THE UNIVERSITY OF ALABAMA® | Division of Finance and Operations

Identity Theft Prevention (Red Flag Rules) Policy

Unit: Compliance, Ethics, and Regulatory Affairs
Effective Date: 06/01/2018
Revision Date: 10/21/2019

Contact: Dr. Marcy Huey
Title: Executive Director for Institutional Compliance

Purpose

The University of Alabama (UA), also referred to herein as "University," recognizes some of its activities are subject to the Federal Trade Commission's (“FTC”) Red Flags Regulation (16 CFR § 681.2), which implements Section 114 of the Fair and Accurate Credit Transactions (FACT) Act of 2003 and the final rules implementing section 315 of the FACT Act. Under these regulations, The University is considered a creditor and must periodically determine, by conducting a risk assessment, whether it offers or maintains “covered accounts.” Upon identifying any covered account(s), the University is required to develop and implement a written Identity Theft Prevention Program (Program) to detect, prevent, and mitigate identify theft in connection with the opening of certain new accounts and the maintenance of certain existing accounts.

This policy and the accompanying Red Flags Identification and Detection Grid implements UA’s Identity Theft Prevention Program and provide additional information to employees when developing internal procedures to help prevent and mitigate a security incident, as well as guidance for reporting a known or suspected security incident.

Policy

The University’s Identity Theft Prevention Program must contain reasonable policies and procedures to:

1. **Identify** relevant red flags for new and existing covered accounts and incorporate those red flags into the Program;
2. **Detect** red flags that have been incorporated into the Program;
3. **Prevent** identity theft by responding appropriately to any red flags that are detected;
4. **Mitigate** identity theft once it has occurred; and
5. **Update** the Program periodically to reflect changes in risks to the customer and the University from identity theft.

I. Program Administration

A. Oversight

Each University department with covered accounts that maintains, disseminates or disposes Personally Identifiable Information (PII) data shall designate an individual who will serve as the department’s Identity Theft Prevention Officer. This Officer will coordinate with the Program Administrator to implement the requirements of this policy. The Executive Director for Institutional Compliance in the Office of Compliance, Ethics, and Regulatory Affairs shall serve as the Program Administrator. The Program Administrator shall work with the Identity Theft Prevention Officers designated by the departments to develop, implement, and monitor the effectiveness of this program and policy. Also, the Program Administrator shall communicate policy changes and needed Program updates to the Identity Theft Prevention Officers. Changes in federal regulations may require immediate changes to this policy.

The Program Administrator will periodically provide a report to University Administration addressing:

1. The overall effectiveness of the University's Identity Theft Prevention Program;
2. Service provider arrangements;
3. Significant incidents involving identity theft and UA's response;
4. Recommendations for material program and policy changes.

B. Staff Training

While the Program Administrator can provide training, when requested, on this policy and on the requirements of the Red Flags Regulations, the individual designated as the Identity Theft Prevention Officer for a department shall provide the staff training necessary to detect, prevent, and mitigate identity theft in their area.

C. Compliance Reports

Annually, or as requested by the Program Administrator, each department's Identity Theft Prevention Officer shall submit a report to the Program Administrator documenting the status of their area's compliance with this Program. This report should address the effectiveness of the department's procedures against the risk of identity theft and should include any recommendations for changes to the Program.

D. Service Provider Arrangements/Contractual Agreements

In the event the University engages a service provider to perform an activity in connection with one or more covered accounts, the University, through its contract review process, shall 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. Require, by written contract that service providers have identity theft policies and procedures in place; and
2. Require, by written contract that service providers report any red flags or identity theft incidents associated with University accounts/records to the University employee with primary oversight of the service provider relationship who must report to the appropriate ITPO. The ITPO should provide this information to the Program Administrator.

E. Non-Disclosure of Specific Practices

For the effectiveness of the University's Identity Theft Prevention Program, knowledge about specific red flag identification, detection, mitigation, and prevention practices should be limited to the Program Administrator, Identity Theft Prevention Officers, and departmental employees who are responsible for the implementation of this policy. Any documents that may be reviewed or produced to develop or implement this Program that list or describe such specific security practices and the information those documents contain are considered confidential and should not be posted online, shared with other non-involved employees, or the public. All documents reviewed or produced as a result of identity theft, or in the investigation of potential identity theft, are considered confidential.

II. Identification of Red Flags

To enable the identification of relevant red flags, University departments should consider the business practices associated with all the types of accounts their department offers or maintains. This should include methods used to open accounts, methods used to access accounts, and any previous experiences with identity theft. Each department shall review current policies and procedures to address detection of red flags for each type of covered account, focusing on verifying identity, authenticating customers, monitoring transactions, and verifying the validity of change of address requests, as well as previous experiences with identity theft.

Categories of red flags include:

1. Notifications and Warnings from a Credit Reporting Agency
2. Suspicious Documents
3. Suspicious Personal Identifying Information (PII)
4. Suspicious Covered Account Activity or Unusual Use of Account

5. Alerts from Others

Additional information to be considered in assessing business processes for red flags is provided in the Red Flags Identification and Detection Grid. Each area should complete their own grid, specific to their red flags, utilizing the Red Flags Identification and Detection Grid Template, including any other red flags identified in the department's procedures to prevent, detect, and mitigate identity theft.

III. Detecting Red Flags

A. Areas to Assess
In order to detect red flags, University personnel should review departmental procedures associated with:

1. New Covered Accounts
2. Existing Covered Accounts
3. Responding to Consumer (Credit) Report Requests

Detailed guidance to assist in assessing each of these areas is provided in the Red Flags Identification and Detection Grid. The Program Administrator can provide assistance in developing or reviewing procedures, if needed.

B. Social Security Numbers
In all cases, special care should be taken to avoid asking for a Social Security Number unless its collection has been explicitly authorized by administration and is required for an approved business purpose.

C. Special Cases
A data security incident that results in unauthorized access to a customer's account record or notice that a customer has provided information related to a covered account to someone fraudulently claiming to represent the University or to a fraudulent website may heighten the risk of identity theft and should be considered red flags.

IV. Preventing and Mitigating Identity Theft

In the event University personnel detect any identified red flags, such personnel shall notify their supervisor or the individual designated as the department's Identity Theft Prevention Officer. Departments should take steps to prevent and/or mitigate any possible concerns, and to protect covered account information and PII. Detailed guidance to assist in developing the appropriate responses to accomplish this is provided in the Red Flags Identification and Detection Grid.

An employee who knows or suspects that a security incident has occurred shall immediately notify their appropriate supervisor and the Identity Theft Prevention Officer and complete a Red Flags Detection Report. The ITPO will report to the Program Administrator as needed. If fraud is known or reasonably suspected, contact the University of Alabama Police Department.

Scope

Managing and protecting data are responsibilities shared by all members of the University community. This policy complements existing University policies related to data security, data protection, and information disclosure. This and other related policies combine to promote UA's effort to comply with the Health Insurance and Portability and Accountability Act (HIPAA), the Family Educational Rights and Privacy Act (FERPA), Gramm Leach Bliley Act (GLBA), Payment Card Industry (PCI) standards, the EU General Data Protection Regulation (GDPR), and other applicable federal and state laws.

A current listing of University departments with covered accounts is maintained on the Identity Theft Prevention Program webpage. All individuals (faculty, staff, students, and visitors), schools, departments, affiliates and/or other similar entities within the University community, including employees of contracted or outsourced non-UA entities, who have access to covered account Personal Identifying Information (PII) are subject to this policy. All customer PII is covered under this policy including, but not limited to, PII data contained in centralized institutional systems, department/unit systems, systems created or operated by third party vendors under the direction of UA, as well as PII data stored or maintained in any other capacity or medium where there is a reasonably foreseeable risk of identity theft.

Definitions

Account: A continuing relationship established by a person with a financial institution or creditor to obtain a product or service for personal, family, household or business purposes.

Covered Account: (i) Any account the University offers or maintains primarily for personal, family or household purposes, that allows multiple payments or transactions, including one or more deferred payments; and (ii) any other account the University identifies as having a reasonably foreseeable risk to customers or the safety and soundness of the University from identity theft. A current listing of University departments with covered accounts is maintained on the Identity Theft Prevention Program webpage.

Identity Theft: A fraud committed or attempted using the identifying information of another person without authority.

Identity Theft Prevention Officer: Someone designated by a department with covered accounts to serve as a liaison to the Program Administrator and is responsible for ensuring that the requirements of the Identity Theft Prevention Policy are incorporated in departmental procedures. This person also may be responsible for ensuring the implementation of other University policies that safeguard and protect data from unauthorized access, use, and disclosure.

Personal Identifying Information (PII): Any name or number that may be used, alone or in conjunction with any other information, to identify a specific person. Below are examples of data fields that are considered PII:

a) Taxpayer Identification Number (SSN, ITIN or EIN)
b) System Generated Identification Number (CWID or patient number, etc.)
c) Government Passport Number
d) Government Issued Driver's License or other Identification Number
e) Alien Registration Number
f) Government Passport Number
g) Name
h) Date of Birth
i) Address
j) Telephone Number(s)
k) Personal Identification Number (PIN)
l) E-mail Address
m) Password
n) Computer Internet Protocol Address
o) Bank or other Financial Account Routing Code

Program Administrator: The individual designated with primary responsibility for oversight of the Identity Theft Prevention Policy.

Red Flag: A suspicious pattern, practice, or specific activity that indicates the possible existence of identity theft.

Service Provider: A person or company that provides a service directly to the University.

Office of the Vice President of Finance and Operations

DocuSigned by:
Signed: Cheryl Mowdy 10/21/2019
DC7FC10D23404E0...
Cheryl Mowdy
Assistant Vice President for Finance and Operations