



Washington and Lee University

Identity Theft Prevention Program for Employee and Student Covered Financial Accounts and Loans

Approved By: <u>Board of Trustees</u>	Related Policies: <u>Information Security Program;</u>
	<u>Confidentiality Policy; Computing and Network Use</u>
History: Issued – <u>May 9, 2009</u>	<u>Policy; Record Retention and Disposition Policy</u>
Revised – _____	Additional References: <u>Office of Human Resources</u>
	<u>Background Check Procedures; Va. Code Section</u>
Responsible Office: <u>Treasurer/Vice-President for</u>	<u>47.1-14 (Notary Public duty of care re: identity</u>
<u>Finance and Administration</u>	<u>verification)</u>

I. INTRODUCTION

Policy Statement

Washington and Lee University (“the University”) adopts this written Identity Theft Prevention Program for Employee and Student Covered Financial Accounts and Loans (“the Program”) as required to comply with the Federal Trade Commission’s Red Flags Rule under Section 114 of the Fair and Accurate Credit Transactions Act of 2003 (“FACTA”), 16 CFR Section 681.2. The Program outlines reasonable procedures to prevent, detect and mitigate the risk of identity theft in covered employee and student financial accounts and loans with the University. The University has a primary relationship with its employees and students other than as a creditor or lender, unlike the creditors/lenders for which the Red Flags Rule was designed. Based on these relationships of employer-employee and student-educational institution, various identity verification measures are already in place under other applicable laws/regulations/programs (e.g., I-9 employment eligibility verification for employees, National Student Clearinghouse and FAFSA for students). The Program does not take the place of any such independent requirements.

Applicability

The Program applies to all employee and student loans with the University and all employee and student financial accounts or payment plans for debts owed to the University that involve multiple transactions or multiple payments. These include, but are not limited to, employee home loans, student tuition loans, loan repayment assistance programs, tuition payment plans,

payroll advances, and employee and student accounts billed monthly. The Program does not apply to financial transactions where the University is not a creditor or lender (e.g., arrangements for employee direct deposit of payroll checks, acceptance of checks or credit cards for on campus purchases or donor gifts to the University, etc.). Neither does the Program apply to any non-financial transaction (e.g., transcript requests, requests for issuance of keys to campus offices, requests to give an employee or student access to a sensitive or confidential database.) Staff, faculty, and students should use common sense and appropriate diligence, and follow other applicable law and/or University policy, in any transaction outside the scope of the Program that could have information security or identity theft implications.

II. DEFINITIONS

“Identity Theft” is a fraud committed or attempted by the unauthorized use of the personal identifying information of another person.

“Red flag” is a pattern, practice, or specific activity that indicates the reasonable possibility of Identity Theft.

“Covered account” includes all employee and student loans with the University and all employee and student financial accounts or payment plans for debts owed to the University that involve multiple transactions or multiple payments.

“Identifying information” is any name or number that may be used, alone or with other information, to identify a specific person. Examples include but are not limited to: name, address, telephone number, social security number, date of birth, driver’s license, alien registration number, passport number, employer or taxpayer identification number, student identification number, and University card number.

III. POLICY

A. Identification of Red Flags

Under this Program, each department that opens or otherwise handles or manages covered accounts should identify specific red flags that are relevant to those covered accounts. The following lists contain red flags that may arise with the opening or administering of various employee and/or student accounts and loans covered under the Program. Departments may identify other circumstances that they consider red flags for their particular covered accounts.

1. **Notifications and Warnings from Credit Reporting Agencies**
 - Report of fraud accompanying a credit report;
 - Notice of a credit freeze on the person;
 - Notice of address discrepancy on a credit report request;
2. **Suspicious Documents**
 - Identification document that appears to be forged, altered, or inauthentic;

- Identification document on which a person's photograph or physical description is not consistent with the person presenting the document;
- Other document with information not consistent with existing employee or student information.

3. Suspicious Personal Identifying Information

- Identifying information presented that is inconsistent with other information the student or employee provides (e.g., inconsistent birth dates) or with other sources of information (e.g., address discrepancy with address on loan application);
- Identifying information presented that is consistent with fraudulent activity (e.g., invalid phone number or fictitious billing address);
- Social security number or other identifying information that is the same as that given by another employee or student;
- Person fails to provide complete personal identifying information when asked to do so.

4. Suspicious Account/Loan Activity

- Change of address for an account followed by a request to change the employee's or student's name;
- Payments stop on an otherwise consistently up-to-date account;
- Account used in a way that is strikingly inconsistent with prior use;
- Mail sent to the employee or student is repeatedly returned as undeliverable;
- Notice to the University that an employee or student is not receiving mail sent by the University;
- Notice to the University that the account has unauthorized activity;
- Notice to the University of unauthorized access to or use of employee or student account information ;
- Breach in the University's computer system security affecting the employee's/student's account or loan.

5. Alerts from Others

- Notice to the University from an employee/student, Identity Theft victim, law enforcement or other person that the University has opened or is maintaining a fraudulent account/loan for a person engaged in Identity Theft.

B. Detecting Red Flags

1. Opening Accounts/Applying for Loans

In order to assist with detection of the applicable red flags identified as associated with opening an account or taking out a loan with the University,

University personnel should be made aware of the types of red flags that may arise with covered accounts relevant to their departments. Where identifying information has not been independently required or routinely verified on the employee or student as part of pre-existing University practices or operations at the time of employment or enrollment, University personnel who do not personally know the employee or student opening the account/taking out the loan should take reasonable steps to verify the person's identity. This may mean asking to see the person's University card, asking for certain other identifying information maintained in University records that can be verified (e.g., date of birth, home address, etc.), or verifying identity through an appropriate University official who personally knows the employee or student. At the time of issuance of employee and student University cards, University personnel who do not personally know the employee/student should verify the person's identity by reviewing a driver's license or other government-issued photo identification.

2. Existing Accounts/Loans

In order to assist with detection of the applicable red flags identified above associated with existing accounts, University personnel should be made aware of the types of red flags that may arise with covered accounts relevant to their departments. University personnel should use reasonable measures as appropriate to monitor transactions on particular accounts, including but not limited to: verifying the identification of students and employees who request account/loan information or attempt to conduct transactions on covered accounts; verifying the validity of requests to change billing addresses by mail or email; providing students/employees a reasonable means of promptly reporting incorrect billing address changes; and verifying changes in banking information given for billing and payment purposes.

C. Preventing and Mitigating Identity Theft

In the event University personnel detect any identified red flags, they should take one or more of the following steps, depending on the circumstances, other procedures or practices in place independent of this Program to address the concern, and the degree of risk posed by the red flag:

- Determine that no response is warranted under the circumstances;
- Continue to monitor a loan/account for evidence of Identity Theft;
- Contact the employee or student to obtain more information or to discuss the concern;
- Change any passwords or other access codes that permit access to the loan/account;
- Decline to open the account/approve the loan/issue the University card or otherwise take steps to halt the suspicious transaction;

- Notify the Treasurer/Vice-President for Finance and Administration to determine the appropriate steps to take (which may include notification of law enforcement if Identity Theft is believed to have occurred).

D. Program Administration

1. Oversight, Staff Training and Program Review

The Treasurer/Vice-President for Finance and Administration (“Treasurer”) is the University official responsible for the Program and will work with the Information Security Program Committee to implement the Program. The Treasurer will be responsible for reviewing particular cases or issues of possible Identity Theft reported by University personnel and determining what preventive/mitigating measures are appropriate under the circumstances. The Treasurer will be responsible for seeing that University personnel working with employee and student accounts and loans receive such training as necessary to effectively implement the Program. At least annually, the Treasurer and the Information Security Program Committee should review the effectiveness of the Program, any significant incidents involving identity theft and the University’s response, any changes to the University’s employee and/or student loans or accounts offered, and any other circumstances relevant to the Program, and make any needed changes to the Program.

2. Service Provider Arrangements

If the University engages a service provider to perform an activity in connection with one or more accounts or loans covered by the Program, the University should require, by contract, that the service provider will perform its activity in accordance with reasonable policies and procedures designed to detect, prevent and mitigate the risk of Identity Theft and that the service provider will report any red flags it detects to the Treasurer or the University employee with primary responsibility for that service provider relationship.

IV. ANNOTATED REVISION HISTORY

This policy has not yet been revised.

\\Mfsadm1\Admdept\Deptgeneralcounsel\W&Lpolicies\Draft Policies (Newtemplate)\2009-4-20.Identity.Theft.Program.Docx