UNIVERSITY OF RICHMOND
IDENTITY THEFT PREVENTION PROGRAM

I. Program Adoption.

After consideration of the size and complexity of the University's operations and account systems, and the nature and scope of the University's activities, the University of Richmond has adopted this Identity Theft Prevention Program ("Program") in compliance with the "Red Flag" rules issued by the Federal Trade Commission, implementing Section 114 of the Fair and Accurate Credit Transactions Act of 2003 ("FACTA").

II. Program Purpose. Under the Red Flag rules, the University is required to establish an "Identity Theft Program" with reasonable policies and procedures to detect, identify, and mitigate Identity Theft in its covered accounts. The University must incorporate relevant Red Flags into a Program to enable the University to detect and respond to potential identity theft. The University shall ensure that the Program is updated periodically to reflect changes in risks to customers or creditors or the University from identity theft.

III. Definitions.

"Covered accounts": As used in this policy, the term "Covered Account" means: (a) any account the University offers or maintains primarily for personal, family or household purposes, that involves multiple payments or transactions; and (b) any other account the University offers or maintains for which there is a reasonably foreseeable risk to customers or to the safety and soundness of the University from Identity Theft. Examples of "covered accounts" at the University include but are not limited to:

- Tuition accounts in Student Accounts
- Perkins Loans
- Miscellaneous invoices through Foodservices, Catering, University Events, etc.
- Memberships through Recreation and Wellness

"Customer": As used in this policy, the term "Customer" means any person with a Covered Account with the University, including, but not limited to a student.

"Identifying Information". As used in this policy, the term "Identifying Information" means any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including:

name
address
telephone number
social security number
other identification number
date of birth

"Identity Theft" As used in this policy, the term "Identity Theft" means a fraud committed using the Identifying Information of another person without authority.

"Red Flag" As used in this policy, the term "Red Flag" means a pattern, practice, or specific activity that indicates the possible existence of Identity Theft.

IV. Responsible University Official. The Controller in conjunction with the University's IS Security Administrator shall serve as Program Administrators. The Program Administrators shall exercise appropriate and effective oversight over the Program. In the initial adoption of this Program, the Board of Trustees has delegated responsibility for implementation, oversight and modification of this Program to the Controller.

IV. Program Administration and Maintenance.

The Program Administrators are responsible for delegating the development, implementation and periodic updates of the Program throughout the University system. The Program Administrators are responsible for overseeing appropriate training of University staff on the Program, for reviewing any staff reports regarding the detection of Red Flags and the steps for identifying, preventing and mitigating Identity Theft, determining which steps of prevention and mitigation should be taken in particular circumstances and considering periodic changes to the Program.

The Program will be periodically reviewed and updated to reflect changes in Identity Theft risks and technology changes. The Program Administrators will consider the University's experiences with Identity Theft, changes in Identity Theft methods; changes in Identity Theft detection, mitigation and prevention methods; changes in types of accounts the University maintains; changes in the University's business arrangements with other entities, and any changes in legal requirements in the area of Identity Theft. After considering these factors, the Program Administrators will determine whether changes to the Program, including the listing of Red Flags, are warranted.

The Program Administrators shall confer with all appropriate University personnel as necessary to ensure compliance with the Program. The Program Administrators shall annually review the effectiveness of the Program.

VI. Identification of Red Flags.

In order to identify relevant Red Flags, the University considers the types of accounts that it offers and maintains, the methods it provides to open its accounts, the methods it provides to access its accounts, and its previous experiences with Identity Theft. The following are relevant Red Flags, in each of the listed categories, which employees should be aware of and diligent in monitoring for:

A. Notifications and Warnings from Credit Reporting Agencies

- Report of fraud accompanying a credit report;
- Notice or report from a credit agency of a credit freeze on a Customer or applicant;
- Notice or report from a credit agency of an active duty alert for an applicant; and
- Indication from a credit report of activity that is inconsistent with a Customer's usual pattern or activity.

B. Suspicious Documents

- Identification document or card that appears to be forged, altered or inauthentic;
- Identification document or card on which a person's photograph or physical description is not consistent with the person presenting the document;
- Other document with information that is not consistent with existing Customer information (such as if a person's signature on a check appears forged); and
- Application for service that appears to have been altered or forged.

C. Suspicious Personal Identifying Information

- Identifying information presented that is inconsistent with other information the customer provides (example: inconsistent birth dates);
- Identifying information presented that is inconsistent with other sources of information (for instance, an address not matching an address on a credit report);
- Identifying information presented that is the same as information shown on other applications that were found to be fraudulent;
- Identifying information presented that is consistent with fraudulent activity (such as an invalid phone number or fictitious billing address);
- An address or phone number presented that is the same as that of another person;
- A person fails to provide complete personal identifying information on an application when reminded to do so; and
- A person's identifying information is not consistent with the information that is on file for the customer.

D. Suspicious Account Activity or Unusual Use of Account

- Change of address for an account followed by a request to change the account holder's name;
- Payments stop on an otherwise consistently up-to-date account;
- Account used in a way that is not consistent with prior use (example: very high activity);
- Mail sent to the account holder is repeatedly returned as undeliverable;
- Notice to the University that a Customer is not receiving mail sent by the University;
- Notice to the University that an account has unauthorized activity;
- Breach in the University's computer system security; and
- Unauthorized access to or use of Customer account information.

E. Alerts from Others

- Notice to the University from a customer, identity theft victim, law enforcement or other person that it has opened or is maintaining a fraudulent account for a person engaged in Identity Theft.

VII. Detecting Red Flags

The Program's general Red Flag detection practices are described in this document. The Program Administrators will develop and implement specific methods and protocols appropriate to meet the requirements of this Program.

A. New Accounts

In order to detect any of the Red Flags identified above associated with the opening of a new account, University personnel will take prudent steps to obtain and verify the identity of the person opening the account. Such steps shall include, but shall not be limited to:

- Requiring certain identifying information, such as name, date of birth, academic records, home address or other identification; and
- Verifying the Customer's identity at the time of issuance of a University identification card or establishment of a University account (*e.g.,* 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 prudent steps to monitor transactions with an account. Such steps shall include, but shall not be limited to:

- Verifying the identification of Customers if they request information (in person, via telephone, via facsimile, via e-mail);
- Verifying the validity of requests to change billing addresses by mail or email and providing the Customer with a reasonable means of promptly reporting incorrect billing address changes; and
- Verifying changes in banking information given for billing and payment purposes.

C. Credit / Background Report Requests

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

- Require written verification from any applicant that the address provided by the applicant is accurate at the time the request for the credit report is made to the consumer reporting agency; and
- In the event that notice of an address discrepancy is received, verify that the credit or background report pertains to the applicant for whom the requested report was made and report to the consumer reporting agency an address for the applicant that the University has reasonably confirmed is accurate.

VII. Responding to Red Flags and Mitigating Identity Theft

In the event University personnel detect any identified Red Flags such personnel shall use one or more of the following steps, as appropriate, to respond and mitigate Identity Theft, depending on the nature and degree of risk posed by the Red Flag:

1. In every case, immediately notify the supervisor or director of the affected area and the Red Flag Program Administrators (Controller and IS Security Administrator) redflag@richmond.edu;

2. In every case, gather the facts and maintain a written log of information and actions taken, along with the time and date stamp of those occurrences;

3. Provide contact information and be available for interaction with the IS Security Administrator and law enforcement if needed;

4. Continue to monitor the Covered Account for evidence of Identity Theft;

5. Contact the affected Customer or applicant;

6. Change any passwords or other security devices that permit access to the Covered Accounts;

7. Refrain from opening a new Covered Account;

8. Provide the Customer with a new identification number or password;

9. Notify law enforcement; or

10. In conjunction with the appropriate Supervisors or Director and the Program Administrators, determine that no response is warranted under the particular circumstances.

Anyone with reason to suspect Identity Theft, can report red flag activity anonymously by visiting the URPD "Silent Witness" website at http://oncampus.richmond.edu/administration/police/witness.htm

Report to Red Flag Administrators redflag@richmond.edu

Please refer to the University's Data Exposure Policy at http://is.richmond.edu/policy/Data_Breach_Policy.htm

VIII. Staff Training and Reporting

University employees responsible for implementing the Program shall be trained under the direction of the Program Administrators in the detection of Red Flags, and the responsive steps to be taken when a Red Flag is detected.

Appropriate staff shall provide reports to the Program Administrators on incidents of Identity Theft, the effectiveness of the Program and the University's compliance with the Program along with any needed changes to the current program on a yearly basis.

IX. 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 require by contract that such service providers have policies and procedures in place and to detect, prevent, and mitigate the risk of Identity Theft.

Revision History

Version	Date Revised	Author	Comments
1.0	March 11, 2009	Annemarie Weitzel, Andrea Stadler, Mary King	Initial draft of policy
2.0	April 21, 2009	Shannon Sinclair	Reviewed and updated by University Counsel
3.0	May 7, 2010		Approved by Board of Trustees
4.0	August 7,2010	Harlean Owens	Changed Responsible University Official from Assoc. VP and Controller to Controller
5.0	Sept. 14, 2010	Harlean Owens	Added Revision History to document and VII 1. From University Network Specialist to IS Security Administrator