

SALEM STATE UNIVERSITY
IDENTITY THEFT PROTECTION PROCEDURES

I. Objective of Program: the University is required to establish an “Identity Theft Protection Program” (Program) to comply with “Red Flag” rules issued by the Federal Trade Commission. This program identifies and establishes reasonable policies and procedures to detect and prevent identity theft of identifying information in its covered accounts.

II. Definitions: the following definitions shall apply to this Program:

“Covered accounts”:

1. Any account the University offers or maintains primarily for personal, family or household purposes, that involves multiple payments or transactions.
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.

“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 (first and last name and/or initials)
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
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.

III. Tips to Detect Suspicious Activity - The following are examples of relevant “Red Flags” which employees should be aware of and diligent in monitoring for:

A. Notifications and Warnings from Credit Reporting Agencies

- Report of fraud accompanying a credit report
- Notice or report from a credit agency of a credit freeze on a customer or applicant
- Notice or report from a credit agency of an active duty alert for an applicant
- Indication from a credit report of activity that is inconsistent with a customer’s usual pattern or activity.

B. 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 (i.e. if a person’s signature on a check appears forged)
- Application for service that appears to have been altered or forged.

C. Suspicious Personal Identifying Information

- Identifying information presented that is inconsistent with other information the customer provides (example: inconsistent birth dates)

SALEM STATE UNIVERSITY
IDENTITY THEFT PROTECTION PROCEDURES

- Identifying information presented that is inconsistent with other sources of information (example: an address not matching an address on a credit report)
- Identifying information presented that is the same as information shown on other applications that were found to be fraudulent
- Identifying information presented that is consistent with fraudulent activity (such as an invalid phone number or fictitious billing address)
- Social Security number presented that is the same as one given by another customer;
- An address or phone number presented that is the same as that of another person
- 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)
- 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

- Change of address for an account followed by a request to change the account holder's name
- Payments stop on an otherwise consistently up-to-date account
- Account used in a way that is not consistent with prior use (e.g. very high activity)
- Mail sent to the account holder is repeatedly returned as undeliverable
- 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
- Breach in the University's computer system security
- Unauthorized access to or use of customer account information

E. 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.

IV. Reasonable Procedures on New and Existing Accounts: in an effort to mitigate identity risk, the following general procedures should be followed on new or existing covered accounts:

A. 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
- Open verification of information making notation on student account of action taken
- Report any suspicious activity immediately to supervisor
- Report and complete Privacy Incident Form (if applicable)

B. 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:

- Determine validity of customer identity by corroborating information stored on account.
- Verify the identification of customers if they request information (in person, via telephone, via facsimile, via email)
- Verify the validity of requests to change billing addresses
- Verify changes in account information given for billing and/or payment purposes.
- Report any suspicious activity immediately to supervisor

SALEM STATE UNIVERSITY
IDENTITY THEFT PROTECTION PROCEDURES

- Report and complete Privacy Incident Form (if applicable)

V. Recommended Steps to follow to Mitigate Identity Theft: In the event University personnel detect any identified Red Flags, such personnel shall use 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 (make notation)
- Change any passwords or other security devices that permit access to accounts
- Not open a new account; (as advised by supervisor)
- Close an existing account; (as advised by supervisor)
- Reopen an account with a new number; (as advised by supervisor)
- Notify law enforcement; (request police report or any forgery or fraudulent report)
- Make notation on any possible incidence on account
- Discuss any questionable situation with supervisor
- Report and complete Privacy Incident Form (if applicable)

VI. Reporting Disclosures: there are various circumstances that require reporting potential privacy disclosures. Such disclosures fall under 3 categories: incidental (which does not require reporting), accidental and intentional (these latter two do require reporting). However one rule of thumb should be followed: **WHEN IN DOUBT, REPORT!**

A. Incidental Disclosures (Not Reportable): are unintended revelations of private data that occur during normal business activities. Staff should use prudent care and precautions to safeguard any and all personal identifying information or data. Example of reasonable precautions would include but are not limited to:

- Keeping ones voice low while discussing information
- Moving to as private a location as possible during discussions
- Covering information to prevent inadvertent viewing of information
- Securing information in a reasonable manner when not in use

B. Accidental Disclosures (Reportable): are unintended exposures of private data that occur when proper procedures are followed. Examples of accidental disclosures include but are not limited to:

- Disclosure of private data to a person who falsely identifies themselves
- A printed report, correspondence, or e-mail containing personal information was distributed in a manner not intended for widespread distribution.
- With an individual's permission, a message was left on person's voice mail; however a wrong number was dialed.

C. Intentional Disclosures (Reportable): are disclosures of private data that occur due to disregard of established policies and procedures with or without malicious intent. **All members of the workforce are obliged to report any known intentional disclosure of private data immediately.** Examples of intentional disclosures include but are not limited to:

- Gaining access to private data by deliberately circumventing security measures by using someone else's password or by other fraudulent means.
- Inappropriately disclosing private data to unauthorized persons.
- Disclosing private data with intent to harm others or to personally profit from such disclosure.
- Purposefully compiling and saving encrypted private data on portable computer or other mediums of storage or transmittal.

VII. Reporting Form and Procedures: the reporting form and procedures may be found on the University's Web site at: <http://www.salemstate.edu/8332.php>.