Rice University Policy No: 841

Identity Theft Prevention Program

I. General Policy

The university takes the necessary steps to protect against identify theft in a manner consistent with the "Red Flags Rule" of the Federal Trade Commission. All faculty and staff should be generally aware of the risk of identity theft (see Section III (a) and (b) of this policy) and those individuals with responsibility for administration or processing of "Covered Accounts" should be familiar with the Identity Theft Prevention Program ("the Program") and should receive training in identity theft and "red flags."

The Rice University Identity Theft Prevention Program was developed using the guidance provided by the Federal Trade Commission (FTC) "Red Flags Rule," found in 16 C.F.R. 681, and was reviewed and approved by the Audit Committee of the Rice University Board of Trustees on September 16, 2009.

II. Definitions

"Covered Account" means (i) an account the University offers or maintains primarily for personal, family or household purposes, that involves or is designed to permit multiple payments or transactions, including applicable student accounts or loans that are administered by the University and (ii) 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.

"Customer" means any staff or faculty member, student, parent or other person with a "Covered Account."

"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, date of birth, government issued driver's license or identification number, alien registration number, passport number, employer or taxpayer identification number, unique electronic identification number, or computer Internet Protocol address or routing code.

"Identity Theft" means fraud committed or attempted using the Identifying Information of another person without authority.

"Program Administrator" means the individual charged by the Vice President of Finance to administer the Identity Theft Prevention Program and manage reports of red flags.

"Red Flag" means a pattern, practice or specific activity that indicates the possible existence of identity theft.

III. Elaboration of Policy

a. Identifying "Red Flags" for Identity Theft

In order to identify relevant red flags, the University considers the types of Covered Accounts that it offers, the methods it provides to open and access accounts and its previous experiences with Identity Theft. The most common red flags to be aware of, and monitor for, are:

1. suspicious or altered documents,
2. suspicious emails requesting information,
3. suspicious or inconsistent personal identifying information,
4. suspicious covered account activity or unusual use of account,
5. notifications and warnings from credit reporting agencies, and
6. alerts or notices from other entities or individuals.

b. Mitigating the Risk of Identity Theft

All university personnel should remain vigilant for the signs of Identity Theft. When an individual detects or suspects a “red flag” is present, that individual should notify his or her supervisor and the Program Administrator. The Program Administrator will take the necessary steps to monitor and mitigate the situation.

c. Administering the Identity Theft Prevention Program

Responsibility for developing, implementing and updating this program lies with the Identity Theft Committee (“Committee”) for the University, which is appointed by and reports to the Vice President for Finance.

At a minimum, the Identify Theft Program must include reasonable policies and procedures to identify, detect, and respond to Red Flags pertaining to Covered Accounts. The Program shall, as appropriate, incorporate existing university policies and procedures and existing internal controls. University staff responsible for implementing the program shall be trained in the detection and mitigation of Red Flags. The Committee should meet at least annually (or more frequently as may be necessary), and with the Program Administrator, will be responsible for:

1. identifying individuals who require training,
2. creating and delivering that training, and tracking completion of the training;
3. reviewing any reports regarding the detection of red flags and the steps for preventing and mitigating Identity Theft related to Covered Accounts,
4. determining, in consultation with the Office of General Counsel, which steps of prevention and mitigation should be taken in particular circumstances, and
5. considering periodic changes to the program to respond to emerging risks.

IV. Cross References to Related Policies

Protection of Personally Identifiable Information, (808)
Payment Policy (840)

V. Responsible Official and Key Offices to Contact Regarding the Policy and its Implementation

Responsible Official:	Vice President of Finance
Key Offices:	Controller, Information Technology, Human Resources, Financial Aid, Housing and Dining

VI. Links to Additional Information

The FTC’s “Red Flags Rule” regulations are at 16 C.F.R. 681, and the FTC has provided guidance on those regulations at “Fighting Identity Theft with the Red Flags Rule: A How-To Guide for Business.”

*Signed David W. Leebron*_____________
President

Policy History
Issued: August 1, 2016