To submit a comment on this draft policy please click here

University of Pittsburgh
Identity Theft (Red Flags)
Policy TBD

Implementing Executive: Executive Senior Vice Chancellor for Finance and Administration, Chief Financial Officer
Responsible Unit: Office of Compliance, Investigations, and Ethics
Category: Financial Policies
Effective Date: TBD

I. Purpose

The University recognizes the responsibility it has to comply with the Federal Trade Commission's (FTC's) Red Flags Rule promulgated pursuant to the Fair and Accurate Credit Transactions Act (FACTA). This Policy is enacted to meet the Red Flags Rule requirement that financial institutions and creditors adopt policies and procedures that protect customers from identity theft.

II. Scope

This Policy applies to University units that maintain and provide access to Covered Accounts (defined below).

III. Definitions

A. Covered Account – as defined by the FACTA, is: (i) an account that the University offers or maintains, primarily for personal, family, or household purposes, which involves or is designed to permit multiple payments or transactions; or (ii) any other account that 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, including financial, operational, compliance, reputation, or legal risks.

B. Identity Theft – as defined by the FACTA, is a fraud committed or attempted using the identifying information of another person without authority.

C. 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: name, address, telephone number, social security number, date of birth, driver's license or identification number, alien registration number, passport number, financial account information, employer or taxpayer identification number.

IV. Policy

It is the policy of the University of Pittsburgh to comply with the requirements of the FTC's Red Flags Rule. That Rule requires the University to implement identity theft protection programs to prevent the fraudulent use (or attempted use) of another person's Identifying Information. Furthermore, as a creditor that protects customer information, the University must take steps to reduce risk from identity fraud and minimize potential damage from fraudulent new accounts. These steps include the development and implementation of an Identify Theft Prevention Program (ITPP), which is designed to detect, prevent, and mitigate identity theft in connection with the opening of a Covered Account or the operation of any existing Covered Accounts with the University.

This Policy authorizes the Office of Compliance, Investigations, and Ethics (CIE) to implement and manage this Program. Departments maintaining or providing access to Covered Accounts must follow the ITPP, including developing supporting procedures that document the department's processes for identifying, responding to, and reporting Red Flags, which is a pattern, practice, or specific activity that indicates the possible existence of identity theft.

The ITPP is tailored to the University's size, complexity, and nature of its operations and must include the following:

- reporting obligations, including the use of Pitt Concern Connection for reporting suspected identity theft;
- identification of Departments that have Covered Accounts;
- descriptions of common Red Flags that departments can include in their procedures;
- timing and nature of reporting of Red Flags by departments;
- training on identifying and reporting Red Flags, which could include:
    - notices of address discrepancy from credit reporting agencies;
    - presentation of incomplete, altered, or forged documents;
    - incorrect answers to challenge questions;
    - receipt of fraud alert or notification of unauthorized activity in a Covered Account; or
    - any other Red Flag indicator identified by units for their specific Covered Accounts; and
- process by which the University validates that agreements with a person or entity that provides a service directly to the University (service providers) include an identity theft prevention program.

CIE is authorized to update the ITPP periodically to reflect changes in identity theft risks, subject to review and approval by the Senior Vice Chancellor and Chief Legal Officer and the Executive Senior Vice Chancellor for Administration and Finance and Chief Financial Officer.

V. Noncompliance

Units must comply with this Policy, and noncompliance may lead to sanctions through procedures stipulated by the ITPP, in the Faculty or Staff Handbook, or the Student Code of Conduct, as applicable.

VI. Contact Information and Public Accessibility

This Policy is posted under Financial Policies on the Office of Policy Development & Management's website and can be found at: https://www.policy.pitt.edu.

For specific questions related to this Policy, please contact CIE

VII. Related Authorities and Policies

University Policy AO 24, Name and Address Lists and Mailing Labels
University Policy AO 35, University Administrative Computer Data Security and Privacy
University Policy CS 23, Use and Management of Social Security Numbers and University Primary IS ("UPI")
University Policy AO 36 – University Identification Cards
University Policy CS 30 – Health Insurance Portability and Accountability Act (HIPAA)
University Policy FN 13 – Level Report Review and Reconciliation
University Policy FN 16 – Payment Card Handling and Acceptance
University Policy FN 20 – Procurement Card
University Policy FN 26 – Travel Card