PRAIRIE VIEW A&M UNIVERSITY
UNIVERSITY ADMINISTRATIVE PROCEDURE

21.01.04.P0.02 Identity Theft Prevention Program
Approved July 8, 2009
Revised November 20, 2015
Revised November 13, 2020
Next Scheduled Review: November 2025

UAP Purpose

The purpose of this University Administrative Procedure (UAP) is to define the university's identity theft prevention program to assist in detecting, preventing, and mitigating identity theft related to new and existing "covered accounts".

Definitions

Covered Accounts – generally a consumer account designed to permit multiple payments or transactions, and any other account for which there is a reasonably foreseeable risk for identity theft. This generally includes student accounts or loans that are administered by the university.

Identifying information – any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," includes:

- 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); and,
- Computer's internet protocol address or routing code.

Identity Theft – a fraud committed using the identifying information of another person.

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

Official Procedures and Responsibilities

1. GENERAL

1.1 In 2007, the Federal Trade Commission (FTC) issued a regulation known as the Red Flags Rule. Under the Red Flags Rule, the university must develop and implement a written identity theft prevention program designed to identify, detect, and respond to "red flags."

2. PROCEDURES AND RESPONSIBILITIES

2.1 Identification of Red Flags

2.1.1 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:

2.1.1.1 Suspicious Documents

2.1.1.1.1 Identification document or card that appears to be forged, altered or inauthentic;

2.1.1.1.2 Identification document or card on which a person's photograph or physical description is not consistent with the person presenting the document;

2.1.1.1.3 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,

2.1.1.1.4 Application for service that appears to have been altered or forged.

2.1.1.2 Suspicious Personal Identifying Information

2.1.1.2.1 Identifying information presented that is inconsistent with other information the customer provides (i.e., inconsistent birth dates);

2.1.1.2.2 Identifying information presented that is inconsistent with other sources of information (i.e., date of birth on application not matching date of birth on FASFA);

2.1.1.2.3 Identifying information presented that is the same as information shown on other applications that were found to be fraudulent;

2.1.1.2.4 Social security number presented that is the same as one given by another customer;

2.1.1.2.5 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,

2.1.1.2.6 A person's identifying information is not consistent with the information that is on file for the customer.

2.1.1.3 Suspicious Account Activity or Unusual Use of Account

2.1.1.3.1 Account used in a way that is not consistent with prior use (i.e., very high activity);

2.1.1.3.2 Notice to the University that a customer is not receiving mail sent by the university;

2.1.1.3.3 Notice to the university that an account has unauthorized activity or charges;

2.1.1.3.4 Breach in the university's computer system security; and,

2.1.1.3.5 Unauthorized access to or use of customer account information.

2.1.1.4 Alerts from Others

2.1.1.4.1 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.

2.2 Detection of Red Flags

2.2.1 New Accounts

2.2.1.1 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:

2.2.1.1.1 Require certain identifying information such as name, date of birth, residential or business address, driver's license or other identification;

2.2.1.1.2 Verify the customer's identity (i.e., review a driver's license or other identification card); and,

2.2.1.1.3 Independently contact the customer.

2.2.2 Existing Accounts

2.2.2.1 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:

2.2.2.1.1 Verify the identification of customers if they request information (in person, via telephone, via facsimile, via email); and,

2.2.2.1.2 Independently contact the customer.

2.3 Response to Red Flags and Mitigation of Identity Theft

2.3.1 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 flags, including but not limited to the following examples:

2.3.1.1 Continue to monitor an account for evidence of identity theft;

2.3.1.2 Contact the customer;

2.3.1.3 Change any passwords or other security devices that permit access to accounts;

2.3.1.4 Not open a new account;

2.3.1.5 Close an existing account;

2.3.1.6 Reopen an account with a new number;

2.3.1.7 Notify law enforcement; or,

2.3.1.8 Determine that no response is warranted under the particular circumstances.

2.4 Program Administration

2.4.1 Service Providers – The university remains responsible for compliance with the Red Flags Rule 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 reasonable procedures designed to detect relevant red flags that may arise in the performance of their service provider's activities. The written agreement should also indicate that the service provider is responsible for notifying the university of the detection of a red flag.

2.4.2 Training – The Texas A&M University System requires specific training to those employees who serve in a business capacity and who have access to sensitive information. The university will continue this process of identifying those positions and assigning applicable trainings as needed.

2.4.3 Program Review – A periodic review and update of the identity theft prevention program and covered accounts will occur. This review will consider the institution's experiences with identity theft situations, changes in identify theft methods, changes in identity theft detection and prevention methods, changes in the types

of accounts 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 to the Senior Vice President for Business Affairs.

Related Statutes, Policies, Regulations and Rules

Federal Trade Commission Red Flags Rule 16 C.F.R. § 681.1

Business and Commerce Code §521.002 (a) (2)

Fair and Accurate Credit Transaction Act of 2003 (FACT Act)

System Regulation 21.01.04 Extension of Credit

Interagency Guidelines on Identity Theft Detection, Prevention, and Mitigation, Appendix A to the Red Flags Rule

Contact Office

Financial Management Services	936-261-1900