


| | | |
|---|--|---|
|  <p>Category: Administration</p> <p>Policy applicable for: FACTA Covered Units</p> | <p><i>Policy Title:</i> FACTA Red Flag Policy</p> <p>Effective Date: 06/10/2010</p> <p>Prior Effective Date: N/A</p> <p>Enabling Acts: ISO 17799:2005, COBIT, NIST SP 800-xx University Board Recommendation 10.06.22.08</p> | <p><i>Policy Number:</i> 1.8.6</p> <p>Policy Owner: Senior VP for Administration Finance and Senior VP for Academic Affairs & Provost</p> <p>Responsible Office(s): UC Covered Units UCIT Office of Information Security</p> |
|---|--|---|

Background

In an effort to protect consumers from ever expanding incidence of identity theft the Fair and Accurate Credit Transactions Act (FACTA) was enacted in 2003 followed by the Federal Trade Commission (FTC), in conjunction with other financial regulatory agencies, publishing 16 CFR §681.2, the Red Flags Rule. Red Flags are described as suspicious information or activities that suggest the possibility of identity thieves using someone else's Personal Identifying Information (PII) to commit fraud. The university is responsible for managing and developing an Identity Theft Prevention Program that detects, prevents and mitigates identity theft. The program is designed to:

- Identify Red Flags associated with new or existing covered accounts;
- Respond appropriately to the detection of Red Flags to prevent and mitigate identity theft;
- Properly incorporate detected Red Flags;
- Ensure proper maintenance and effective use of the program by implementing periodic program review.

The FTC is authorized to commence action in federal district court in the event of a knowing violation of FACTA, with civil penalties up to \$2,500 for each violation.

Policy

To detect and prevent identity theft at the university, an Identity Theft Prevention Program has been developed. Identity theft is the unauthorized use of another individual's Personal Identifying Information (PII). PII may include Social Security number, account number, date of birth, driver's license number, passport number, and other unique identification numbers or code.

The Identity Theft Prevention Program outlines identity theft characteristics and offers processes for detection, prevention and mitigation of identity theft in order to protect the university community from fraudulent and illicit financial activity. The program provides a framework that aids in identifying business processes vulnerable to identity theft and

fraud, aid in detection and response to signs of potential identity theft, and detail appropriate training for faculty and staff regarding their responsibilities in relation to the Identity Theft Prevention Program.

The core designated FACTA covered units that are subject to the policy and FACTA Red Flag Identity Theft Prevention Program include:

1. Public Safety
2. UCIT Information Security
3. UCIT Integration Services
4. Human Resources
5. Office of the Bursar
6. Student Financial Aid
7. Campus Services
8. University Health Services

Additionally, other departments may be required to comply with FACTA and associated changes in the law, or that are necessary for the orderly operation of the university as determined in writing by the Senior Vice President for Administration and Finance and Senior Vice President for Academic Affairs and Provost.

Departments must be vigilant to ensure personnel are trained on and follow compliance and reporting requirements identified in FACTA. Breaches in personally identifiable information must be reported to UC Public Safety and UCit Office of Information Security within 24 hours of the suspected or known breach.

Definitions

Covered accounts: a consumer account or payment plan that involves multiple payments over time.

Personally Identifiable Information (PII) / Identifying Information: any name or number that may be used, alone or in conjunction with any other information, to identify a specific person.

Identity Theft: fraudulently using the identifying information of another person.

Red Flag: suspicious information or a pattern, practice, or activity that suggests the possibility of identity theft; the use of another individual's identity to commit fraud.

Procedure

See University of Cincinnati FACTA Red Flag Identity Theft Prevention Program Document (see *Related Links*).

Related links

[Presentation – Understanding Red Flag Regulations and Ensuring Compliance](#)

Human Resources
Office of the Bursar
Public Safety
Student Financial Aid
UC FACTA Red Flag Identity Theft Prevention Program Document
UCIT Information Security

Phone Contacts:

| | |
|-------------------------------------|---------------------|
| UC Public Safety | 513-556-1111 |
| UCIT Office of Information Security | 513-558-ISEC (4732) |
| Director, Information Security | 513-556-9177 |
| UC Office of the CIO | 513-556-2228 |