STEPHEN F. AUSTIN
STATE UNIVERSITY
Office of the General Counsel

POLICY SUMMARY FORM

Policy Name: Identity Theft Prevention

Policy Number: 14.5

Is this policy new, being reviewed/revised, or deleted? Review/Revise

Date of last revision, if applicable: April 14, 2015

Unit(s) Responsible for Policy Implementation: Vice President for Finance and Administration

Purpose of Policy (what does it do): Establish an identity theft programs in order to detect, prevent and mitigate identity theft.

Reason for the addition, revision, or deletion (check all that apply):

☒ Scheduled Review ☐ Change in law ☐ Response to audit finding

☐ Internal Review ☐ Other, please explain:

Please complete the appropriate section:

Specific rationale for new policy:

Specific rationale for <u>each</u> substantive revision: No substantive changes

Specific rationale for deletion of policy:

Additional Comments:

Reviewers:

Judith Kruwell, Director of Financial Services
Michaelyn Greene, Director of Administrative Services
Danny Gallant, Vice President for Finance and Administration

Identity Theft Prevention

Original Implementation: April 21, 2009
Last Revision: ~~April 14, 2015~~*April 24, 2018*

Purpose

The purpose of this policy is to establish an Identity Theft Program (~~"~~program~~"~~) designed to detect, prevent and mitigate identity theft in connection with covered accounts and to provide continued administration of the program in compliance with applicable regulations. The program will include reasonable procedures to:

~~1.~~• Identify risks that signify potentially fraudulent activity within new or existing covered accounts;
~~2.~~• Detect risks when they occur in covered accounts;
~~3.~~• Respond to risks if fraudulent activity has occurred and act if fraud has been attempted or committed; and
~~4.~~• Update the program periodically to reflect changes in risks to students, covered accounts and previous experience with identity theft.

This policy is in addition to any other information security policies currently at Stephen F. Austin State University.

Definitions

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

Covered account means:
~~1.~~• 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; and
~~2.~~• Any other account that the university offers or maintains for which there is a reasonably foreseeable risk to customers or to the safety and soundness of the financial institution or creditor from identity theft, including financial, operational, compliance, reputation, or litigation risks.

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

Red Flag Rules are rules issued by the Federal Trade Commission (FTC) on November 7, 2007 regarding identity theft. These rules implement Sections 114 and 115 of the Fair and Accurate

Credit Transactions Act and require certain policies and procedures be developed that are designed to detect, prevent and mitigate identity theft.

Service Provider means a person that provides a service directly to the university.

Elements *o*~~O~~f *t*~~T~~he *P*~~p~~rogram

Identification of Red Flags

The program includes relevant red flags from the following categories as appropriate:

- ~~1.~~ Alerts, notifications, or warnings from ~~a~~ credit reporting agencies;
- ~~2.~~ The presentation of suspicious documents;
- ~~3.~~ The presentation of suspicious personal identifying information;
- ~~4.~~ Unusual use of, or suspicious activity related to, the covered account.

Detecting Red Flags

The program addresses the detection of red flags in connection with the opening of covered accounts and existing covered accounts by:

- ~~1.~~ Obtaining identifying information about, and verifying the identity of~~,~~ a person opening a covered account; and
- ~~2.~~ Authenticating customers, monitoring transactions, and verifying the validity of change of address requests in the case of existing covered accounts.

Responding to Fraudulent Activity

Once potentially fraudulent activity is detected, an employee must act quickly, as a rapid appropriate response can protect employees, students, and the university from damages and loss.

- ~~1.~~ The employee will gather all related documentation and present this information to his/her immediate supervisor.
- ~~2.~~ The supervisor will complete additional authentication to determine whether the attempted transaction was fraudulent or authentic, and will respond appropriately.
- ~~3.~~ If the activity is deemed fraudulent, procedures as outlined in the university Fraud Policy (2.7) will be followed.

Periodic Updates to 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 in the current

business environment. Periodic reviews may include an assessment of:

- ~~1.~~ The types of covered accounts offered or maintained;
- ~~2.~~ The methods provided to open covered accounts;
- ~~3.~~ The methods provided to access covered accounts;
- ~~4.~~ Previous experience with identity theft;
- ~~5.~~ Red flags as identified above and the need to define new red flags; and
- ~~6.~~ Response procedures defined above and their efficacy to reduce damage to the university and its customers.

Program Administration

Oversight of the Program

Oversight of the program will lie with the vice president *for*~~of~~ finance and administration. The vice president for finance and administration will be responsible for appointing a program officer with the specific responsibility for the program's development, implementation, and administration; reviewing reports prepared by staff regarding compliance with red flag rules; and approving material changes to the program as necessary to address changing identity theft risks.

Reports

The program officer responsible for the development, implementation, and administration of the program will report, in writing, to the vice president for finance and administration at least annually on program compliance. The report should address such issues as: the effectiveness of the policy and procedures in addressing the risk of identity theft in connection with covered accounts; service provider arrangements; significant incidents involving identity theft and management's response and recommendations for material changes to the program.

Staff Training

Staff, officials, and contractors ~~for~~ who~~m~~ ~~it is reasonably foreseeable~~ may come into contact with covered accounts or personally identifiable information that may constitute a risk to the university or its customers must complete the red flag training to ensure compliance with the identity theft prevention policy.

Oversight of Service Provider Arrangements

It is the responsibility of the university to ensure that the activities of all service providers are conducted in accordance with reasonable policies and procedures designed to detect, prevent, and mitigate the risk of identity theft. Contractual arrangements with service providers should

specifically require the service provider to maintain its own identity theft prevention program consistent with the guidance of the red flag rules.

Cross Reference: Fair and Accurate Credit Transactions Act of 2003; 16 CFR 681; Fraud (2.7)

Responsible for Implementation: Vice President for Finance and Administration

Contact for Revision: Vice President for Finance and Administration

Forms: None

Board Committee Assignment: Finance and Audit