FIN-031

Prevention, Detection, and Mitigation of Identity Theft

Effective Date Friday, October 22, 2010

Status Final

Last Revised Thursday, October 16, 2025

Policy Type University

Contact Office Controller (Office of the University)

Oversight Executive
Executive Vice President and Chief Operating Officer

Applies To Academic Division, Medical Center, and College at Wise.

Table of Contents

Policy Statement
1. Responsibilities
2. Compliance with Policy

Procedures

Reason for Policy

In response to the increasing nationwide incidence of identity theft, the Federal Trade Commission, along with the banking regulatory agencies, issued a so-called “Red Flags Rule” intended to protect consumers from this crime. “Red Flags” are circumstances that should cause creditors and financial institutions to suspect that identity thieves may be using the identifying information of others to commit fraud.

The University is committed to complying with federal regulations concerning the detection, prevention, and mitigation of identity theft. In accordance with the Fair and Accurate Credit Transaction Act (FACTA) of 2003 and the subsequent “Red Flags Rule” of 2007, the University is required to establish a comprehensive, coordinated, and University-wide approach for facilitating the detection, prevention, and mitigation of identity theft.

Definition of Terms

Covered Accounts

Description A consumer account or payment plan that involves multiple payments over time.

Identifying Information

Description

Any name or number that may be used, alone or in conjunction with any other information, to identify a specific person.

Identity Theft

Description A fraud committed using the identifying information of another person.

Red Flag

Description

Suspicious information or activities that suggest the possibility of identity thieves using someone else's identifying information at the University to commit fraud. Red flags fall into several categories including but not limited to:

- Suspicious documents such as altered or forged identification cards.
- Suspicious personal identifying information such as fictitious addresses or telephone numbers.
- Suspicious activity related to accounts such as mail that is repeatedly sent and returned as undeliverable.

Policy Statement

To detect and stop identity thieves from using someone else's identifying information at the University, an Identity Theft Prevention Program will be maintained. (This is distinct from data security which is covered under other University policies; see Related Information.) Identity theft is committed by using the identifying information of another person without their authority. Identifying information may include such things as a Social Security number, account number, date of birth, driver's license number, passport number, and other unique identification numbers or codes.

The Identity Theft Prevention Program describes the characteristics of identity theft and helps detect, prevent, and mitigate the effects of identity theft to protect individuals and the University from fraudulent transactions. This program coordinates, reviews, and oversees policies and procedures to:

- Identify business processes at risk of identity theft fraud.
- Detect and respond appropriately to signs of potential identity theft.
- Educate appropriate faculty, staff, and others regarding their responsibilities under the Identity Theft Prevention Program.
- Update the Identity Theft Prevention Program to appropriately respond to new or evolving risks.

The executive vice president and chief operating officer, oversight executive for the program, delegates administration of the program to the vice president and chief financial officer and the vice president and chief information officer.

1. **Responsibilities:**
   The ***assistant vice president for finance and university controller*** is responsible for:

- Administering the program, including notifying an office if it is determined they have covered accounts at risk for identity theft.
- Determining whether processes identified by offices should be included in the program.
- Training for managers and employees handling covered accounts.
- Overseeing and monitoring of the program, including review of unit-level internal controls.
- Overseeing the annual certification process through the Agency Risk Management and Internal Control Standards (ARMICS).

Offices handling covered accounts are responsible for:

- Identifying and bringing to the attention of the university controller any processes that would be at risk for such fraud.
- Implementing the Identity Theft Prevention Program for those applicable business processes.
- Assessing whether identifying information provided by individuals (i.e., students, patients, etc.) may have red flags of identity theft.
- Documenting potential identity theft fraud and report the information to the university controller.

These areas include but are not limited to:

- Student Financial Services
- General Accounting
- Medical Center
- Any departments other than the Medical Center that provide and bill for medical services
- Any departments in the College at Wise that bill for services

A complete list of offices with covered accounts and guidance information related to the Identity Theft Prevention Program is provided at the University's Red Flags Rule Program. (Of note, it has been determined that payroll deductions for University parking, Intramurals, etc., are low-risk and therefore not included in the program.)

2. **Compliance with Policy:**
   Failure to comply with the requirements of this policy may result in disciplinary action up to and including termination in accordance with relevant University policies.

   Direct questions about this policy to the Office of the University Controller.

Procedures

University's Red Flags Rule Program
Identity Theft: Don't Be a Victim
Report an Information Security Incident

Related Information

Red Flags Rule
Supporting policies include, but are not limited to:

GOV-002: Reporting and Investigation of Fraudulent Transactions
HRM-002: Issuance and Use of Physical and Mobile University ID Credentials (formerly Identification Cards)
HRM-044: Maintaining Faculty Personnel Records
IRM-003: Data Protection of University Information

IRM-004: Information Security of University Technology Resources
IRM-012: Information Security Incident Reporting
IRM-017: Records and Information Management
STU-002: Rights of Students at the University of Virginia Pursuant to the Family Educational Rights and Privacy Act
Health System Policy; Confidentiality of Patient Information
Medical Center Policy: Patient Identification
Health System Policy: Verification for Release of Patient Information
Medical Center Policy: Prevention, Detection, and Mitigation of the Theft of Patients' Identities

Major Category Finance and Business Operations

Next Scheduled Review Monday, October 16, 2028

Revision History

Updated office and position titles, references and links 10/16/25; Confirmed 9/2/25; Added Compliance section 12/16/21.

Category Cross Reference
Information Resource Management

Approved By Executive Vice President and Chief Operating Officer

Approved Date Friday, October 22, 2010