UNIVERSITY OF CALIFORNIA, MERCED

Red Flag and Security Incident Reporting Policy

RESPONSIBLE OFFICIAL : Executive Vice Chancellor/Provost

RESPONSIBLE OFFICIAL : Business & Financial Services

EFFECTIVE DATE : November 1, 2009

REVISION NUMBER : Original

NUMBER OF PAGES : 5 pages

REFERENCES AND RESOURCES:

1. Part 681 of the Code of Federal Regulations implementing Sections 114 and 115 of the Fair and Accurate Credit Transactions Act (FACTA) of 2003;

2. Federal Trade Commission' "Red Flag Requirements" issued in the Federal Register (72 FR 63718) finalizing *The Identity Theft Red Flags Rule (Rule)*, November 9, 2007;

3. The University of California Identity Theft Prevention "Red Flags Rule" Plan adopted by The Regents January 7, 2009;

SUMMARY OF POLICY (PURPOSE)

Pursuant to the Federal Trade Commission's Red Flags Rule (Rule), which implements Section 114 of the Fair and Accurate Credit Transactions Act of 2003, The Regents of the University of California have adopted a systemwide Identity Theft Prevention Implementation Plan (Plan). Under the Plan, each campus is responsible to:

- Identify and document those processes that meet the criteria of Covered Accounts or otherwise are subject to the Rule.
- Identify the controls in place to detect, prevent, and mitigate Identity Theft.
- Review the Plan and then supplement it with written campus-specific actions and plans.
- Review and update the campus specific actions and plans annually.

The purpose of this policy is to establish the departmental requirements and outline mechanisms to prevent, detect, and respond to Identity Theft where the University

acts as either a Creditor or a financial institution in connection with Covered Accounts as defined under the Rule. The ultimate goal is the detection, prevention, and mitigation of Identity Theft.

DEFINITION(S)

Covered Account means a University business account that a department or unit of UC MERCED functioning as a Creditor offers or maintains for the benefit of faculty, staff or students or members of the public, primarily for the personal, family, or household purposes of the individual that involves or is designed to permit multiple payments or transactions. These are accounts where payments are deferred and made by a borrower periodically over time.

Creditor means with respect to the University a UC MERCED department, unit or function that regularly extends, renews, or continues credit and any person or any UC MERCED department, unit or function that regularly arranges for the extension, renewal, or continuation of credit.

Identity Theft, for the purpose of this policy, means fraud committed or attempted using the Identifying Information of another person without that person's knowledge or consent.

Identifying Information, for the purposes of this policy, means any name or number that may be used, alone or in conjunction with any other information to identify a specific person, including any –

1. Name, Social Security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number;

2. Unique biometric data, such as fingerprints, voice print, retina or iris image, or other unique physical representation;

3. Unique electronic identification number, address, or routing code; or

4. Telecommunication Identifying Information or access device (as defined in 18 U.S.C 1029(e)).

Medical Identity Theft means fraud committed or attempted using the Identifying Information of another, without that person's knowledge or consent, to obtain medical services or goods or to make false claims for medical services or goods.

Red Flag means a pattern, practice, or specific activity that indicates the possible existence of Identity Theft. Examples of "Red Flags" include alerts from credit agencies, presentation of suspicious documents, discrepancies in known facts (address, Social Security Number or other information on file), suspicious account activity, or notices from others about possible Identity Theft.

Workforce means all faculty, staff, students, trainees, volunteers, and business associates (including third party vendors) who access or may have access to restricted or confidential information during the course of their duties.

STATEMENT

All UC Merced departments that work with Covered Accounts are required to comply with the following:

A. Implementation of the Department Plan and Training

1. Each department must develop and implement a written plan that specifies administrative controls to prevent, detect, and respond to (investigate and mitigate) Red Flag warnings in connection with the opening of a Covered Account or the administration of any existing Covered Account. A listing of UC MERCED departments that have been initially identified as having Covered Accounts is attached as Attachment A (this list is current as of the issuance date of this policy).
2. All departments must periodically determine whether they offer or maintain any Covered Accounts and, if so, they must develop an implementation plan in accordance with this policy, in the format set forth in Attachment B.
3. Each UC MERCED department head or designee whose department has Covered Accounts shall conduct an annual risk assessment to review methods used to open Covered Accounts, methods used to access accounts, previous experience with Identity Theft or Medical Identity Theft, and any new risks or threats that have emerged since the last review. Each department is responsible for documenting its controls, developing a written plan to mitigate against Identity Theft or Medical Identity Theft, training its Workforce regarding Red Flags and the departmental plan and controls, and ensuring that the Workforce is aware of the departmental plan and the controls so that they may effectively carry these out. Plans, controls, and training should be reviewed and updated annually. Attachment B provides a template that must be used by departments to document their plans and controls.
4. Each department must become familiar with this policy, the UC Identity Theft Prevention “Red Flags Rule” Implementation Plan, and the implementation plan developed for their own UC MERCED department.

B. Monitoring Activity

As part of their Identity Theft prevention program, departments shall monitor activity for the detection of Red Flags. A complete listing of potential Red Flags identified by the Federal Trade Commission is attached as Attachment C. Red Flags generally fall into one of the following broad categories:

Alerts - alerts, notifications, or warnings from a consumer reporting agency including fraud alerts, credit freeze alerts, or official notice of address discrepancy.

Suspicious documents - such as those appearing to be forged or altered, or where the photo ID does not resemble its owner, or an application which appears to have been cut-up, re-assembled and photocopied.

Suspicious personal Identifying Information - such as discrepancies in address, Social Security Number, or other information on file.

Unusual use of, or other suspicious account activity - such as material changes in payment patterns, notification that the account holder is not receiving mailed statements or that the account has unauthorized charges.

Notice from others indicating possible Identity Theft - such as the institution receiving notice from the victim of Identity Theft, law enforcement, or another account holder reports that a fraudulent account was opened.

C. Reporting Incidents

Detection of Red Flags in connection with the opening of Covered Accounts as well as existing Covered Accounts can be made through such methods as:

Obtaining and verifying identity

Authenticating customers

Monitoring transactions

1. The detection of a Red Flag by members of the Workforce shall be reported to a manager or supervisor and other appropriate administrators as defined in the control procedures developed by the department. If it appears that there has been an instance of Identity Theft, the department head should report this to the UC Police Department, Office of Insurance and Risk Management, and the department's designated Security Breach Coordinator. Health System employees should report suspected or detected Medical Identity Theft in accordance with the procedures set forth in the UC MERCED Health System *Identity/Medical Identity Theft Prevention and Response Policy.*

2. A department remains responsible for compliance with the Rule even if it outsources operations to a third party service provider. The written agreement between the University and the third party service provider shall require the third party service provider to have reasonable policies and procedures designed to detect relevant Red Flags that may arise in the performance of the service provider's activities and to prevent or mitigate Identity Theft or Medical Identity Theft.
3. All members of the Workforce who process any information related to Covered Accounts shall receive training following their initial appointment on the Rule, Red Flags, and the department's controls and plan for detecting and mitigating Identity Theft or Medical Identity Theft.
4. The Campus Ethics and Compliance Committee will conduct a compliance review on an annual basis to ensure that overall campus plans and controls are current and operating effectively.

V. RESPONSIBILITIES

Department heads with Covered Accounts are ultimately responsible for the deployment and maintenance of their respective department implementation plan. Additionally, department heads are responsible for ensuring that Identity Theft risks are assessed annually, that responsibilities for overseeing the implementation program and monitoring for Red Flag activity are assigned, that the affected Workforce has been properly trained, and that the department's implementation plan complies with this Policy including annual review and update as required.

The Executive Vice Chancellor/Provost or designee shall act as the UC MERCED Red Flags Rule Policy Coordinator and is responsible for coordinating actions of individual departments, reviewing risk assessments, answering questions about responsibilities, including questions about the Red Flags Rule requirements or the UC Implementation Program or referring such questions to counsel.

UC MERCED departments with Covered Accounts shall conduct annual risk assessments to review methods used to open Covered Accounts, methods used to access accounts, previous experience with Identity Theft or Medical Identity Theft, and any new risks or threats that have emerged since the last review.

The Workforce shall be familiar with this policy, participate in mandatory training, be familiar with and understand their department implementation plan, and ensure that they are compliant with the department implementation plan.

VI. ATTACHMENTS

A. Merced Inventory of Covered Accounts

B. of California, Merced Identity Theft Prevention "Red Flags Rule" Implementation Plan Template

C. "Red Flags" as Identified by the Federal Trade Commission