UCLA Policy 313: Prevention of Identity Theft

Issuing Officer:	Executive Vice Chancellor and Provost
Responsible Dept:	Business & Finance Solutions
Effective Date:	July 29, 2009
Supersedes:	New

I. REFERENCES

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" Implementation Plan adopted by The Regents January 7, 2009;
4. UCLA Health System *Identity/Medical Identity Theft Prevention and Response Policy*.

II. 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.

III. DEFINITIONS

Covered Account means a University business account that a department or unit of UCLA 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 UCLA department, unit or function that regularly extends, renews, or continues credit and any person or any UCLA 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.

IV. STATEMENT

All UCLA 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 UCLA 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 UCLA 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 UCLA 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 UCLA 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 Associate Vice Chancellor, Business & Finance Solutions/Controller or designee shall act as the UCLA 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.

UCLA 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. UCLA Inventory of Covered Accounts, as of August 1, 2009.
B. University of California, Los Angeles Identity Theft Prevention "Red Flags Rule" Implementation Plan Template.
C. Possible "Red Flags", as identified by the Federal Trade Commission.

Issuing Officer

/s/ Scott L. Waugh

Executive Vice Chancellor & Provost

Questions concerning this policy or procedure should be referred to the Responsible Department listed at the top of this document.

UCLA Inventory of Covered Accounts

As of August 1, 2009

Proposed additions or amendments to this listing may be requested by contacting Business & Finance Solutions.

Department/Sub-Department	Description of Covered Accounts
Campus Human Resources/Benefits	Collection of Employee Benefits Premiums
Business & Finance Solutions/Payroll	Salary Overpayments Payroll Advances
Business & Finance Solutions/Student Financial Services	Student Billing and Receivables BruinCard
Graduate Division/ Graduate Student Support	Fee Tuition/Remission Fellowships TA Advance Loans
Graduate Division/Office of Postdoctoral and Visiting Scholar Services	Fellowships
Health Systems/FPG Ambulatory Clinical Practices	Insurance Card Medical Record
Health Systems/FPG Billing Office	Professional Billing Account
Health Systems/Medical Center/Admissions and Registration	Patient Admission and Registration
Health System Cashiering Services	Payment for Services and Billing Inquiries
Health Systems/Medical Center/Patient Business Services	Patient Account for Payment of Services
Housing and Hospitality Services	Housing/Student Housing Account Faculty Rental/Faculty Housing Account Dining Services/Student Housing Account Lake Arrowhead Conference Center/Hotel Guest Account Guest House/Hotel Guest Account Conferences & Catering/Internal/External Guest Account
School of Dentistry, Billing Office	Professional Billing Account
Student Affairs/Arthur Ashe Student Health and Wellness Center	Income accounts for patient services Verification of patient identity at point of service
Student Affairs/Financial Aid Office	Student Financial Aid (including scholarships, fellowships, Perkins Loans)
Student Affairs/Student Loan Services and Collections	Short-Term Loans Long-Term Student Loans Student Billing and Receivables Accounts Non-BAR Accounts Receivable Credit Card Data (related to payments received toward covered accounts) Credit Bureau Data
Student Affairs/Counseling and Psychological Services	Student Mental Health Treatment Record
University Extension/Division of Continuing Education	UCLA Extension Student Records UCLA Extension Client Accounts UCLA Extension Continuing Education of the Bar Client Accounts

University of California, Los Angeles
Identity Theft Prevention "Red Flags Rule" Implementation Plan Template

Note: Once an Implementation Plan is completed, it is to be considered a confidential document and not for public disclosure. Employees who prepare the plan or have access to it must take appropriate steps to ensure that the data therein is securely maintained.

This Implementation Plan is submitted in compliance with Part 681 of the Code of Federal Regulations implementing Sections 114 and 315 of the Fair and Accurate Credit Transactions Act (FACTA) of 2003, pursuant to the Federal Trade Commission's Red Flags Rule ("Rule"), and in accordance with the University of California Identity Theft Prevention "Red Flags Rule" Implementation Plan, and the University of California, Los Angeles Identity Theft Prevention "Red Flags Rule" Implementation Plan (UCLA Implementation Plan).

This Plan establishes departmental requirements and guidelines pursuant to the UCLA Implementation Plan including:

- Clearly identifying and documenting Covered Accounts.
- Establishing sources to identify Red Flags.
- Identifying the controls to detect, prevent and mitigate Identity Theft.
- Providing employee training.
- Ensuring compliance by third party service providers.

Department Name: _____

1) **Covered Accounts:** The matrix attached to the UCLA Implementation Plan identifies the accounts covered by the Red Flag Rules. The Matrix will be updated periodically.

2) **Identified Red Flags:**

   a) Notifications and Warnings:

   b) Suspicious Documents:

   c) Unusual Use of Accounts:

   d) Suspicious Identifying Information:

3) **Detection of Red Flags:** The following actions will be taken to verify identity, authenticate customers, monitor transactions, and/or verify the validity of address changes:

4) **Mitigation of Identity Theft:**

5) **On-Going Oversight and Plan Review:**

6) Third Party Contract Compliance:

7) **Employee Training:**

Submitted by: _____ **Title:** _____

Date: _____

Red Flags Rule Covered Accounts Inventory Matrix Template

Department Name: _____

Date: _____

Department/Sub-Department	Description of Covered Account
(e.g., Business & Finance Solutions/Student Financial Services)	(e.g., BruinCard)

University of California, Los Angeles

Identity Theft Prevention "Red Flags Rule" Implementation Plan Template

Red Flag Regulation Compliance
Campus - Effective <date>

Identified Account	Responsible Dept/Individual	Relevant Red Flags	Detection Mechanism	Response Required	Resolution	Oversight	Program Update	Sr Mgmt Sign-Off	Staff Training	3rd Party Comply
Covered Account A		Verify ID for alteration or forgery	View identification	Notify mgmt, no assistance	Retain card, report	Fraudulent activity - report to Director	Review and update annually	AVC	Annually	N/A
		Verify the ID picture matches the customer	View identification	Notify mgmt, no assistance	Retain card, report	Fraudulent activity - report to Director	Review and update annually	AVC	Annually	N/A
		Verify information on ID is consistent with information on file	View identification	Notify mgmt, no assistance	Retain card, report	Fraudulent activity - report to Director	Review and update annually	AVC	Annually	N/A
Sample Detailed steps for a covered account		Verify requests for information updates are not altered, forged, or destroyed and reassembled	Scrutinize paperwork submitted	Notify mgmt, no assistance	Retain paperwork, require new	Fraudulent activity - report to Director	Review and update annually	AVC	Annually	N/A
		No information shared if FERPA restriction	FERPA flag in BAR	No assistance	No assistance	Fraudulent activity - report to Director	Review and update annually	AVC	Annually	N/A
		UID matches another customer.	System pulls up two identities	Notify mgmt, no assistance	Investigate and resolve with management	Fraudulent activity - report to Director	Review and update annually	AVC	Annually	N/A
		Account is not consistent with regular patterns of activity	Large deposits, rapid depletion of funds	Notify mgmt, no assistance	Investigate and resolve with management	Fraudulent activity - report to Director	Review and update annually	AVC	Annually	N/A
		Call or email if mail is returned twice	Return mail documentation 448 screen	Notify mgmt	Investigate and resolve with management	Fraudulent activity - report to Director	Review and update annually	AVC	Annually	N/A
		Three different address changes in the past ninety (90) days.	Return mail documentation 448 screen	Notify mgmt	Investigate and resolve with management	Fraudulent activity - report to Director	Review and update annually	AVC	Annually	N/A
		No information on an account if no UID and customer name	Customer reports via phone, email, in person	Notify mgmt, no assistance	Notify mgmt, no assistance	Fraudulent activity - report to Director	Review and update annually	AVC	Annually	N/A
		No response regarding medical type services	Customer reports via phone, email, in person	No assistance	No assistance	Fraudulent activity - report to Director	Review and update annually	AVC	Annually	N/A
Covered Account B										

Possible "Red Flags" as Identified by the Federal Trade Commission

The Federal Trade Commission supplement to the regulation identifies 26 possible red flags. These red flags are not a checklist, but rather, are examples that financial institutions and creditors may want to use as a starting point.

Alerts, Notifications or Warnings from a Consumer Reporting Agency

1. A fraud or active duty alert is included with a consumer report.
2. A consumer reporting agency provides a notice of credit freeze in response to a request for a consumer report.
3. A consumer reporting agency provides a notice of address discrepancy, as defined in §681.1(b) of the regulations.
4. A consumer report indicates a pattern of activity that is inconsistent with the history and usual pattern of activity of an applicant or customer, such as:
    a. A recent and significant increase in the volume of inquiries;
    b. An unusual number of recently established credit relationships;
    c. A material change in the use of credit, especially with respect to recently established credit relationships; or
    d. An account that was closed for cause or identified for abuse of account privileges by a financial institution or creditor.

Suspicious Documents

5. Documents provided for identification appear to have been altered or forged.
6. The photograph or physical description on the identification is not consistent with the appearance of the applicant or customer presenting the identification.
7. Other information on the identification is not consistent with information provided by the person opening a new covered account or customer presenting the identification.
8. Other information on the identification is not consistent with readily accessible information that is on file with the financial institution or creditor, such as a signaturecard or a recent check.
9. An application appears to have been altered or forged, or gives the appearance of having been destroyed and reassembled.

Suspicious Personal Identifying Information

10. Personal identifying information provided is inconsistent when compared against external information sources used by the financial institution or creditor. For example:
    a. The address does not match any address in the consumer report; or
    b. The Social Security Number (SSN) has not been issued, or is listed on the Social Security Administration's Death Master File.
11. Personal identifying information provided by the customer is not consistent with other personal identifying information provided by the customer. For example, there is a lack of correlation between the SSN range and date of birth.
12. Personal identifying information provided is associated with known fraudulent activity as indicated by internal or third party sources used by the financial institution or creditor. For example:
    a. The address on an application is the same as the address provided on a fraudulent application; or
    b. The phone number on an application is the same as the number provided on a fraudulent application.`
13. Personal identifying information provided is of a type commonly associated with fraudulent activity as indicated by internal or third-party sources used by the financial institution or creditor. For example:
    a. The address on an application is fictitious, a mail drop, or a prison; or
    b. The phone number is invalid, or is associated with a pager or answering service.

14. The SSN provided is the same as that submitted by other persons opening an account or other customers.
15. The address or telephone number provided is the same as or similar to the account number or telephone number submitted by an unusually large number of other persons opening accounts or other customers.
16. The person opening the covered account or the customer fails to provide all required personal identifying information on an application or in response to notification that the application is incomplete.
17. Personal identifying information provided is not consistent with personal identifying information that is on file with the financial institution or creditor.
18. For financial institutions and creditors that use challenge questions, the person opening the covered account or the customer cannot provide authenticating information beyond that which generally would be available from a wallet or consumer report.

Unusual Use of, or Suspicious Activity Related to, the Covered Account

19. Shortly following the notice of a change of address for a covered account, the Institution or creditor receives a request for a new, additional, or replacement card or a cell phone, or for the addition of authorized users on the account.
20. A new revolving credit account is used in a manner commonly associated with known patterns of fraud patterns. For example:
    a. The majority of available credit is used for cash advances or merchandise that is easily convertible to cash (e.g., electronics equipment or jewelry); or
    b. The customer fails to make the first payment or makes an initial payment but no subsequent payments.
21. A covered account is used in a manner that is not consistent with established patterns of activity on the account. There is, for example:
    a. Nonpayment when there is no history of late or missed payments;
    b. A material increase in the use of available credit;
    c. A material change in purchasing or spending patterns;
    d. A material change in electronic fund transfer patterns in connection with a deposit account; or
    e. A material change in telephone call patterns in connection with a cellular phone account.
22. A covered account that has been inactive for a reasonably lengthy period of time is used (taking into consideration the type of account, the expected pattern of usage and other relevant factors).
23. Mail sent to the customer is returned repeatedly as undeliverable although transactions continue to be conducted in connection with the customer's covered account.
24. The financial institution or creditor is notified that the customer is not receiving paper account statements.
25. The financial institution or creditor is notified of unauthorized charges or transactions in connection with a customer's covered account.

Notice from Customers, Victims of Identity Theft, Law Enforcement Authorities, or Other Persons Regarding Possible Identity Theft in Connection With Covered Accounts Held by the Financial Institution or Creditor

26. The financial institution or creditor is notified by a customer, a victim of identity theft, a law enforcement authority, or any other person that it has opened a fraudulent account for a person engaged in identity theft.