

PRAIRIE VIEW A&M UNIVERSITY

Administrative Procedures Manual

21.01.04.P0.01 Identity Theft Red Flag and Security Incident Reporting

Approved (July 8, 2009)

Next Scheduled Review (April-2012)

1. Purpose

- 1.1 The purpose of the Identify Theft Red Flag and Security Incident Reporting Procedure is to provide information to assist individuals in 1) detecting, preventing, and mitigating identity theft in connection with the opening of a “covered account” or any existing “covered account” or who believe that a security incident has occurred and 2) reporting a security incident.

In 2003, the U.S. Congress enacted the Fair and Accurate Credit Transaction Act of 2003 (FACT Act) which required the Federal Trade Commission (FTC) to issue regulations requiring “creditors” to adopt policies and procedures to prevent identify theft. In 2007, the Federal Trade Commission (FTC) issued a regulation known as the Red Flag Rule. The rule requires “financial institutions” and “creditors” holding “covered accounts” to develop and implement a written identity theft prevention program designed to identify, detect and respond to “Red Flags.”

2. Definitions

Pursuant to the Red Flag regulations at 16 C. F. R. § 681.2, the following definitions shall apply to this procedure:

2.1 Covered accounts:

- 2.1.1 Any account the University offers or maintains primarily for personal, family or household purposes, that involves multiple payments or transactions.
- 2.1.2 Any other account the University offers or maintains for which there is a reasonably foreseeable risk to customers or to the safety and soundness of the University from Identity Theft.

- 2.2 Credit: The right granted by a creditor to a debtor to defer payment of debt or to incur debt and defer its payment or to purchase property or services and defer payment therefore.

- 2.3 Creditor – A creditor is a person or entity that regularly extends, renews, or continues credit and any person or entity that regularly arranges for the extension, renewal, or continuation of credit. Examples of activities that indicate a college or university is a “creditor” are:

- participation in the Federal Perkins Loan program;
- participation as a school lender in the Federal Family Education Loan Program;
- Offering institutional loans to students;
- Offering a plan for payment of tuition or fees throughout the semester, rather than requiring full payment at the beginning of the semester.

- 2.4 Customer: Any person with a covered account with a creditor.

- 2.5 Personal Information: – Specific items of personal information identified in as defined in Business and Commerce Code, § 521.002 (a)(2). This information includes an individual’s first name or first initial and his or her last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted or redacted: Social Security Number, driver’s license/Texas identification card number, health insurance information, medical information, or financial account number such as credit card number, in combination with any required security code, access code, or password that would permit access to an individual’s financial account.

PRAIRIE VIEW A&M UNIVERSITY
Administrative Procedures Manual

2.6 Identifying information: Any name or number that may be used, alone or in conjunction with any other information, to identify a specific person,” including:

- name
- address
- telephone number
- 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 electronic identification number (student identification number)
- computer’s Internet Protocol address or routing code

2.7 Identity Theft: A fraud committed using the identifying information of another person.

2.8 Red Flag: A pattern, practice, or specific activity that indicates the possible existence of Identity Theft.

2.9 Security Incident: A collection of related activities or events which provide evidence that personal information could have been acquired by an unauthorized person.

3. Procedures and Responsibilities

3.1 Identification of Red Flags: In order to identify relevant Red Flags, the University considers the types of accounts that it offers and maintains, the 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, in each of the listed categories, which employees should be aware of and diligent in monitoring for:

3.1.1. Suspicious Documents

- Identification document or card that appears to be forged, altered or inauthentic;
- Identification document or card on which a person’s photograph or physical description is not consistent with the person presenting the document;
- 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
- Application for service that appears to have been altered or forged.

3.1.2. Suspicious Personal Identifying Information

- Identifying information presented that is inconsistent with other information the customer provides (example: inconsistent birth dates);
- Identifying information presented that is inconsistent with other sources of information (for instance, date of birth on application not matching date of birth on FASFA);
- Identifying information presented that is the same as information shown on other applications that were found to be fraudulent;
- Social security number presented that is the same as one given by another customer;
- 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
- A person’s identifying information is not consistent with the information that is on file for the customer.

3.1.3. Suspicious Account Activity or Unusual Use of Account

PRAIRIE VIEW A&M UNIVERSITY

Administrative Procedures Manual

- Account used in a way that is not consistent with prior use (example: very high activity);
- Notice to the University that a customer is not receiving mail sent by the University;
- Notice to the University that an account has unauthorized activity or charges;
- Breach in the University's computer system security; and
- Unauthorized access to or use of customer account information.

3.1.4. Alerts from Others

- Notice to the University from a customer, identity theft victim, law enforcement or other person that it has opened or is maintaining a fraudulent account for a person engaged in Identity Theft.

3.2 Detecting Red Flags.

3.2.1 New Accounts

In order to detect any of the Red Flags identified above associated with the opening of a new account, University personnel will take the following steps to obtain and verify the identity of the person opening the account:

- Require certain identifying information such as name, date of birth, residential or business address, driver's license or other identification;
- Verify the customer's identity (for instance, review a driver's license or other identification card);
- Independently contact the customer.

3.2.2 Existing Accounts

In order to detect any of the Red Flags identified above for an existing account, University personnel will take the following steps to monitor transactions with an account:

- Verify the identification of customers if they request information (in person, via telephone, via facsimile, via email);
- Independently contact the customer.

3.3 Responding to Red Flags and Mitigating Identity Theft.

3.3.1 In the event University personnel detect any identified Red Flags, such personnel shall take all appropriate steps to respond and mitigate identity theft depending on the nature and degree of risk posed by the Red Flag, including but not limited to the following examples:

- Continue to monitor an account for evidence of Identity theft;
- Contact the customer;
- Change any passwords or other security devices that permit access to accounts;
- Not open a new account;
- Close an existing account;
- Reopen an account with a new number;
- Notify law enforcement; or
- Determine that no response is warranted under the particular circumstances.

3.4 Service Providers.

3.4.1 The University remains responsible for compliance with the Red Flag Rules even if it outsources operations to a third party service provider. The written agreement between the University and the third party service provider shall require the third party to have

PRAIRIE VIEW A&M UNIVERSITY
Administrative Procedures Manual

reasonable policies and procedures designed to detect relevant Red Flags that may arise in the performance of their service provider's activities. The written agreement must also indicate whether the service provider is responsible for notifying only the University of the detection of a Red Flag or if the service provider is responsible for implementing appropriate steps to prevent or mitigate identify theft.

3.5 Training

3.5.1 All employees who process any information related to covered accounts shall receive training following appointment on the procedures outlined in this document. Refresher training may be provided annually.

3.6 Annual Review

3.6.1 An annual review of the Red Flag procedures and covered accounts will occur in the month of February. The University's Information Security Office will be responsible for the annual review with the departments affected by the Red Flag procedures. This group will consider the institution's experiences with identify theft situations, changes in identify theft methods, changes in identity theft detection and prevention methods, changes in the types of account the institution maintains and changes in the institution's business arrangements with other entities. The status of the review and any updates will be reported with any recommendations for changes to the Vice President for Business Affairs no later than the first working day in March.

Contact Office: Information Security Officer; 936/261-9351