OLD DOMINION UNIVERSITY
University Policy

Policy #3011
IDENTITY THEFT PROTECTION (RED FLAG) PROGRAM

Responsible Oversight Executive: Vice President for Administration and Finance
Date of Current Revision or Creation: October 30, 2017

A. PURPOSE

The purpose of this policy is to implement an Identity Theft Prevention Program pursuant to the Federal Trade Commissions' Red Flags Rule under the Fair Credit Reporting Act to detect, prevent and mitigate incidents of identity theft in order to protect its students, employees and others who entrust their personal information with the University.

B. AUTHORITY

Code of Virginia Section 23.1-1301, as amended, grants authority to the Board of Visitors to make rules and policies concerning the institution. Section 6.01(a)(6) of the Board of Visitors Bylaws grants authority to the President to implement the policies and procedures of the Board relating to University operations.

Rules issued by the Federal Trade Commission pursuant to the Fair Credit Reporting Act ("FCRA") 15 U.S.C. §1681

Regulations issued by the Federal Trade Commission, Electronic Code of Federal Regulations, Title 16, Part 681

Code of Virginia Section 18.2-186.3, Identity Theft

Board of Visitors Policy 1601 – Identity Theft Protection

C. DEFINITIONS

Covered Account – All student accounts or loans administered by the University.

Credit Transaction – Any transaction where the University loans, defers payment, or extends credit to an individual.

Debit Cards – Any card that allows a balance to decline and/or be refreshed for use in purchase transactions.

Identity Theft – A fraud committed or attempted using the personally identifiable information (PII) of another person without authority.

Personally Identifiable Information (PII) – Any information used to identify a specific person, including, but not limited to, name, address, and telephone number when combined with social security number, date of birth, government-issued numbers (such as passport, driver's license, alien registration or taxpayer identification), medical record number, or a unique electronic or account number in combination with any required security code, access code or password, or unique biometric data such as fingerprint, voice print, or retina or iris image.

Red Flag – A transaction that a reasonable person should suspect that they may be interacting with an individual using someone else's identity. A pattern, practice or specific activity that indicates a possible existence of identity theft.

Suspicious Activities Report (SAR) – A report of suspicious activity that arises when a University employee is confronted with a Red Flag. The report shall be in writing and forwarded to the Associate Controller and shall specifically state the party or parties involved, the conduct creating the red flag, and the action or refusal to take action that was a result of the suspicious behavior.

D. SCOPE

This policy applies to all employees and employees of affiliated organizations who are paid through the University. Employees include all staff, administrators, faculty, full- or part-time, and classified or non-classified persons who are paid by the University. Affiliated organizations are separate entities that exist for the benefit of the University through an operating agreement and include the Foundations, the Community Development Corporation, and the Alumni Association.

E. POLICY STATEMENT

Old Dominion University is committed to complying with Federal regulations concerning the detection, prevention and mitigation of identity theft. In accordance with the Fair Credit Reporting Act (FCRA) and the subsequent "Red Flags Rule" of 2007, the University is required to establish and maintain an Identity Theft Protection Program (hereinafter referred to as "Program") to detect, prevent and mitigate identity theft in connection with new and existing covered accounts.

This policy applies in three applications affecting diverse University constituencies. The first application occurs in the use of criminal background checks performed to employ an individual. The second application occurs in any credit transaction. The third application occurs in the issuance, reissuance or refilling of debit cards.

Each department or unit within the University that conducts background checks or performs any credit or debit transaction shall develop reasonable written 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. Respond appropriately to any Red Flags that are detected to prevent and mitigate identity theft; and
4. Ensure the Program is reviewed at least annually in order to identify and address changes in risks to students, employees, and/or job applicants or to the safety and soundness of the student, employee, and/or job applicant from identity theft.

F. PROCEDURES

1. IDENTIFICATION OF RED FLAGS

In order to identify relevant Red Flags, the University considers the types of accounts that it offers and maintains, methods it provides to open its accounts, 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 Reporting Agencies
Red Flags:
   i. Receipt of a notice of address discrepancy in response to a report request;
   ii. Non-approval of a credit transaction due to possible fraudulent usage.

b. Suspicious Documents
Red Flags:
   i. Identification document or card that appears to be forged, altered or inauthentic;
   ii. Identification document or card on which a person's photograph or physical description is not consistent with the person presenting the document;
   iii. Other document with information that is not consistent with existing student, employee, or job applicant information; and
   iv. Application for service that appears to have been altered or forged.

c. Suspicious Personally Identifiable Information (PII)
Red Flags:
   i. PII presented that is inconsistent with other information the student**,** employee, or job applicant provides (example: inconsistent birth dates);
   ii. PII presented that is inconsistent with other sources of information (for instance, an address not matching an address on a loan application);
   iii. PII presented that is the same as information shown on other applications that were found to be fraudulent;
   iv. PII presented that is consistent with fraudulent activity (such as an invalid phone number or fictitious billing address);
   v. Social security number presented that is the same as one given by another student, employee, or job applicant;
   vi. An address or phone number presented that is the same as that of another person;
   vii. A person fails to provide complete PII on an application when reminded to do so; and
   viii. A person's PII is not consistent with the information that is on file for the student**,** employee, or job applicant.

d. Suspicious Covered Account Activity or Unusual Use of Account
Red Flags:
   i. Change of address for an account followed by a request to change the student's, employee's**,** or job applicant's name;
   ii. Payments stop on an otherwise consistently up-to-date account;
   iii. Account used in a way that is not consistent with prior use;
   iv. Mail sent to the student, employee or job applicant that is repeatedly returned as undeliverable;
   v. Notice to the University that a student, employee or job applicant is not receiving mail sent by the University;
   vi. Notice to the University that an account has unauthorized activity;

vii. Breach in the University's computer system security involving PII; and
viii. Unauthorized access to or use of student account information.

e. Alerts from Others

Notice to the University from a student, employee, job applicant, identity theft victim, law enforcement or other person that the University has opened or is maintaining a fraudulent account for a person engaged in identity theft.

2. DETECTING RED FLAGS

a. Student Enrollment

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

i. Require certain PII such as name, date of birth, academic records, home address or other identification; and
ii. Verify the student's identity at time of issuance of student identification card (review of driver's license or other government-issued photo identification).

b. Existing Accounts

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

i. Verify the identification of students if they request information (in person, via telephone, via facsimile, via email);
ii. Verify the validity of requests to change billing addresses by mail or email and provide the student a reasonable means of promptly reporting incorrect billing address changes; and
iii. Verify changes in banking information given for billing and payment purposes.

c. Criminal Background Check Requests

In order to detect any of the Red Flags identified above for employment in a position for which a criminal background report is sought, University personnel will take the following steps to assist in identifying address discrepancies:

i. Require written verification from any job applicant that the address provided by the applicant is accurate at the time the request for the background check is made; and
ii. In the event that notice of an address discrepancy is received, verify that the background check pertains to the job applicant for whom the requested report was made.

3. 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:

i. Continue to monitor a covered account for evidence of identity theft;
ii. Contact the student, employee or job applicant;
iii. Change any passwords or other security devices that permit access to covered accounts;
iv. Do not open a new covered account;
v. Provide the student, employee or job applicant with a new identification number;
vi. Notify the Program Administrator for determination of the appropriate step(s) to take;
vii. Notify law enforcement;
viii. File or assist in filing a Suspicious Activities Report ("SAR"); or
ix. Determine that no response is warranted under the particular circumstances.

b. Protect Personally Identifiable Information (PII):

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

i. Ensure that its website containing PII is secure or provide clear notice that the website is not secure;
ii. Ensure complete and secure destruction of paper documents and computer files containing student, employee or job applicant account information when a decision has been made to no longer maintain such information; ensure that those records containing PII are destroyed within six months of the expiration of their retention period;
iii. Ensure the computer systems follow the IT Security Program and that systems handling PII are reviewed for risk, classified appropriately, and that appropriate controls are used;
iv. Avoid use of social security numbers;
v. Require and keep only the kinds of student, employee and job applicant information that are necessary for University purposes; and
vi. Adhere to Information Technology Services (ITS) Standard 2.3.0, Data Administration and Classification, for all PII maintained in any electronic format.

4. PROGRAM ADMINISTRATION

a. Oversight

Responsibility for developing, implementing and updating this Program lies with the Associate Controller.

b. Staff Training and Reports

Each department or unit that conducts background checks, issues debit cards or issues credit transactions is responsible for ensuring that staff are trained as necessary, to effectively implement the Program. University employees are expected to notify the Associate Controller once they become aware of an incident of identity theft or of the University's failure to comply with this Program.

Each department or unit within the University that conducts background checks, issues debit cards or issues credit transactions shall annually (prior to November 1) provide the Associate Controller a copy of the written procedures and sign-in sheet used at the annual training session. The Associate Controller shall provide a summary of all procedures and training to the Audit Committee of the Board of Visitors for their review with recommendations, if any, of suggested changes to better identify and react to Red Flags.

c. Service Provider Arrangements

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 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.

i. Require, by contract, that service providers have such policies and procedures in place; and
ii. Require, by contract, that service providers review the University's Program and report any Red Flags to the Associate Controller or the University employee with primary oversight of the service provider relationship.

d. Program Updates

The Associate Controller will periodically review and update this Program to reflect changes in risks to students, employees and job applicants. In doing so, the Associate Controller will consider the University's experiences with identity theft situations, changes in identity theft methods, changes in identity theft detection and prevention methods, and changes in the University's business arrangements with other entities. After considering these factors, the Associate Controller will determine whether changes to the Program, including the listing of Red Flags, are warranted. If warranted, the Associate Controller will update the Program.

G. RECORDS RETENTION

Applicable records must be retained for three years and then destroyed in accordance with the Commonwealth's Records Retention Schedule 102, Series 012103 (Financial Account Reports).

H. RESPONSIBLE OFFICER

Assistant Vice President for Finance/University Controller

I. RELATED INFORMATION

University Policy 1002 – Code of Ethics
University Policy 1003 – University Responsibility for Compliance
University Policy 3002 – Authority of Internal Audit Department

POLICY HISTORY

****

Policy Formulation Committee (PFC) & Responsible Officer Approval to Proceed:

/s/ Mary Deneen — October 18, 2017
Responsible Officer — Date

Policy Review Committee (PRC) Approval to Proceed:

/s/ Donna W. Meeks — April 11, 2017
Chair, Policy Review Committee (PRC) — Date

Executive Policy Review Committee (EPRC) Approval to Proceed:

/s/ Gregory DuBois — October 23, 2017
Responsible Oversight Executive — Date

University Counsel Approval to Proceed:

/s/ R. Earl Nance — October 24, 2017
University Counsel — Date

Presidential Approval:

/s/ John R. Broderick — October 30, 2017
President — Date

Policy Revision Dates: June 24, 2010; October 30, 2017

Scheduled Review Date: October 30, 2022