Identity Theft Prevention Program

Policy CP005
Responsible Administrator(s): Vice President for Human Resource Management and Labor Relations and Vice President for Enrollment Management and Student Success
Responsible Office(s): Human Resource Management and Labor Relations and Enrollment Management and Student Success
Issue Date: June 2009
Last Updated: August 2019

Policy Statement

It is the policy of the Fashion Institute of Technology (the "college") to comply with the requirements of the Federal Trade Commission's Red Flags Rule, which was promulgated pursuant to section 114 of the Fair and Accurate Credit Transactions Act ("FACTA"). The Red Flags Rule requires financial institutions and creditors that hold covered accounts to develop and implement an Identity Theft prevention program for new and existing covered accounts. Under this rule, colleges and universities are considered creditors engaged in lending activities and deferred payment practices commonly associated with banks, finance companies, automobile dealers, mortgage brokers, utility companies, and telecommunication companies.

This policy sets forth the actions which must be taken by the college and by certain supervisors and administrators in order to identify, detect, report, and mitigate incidents of Identity Theft in connection with new and existing covered accounts, which are used primarily for personal purposes and involve multiple financial transactions, or for which there is reasonable foreseeable risk from Identity Theft.

Reason for the Policy

This policy attempts to reduce potential Identity Theft risks to the college and its community through an Identity Theft Prevention program designed to help identify, detect, and respond to patterns, practices, or specific activities known as "red flags" that could indicate Identity Theft in connection with the opening of a covered account or an existing covered account.

The program sets forth the actions which must be taken by the college through certain members of its staff, managers and administrators in order to prevent the use of personal identifying information to commit Identity Theft. The program also demonstrates the college's commitment to the security of personal identifying information collected and managed by the college.

Who is Responsible for this Policy

- Identity Theft Prevention Program Administrators
- Identity Theft Prevention Program Managers
- Identity Theft Prevention Committee

Who is Affected by this Policy

- All college employees who access, use or control personal identifying information in connection with a covered account

Policy Text

FIT acknowledges the importance of its responsibilities and all reports of Identity Theft will be investigated and acted upon, up to and including the involvement of law enforcement agencies, when required. The college has established an Identity Theft Prevention Program and an Identity Theft Prevention Committee in order to meet these responsibilities. Training shall also be offered to certain managers and administrators of the college to ensure they learn to identify, detect, prevent, and mitigate potential Identity Theft risks.

Definitions

- **Identity Theft:** A "fraud committed or attempted using the identifying information of another person without authority."

- A **Red Flag:** A "pattern, practice, or specific activity that indicates the possible existence of Identity Theft."

- A **Covered Account:** An account the college offers or maintains that permits multiple transactions or poses a reasonably foreseeable risk of being used to promote an Identity Theft. Such an account may be identified as potentially posing a reasonably foreseeable risk of Identity Theft to students, patients, employees and other relevant third parties, including financial, operational, compliance, reputation, or litigation risks. For purposes of this program, this may include, but are not limited to:
    - Certain student accounts or loans administered by the college or by third parties hired by the college to administer such accounts;
    - Accounts established to register patients at Health Services;
    - Certain tenant accounts;
    - Certain faculty accounts or loans; and
    - Certain potential employee information.

- **Program Administrator(s):** The individual(s) designated with primary responsibility for oversight of the Program and the Identity Theft Prevention Committee. After the initial Program Administrator, the subsequent Program Managers shall be designated by the Identity Theft Committee.

- **Personally Identifiable Information ("PII"):** "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: 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, student identification number, computer's Internet Protocol address, or routing code.

Principles

The Identity Theft Prevention Program encompasses procedures designed to:

- Identify common red flags or patterns, practices, and specific activities that could indicate the possible existence of Identity Theft;
- Detect red flags associated with opening a new covered account or with an existing covered account at the college;
- Establish protocols for reporting red flags to prevent and mitigate Identity Theft; and
- Ensure that the program is updated periodically to reflect such changes in risks, as additions or removal of types of covered accounts, changes in Identity Theft detection and prevention methods, changes or updates in law or regulations, or the emergence of new types of risk.
- Train college employees who access, use or control personal identifying information in connection with a covered account in the detection of red flags and the responsive steps to be taken when a red flag is detected.

Responsibilities

- **Identity Theft Prevention Program Administrators**:
  The following individuals are designated as Identity Theft Prevention Program Administrators under this policy:
  - **Vice President of Enrollment Management and Student Success or their designee**
  - **Vice President of Human Resource Management and Labor Relations or their designee**

  These individual(s) hold primary responsibility for administration and oversight of the Program, including the identification of Program Managers. They or their designee(s) are also responsible for ensuring the appropriate training of the program for college staff with administrative responsibilities over the Covered Accounts.

- **Identity Theft Prevention Managers:**
  The following individuals are designated as Identity Theft Prevention Managers under this policy:
  - **Director of Records and Registration or their designee**
  - **Director of Human Resources Information Technology or their designee**

  These individuals or their designee(s) are responsible for identifying employees, including new employees, who handle personally identifiable information in connection with Covered Accounts. Program Managers are also responsible for reporting to the Program Administrator(s) any Red Flags reported by these employees, as well as updating and administering appropriate training related to Red Flag detection.

  These individuals lead the Identity Theft Prevention Committee and maintain all relevant findings and reports investigated by the committee. Retention and disposition of these records should follow guidelines pursuant to the college's policy on Records Retention and Disposition.

- **Identity Theft Prevention Committee**:
  This Committee is led by the Identity Theft Prevention Managers and is comprised of senior officers, or their designees, from the following areas under this policy, as appointed by :
  - Division of Finance and Administration

- Division of Information Technology
- Office of Admissions
- Office of the Bursar
- Office of Financial Aid
- Office of Human Resources Management and Labor Relations
- Office of the Registrar
- Office of International Programs
- Office of Policy and Compliance

This committee is responsible for considering periodic changes to the program, and for reviewing, documenting, and maintaining any reports regarding the detection of Red Flags. They must complete FACTA Red Flags training as assigned.

Procedures

- **Reporting a Red Flag**
  As soon as a Red Flag is identified, an employee must inform the appropriate Identity Theft Prevention Manager as soon as possible. The Identity Theft Prevention Manager will conduct any necessary inquiries to determine the validity of the Red Flag. If it is determined that Identity Theft has occurred, the Identity Theft Prevention Manager will immediately notify the Identity Theft Prevention Program Administrators.
    - **For suspected Red Flags related to student PII**: Director of Records and Registration
    - **For suspected Red Flags related to employee PII:** Director of Human Resources Information Technology

- **Red Flag Response**
  Appropriate actions will be dependent on the type of Red Flag identified, type of transaction, relationship with the victim of the fraud, availability of contact information for the victim of the fraud, and numerous other factors. A senior representative of the college involved in responding to the incident will also seek advice of counsel regarding the duty to provide notice and any other related legal obligations.

  In all situations where it is determined a Red Flag has been positively identified, the appropriate Program Manager, in collaboration with the department head responsible for the account, will document what occurred, describe the matter and any specific actions taken to mitigate the impact of the effect of the actual or potential Identity Theft discovered, and consult with the Office of Internal Controls and Management Analysis on the actions taken. The documentation will also include a description of any additional actions the department believes are systemically necessary (such as updating policies and procedures) in response to the identified Red Flag to handle or prevent similar situations in the future.

- **Staff Training**
  College employees who process any information related to a covered account will be trained in the detection of red flags and the responsive steps to be taken when a red flag is detected. The program administrator shall exercise discretion in determining the training necessary. In addition, to ensure maximum effectiveness, refresher training may be provided annually.

- **Oversight of Service Providers**
  The college remains responsible for compliance with the Red Flags Rule even if it outsources operations to a third party service provider. In the event that the college engages a service provider to perform an activity in connection with one or more covered accounts, the program administrator shall consult with the Office of General Counsel to review such arrangements in order to ensure that the activities of the service provider are conducted in accordance with reasonable policies and procedures designed to detect, prevent and mitigate the risk of Identity Theft.

Violations

Under the FACTA Red Flag Rules, the federal government is empowered to impose civil penalties of up to $2,500 per violation, and it is possible each violation could be assessed against each Covered Account maintained by the college.

Inappropriate use or misuse of student or employee PII is a violation of college policy as well as state and federal laws. Any knowledge of a violation of this policy, or of misuse of student or employee PII must immediately be reported to the appropriate Identity Theft Prevention Manager.
Employees who are found in violation of this policy may be subject to discipline, up to and including termination. For Bargaining Unit employees, any disciplinary action will be held in accordance with the Collective Bargaining Agreement.

Related Policies

- Acceptable Use for FIT IT Systems
- FERPA
- FIT Campus Card and Campus Access
- Records Retention and Disposition

Related Documents

- Federal Trade Commissioner’s (FTC’s) Red Flags Rule
- NYS Attorney General
- Identity Theft Resource Center
- NYS Office of Cyber Security

Contacts

- **Director of Records and Registration**
  Office of the Registrar
  227 27th Street, Feldman Center, C158
  New York, NY 10001
  (212) 217-3820

- **Office of Human Resources Management and Labor Relations**
  333 7th Ave, 16th Floor
  New York, NY 10001
  (212) 217-3650
  Humanresources1@fitnyc.edu