University of Hawai‘i FTC Red Flags Rule Identity Theft Prevention Program
Creation Approved by the UH Board of Regents on April 16, 2009

I. Program Adoption

The University of Hawai‘i ("UH" or "University") developed this FTC Red Flags Rule Identity Theft Prevention Program ("Program") pursuant to the Federal Trade Commission's Red Flags Rule, 16 CFR Part 681 ("Rule"), which implements Section 114 of the Fair and Accurate Credit Transactions Act of 2003. This Program was developed with oversight and approval of the University of Hawai‘i Board of Regents. After consideration of the size and complexity of the UH System and the nature and scope of its activities, the Board determined that this Program was appropriate for the UH System, and therefore approved the creation of this Program on April 16, 2009. This Program shall apply to all campuses and activities of the UH System.

II. Purpose and Elements

The purpose of this policy is to establish an Identity Theft Prevention Program designed to detect, prevent and mitigate identity theft in connection with the opening of a covered account and to provide for continued administration of the Program. This Program should be carried out in conjunction with the existing UH Executive Policy, E2.214 on the Security and Protection of Sensitive Information, which provides comprehensive guidelines for information security. This Program supplements the existing Executive Policy to comply with the Red Flags Rules, which requires the University to adopt an Identity Theft Protection Program containing specific elements. The Program shall include reasonable policies and procedures to:

A. Identify relevant red flags for covered accounts offered or maintained by the University and incorporate those red flags into the Program;
B. Detect red flags that have been incorporated into the Program;
C. Respond appropriately to any red flags that are detected to prevent and mitigate identity theft; and
D. Ensure the Program is updated periodically to reflect changes in risks to students and other holders of covered accounts and the safety and soundness of the University from identity theft.

The Program shall, as appropriate, incorporate other existing policies and procedures that control reasonably foreseeable risks.

III. Definitions

"Identity Theft" is a fraud committed or attempted using the identifying information of another person without authority.

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

"Covered Account" is a continuing relationship established by an individual with the University in which the University extends credit to the individual to obtain goods or services, or accepts a deposit from the individual, primarily for personal, family or household purposes, and that involves or is designed to permit multiple payments or transactions.

"Committee" means an Identity Theft Program Committee comprised of the Vice President for Budget & Finance/Chief Financial Officer, the Vice President for Information Technology Services/Chief Information Officer, the Vice President for Student Affairs, and the Vice President for Administration, or their respective designees.

IV. Covered Accounts

The University has identified three types of Covered Accounts:

A. Tuition and Mandatory Student Fees Installment Payment Plan;
B. Student Loans;
C. Services, Rentals, and Miscellaneous Fees, such as medical services, childcare services, facility rentals and use, parking, faculty housing rentals, etc.
D. University Programs providing debit card-like services

The University shall periodically review this list and identify any other Covered Accounts offered by the University, which shall be incorporated into this Program.

V. Identification of Relevant Red Flags

In order to identify relevant Red Flags, the University considers the types of accounts that it offers and maintains, methods it provides to open its accounts, methods it provides to access its accounts, and its previous experiences with Identity Theft. The University will take reasonable steps to identify all persons seeking to open or use a Covered Account, such as requiring a photo ID card, requesting a service in writing, etc., as appropriate based on the nature of the transaction.

The University identifies the following Red Flags:

A. Suspicious Documents, i.e., identification documents appear to have been altered or forged or identification documents or card on which a person's photograph, signature or physical description is not consistent with the person presenting the document.
B. Suspicious Personal Identifying Information, i.e., identifying information presented is inconsistent with other information the student provides or with other sources of information; Social Security Number presented is the same as one given by another person; or an address or phone number presented is the same as that of another person.
C. Suspicious Covered Account Activity or Unusual Use of Account, i.e., change of address for an account followed by a request to change the student's name; payments stop on an otherwise consistently up-to-date account; or account used in a way that is not consistent with prior use.

D. Alerts from Others, i.e., report of fraud accompanying a credit report; notice to the UH System from another student, identity theft victim, law enforcement agent or others that the UH System is maintaining a fraudulent account for a person engaged in identity theft.

VI. Response to Detected Red Flags

The Program shall provide for appropriate response to detected red flags to prevent and mitigate identity theft commensurate with the degree of risk posed. In determining an appropriate response, the University shall consider any aggravating factors that may heighten the risk of identity theft. Appropriate responses to the relevant red flags include, but are not limited to the following:

A. Deny access to the Covered Account until other information is available to eliminate the red flag;
B. Monitor a Covered Account for evidence of identity theft;
C. Contact the affected student, staff member, faculty member, or other individual;
D. Change any passwords, security codes or other security devices that permit access to a Covered Account;
E. Prevent the opening of a new Covered Account;
F. Not attempt to collect on a Covered Account that is determined to have been fraudulently established;
G. Notify law enforcement; or
H. Determine no response is warranted under the particular circumstances.

VII. Program Administration

Responsibility for developing, implementing and updating this Program lies with the Committee. The Committee will periodically review and update the Program after review of the University's experiences with identity theft, changes in identity theft methods, changes in identity theft detection and prevention methods, and changes in types of accounts the University maintains.

The Committee shall oversee the establishment and implementation of training programs for staff members responsible for implementing the Program. Members of the Committee shall ensure that the University exercises appropriate and effective oversight of service provider arrangements within their respective areas. The Committee shall report at least annually to the President or the President's designee, who shall be at the level of senior management, on compliance with this Program.

This Program is intended to comply with the Red Flags Rule, including the Interagency Guidelines appended thereto, and shall be interpreted and applied accordingly.