FTC Red Flags Rule

Effective Date: April 2010

Approval: December 17, 2015

Maintenance of Policy: Chief Information Officer

PURPOSE: 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.

SCOPE: This policy applies to all units of the University of Dayton, as well as contracted service providers, involved in the administration of covered accounts.

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. Account includes:

i. An extension of credit, such as the purchase of property or services involving a deferred payment.
ii. A deposit account.

REFERENCE DOCUMENTS:

1. http://www.ftc.gov/policy/federal-register-notices/identity-theft-red-flags-and-address-discrepancies-under-fair-and

APPLICABLE REGULATIONS:

1. Fair and Accurate Credit Transaction Act of 2003
2. Red Flag Program Clarification Act of 2010

POLICY HISTORY:

Approved as Amended

December 17, 2015

Approved in Original Form

April 2010

DEFINITIONS (continued):

Covered Accounts:

i. An account that the University offers or maintains that involves or is designed to permit multiple payments or transactions.
ii. Any other account that a financial institution or creditor offers or maintains for which there is a reasonably foreseeable risk to customers or to the University of Dayton of identity theft.

The University of Dayton has identified ten types of accounts, five of which are covered accounts administered by the University and five that are administered by a service provider.

University covered accounts:

1. Refund of credit balances involving loans
2. Refund of credit balances, without loans
3. Deferment of tuition payments
4. Emergency loans
5. University non-student business accounts

Service Provider Covered Account: Refer to Program Administration section, item D. Service Provider Arrangements below

1. Tuition payment plan administered by SallieMae TuitionPay™ Plan
2. Collection agencies used for delinquent accounts:
   American Collection Systems, Inc.
   General Revenue Corporation
   National Credit Management
   Reliant Capital Solutions, LLC
   Williams & Fudge, Inc.
   National Enterprise Systems
   Conserve
3. Collection agency used for delinquent invoices:
   Diversified Credit Service, Inc.
4. Federal Perkins Loan Billing servicer – Campus Partners
5. 403(b) loans from TIAA, Fidelity, and /or Lincoln National.

The University of Dayton may eliminate and/or add covered accounts as business needs change.

Credit: The rights granted by a creditor to a debtor to defer payment of debt or to incur debt and defer its payment or to purchase property or services and defer payment.

Creditor: Any person, corporation, government or governmental subdivision, or agency, trust, estate, partnership, cooperative, or association who regularly extends, renews, or continues credit; any person who regularly arranges for the extension, renewal, or continuation of credit; or any assignee of an original creditor who participates in the decision to extend, renew, or continue credit.

Customer: Person that has a covered account with a financial institution or creditor.

Debit Card: Any card issued by a financial institution to a consumer for use in initiating an electronic fund transfer from the account of the consumer at such financial institution, for the purpose of transferring money between accounts or obtaining money.

DEFINITIONS (continued):

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 Driver's License or Identification Number
- Alien Registration Number
- Government Passport Number
- Employer or Taxpayer Identification Number
- Unique Electronic Identification Number
- Computer's Internet Protocol Address or Routing Code
- University of Dayton assigned student Identification number

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

Notice of Address Discrepancy: A notice sent to a user by a consumer reporting agency pursuant to 15 U.S.C. 1681c(h)(1), that informs the user of a substantial difference between the address for the consumer that the user provided to request the consumer report and the address(es) in the agency's file for the consumer.

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

Service Provider: A person or entity that provides a service directly to the financial institution or creditor.

POLICY:

Identification Of Red Flags

In order to identify relevant Red Flags, the University of Dayton considers the types of accounts that it offers and maintains, the methods it provides to open its accounts, the methods it provides to access its accounts, and its previous experiences with Identity Theft. 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

POLICY [continued]:

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

POLICY [continued]:

E. Alerts from Others

Red Flags

1. 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. If an individual wishes to file a report anonymously, he or she may do so through the University of Dayton Confidential Reporting Line, provided by a third party at www.udayton.ethicspoint.com or 1-855-550-0654."

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

POLICY (continued):

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 an Identity Theft Committee for the University. The Committee is headed by a Program Administrator, who is the Bursar of the University of Dayton. Two or more other individuals appointed by the head of the University or the Program Administrator comprise the remainder of the committee membership. The Program Administrator will be responsible for the 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. At least annually, the Program Administrator will consider the University's experiences with Identity Theft situations, changes in Identity Theft methods, changes in Identity Theft detection and prevention methods, changes in types of accounts the University maintains and changes in the University's business arrangements with other entities.

POLICY [continued]:

After considering these factors, the Program Administrator will determine whether changes to the Program, including the listing of Red Flags, are warranted. If warranted, the Program Administrator will update the Program or present the President's Council with his or her recommended changes and the President's Council will make a determination of whether to accept, modify or reject those changes to the Program.

C. Staff Training and Reports

University staff responsible for implementing the Program shall be trained either by or under the direction of the Program Administrator 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

E. Specific Program Elements and Confidentiality

For the effectiveness of Identity Theft prevention Programs, the Red Flag Rule envisions a degree of confidentiality regarding the University's specific practices relating to Identity Theft detection, prevention and mitigation. Therefore, under this Program, knowledge of such specific practices is to be limited to the Identity Theft Committee and those employees who need to know them for purposes of preventing Identity Theft. Because this Program is to be adopted by a public body and thus publicly available, it would be counterproductive to list these specific practices here. Therefore, only the Program's general red flag detection, implementation and prevention practices are listed in this document.

F. The person who is the Bursar will be the Program Administrator of the Red Flag Program.

The University of Dayton has determined that the individual who holds the position of University Bursar is the most appropriate individual to be the Program Administrator. Currently that position is held by Gwen Klemmer.