Fitchburg State University Identity Theft Prevention Program – updated 11/17/09

Program Adoption

Fitchburg State University (University) developed this Identity Theft Prevention Program to detect, prevent and mitigate identity theft in connection with covered accounts and to provide for continued administration of the program in compliance with the Federal Trade Commission's Red Flags Rule[1], which implements Part 681 of Title 16 of the Code of Federal Regulations, Sections 114 and 315 of the Fair and Accurate Credit Transactions Act (FACTA) of 2003. After consideration of the size of the University's operations and systems, the nature and scope of the University's activities, and prior history of identity theft, the Board of Trustees determined that this program was appropriate for Fitchburg State University.

Purpose

The purpose of this program is to detect, prevent and mitigate identity theft in connection with the opening of a new covered account or an existing covered account and to provide for continued administration of the program. The program includes reasonable policies and procedures to:

1. Identify relevant red flags for covered accounts the University offers or maintains and incorporate those red flags into the program;
2. Detect red flags that have been incorporated into the program;
3. Respond appropriately to any red flags that are detected to prevent and mitigate identity theft;
4. Verify compliance of third party service providers involved in managing covered accounts offered but not maintained by the University; and
5. Ensure the program is updated periodically to reflect changes in risks to students and to the safety and soundness of the institution from identity theft.

The program shall, as appropriate, incorporate existing policies and procedures that control foreseeable risks.

Definitions

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

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

A **covered account** means an account that the University offers or maintains, primarily for personal, family or household purposes that involves or is designed to permit multiple payments or transactions.

Or, any other account that the University offers or maintains for which there is a reasonable foreseeable risk to students, faculty or staff, or to the safety and soundness of the institution from identity theft.

The **Program Administrator** is the individual designated with primary responsibility for oversight of the program.

A **Creditor** is an entity that 1) regularly extends, renews or continues credit; or 2) regularly arranges for the extension, renewal, or continuation of credit; or 3) is involved in the decision to extend, renew, or continue credit.

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, 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, unique biometric data, unique electronic identification information of access device, or telecommunication identifying information or access device.

Covered Accounts

Fitchburg State University has identified six types of covered accounts, four of which are accounts administered by the University and two types of accounts that are administered by service providers.

University covered accounts:

1. Campus card ("OneCard") which can be used as a debit card to make purchases at "participating merchant" locations off campus;
2. Refund of credit balances involving federal loans;
3. Refund of credit balances without federal loans;
4. Emergency loans.

Service provider covered accounts:

1. Extended tuition payment plan administered by Tuition Management Systems (TMS); refer to "Oversight of Service Provider Arrangements" on page 5;
2. Accounts managed by collections agencies; refer to "Oversight of Service Provider Arrangements" on page 5.

Relevant Red Flags

In order to identify relevant Red Flags, the University takes the following into consideration:

1. The types of covered accounts as noted above;
2. The methods provided to open covered accounts, apply for admission and register for courses that may require some or all of the following information:
    a. Common application with personal identifying information
    b. High school transcript
    c. Official ACT or SAT scores
    d. Two letters of recommendation
    e. Entrance medical record

f. Medical history
g. Immunization history
h. Insurance card

3. The methods provided to access covered accounts:
   a. Disbursement obtained in person require a picture identification
   b. Disbursements obtained by mail can only be mailed to an address on file
4. The University's previous history of identity theft

Any alert notification or warning of address discrepancies obtained through a combination of suspicious activities, questionable documents, and/or personal identifying information identified as a Red Flag by University employees or brought to the attention of the University by a victim of identity theft, or by a consumer will be used (in part) to detect Red Flags. The following are relevant Red Flags which employees should be aware of and diligent in monitoring for in general:

1. Documents provided for identification appear to be altered or forged;
2. The photograph or physical description on the identification is not consistent with the appearance of the student presenting the identification;
3. A request made from a non-University issued email account;
4. A request to mail something to an address not listed on file; and
5. Notice from students, faculty, staff, law enforcement authorities, or other persons regarding possible identity theft in connection with covered accounts.

Detection of Red Flags

The program is also designed to detect Red Flags relevant to each type of covered account identified on page 2 as follows:

1. **Change of name or address associated with a covered account –** requests must be made in person by presenting a picture ID. Any individual requesting a name or address change who cannot be physically present to provide verification of their identity must be asked challenging questions. The person's relationship with the University is then verified using the University's student and administrative information system. Confirmation notices are then mailed to old and new addresses (in the case of address changes) with clear procedures for recipients to notify the University in the event of suspected fraud.

   Red Flag – Picture ID does not appear to be authentic or not matching the appearance of the individual presenting it. The person's relationship with the University cannot be verified using the student and administrative information system.

2. **Issuing a new or replacement OneCard –** requests must be made in person by presenting a picture ID. Any individual requesting a name or address change who cannot be physically present to provide verification of their identity must be asked challenging questions. The person's relationship with the University will then be verified using the University's student and administrative information system.

   Red Flag – Picture ID does not appear to be authentic or not matching the appearance of the individual presenting it. The person's relationship with the University cannot be verified using the student and administrative information system. Or a replacement card is requested by someone within at least 30 days after notice of name or address change.

3. **Refund of a credit balance involving a federal loan –** as directed by federal regulation (U.S. Department of Education) these balances are required to be refunded in the parent's name and mailed to the address on file within the time period specified. No request is required.

   Red Flag – none of this is initiated by the University.

4. **Refund of a credit balance, no federal loan** – requests from current students must be made in person by presenting a picture ID or in writing from the student's University-issued email account. The refund check can only be mailed to an address on file or picked up in person by showing a picture ID. Requests from students not currently enrolled or graduated from the Univeristy must be made in writing.

   Red Flag – Picture ID does not appear to be authentic or not matching the appearance of the student presenting it. Request not coming from a University issued student email account.

5. **Deferment of tuition payment** – requests are made in person only by presenting a picture ID and require the student's signature.

   Red Flag - Picture ID does not appear to be authentic or not matching the appearance of the student presenting it.

6. **Emergency loan** – requests must be made in person by presenting a picture ID or in writing from the student's University issued email account. The loan check can only be mailed to an address on file or picked up in person by showing a picture ID.

   Red Flag – Picture ID does not appear to be authentic or not matching the appearance of the student presenting it. Request not coming from a University issued email account.

7. **Extended tuition payment plan** – student must contact an outside service provider and provide personal identifying information to them.

   Red Flag - Notice from the service provider to the institution concerning information on a credit report, returned mail from a current address or any other detected Red Flag.

Responses

The program provides for appropriate responses to detected Red Flags to prevent and mitigate identity theft. The appropriate responses are as follows:

1. Decline request to change name and/or address associated with a covered account until other information is available to eliminate the Red Flag;
2. Do not issue a new or replacement OneCard until proper validation has occurred;
3. Deny access to the covered account until other information is available to eliminate the Red Flag;
4. Contact the individual(s) associated with the covered account;
5. Change any passwords, security codes or other security devices that permit access to the covered account;
6. Notify law enforcement; or
7. Determine no response is warranted under the particular circumstances.

Oversight of the Program

The University's Assistant Vice President/Chief Information Officer is the designated Program Administrator responsible for developing, implementing and updating this program. This includes responsibility for ensuring appropriate training is made available to University personnel, reviewing any internal reports regarding the detection of Red Flags, determining which steps of prevention and mitigation should be taken in particular circumstances and considering the necessity of periodic changes to the program.

Updating the Program

This program will be periodically reviewed and updated to reflect changes in identity theft risks and technological changes. At least once per year in October, the Program Administrator will consider the University's experiences with identity theft, changes in identity theft methods, changes in identity theft detection and prevention methods, changes in types of accounts the University maintains and changes in the University's business arrangements with other entities. After considering these factors, the Program Administrator will determine whether changes to the program, including the listing of Red Flags, are warranted. If warranted, the Program Administrator shall present any recommended changes to the President's Council and then update the program with approved changes in collaboration with appropriate personnel. The President's approval shall be sufficient to make changes to the University's Identity Theft Program.

Staff Training

University staff responsible for administering covered accounts will be required to review documentation and participate in training provided by the University with respect to the Identity Theft Program, and the responsive steps that need to be taken when a Red Flag is detected.

Oversight of Service Provider Arrangements

The University shall take steps to ensure that the activity of a service provider is conducted in accordance with reasonable policies and procedures designed to detect, prevent, and mitigate the risk of identity theft whenever the organization engages a service provider to perform an activity in connection with one or more covered accounts. The University will maintain an updated list of service providers and attestations of compliance for each of their FTC Red Flags programs.

---

[1] **Background on the Red Flags Rule**

Due to the criminal value of personal identifiable information and the ease with which fraud can now be perpetrated with it, regulatory and consumer-driven scrutiny is being placed not only on institutions guarding such information but also on how they respond to a data breach. It is now illegal to not notify the victims when their personal information may have been compromised in 44 states. In addition, the federal government is increasing its focus on identity theft with the Federal Trade Commission's Fair and Accurate Credit Transactions ACT ("FACTA") Section 114 "Red Flag" Rules that mandate the creation of an Identity Theft Program (beyond a "policy"). This program must include a pro-active approach to detect and mitigate identity theft including; a process for evaluating and managing identity theft policies and procedures, a plan to respond to and mitigate fraud (as well as a Data Breach Response plan), identity theft training, and formal approval by the Board of Directors, all of which needs to be continuously updated as situations warrant. The University must incorporate relevant Red Flags into a program to enable the University to detect and respond to potential identity theft.