

# OLD DOMINION UNIVERSITY

## University Policy

### Policy #3011

### IDENTITY THEFT PROTECTION (RED FLAG) PROGRAM

**Responsible Oversight Executive:**

Vr 0 (U)0.8 2 (es.in) (r 0 (Omi.))TS)50 (E)-6 (3.9w 3 ( )Tj 0.0

[16, Part 681](#)

[Electronic Code of Federal Regulations, Title](#)

[Code of Virginia Section 18.2186.3, 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

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,

## F. PROCEDURES



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 d 14.7

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

