Identity Theft Red Flag Prevention Policy

1.0 Overview

This Red Flag Identity Theft Program ("Program") is promulgated pursuant to the Federal Trade Commission (FTC) regulation known as the Red Flag Rule ("Rule") (Sections 114 and 315 of the Fair and Accurate Credit Transactions Act), that is intended to reduce the risk of identity theft.

The purpose of this policy is to establish an Identity Theft Prevention Program to detect, prevent, and mitigate identity theft in connection with the opening of a covered account or an existing covered account and to provide for continued administration of the Program. The Program shall include reasonable policies and procedures to:

1. Identify relevant red flags for covered accounts it offers or maintains and incorporate those red flags into the program
2. Detect red flags that have been incorporated into the Program
3. Respond appropriately to any red flags that are detected to prevent and mitigate identity theft
4. Ensure the Program is updated periodically to reflect changes in risks to customers and to the safety and soundness of the creditor from identity theft

The program shall, as appropriate, incorporate existing policies and procedures that control reasonably foreseeable risks.

2.0 Policy

IDENTIFICATION OF RED FLAGS

In order to identify relevant Red Flags, the University considers the types of accounts that it offers and maintains, the methods it provides to open its accounts, and the methods it provides to access its accounts. The University identifies the following red flags, in each of the listed categories:

A. Notifications and Warnings from Credit Reporting Agencies

Red Flags

1. A fraud alert included with a credit report

2. Notice or report from a credit agency of a credit freeze on a customer or applicant
3. Notice or report from a credit agency of an active duty alert for an applicant
4. Indication from a credit report of activity that is inconsistent with a customer's usual pattern or activity

B. Suspicious Documents

Red Flags

1. Identification document or card that appears to be forged, altered or inauthentic
2. Identification document or card on which a person's photograph or physical description is not consistent with the person presenting the document
3. Other document with information that is not consistent with existing customer information (such as if a person's signature on a check appears forged)
4. Application for service that appears to have been altered or forged

C. Suspicious Personal Identifying Information

Red Flags

1. Identifying information presented that is inconsistent with other information the customer provides (example: inconsistent birth dates)
2. Identifying information presented that is inconsistent with other sources of information (for instance, an address not matching an address on a credit report)
3. Identifying information presented that is the same as information shown on other applications that were found to be fraudulent
4. Identifying information presented that is consistent with fraudulent activity (such as an invalid phone number or fictitious billing address)
5. Social security number presented that is the same as one given by another customer
6. An address or phone number presented that is the same as that of another person
7. A person 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)
8. A person's identifying information is not consistent with the information that is on file for the customer

D. Suspicious Account Activity or Unusual Use of Account

Red Flags

1. Change of address for an account followed by a request to change the account holder's name
2. Payments stop on an otherwise consistently up-to-date account
3. Account used in a way that is not consistent with prior use (example: very high activity)
4. Mail sent to the account holder is repeatedly returned as undeliverable
5. Notice to the University that a customer is not receiving mail sent by the University
6. Notice to the University that an account has unauthorized activity
7. Breach in the University ’s computer system security
8. Unauthorized access to or use of customer account information

DETECTING RED FLAGS

A. New Accounts

In order to detect any of the Red Flags identified above associated with the opening of a new account, University personnel will take the following steps to obtain and verify the identity of the person opening the account:

Detect

1. Require certain identifying information such as name, date of birth, residential or business address, principal place of business for an entity, driver's license or other identification
2. Verify the customer's identity (for instance, review a driver's license or other identification card)
3. Review documentation showing the existence of a business entity; and
4. Independently contact the customer

B. Existing Accounts

In order to detect any of the Red Flags identified above for an existing account, University personnel will take the following steps to monitor transactions with an account:

Detect

1. Verify the identification of customers if they request information (in person, via telephone, via facsimile, via email)
2. Verify the validity of requests to change billing addresses
3. Verify changes in banking information given for billing and payment purposes

PREVENTING AND MITIGATING IDENTITY THEFT

In the event University personnel detect any identified Red Flags, such personnel shall take one or more of the following steps, depending on the degree of risk posed by the Red Flag:

A. Prevent and Mitigate

1. Continue to monitor an account for evidence of Identity Theft
2. Contact the customer
3. Change any passwords or other security devices that permit access to accounts;
4. Not open a new account
5. Close an existing account
6. Reopen an account with a new number
7. Notify the Program Administrator for determination of the appropriate step(s) to take
8. Notify law enforcement or determine that no response is warranted under the particular circumstances

B. Protect customer identifying information

In order to further prevent the likelihood of identity theft occurring with respect to University accounts, the University will take the following steps with respect to its internal operating procedures to protect customer identifying information:

1. Ensure that its website is secure or provide clear notice that the website is not secure
2. Ensure complete and secure destruction of paper documents and computer files containing customer information

3. Ensure that office computers are password protected and that computer screens lock after a set period of time
4. Keep offices clear of papers containing customer information
5. Request only the last 4 digits of social security numbers (if any)
6. Ensure computer virus protection is up to date
7. Require and keep only the kinds of customer information that are necessary for University purposes

PROGRAM ADMINISTRATION.

A. Oversight

Responsibility for developing, implementing and updating this Program lies with within the Division of Finance, under the office of the Controller. The Controller is responsible for overall Program administration, for ensuring appropriate training of University staff on the Program, for 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.

B. Program Updates

This Program will be periodically reviewed and updated to reflect changes in risks to customers and the soundness of the University from Identity Theft.

C. Staff Training and Reports

University staff responsible for implementing the Program shall be trained either by or under the direction of the Controller or his/her designee in the detection of Red Flags, and the responsive steps to be taken when a Red Flag is detected.

D. Service Provider Arrangements

In the event the University engages a service provider to perform an activity in connection with one or more accounts, the University will take the following 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:

1. Use our best efforts to insure that service providers have such policies and procedures in place
2. And, that service providers review the University ’s Program and report any Red Flags to the Program Administrator

3.0 WPI Red Flag Roles

RED FLAG CONTACT PERSON
Patrick Hitchcock
Worcester Polytechnic Institute
100 Institute Road
Worcester, MA 01609

INFORMATION SECURITY CONTACT
John Schwartz - Chief Information Security Officer (CISO)
Worcester Polytechnic Institute
100 Institute Road
Worcester, MA 01609
Phone: (508) 831-6868

5.0 Enforcement

Any person that violates any of the measures found in this policy will be subject to the same disciplinary actions outlined in WPI’s Confidentiality Agreement for employees, or the Acceptable Usage Policy and Code of Conduct for students.

6.0 Approval and Revisions

Policy Category: Institutional Risk & Compliance

Policy Approved By: Approved by WPI's Information Security, Risk and Compliance Committee on 10/11/18.

Policy Reviewed Annually By: John Schwartz (CISO)

Related University Policies:

Written Information Security Program

Gramm-Leach-Bliley Policy

Last Modified: 10/30/19