Ohio Administrative Code

Rule 3337-48-01 Identity theft prevention (red flag rules).

Effective: May 17, 2019

The version of this rule that includes live linksto associated resources is online at https://www.ohio.edu/policy/48-001

(A) Overview

The red flags rule was issued in 2007 under Section 114 of the Fair and Accurate Credit Transactions Act (FACTA) of 2003 and published at 16 CFR 681.1. The red flags rule was established to protect consumers from the incidence of identity theft. The purpose of this policy is to assist employees in identifying, detecting and responding to patterns, practices and/or specific activities known as red flags that could indicate identify theft.

(B) Definitions

(1) Covered account: Includes all student, patient, and employee accounts or loans that are administered by Ohio University.

(a) Any account that involves or is designated to permit multiple payments or transactions; or

(b) Any other account maintained by the university for which there is a reasonably foreseeable risk of identity theft to students, faculty, staff, customers or other applicable constituents, or for which there is a reasonably foreseeable risk to the safety or soundness of the university from identity theft, including financial, operational, compliance, reputation or litigation risks.

(2) 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, government issued drivers license or identification number, alien registration number, government passport number, employer or taxpayer identification number, student identification number, computer internet protocol address or routing

code, credit card number or other credit card information.

(3) Red flag: A pattern, practice or specific activity that indicates the possible existence of identity theft.

(4) Identity theft: A fraud committed or attempted using the identifying information of another person without authority.

(5) Service provider: A person or entity that performs an activity in connection with a covered account on behalf of the university (examples: collection agencies, billing servicers).

(C) Covered account

(1) Covered accounts maintained by Ohio university include, but are not limited to, the following:

(a) Student loans (including Perkins loans and institutional loans)

(b) Student accounts (including bobcat cash)

(c) Patient/client accounts (including well works, clinics, etc.)

(D) Identification and detection of red flags

(1) Ohio universitys identity theft prevention program addresses the detection of red flags in connection with the opening of covered accounts and existing covered accounts, such as by:

(a) Obtaining identifying information about, and verifying the identity of a person. For example, requiring persons to show a valid photo ID or other proof of identity for any person conducting business with the university when opening a covered account and with existing accounts.

(b) Authenticating customers, monitoring transactions, and verifying the validity of change of address requests in the case of existing accounts.

(2) The following examples of red flags are potential indicators of fraud or identity theft. The risk factors for identifying relevant red flags include the types of covered accounts offered or maintained; the methods provided to open or access covered accounts; and, previous experience with identity theft. Any time a red flag or a situation closely resembling a red flag is apparent, it must be investigated for verification. Some examples are:

(a) Alerts, notifications or warnings from a credit or consumer reporting agency.

(b) Suspicious documents.

(c) Suspicious personal identifying information.

(d) Unusual use of, or suspicious activity related to, the covered account.

(E) Responding to red flags

Once a red flag or potential red flag is detected, the employee must act quickly with consideration of the risk posed by the red flag. The employee detecting the red flag must gather all related documentation, write a description of the situation and present this information to the program administrator for determination. The program administrator will complete additional authentication to determine whether the attempted transaction was fraudulent or authentic.

(F) Protecting personal information

Employees designated by the program administrator must review on an annual basis the university's red flag program. University personnel are also encouraged to use good judgment in securing covered account information. Furthermore, designated employees must review policy 12.020 student records, policy 93.001 data classification, policy 40.007 public records requests, and other applicable laws and policies. If an employee is uncertain of the sensitivity of a particular piece of information, he/she must contact his/her supervisor. If the supervisor is uncertain, they must contact the program administrator for further advice.

(G) Program administration

Operational responsibility of the program at the university is delegated to a program administrator. The duties of the program administrator are oversight, development, implementation and administration of the program; approval and implementation of needed changes to the program; and staff training. The program administrator is also responsible for ensuring that appropriate steps are taken for preventing and mitigating identity theft, for reviewing any staff reports regarding the detection of red flags, and for determining which steps must be taken in particular circumstances when red flags are suspected or detected.

(H) Staff training

Staff training must be conducted for all employees who may come into contact with covered accounts or identifying information, as determined by the program administrator. The program administrator must retain training records for all designated employees showing that all designated employees have received annual training.

(I) Periodic updates to the program

(1) The program will be re-evaluated annually to determine whether the program addresses currently relevant and emerging risks for identity theft. Consideration will be given to the university's experiences with identity theft situations; changes in identity theft methods, detection methods or prevention methods; and, changes in the universitys business arrangements with other entities.

(2) Periodic reviews will include an assessment of which accounts are covered by the program. As part of the review, red flags may be revised, replaced or eliminated. Defining new red flags may also be appropriate. Actions to take in the event that fraudulent activity is suspected or discovered may also require revision to the program.

(J) Overview of service provider arrangements

It is the responsibility of the university to ensure that the activities of all service providers are conducted in accordance with reasonable policies and procedures designated to detect, prevent, and mitigate the risk of identity theft. In the event the university engages a service provider to perform

an activity in connection with one or more covered accounts, the university will take steps to ensure the service provider performs its activity in accordance with reasonable policies and procedures designed to detect, prevent and mitigate the risk of identity theft.

The version of this rule that includes live links to associated resources is online at https://www.ohio.edu/policy/48-001