NUMBER: 1601

TITLE: Identity Theft Protection

APPROVED: December 5, 2008; Revised June 12, 2014; Revised December 9, 2022

SCHEDULED REVIEW DATE: December 2027

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.

Common red flags include:

- Receipt of Alerts or Notices of Dispute from a credit agency;
- Identification documents or cards that appear to be forged or altered;
- Identification documents or cards on which a person's photograph or physical description is not consistent with the person presenting the document;
- Inconsistencies in information among different documents presented;
- Presentation of identifying information that is inconsistent with information from other sources;
- Social security number presented that is the same as one given by another student or employee;
- Notice to the University of unauthorized student or employee account activity.

A. The University is a user of consumer reports and is required to have protections in place to prevent identity theft. The University conducts background checks of certain employment applicants. To prevent identity theft, review of the applications and related documentation should be thorough. The University requires employees, who view suspected altered documents, questionable documentation, or any irregularity in the information provided by applicants, to bring it to the attention of supervisors.

A verified address is submitted to the consumer reporting agency providing background checks to the University. Verification of address may include but not be limited to the following:

1. Internal Sources such as Banner when available (i.e., applicant was a former student).
2. Official documents such as a driver's license and others.
3. Documents from third party sources such as utility bills, etc.
4. Any other reasonable means.

In the event the University receives a Notice of Address Discrepancy or an alert from a credit reporting agency, the University shall confirm the address of the applicant to avoid

potential identity theft. The University will notify the agency conducting the background check of the confirmation of the address.

In the event that significant doubt remains as to the identity of the applicant, the application process shall be terminated until such time that the discrepancy is cleared.

B. The University is a creditor in transactions, including the Travel Card program. The Board of Visitors shall periodically review the methods used to open accounts to protect against identity theft. The University recognizes that the University needs to protect an account holder's identity. Each issuer of credit on behalf of the University will submit a written plan for preventing identity theft to the Associate Vice President for Finance/University Controller. The plan shall include means of detection of identity theft and verification of information on the credit application. The plan shall provide for employee training in the prevention of identity theft. The Associate Vice President for Finance/University Controller shall annually review credit application procedures.

C. The University must provide protections to debit card users. Debit card are defined as any card that allows a balance to decline and/or be refreshed for use in purchase transactions. The department responsible for the University debit card program shall verify a change of address request within 30 days from the date of the request by e-mail to the debit card user's University e-mail address. The debit card user shall promptly notify the University within three calendar days by return e-mail of an incorrect address change.

D. 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 and will annually review training programs. The Office of Information Technology Services shall annually review the procedures used to store personally identifiable information to protect information from improper use and training programs within each appropriate department or unit to ensure technology related guidance is accurate and up to date.

E. In any event in which circumstances rise to the level of suspicious activity, employees are directed to file a Suspicious Activity Report for Red Flags. The Associate Vice President for Finance/University Controller will determine if additional review or action is required and ensure notification to law enforcement as appropriate.

F. Related information: Old Dominion University Policy #3011 Identity Theft Protection (Red Flag) Program.