FLORIDA INTERNATIONAL UNIVERSITY

OFFICIAL UNIVERSITY POLICY

Preventing Identity Theft on Covered Accounts Offered or Maintained by Florida International University# 1110.032

INITIAL EFFECTIVE DATE:	LAST REVISION DATE:	RESPONSIBLE UNIVERSITY DIVISION/DEPARTMENT
August 1, 2009	July 18, 2023	Office of the Controller

POLICY STATEMENT

Florida International University shall develop, implement and maintain a written Identity Theft Prevention Program which is designed to detect, prevent, and mitigate identity theft in connection with the opening of a Covered Account or an existing Covered Account and to provide for continued administration of the Program.

To the extent that Florida International University employees work with, or have access to, personal identifying information contained in Covered Accounts offered or maintained by the University, such employees must familiarize themselves with, and follow, Florida International University's Identity Theft Prevention Program. Training on the specifics of this Program shall be offered by the Identify Theft Prevention Committee and overseen by the Program Administrator designated by the University President.

Outside entities and service providers that open or maintain Covered Accounts on behalf of the University shall ensure that they have in place reasonable policies and procedures designed to detect, prevent, and mitigate the risk of Identity Theft. These outside entities and service providers shall provide evidence of these reasonable policies and procedures including, as appropriate, training and education of their staff on how to effectively detect, prevent, and mitigate the risk of Identity Theft.

SCOPE

This policy applies to the University community and outside service providers that open or maintain Covered Accounts on behalf of the University.

REASON FOR POLICY

In order to comply with the Federal Trade Commission's Red Flags Rule, which implements Sections 114 and 315 of the Fair and Accurate Credit Transactions Act of 2003, the University must develop, implement and maintain a written Identity Theft Prevention Program. This Program, together with relevant University regulations, policies and procedures, shall serve to protect University students, faculty and staff from identity theft.

DEFINITIONS	
TERM	**DEFINITIONS**
Covered Account	An account maintained by the University that involves or is designed to permit multiple payments or transactions such as a student financial aid loan, short-term loan account, emergency loan account, or student or staff debit card account.
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 and student identification number.
Identity Theft	A fraud committed or attempted using the identifying information of another person without authority.
Program Administrator	The individual designated with primary responsibility for oversight of the Program. The President shall designate the University's Program Administrator.
Identity Theft Prevention Committee	The cross functional team responsible for developing, implementing, and updating the Identity Theft Prevention Program and Training. (Contact email: redflags@fiu.edu)
Red Flag	A pattern, practice, or specific activity that indicates the possible existence of Identity Theft.

ROLES AND RESPONSIBILITIES

Refer to Florida International University's Identity Theft Prevention Program.

RELATED RESOURCES

Division of Finance and Administration Policy:

- Address Validation Requirements in Connection with Covered Accounts Offered or Maintained by Florida International University

IT Security Policies:

- Gramm-Leach-Bliley Act: Safeguards to Protect Confidential Financial Information
- Information Technology Security
- Information Technology Security (SEIU)

IT Security Procedures:

- Data Stewardship
- Sharing Access to IT Resources; Password Management
- System and Application Management

University Program:
Florida International University's Identity Theft Prevention Program

https://controller.fiu.edu/wp-content/uploads/sites/24/2023/07/Identity-Theft-Prevention-Program_Final_7.7.23.pdf

CONTACTS

Office of the Controller
11200 SW 8th Street, CSC 410
Miami, FL 33199
Phone: 305-348-2161
redflags@fiu.edu

HISTORY

Initial Effective Date: New policy of the institution adopted on March 2, 2009, to be effective as of August 1, 2009.
Review Dates (*review performed, no updates*): January 4, 2024.
Revision Dates (*updates made to document*): March 31, 2023; July 18, 2023.

FLORIDA INTERNATIONAL UNIVERSITY

OFFICIAL UNIVERSITY PROCEDURE

Preventing Identity Theft on Covered Accounts Offered or Maintained by Florida International University# 1110.032b

INITIAL EFFECTIVE DATE:	LAST REVISION DATE:	RESPONSIBLE UNIVERSITY DIVISION/DEPARTMENT
August 1, 2009	July 18, 2023	Office of the Controller

PROCEDURE STATEMENT

Florida International University's Identity Theft Prevention Program is available online and may be viewed at the University's Controllers web site.

The Program shall serve to:

1. Identify relevant Red Flags for new and existing Covered Accounts and incorporate those Red Flags into the Program.
2. Detect Red Flags that have been incorporated into the Program.
3. Respond appropriately to any Red Flags that are detected to prevent and mitigate Identity Theft.
4. Ensure the Program is updated periodically to reflect changes in risks to University students and staff and to the safety and soundness of the institution from Identity Theft.

The Identity Theft Prevention Program Administrator or their designee shall present the University's Identity Theft Prevention Program to the Florida International University Board of Trustees for initial approval and shall be responsible for periodically updating the Program. The Program Administrator or their designee shall report to the Board of Trustees, or the appropriate Committee thereof, on an annual basis regarding the status of the Identity Theft Prevention Program at the institution.