FP-32: Identifity Theft Prevention Policy

This proposed policy was developed in response to a regulation issued by the Federal Trade Commission intended to reduce the risk of identity theft. The regulation requires financial institutions and colleges and universities who grant student loans and/or accept payments on account to implement an identity theft prevention program that guides employees in identifying and responding to patterns, practices, or specific activities (Red Flags) that indicate the possible existence of identity theft.

Contact: Program Administrator for Identity Theft Prevention (aka Red Flag Rules)
East Tennessee State University
Box 70601
Johnson City, TN 37614
Phone: 423/439-4893
Email: Redflag@etsu.edu

I. General

ETSUs Identity Theft Prevention Program is designed to detect, prevent, and/or mitigate identity theft in connection with the opening and maintenance of constituent covered accounts. Covered accounts are accounts that involve or are designed to permit multiple payments or transactions including accounts with health care providers. Examples include, but are not limited to, student financial aid accounts, bookstore accounts, and patient accounts. The Identity Theft Prevention Program defines processes and procedures to guide employees in departments involved with covered accounts in identifying and responding to patterns, practices, or specific activities (Red Flags) that indicate the possible existence of identity theft. Red Flags generally fall within one of the following four categories: suspicious documents, suspicious personal identifying information, suspicious or unusual use of accounts, and/or alerts from others (e.g. customer, identity theft victim or law enforcement). Examples of Red Flags include, but are not limited to, documents that appear to be forged or altered, conflicting demographic information, mail returned as "undeliverable" although transactions continue on the account, or a notice or inquiry from a fraud investigator.

This policy applies to the entire University. It outlines employee responsibilities, processes, and required training pertaining to ETSUs Identity Theft Prevention Program and ensures compliance with the Fair and Accurate Credit Transactions (FACT) Act of 2003 and the accompanying requirement (section 114) to develop and implement a written Identity Theft Prevention Program (16 CFR Part 681, aka "Red Flags Regulation "or "Red Flags Rule").

Back to Top

II. Section 1: Purpose

The risk to constituents from data loss and identity theft is of significant concern to ETSU. Therefore, the University adopts this Identity Theft Prevention Policy and enacts this program in an effort to detect, prevent and mitigate identity theft and to help protect the institution and constituents from damages related to the loss or misuse of identifying information due to identity theft. Under this Policy the program will:

1. Identify patterns, practices or specific activities (red flags) that could indicate the existence of identity theft with regard to new or existing covered accounts (defined below in Section 2);

2 Detect red flags that are incorporated in the program;

3. Respond appropriately to any red flags that are detected under this program to prevent and mitigate identity theft;

4. Ensure periodic updating of the program, including reviewing the accounts that are covered and the identified red flags that are part of this program; and,
5. Promote compliance with state and federal laws and regulations regarding identity theft protection.

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.

Back to Top

III. Section 2: Definitions

Constituents are students, employees, alums, donors, patients and applicants.

Covered account includes:

1. Any account that involves or is designated to permit multiple payments or transactions; or
2. Any other account maintained by the Institution for which there is a reasonably foreseeable risk of identity theft to constituents, or for which there is a reasonably foreseeable risk to the safety or soundness of the Institution from identity theft, including financial, operational, compliance, reputation or litigation risks.

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 but not limited to: name, address, telephone number, social security number, date of birth, government issued drivers license or identification number, alien registration number, government passport number, employer or taxpayer identification number, constituent identification number, computer Internet Protocol address or routing code, credit card number or other credit card information.

Identity theft means a fraud committed or attempted using the identifying information of another person without authority.

"Red flag" is a pattern, practice or specific activity that indicates the possible existence of identity theft.

Program Administrator is the individual designated with primary responsibility for oversight of the program. See Section 7.

Back to Top

IV. Section 3: Identification of Red Flags

The following examples of red flags are potential indicators of fraud or identity theft. The risk factors for identifying relevant red flags include the types of covered accounts offered or maintained; the methods provided to open or access covered accounts; and, previous experience with identity theft. Any time a red flag or a situation closely resembling a red flag is apparent; it should be reported to and investigated for verification by the Program Administrator (Redflag@etsu.edu or 423/439-4893).

Alerts, notifications or warnings from a credit or consumer reporting agency. Examples of these red flags include the following:

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 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.
Suspicious documents. Examples of these red flags include the following:
1. Documents provided for identification that appears to have been altered, forged or are inauthentic.
2. The photograph or physical description on the identification document is not consistent with the appearance of the individual presenting the identification.
3. Other information on the identification 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 is not consistent with readily accessible information that is on file with the Institution, such as a signature card or a recent check.
5. An application appears to have been altered or forged, or gives the appearance of having been destroyed and reassembled.
Suspicious personal identifying information. Examples of these red flags include the following:
1. Personal identifying information provided is inconsistent when compared against other sources of information used by the Institution. For example:

The address does not match any address in the consumer report; or,
The Social Security number (SSN) has not been issued or is listed on the Social Security Administration's Death Master File.
2. Personal identifying information provided by the individual is not consistent with other personal identifying information provided by that individual. For example, there is a lack of correlation between the SSN range and date of birth.
3. Personal identifying information provided is associated with known fraudulent activity. For example:
The address on an application is the same as the address provided on a fraudulent application; or,
The phone number on an application is the same as the number provided on a fraudulent application.
4. Personal identifying information provided is of a type commonly associated with fraudulent activity. For example:
The address on an application is fictitious, a mail drop, or a prison; or
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 personal identifying information on an application or in response to notification that the application is incomplete.
8. Personal identifying information provided is not consistent with personal 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.
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 Institution receives a request for a new, additional, or replacement card, 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. There is, for example:

Nonpayment when there is no history of late or missed payments;
A material change in purchasing or usage patterns.
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).
Mail sent to the individual is returned repeatedly as undeliverable although transactions continue to be conducted in connection with the individual's covered account.
5. The Institution is notified that the individual is not receiving paper account statements.
6. The Institution is notified of unauthorized charges or transactions in connection with an individual's covered account.
7. The Institution receives notice from customers, victims of identity theft, law enforcement authorities, or other persons regarding possible identity theft in connection with covered accounts held by the Institution.
8. The Institution is notified by a 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.
9. A breach in the Institutions computer security system.
Back to Top

V. Section 4: Detecting Red Flags

Student Enrollment. In order to detect red flags associated with the enrollment of a student, the Institution will take the following steps to obtain and verify the identity of the individual opening the account:
1. Require certain identifying information such as name, date of birth, academic records, home address or other identification; and
2. Verify the students identity at the time of issuance of the student identification card through review of drivers license or other government-issued photo identification.
Existing Accounts. In order to detect red flags associated with an existing account, the Institution will take the following steps to monitor transactions on an account:
1. Verify the identification of students if they request Information;
2. Verify the validity of requests to change billing addresses by mail or email, and provide the student a reasonable means of promptly reporting incorrect billing address changes; and,
3. Verify changes in banking information given for billing and payment purposes.
Consumer/Credit Report Requests. In order to detect red flags for an employment or volunteer position for which a credit or background report is sought, the Institution 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 Institution has reasonably confirmed is accurate.

Back to Top

VI. Section 5: Responding to Red Flags

Once a red flag or potential red flag is detected, the Institution must act quickly with consideration of the risk posed by the red flag. The Institution should quickly gather all related documentation, write a description of the situation and present this information to the Program Administrator for determination.

The Program Administrator (see Section 7) will complete additional authentication to determine whether the attempted transaction was fraudulent or authentic.
The Institution may take the following steps as is deemed appropriate:
1. Continue to monitor the covered account for evidence of identity theft;
2 Contact the student or applicant for which a credit report was run;
3. Change any passwords or other security devices that permit access to covered accounts;
4. Close and reopen the account;
5. Determine not to open a new covered account;
6. Provide the student with a new student identification number;
7. Notify law enforcement;
8. Determine that no response is warranted under the particular circumstances.
9. Cancel the transaction.

Back to Top

VII. Section 6: Protecting Personal Information

In order to prevent the likelihood of identity theft occurring with respect to covered accounts, the Institutions may take the following steps with respect to its internal operating procedures:
1. Lock file cabinets, desk drawers, overhead cabinets, and any other storage space containing documents with covered account information when not in use.
2. Lock storage rooms containing documents with covered account information and record retention areas at the end of each workday or when unsupervised.
3. Clear desks, workstations, work areas, printers and fax machines, and common shared work areas of all documents containing covered account information when not in use.
4. Documents or computer files containing covered account information will be destroyed in a secure manner. Institution records may only be destroyed in accordance with the Board's records retention guideline, TBR Guideline G-070 Disposal of Records.
5. Ensure that office computers with access to covered account information are password protected.

6. Ensure that computer virus protection is up to date.
7. Avoid the use of social security numbers.
8. Utilize encryption devices when transmitting covered account information.
9. Avoid storing personally identifiable information on non-encrypted portable media, laptops, and hard drives of desktop computers.

Institutional personnel are encouraged to use common sense judgment in securing covered account information to the proper extent. Furthermore, this section should be read in conjunction with the Family Education Rights and Privacy Act (FERPA), the Tennessee Public Records Act, and other applicable laws and policies. If an employee is uncertain of the sensitivity of a particular piece of information, he/she should contact his/her supervisor. The Office of the General Counsel may be contacted for advice.

Back to Top

VIII. Section 7: Program Administration
Oversight and Appointment of the Institutional Program Administrator

Responsibility for developing, implementing and updating this Program lies with an Identity Theft Prevention Program Committee for the University. The Committee is headed by a Program Administrator appointed by the President. Two or more other individuals appointed by the Vice President for Finance and Administration shall comprise the remainder of the committee membership. The Program Administrator with assistance from the Committee members is responsible for operational responsibility of the program which shall include but not be limited to :

the oversight, development, implementation and administration of the program;
approval and implementation of needed changes to the program;
staff training ;
ensuring that appropriate steps are taken for preventing and mitigating identity theft ;
reviewing any staff reports regarding the detection of red flags ; and
determining which steps should be taken in particular circumstances when red flags are suspected or detected

Vice Presidents, deans, directors, and department heads of areas that work with covered accounts are responsible for implementing departmental processes for complying with this policy and ensuring that employees responsible for compliance attend required training. Employees in these departments are responsible for:

complying with the Program,
identifying relevant Red Flags appropriate for their operations,
implementing policies and procedures to detect the Red Flags,
responding appropriately to prevent and mitigate identity theft,
attending Red Flag training, and
reporting all incidents of identity theft as well as any suspicious behavior that may be related to identity theft to the Program Administrator

The Chief Information Officer shall provide technical support to departments and the Program Administrator.

A report to the Institutions President should be made annually concerning institutional compliance with and effectiveness of the program and the responsibility for such report may be placed with the Program Administrator. This report should address service provider arrangements, the effectiveness of the program in addressing the risk of identity theft; significant incidents of identity theft and the institutions response; and, any recommendations for material changes to the program.

Staff training

Staff training shall be conducted for all employees for whom it is reasonably foreseeable, as determined by the Program Administrator, may come into contact with covered accounts or identifying information. This training shall include the responsive steps to be taken when a Red Flag is detected. 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 program.

Overview of service provider arrangements

It is the responsibility of the Institution to ensure that the activities of all service providers are conducted in accordance with reasonable policies and procedures designated to detect, prevent, and mitigate the risk of identity theft. In the event the Institution engages a service provider to perform an activity in connection with one or more covered accounts, the Institution 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 Institutions program and report any red flags to the Program Administrator.

Specific language for inclusion in contracts can be found in TBR Guideline G-030 Contracts and Agreements.

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.

Periodic Updates to the Program

At periodic intervals established in the program, or as required, the program will be re-evaluated to determine whether all aspects of the program are up to date and applicable. Consideration will be given to the Institutions experiences with identity theft situations; changes in identity theft methods, detection methods or prevention methods; and, changes in the Institutions business arrangements with other entities.

Periodic Reviews

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 suspected or discovered may also require revision to the program.

Contact: Program Administrator for Identity Theft Prevention (aka Red Flag Rules)
East Tennessee State University
Box 70601
Johnson City, TN 37614
Phone: 423/439-4893
Email: Redflag@etsu.edu

Back to Top

SOURCE: TBRPolicy 4:01:05:60; **approved by ETSU Identity Theft Prevention Program Committee on 12/14/09**

Original effective date: December 17, 2009