request information (in person, via phone, via email). Monitor requests for transcripts, statements, or other information for possible fraud.

7. Review SSN and date-of-birth discrepancies that may be submitted through the Admissions/FAFSA process.

8. Audit for duplicate SSN's in Banner to correct account creation or modification errors.

Document Imaging System-Xtender Solution (Future Implementation)

1. Scan driver's license or other government-issued photo ID for ongoing identification verification (document imaging system)

2. Capture account holder signatures for further verification and comparison to other documents (document imaging system)

3. Create better account verification questions and answers based on Banner data elements (shared among many departments). There should be three to five questions to assist in authenticating identity.

Authenticate Students and Employees

1. Require strong authentication methods (across all systems) for students and staff to access and maintain their records and perform transactions.

2. Monitor systems and logs for repeated account lockouts or failed password attempts.

3. Change account credentials, PIN's or passwords if theft or compromise is suspected – if a suspicious activity or red flag indicator is presented that points to a reasonable likelihood of compromise, account and user credentials should be modified to block access until use and identification can be verified.

4. Require identity confirmation to perform manual PIN or password resets (that can't be completed through self-service modules).

5. Increase the strength of the Banner credential (tie to domain credential)

6. Strengthen "self service" PIN reset process (security question and answer).

7. Strengthen manual PIN reset process and coordinate between multiple offices (authenticating identity, creating a secure PIN, required change on first login)

8. Provide an email confirmation to account holders for manual PIN resets through self-service systems

9. Audit for frequent manual PIN or password resets, or other significant credential changes and might indicate hacking or other credential abuse.

10. Eliminate SSN as alternate credential (ID number)

11. Eliminate birth date as initial PIN

12. Implement a password change policy (across all systems)

Monitor Transactions or Account Activity

1. Departments should develop a matrix of transactions that can be tracked and monitored for red flags and other suspicious activity (credential abuse, check refunds, etc.).

2. Verify Address Changes – Address changes are one common area where identity theft can begin. Changing addresses may provide access to other printed material that can be used in theft of information.

3. Match address changes to postal service records (is it a valid address?)

4. Monitor returned mail, incomplete address records.

5. Audit for no active mailing address, but ongoing account activity.

6. Email confirmation of certain address changes.

7. External partners or reporting agencies may provide fraud or active duty alerts. Request notices of a credit freeze, notices of address discrepancies, a recent increase in volume of inquiries, an unusual number of recent credit relationships, accounts being closed or identified for abuse.

8. Track alerts and notifications from the IRS that a Social Security number is wrong or a duplicate (student or employee tax information).

9. Monitor credit card charge disputes that may indicate fraud or abuse.

10. Monitor for suspicious account activity – address changes followed by a refund request, rapid increase in activity level or inquiry level, mail sent that is returned multiple times as undeliverable, documents or checks submitted that match other fraudulent activity (bounced checks, etc.), missing statements/invoices or other paper records, unusual cancelling of transactions, personally indentifying information that is associated with other fraudulent activities (scams, phishing).

11. Monitor alerts from students or employees reporting their information has been misused (victims), reports from law enforcement about identity theft and fraud, reports from

others about suspicious activity pertaining to a student or employee (identity has been stolen and is now being misused).

12. Contact/notify the student or employee to verify activities or transactions – the monitoring of routine transactions to determine unusual use patterns or suspicion of inappropriate activity may require personal contact or notification of the student or employee.

Create and Maintain a Secure Online Environment

1. Maintain strong control over data – all institutional data should be carefully guarded and controlled. Sensitive Personal Information (SPI) requires ever greater management. Extra safeguards must be in place to not distribute SPI more broadly than required. Keeping SPI data stored centrally is the first step in managing its use.

2. Ensure that campus computers are secure - ensure that office computers are password protected, up-to-date, with virus protection, security firewalls, and strong credentials. Encrypt data stored on desktop and laptop devices to reduce risk of theft or loss. Require secure access to wireless networks.

3. Ensure the websites and other online resources are secure - Ensure that servers, websites and databases are well protected, regularly tested, and up-to-date. Perform regular audits of systems, servers, services, and logs to assure data security.

4. Monitor for suspicious network activity and might indicate keystroke loggers, or other malware used to capture device activity. Network sensors, firewalls, intrusion detection systems and reports.

5. Lock down compromised accounts and require password resets and user notification in the event of suspicious account activity or release/communication of credentials.

6. Regularly audit desktop, laptop, and server security procedures and policies to assure a high level of protection is in place. Perform penetration testing to confirm security of resources.

7. Limit access to the Social Security number field in Banner

8. Automate permission creation and maintenance based on attributes stored in Banner that govern access

Hard Copy and Electronic Record Protection

All University employees must take steps to protect sensitive personal information they have access to or collect from students and staff. The following policies and procedures should be followed.

A. Hard copy records

1. File cabinets, desk drawers, or other storage locations that contain documents with sensitive information will be locked and secured when not in use.

2. Paper documents containing sensitive information will not be left on desks, tables, work areas, printers, fax machines, or other non-secure locations.

3. Documents containing sensitive information will not be stored longer than is needed and will be securely destroyed and discarded when no longer needed.

4. Indentified paper/hard copy records to be reviewed

5. Income Tax returns stored for Financial Aid processing

6. Paper registration and student files (registration, internships, others.)

7. Employee forms that contain SPI data

B. Electronic records

1. Electronic records that contain SPI data shall be stored and maintained on central servers. Whether the record is in a database form, an email message, a Word or Excel document – the most effective method to protect the data is to know where it is stored.

2. While email is a convenient messaging tool, **AVOID** transmitting confidential or sensitive personal information through email. Messages can be potentially intercepted as they travel across the internet, and once data is transmitted via email the opportunity to contain the distribution is lost.

3. Employees who create, store or manage documents and worksheets on campus provided computers (desktops or laptops) shall keep those documents within their “Documents” folder tree so that they are stored centrally and encrypted on the local device.

4. SPI data shall not be stored on portable media (e.g., CD’s, DVD’s, USB drives, or removable hard disk drives).

5. SPI data (and most other campus/employee data for that matter) shall not be stored on home computers or personally owned mobile devices.

Certain information should not be kept

Compliance with Payment Card Industry-Data Security Standards (PCI-DSS) requires that credit card transactions not be stored within on-campus databases or on local servers that have not passed external audit controls. This means that a third-party payment processor will be used for all online transactions that process credit card payments.

TRAINING PROGRAM

The training module for the University's red flags *Identity Theft Prevention Program* will consist of the following:

1. Topics of Discussion

    a. Program Adoption and University Requirements
    b. Purpose and Definitions
    c. Covered Accounts
    d. Identification of Red Flags
    e. Notifications of Warnings
    f. Suspicious Documents
    g. Suspicious Personally Identifying Information
    h. Suspicious Covered Account Activity or Unusual Use of Accounts
    i. Detecting Red Flags
    j. Responding to Red Flags
    k. Prevention and Mitigation of Identity Theft
    l. Protecting Personal Information
    m. Short Quiz
    n. Frequently Asked Questions
    o. Question and Answer Period

2. Requirements for Certification

    a. Attendance at one of the required training sessions held during the academic year.
    b. Signed Employee Red Flags *Identity Theft Prevention Program* Agreement Form

3. Confirmation of Certification

    a. Certificate (signed by the University President)

RECOMMENDATIONS: AWARENESS AND PREVENTION ACTIVITIES

Inclusive of the University's red flags *Identity Theft Prevention Program*, other awareness processes and/or practices relative to policies and prevention techniques regarding identity theft have been identified. For example:

1. Provide appropriate policies, procedures and standards to document best practices for data security, identity theft tricks and techniques, emerging tools to reduce the risk and mitigate the occurrences of fraud and misuse. Publish guidelines and procedures as appropriate.

2. Create a culture or awareness and knowledge about Identity theft, and the procedures in place to mitigate the risk.

3. Require FERPA training for all employees that have regular access to academic records (to include academic records in addition to the SPI data that could be used for identity theft).

4. Establish Security Awareness Month (including identity theft and FERPA awareness)

5. Encourage employees to request copies of credit reports at least once a year.

6. Annual FERPA “refresher” for all employees that access academic records.

7. Create an online "refresher" user security training program.

8. Provide appropriate policies, procedures and standards to inform departmental employees regarding identity theft and the indicators outlined under this policy. Publish guidelines and procedures as appropriate.

9. Require VPN training for all employees provided off-campus access to secure centralized resources.

RESOURCES

- AARP, Preventing Identity Theft Seminar- www.aarp.org/learntech/personal_finance/identity_theft_intro.html
- Center for Identity Management Information Protection, "Identity Fraud Trends and Patterns" www.utica.edu/academic/institutes/ecii/publications/media/cimip_id_theft_study_oct_22_noon.pdf
- Consumer Federation of America report, "To Catch a Thief: Are Identity Theft Services Worth the Cost?" (March 2009), www.consumerfed.org/pdfs/ID_THEFT_REPORT.pdf
- Federal Data Accountability and Trust Act - http://simonhunt.wordpress.com/2009/09/30/h-r-2221-the-federal-data-accountability-and-trust-act/
- Federal Bureau of Investigation, Internet Fraud Complaint Center - www.ic3.gov
- Federal Trade Commission Identity Theft Information - www.consumer.gov/idtheft/
- Identity Theft Resource Center - http://www.idtheftcenter.org
- Law Library Exchange Identity - Identity Theft Resource Guide - www.llrx.com/features/idtheft.htm
- National Criminal Justice Reference Service- www.ncjrs.org/spotlight/identity_theft/summary.html
- U.S. Dept. of Education, Assists with Fed. Student Loan Fraud - www.ed.gov/misused
- U.S. Dept. of Justice - www.usdoj.gov/criminal/fraud/idtheft.html
- Washington Post identity theft page - www.washingtonpost.com/wp-srv/technology/interactives/identitytheft/idtheft.html
- Tennessee Code Annotated, part 21, title 47, chapter 18 — Identity Theft Deterrence

47-18-2101. Short title. —
47-18-2102. Definitions. —
47-18-2103. Prohibited practices. —
47-18-2104. Private rights of action. —
47-18-2105. Civil penalties and remedies. —
47-18-2106. Violation of Tennessee Consumer Protection Act. —
47-18-2107. Release of personal consumer information. —
47-18-2108. Security freeze at the request of the consumer. —
47-18-2109. Notice to consumer regarding security freeze. —
47-18-2110. Protecting social security numbers from disclosure. —

Effective date: November 1, 2009
Authority: Board of Regents Policy #4:01:05:60, *Identity Theft Prevention Policy*;
Tennessee Code Annotated, part 21, title 47, chapter 18
Source: March 26, 2009 Board Meeting; June 19, 2009.
Approved: October _10-26-2009

CONTACT

Dr. John Cade
Program Administrator
615-963-5107
jcade@tnstate.edu