PROCEDURE LIT.4.02.01
DETECTING IDENTITY THEFT

SCOPE: FACULTY AND STAFF

1. Definitions

1.1. Covered Accounts – An account designated to permit multiple payments or transactions, or any other account for which there is a reasonably foreseeable risk of identity theft.

1.2. Identity Theft – Fraud committed or attempted using the identifying information of another person without authorization.

1.3. Personal Identifying Information – Any name or number that may be used, alone or in conjunction with any other information, to identify a specific person, including but not limited to:

1.3.1. Name;
1.3.2. Address;
1.3.3. Telephone number;
1.3.4. Social security number;
1.3.5. Date of birth;
1.3.6. Government issued driver's license or identification number;
1.3.7. Alien registration number;
1.3.8. Government passport number;
1.3.9. Employer or taxpayer identification number;
1.3.10. Student identification number;
1.3.11. Computer Internet Protocol address; or
1.3.12. Routing code

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

2. Identification of Red Flags

2.1. To identify relevant Red Flags, Lamar Institute of Technology (LIT) considers the types of accounts that it offers and maintains, the methods it provides to open and access covered accounts, and its previous experiences with identity theft.

2.2. The following items are considered Red Flags (risk factors):

2.2.1. Notifications and Warnings from Credit Reporting Agencies;
2.2.2. The presentation of suspicious documents, such as inconsistent photo identification or personal identifying information;
2.2.3. The presentation of suspicious personal identifying information (personal information inconsistent with other information on file);
2.2.4. Suspicious covered account activity or unusual use of account; or
2.2.5. Alerts from others

3. Detecting Red Flags

3.1. LIT personnel will verify:

3.1.1. The identification of customers requesting information about themselves or their accounts whether the request is made in person or via telephone, facsimile, or email.
3.1.2. The validity of a request to change account-related addresses or contact information.
3.1.3. The accuracy of changes in bank account information that might impact billing and payment.

4. Responding to Red Flags

4.1.1. LIT personnel will notify the Program Administrator upon identifying a red flag.
4.1.2. The Program Administrator will determine appropriate response actions. Such actions will be made to mitigate identity theft, and may include:

4.1.2.1. Monitoring a covered account for evidence of identity theft;
4.1.2.2. Contacting the customer;
4.1.2.3. Changing any passwords, security codes, or other security measures that permit access to a covered account;
4.1.2.4. Notifying law enforcement; or
4.1.2.5. Determining that no response is warranted under the particular circumstances.

4.1.3. The Program Administrator shall notify IT if the Red Flag suggests the possibility of a breach in information security
4.1.4. The Program Administrator will log all reported Red Flag detections and actions taken. This information will be included in their annual report to the President.

Related Policies: LIT.4.02

Relevant Forms/Documents:

Relevant TSUS Policies/Forms/Documents: TSUS Rules and Regulations Chapter III, 6(20)

Relevant Statutes: Code of Federal Regulations Title 16, Chapter I, Subchapter F, Part 681

Relevant SACSOC Standards:

Document History:
Adopted: March 2025
Reviewed:
Revised: