BGSU
BOWLING GREEN STATE UNIVERSITY

3341-6-56 Theft Prevention Policy (Red Flag Rules).

Applicability	All University units
Responsible Unit	The Vice President for Finance and Administration and Chief Financial Officer
Policy Administrator	Bursar's Office, Information Technology Services

(A) Policy Statement and Purpose

Bowling Green State University has developed an identity theft prevention program pursuant to the Federal Trade Commission's (FTC) Red Flag Rules, found at 16 CFR § 681.2, which implements Section 114 of the Fair and Accurate Credit Transactions Act (FACTA) of 2003. The university's program is designed to detect, prevent and mitigate identify theft in connection with the opening of a covered account or any existing covered accounts within the university, and is appropriate to the size and complexity of the university as a creditor and the nature and scope of its activities.

The Red Flag Rules require a creditor to periodically determine, by conducting a risk assessment, whether it offers or maintains covered accounts. The university adopts this identity theft prevention program to detect, prevent, and mitigate identity theft in connection with the opening of a "covered account" or any existing "covered account," and to provide for continued administration of the program. Upon identifying any covered account(s), the creditor is required to develop and implement a written Identity Theft Prevention Program designed to:

(1) Identify patterns, practices, or specific activities ("red flags") that indicate the possible existence of identity theft with regard to new or existing covered accounts;

(2) Detect red flags that have been incorporated into the program;

(3) Respond appropriately to any red flags that are detected under the program;

(4) Ensure periodic updating of the program, including reviewing the accounts that are covered and the identified red flags that are part of the program; and

(5) Promote compliance with state and federal laws and regulations regarding identity theft protection.

(B) Policy Definitions

(1) "Identity theft" refers to fraud committed or attempted using the identifying information of another person without authority.

(2) "Account" refers to a continuing relationship established by a person with a creditor to obtain a product or service for personal, family, household or business purposes. It includes

(a) an extension of credit, such as the purchase of property or services involving a deferred payment, and

(b) a deposit account.

(3) "Covered account" refers to

(a) an account that a creditor offers or maintains, primarily for personal, family, or household purposes, that involves or is designed to permit multiple payments or transactions and

(b) any other account that the creditor offers to maintain for which there is a reasonably foreseeable risk to customers or to the safety and soundness of the creditor from identity theft, including financial, operational, compliance, reputation, or litigation risks.

(4) "Red flag" refers to a pattern, practice or specific activity that indicates the possible existence of identity theft.

(5) "Identifying information" refers to any name that may be used, alone or in conjunction with any other information, to identify a specific person.

(6) "Service Provider" refers to a person that provides a service directly to the financial institution or creditor.

(C) Policy

(1) The Controller's office will identify and inventory all covered accounts and service providers to be included in the Red Flags Program.

(2) BGSU will identify relevant red flags based on the criteria listed below and will include them in the Red Flags Program for training and awareness.

(a) Types of covered accounts offered and maintained

(b) Methods provided for opening and accessing each of those accounts

(c) Prior experiences with Identity Theft

(d) Size, complexity, nature and scope of our institution and its activities.

(3) BGSU will implement processes and procedures to validate identities of covered account owner prior to opening a new account or allowing access to an existing covered account.

(4) Upon detection of possible Identity Theft of a BGSU covered account, university personnel involved in the administration of the covered accounts will take appropriate steps to investigate, prevent, mitigate and/or resolve occurrences of Identity Theft.

(5) University departments, delegated responsibility for the development, implementation and administration of this Program with respect to specific covered accounts, should develop and implement plans to effectively train their staff in the identification, detection, prevention and mitigation of the Red Flags identified

above that are unique to their specific covered accounts. Staff training should be conducted on a regular basis and as necessary under the circumstances related to the administration of the particular covered account.

(D) Oversight of the Program

Successful implementation of the Identity Theft Program ultimately is the responsibility of each office, the employees of each office that maintains accounts or databases covered by the Program, and the university community as a whole. As permitted by the Red Flags Rule regulations, responsibility for overseeing the administration of the Program has been delegated by the Board of Trustees to the Vice President for Finance and Administration and Chief Financial Officer of the university.

The program administrator will be responsible for day-to-day administration, ensuring appropriate training of university staff on the program, reviewing any staff reports regarding the detection of red flags and the steps for preventing and mitigating identity theft, determining which steps of prevention and mitigation should be taken in particular circumstances, and considering periodic changes to the program.

(E) Oversight of Service Provider Arrangements

The university shall take steps to ensure that the activity of a service provider is conducted in accordance with reasonable policies and procedures designed to detect, prevent and mitigate the risk of identity theft whenever the organization engages a service provider to perform an activity in connection with one or more covered accounts. The university will require, by contract, that service providers have such policies and procedures in place and report any red flags to the program administrator.

(F) Approval by the Board of Trustees

Under the Red Flags Regulations, implementation and oversight of the Identify Theft Program is the responsibility of the governing body or an appropriate committee of such governing body. Approval of the initial plan must be appropriately documented and maintained. After its initial approval of the Program, however, the governing body may delegate its responsibility to implement and oversee the Identify Theft Program. As the governing body of Bowling Green State University, the Board of

Trustees, through is Audit Committee, as of the date below, hereby approved the initial Identity Theft Program. Having made such initial approval, the Board of Trustees hereby delegates the responsibility for implementing, monitoring, and overseeing the university's Identity Theft Program to the Vice President for Finance and Administration and Chief Financial Officer.

Registered Date: May 10, 2017