

Francis Marion University

Identity Theft Prevention Program for Covered Accounts

Program Adoption

Francis Marion University developed this Identity Theft Prevention Program (hereinafter Program) pursuant to the Federal Trade Commission's Red Flags Rule which implements Section 114 of the Fair and Accurate Credit Transactions Act (FACT Act) of 2003. The nature and scope of the University's activities relating to operations and accounts were considered to determine this Program.

Purpose

The purpose of this policy is to establish an Identity Theft Prevention Program designed to detect, prevent and mitigate identity theft in connection with the opening of a Covered Account or an existing Covered Account and to provide for continued administration and support of the Program. The Program shall include reasonable policies and procedures to:

- 1) Identify relevant Red Flags (patterns, practices, and specific activities that signal possible identity theft) for Covered Accounts the University offers or maintains and incorporate those Red Flags into its Program;
- 2) Detect Red Flags that have been incorporated into the Program of the University;
- 3) Respond appropriately to any Red Flags that are detected to prevent and mitigate identity theft; and
- 4) Ensure the Program is updated periodically to reflect changes in risks from identity theft.

Definitions

- **Identity Theft:** Fraud committed or attempted using the identifying information of another person without authority.
- **Covered Account:** An account that is primarily designed to permit multiple payments or transactions such as a loan or account that is billed monthly.
- **Red Flag:** A pattern, practice or specific activity that indicates the possible existence of identity theft.
- **Identifying Information:** Any name or number which may be used alone or in conjunction with other information to identify a specific person including name, address, phone number, social security number, student identification number, birth date, personal e-mail account, governmental issued driver's license or identification number, taxpayer identification, alien registration, or passport numbers.
- **Program Administrator:** Person designated to manage the Identity Theft Program.

FMU Covered Accounts Relevant to this Policy

- 1) The University participates in the Federal Perkins Loan Program;
- 2) The University offers and establishes student payment plans;
- 3) The University utilizes credit reports from Credit Reporting Agencies to screen job applicants for Campus Police positions.

Identifying Relevant 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, the methods it provides to access its accounts and its previous experiences with Identity Theft. The following are relevant Red Flags and examples signaling possible Identity Theft:

A. Notification and Warnings from Credit Reporting Agencies

- 1) Report of fraud accompanying a credit report;
- 2) Notice or report from a credit agency of a credit freeze on a customer or applicant;
- 3) Notice or report from a credit agency of an active duty alert for an applicant; and
- 4) Indication from a credit report of activity that is inconsistent with a customer's usual pattern or activity.

B. Suspicious Documents

- 1) Identification document or card that appears to be forged, altered or inauthentic;
- 2) Photograph or physical description on the identification that is not consistent with the appearance of the student or borrower presenting the identification;
- 3) Other document with information that is not consistent with existing customer information (such as if a person's signature on a check appears forged); and
- 4) Application for service that appears to have been altered or forged.

C. Suspicious Personal Identifying Information

- 1) Identifying information presented that is inconsistent with other information the customer provides (example: inconsistent birth dates);
- 2) Identifying information presented that is inconsistent with other sources of information (for instance, an address not matching an address on a credit report);
- 3) Identifying information presented that is the same as information shown on other applications that were found to be fraudulent;
- 4) Identifying information presented that is consistent with fraudulent activity (such as an invalid phone number or fictitious billing address);
- 5) Social Security Number (SSN) presented is the same as one given by another customer;
- 6) An address or phone number presented that is the same as that of another person;

- 7) A person fails to provide complete personal identifying information on an application when reminded to do so (however, by law Social Security numbers must not be required); and
- 8) A person's identifying information is not consistent with the information that is on file for the customer.

D. Suspicious Account Activity or Unusual Use of Account

- 1) Change of address for an account followed by a request to change the account holder's name;
- 2) Payments stop on an otherwise consistently up-to-date account;
- 3) Account used in a way that is not consistent with prior use (example: very high activity);
- 4) Mail sent to the account holder is repeatedly returned as undeliverable;
- 5) Notice to the University that a customer is not receiving mail sent by the University;
- 6) Notice to the University that an account has unauthorized activity;
- 7) Breach in the University's computer system security; and
- 8) Unauthorized access to or use of customer account information.

E. Alerts from Others

- 1) Notice to the University from a customer, identity theft victim, law enforcement or other person that the University has opened or is maintaining a fraudulent account for a person engaged in Identity Theft; and
- 2) Notification to the University of unauthorized charges or transactions in connection with a student or borrower's Covered Account.

Detecting Red Flag Activity

The Red Flag detection practices are described below:

A. Student Enrollment - New Accounts:

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 account:

- 1) Require certain identifying information such as name, date of birth, address, driver's license or other identification;
- 2) Verify the customer's identity (review license or 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 transactions on an account:

- 1) Verify the identification of a student if they request information (in person, via phone, via facsimile, via email);
- 2) Verify the validity of request to change billing addresses by mail or email;
- 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;
- 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 Red Flags and Mitigating Identity Theft

In the event University staff detects any identified Red Flags, any of the following responses shall be taken to respond and mitigate the identity theft, depending on the situation:

- 1) Continue to monitor an account for evidence of Identity Theft;
- 2) Contact the student or borrower;
- 3) Change any passwords, security codes, or other security devices that permit access to a Covered Account;
- 4) Not open a new Covered Account;
- 5) Close an existing Covered Account;
- 6) Reopen a Covered Account with a new account number;
- 7) Not attempting to collect on a Covered Account;
- 8) Notify the Program Administrator;
- 9) Notify law enforcement; and/or
- 10) Determine no response is warranted under the particular circumstances.

Protect Student 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 student identifying information:

- 1) Ensure that its website is secure or provide clear notice that the website is not secure;

- 2) Ensure complete and secure destruction of paper documents and computer files containing student account information when a decision has been made to no longer maintain such information;
- 3) Ensure that office computers with access to Covered Account information are password protected;
- 4) Avoid use of Social Security Numbers;
- 5) Ensure computer virus protection is up to date; and
- 6) Require and keep only the kinds of student information that are necessary for University purposes.

Ensuring the Program is Administered and Updated Properly to Minimize Risk

A. Oversight

Responsibility for developing, implementing, and updating this Program lies with the Program Administrator who may be the Vice President for Business Affairs or his or her appointee. The Program Administrator will be responsible for ensuring appropriate training of University Staff on the Program, for reviewing any staff reports regarding the detection of Red Flags and the steps for preventing and mitigating Identity Theft, determining which steps of prevention and mitigation should be taken in particular circumstances and considering periodic changes to the Program.

B. Staff Training and Reporting

- 1) University employees responsible for implementing the Program shall be trained either by or under the direction of the Program Administrator in the detecting of Red Flags and the responsive steps to be taken when a Red Flag is reported.
- 2) Appropriate staff shall provide reports to the Program Administrator on incidents of identity theft, the effectiveness of the Program and the University's compliance with the Program. The reports should address such issues as effectiveness of the policies and procedures in addressing the risk of identity theft in connection with Covered Accounts, service provider arrangements, significant incidents involving identity theft and the University's response and recommendations for changes to the Program.

C. Service Provider Agreements

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 for the University's Covered Accounts.

Updating the Program

The University will update the Program annually in December, to reflect changes in risks to students or borrowers or to the safety and soundness of the University from identity theft, based on factors such as:

- 1) The experiences of the University with identity theft;
- 2) Changes in methods of identity theft;
- 3) Changes in methods to detect, prevent, and mitigate identity theft; and
- 4) Changes in the types of accounts that the University offers or maintains.