University of Cincinnati
FACTA "Red Flag" Identity Theft Prevention Program

Contents

University of Cincinnati

FACTA "Red Flag" Identity Theft Prevention Program

Overview:

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 suggests the possibility of identity thieves using someone else's Personal Identifying Information (PII) to commit fraud. The University is responsible for 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.

Definition of Terms:

Covered accounts: a consumer account or payment plan that involves multiple payments over time. These groups would include, but may not be limited to, Bursar and Financial Aid, Human Resources, and Campus Services.

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.

Covered Accounts

University units are subject to this program if the unit conducts any of the following activities:

1. The unit provides goods or services and payment is directed to an established University account;
2. The unit has management and/or oversight responsibility for a University-established account;
3. The unit provides loans to students or other customer groups.

Questions regarding whether your area is subject to the program should be directed to OGC at (513) 556-3483 or IT Security.

List of Red Flags:

Red Flags indicate the possibility of identity thieves using someone else's personal identifying information. In an effort to stop or mitigate such activity at the University, all faculty, staff members, or students with responsibility for covered accounts or transactions that are posted to covered accounts should be familiar with the red flags. The following are common examples of

Red Flags. Of the examples listed some may apply to a given department and their processing procedures, others may not. Other Red Flags may exist that are not currently covered and individuals and supervisors are requested to help identify these potential Red Flags and incorporate such items into the overall procedural detection documentation.

Suspicious Documents:

- Identification document or card that appears to be forged, altered or inauthentic;
- Identification document or card on which a student or patient's photograph or physical description is not consistent with the person presenting the document;

Suspicious Personal Identifying Information

- Identifying information presented that is inconsistent with other information the student or patient provides (for example, inconsistent birth dates);
- Identifying information presented that is inconsistent with other sources of information (for instance, an address on identification not matching an address in the student system);
- Identifying information presented that matches information shown on other applications that were found to be fraudulent;
- Identifying information presented that is consistent with fraudulent activity (such as an invalid phone number or fictitious billing address);
- Social security number presented that is the same as one given by another student or patient;
- An address or phone number presented that is the same as that of another student or patient;
- A student or patient fails to provide complete personal identifying information on an application when reminded to do so (however, by law social security numbers must not be required);
- A student or patient's identifying information is not consistent with the information that is on file for the customer; and
- A student or patient who has an insurance number but never produces an insurance card or other physical documentation of insurance.

Account Oversight - Notifications and Warnings from Credit Reporting Agencies

- A Credit Report with appended Fraud Report;
- A Credit Agency Notice or Report of a credit freeze on a customer or applicant;
- A Credit Agency Notice or Report of an active duty alert for an applicant; and
- Indication from a credit report of activity that is inconsistent with a customer's usual pattern or activity.

Suspicious Account Activity or Unusual Use of Account

- A complaint or question from a student or patient based on the person's receipt of:
    1. a bill for another individual;
    2. a bill for a product or service that the student or patient denies receiving;
    3. a bill from a higher education institution or health care provider that the student or patient never patronized;
    4. a notice of insurance benefits (or Explanation of Benefits) for services never received.

- Change of address for an account followed by a request to change the account holder's name;
- Payments stop on an otherwise consistently up-to-date account;
- Account used in a way that is not consistent with prior use (for example, very high activity);
- Mail sent to the account holder is repeatedly returned as undeliverable;
- Notice to the University that a customer is not receiving mail sent by the University;
- Breach in the University's computer system security;
- Notice to the University that an account has unauthorized activity;
- Unauthorized access to or use of student account information; and
- A notice or inquiry from an insurance fraud investigator for a private insurance company or a law enforcement agency.

Alerts from Others

- Notice to the University from a customer, identity theft victim, law enforcement or other person that it has opened or is maintaining a fraudulent account for a person engaged in Identity Theft.

Red Flag Detection, Prevention and Mitigation of Identity Theft:

- Proper Identification (current photo identification, name, address, date of birth) shall be provided, when applicable, by the student, patient, individual or account holder when:
    - Opening a covered account;
    - Allowing access to established covered account;
    - Issuing new or replacement ID card(s);
- Account holders shall receive notification of changes to their covered accounts made online as a method of confirmation of such changes and instructions regarding invalid changes;
- Department verification of suspicious changes made to covered accounts that relate to account holder identity, administration of account, and billing and payment information;
- Upon detection of a Red Flag, proper prevention/mitigation response including:
    - Analysis of Red Flag to determine vulnerability and/or criticality of incident;
    - Notify unit head / Office of Information Security;
    - If required, close existing covered account;
    - Decline to open a new covered account;
- Proper monitoring of a Red Flagged account for additional suspicious activity;
- Proper maintenance of accounts with attention to password policy and security processes;
- Reopen compromised account with new account number;

Training:

The University/Department provides required Red Flag Rule training. Required annual training applies to:

- Any individual managing a unit or department with covered accounts or one that provides loans. (Training Coming Soon); and/or

- Staff Training, any individual handling transactions for covered accounts, will be the responsibility of the Department Supervisors.

Annual Certification of Compliance by Unit/Department
Compliance with the Red Flag Rule program will be certified on an annual basis. Responsible officials for the covered units will certify compliance via reports to the University Compliance Committee.

Program Administration:

- Approval and Oversight:
  According to Board Rule titled Establishment of a Financial Red Flag Program (10.06.22.08), Sr. Vice President for Administration & Finance is responsible for oversight.
- Program Assessment and Update:
  The University's Identity Theft Prevention Program shall be reviewed annually or at a time that a risk assessment determines the need for review of the program as a whole or an individual element.
- Reporting: University departments responsible for the development, implementation and administration of the Program should supply a compliance report to the Compliance Committee annually.
  Program efficiency regarding identity theft deterrence and mitigation associated with new or existing covered accounts, handling of instances of identity theft, service provider arrangements and recommendations for program improvements should be addressed.
- Staff Training: University departments responsible for the development, implementation and administration of the Program will provide effective training of staff to promote detection, prevention and mitigation of identity theft. Red Flags training should be tailored to the processes and responsibilities relating to a given department and is to be conducted on an annual review basis.
- Oversight of Service Providers: If and when the University engages a service provider to perform an activity in connection with a covered account, University departments delegated responsibility for administering this Program with respect to that particular covered account, should take steps necessary to ensure that the activity of the service provider is conducted in accordance with reasonable policies and procedures designed to detect, prevent, and mitigate the risk of identity theft.