NUMBER: 1601

TITLE: Identity Theft Protection

APPROVED: December 5, 2008

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 should be thorough. The review shall include review of documentation. 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 many transactions. The Board of Visitor's 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 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 University Controller shall annually review the application procedures and training programs to insure that safeguards from identity theft are in place. The Office of Computing and Communications Services shall annually review the procedures used to store personally identifiable information to protect information from improper use.

C. The University must provide protections to debit card users to verify a change of address request within 30 days from the date of the request. The University shall verify the change of address request by e-mail to the University e-mail address. The Cardholder shall promptly

notify the University within three calendar days by return e-mail of an incorrect address change.