Identity Fraud Prevention and Response

Responsible Executive: Linda Morris Williams
Associate Chancellor
Chief Ethics and Compliance Officer

Responsible Office: Chancellor’s Office

Contact: Barbara VanCleave Smith
Director of Controls, Accountability and Risk Management
Interim Campus Representative for Red Flags Rule
643-4171, carmo@berkeley.edu

Policy Statement

The University of California, Berkeley will strive to prevent identity fraud on campus and will respond appropriately when attempts at identity fraud are discovered.

Who Is Affected by This Policy

Departments that engage in financial transactions with students and employees

Who Administers This Policy

Campus Ethics and Compliance Officer
Campus Representative for Red Flags Rule
Departments that engage in financial transactions with students and employees
UC Police
Why We Have This Policy

Identity *fraud* follows identity *theft*: first someone steals another individual’s personal information, then tries to use that stolen personal information to obtain money, goods, or other advantages. The campus has always had procedures and controls in this area, but due to recent changes in federal law, departments that engage in certain financial transactions with students and employees must now systematically look for so-called “red flags” indicating possible identity fraud.

The recent changes in federal law can be found in the Federal Trade Commission's (“FTC”) Red Flags Rule, which implements Section 114 of the *Fair and Accurate Credit Transactions Act of 2003*. Under the FTC’s Red Flags Rule, the campus is required to establish an Identity Fraud Prevention Program that contains policies and procedures to:

1. Identify potential red flags for covered accounts;
2. Create an Identity Fraud Prevention Program to prevent or mitigate the effects of identity fraud;
3. Detect red flags;
4. Respond appropriately to red flags;
5. Ensure the Identity Fraud Prevention Program is updated periodically to reflect changes in risks to account holders.

The Red Flags Rule applies to accounts that involve multiple payments or transactions, such as a loan or account that is billed or payable monthly. At UC Berkeley, this definition covers student accounts and loans and employee loans. However, as a matter of good business practice, the campus is applying this policy to all campus accounts, not just to accounts covered by the FTC definition.
Responsibilities

Compliance, Accountability, Risk and Ethics Committee (CARE):
- Oversees the campus Red Flags Program.
- Maintains oversight for
  - Ensuring appropriate training of campus staff on the Red Flags Program.
  - Reviewing reports regarding the detection of red flags and the steps for preventing and mitigating identity fraud.
  - Determining which steps of prevention and mitigation should be taken in particular circumstances and considering periodic changes to the plan.

Chief Ethics and Compliance Officer (CECO):
- At least quarterly, reports to the Compliance, Accountability, Risk and Ethics Committee (CARE) on compliance with this policy.
- Considers periodic changes to the Identity Fraud Prevention and Response Program (Red Flags Program) and recommends them to CARE.

Campus Representative for Red Flags Rule:
- Notifies the CECO of any real or suspected instance of identity fraud or of the campus’s failure to comply with this policy.
- Updates inventory of “covered accounts” as required by the University of California Office of the President.
- Trains campus staff in this policy.
- Periodically reviews mechanisms to prevent and mitigate identity fraud and recommends changes to the CECO and CARE.

Campus Units engaging in financial transactions with students or employees:
- Review staff reports regarding the detection of red flags and steps for preventing and mitigating identity fraud.
- Determine which prevention and mitigation steps should be taken in particular circumstances.
- Notify the Campus Representative for Red Flags Rule when a real or suspected instance of identity fraud occurs.

UC Police Department:
- Investigates real or suspected incidents of identity fraud.
Procedures

These procedures comprise the campus’s Identity Fraud Prevention and Response Program.

I. Identification of Red Flags

To identify red flags indicating a possible attempt at identity fraud, the campus considers:

- the types of accounts offered and maintained;
- the methods provided to open accounts;
- the methods provided to access accounts; and
- previous experiences with identity fraud.

The campus has identified the following red flags that may indicate an individual’s identity was compromised:

A. Alerts from Others

Notice to the campus from an account holder, identity fraud victim, law enforcement agency, or other that the campus has opened or is maintaining an account for a person engaged in identity fraud.

B. Suspicious Documents

1. Identification document or card that appears to be forged, altered, or inauthentic;
2. Identification document or card on which a person’s photograph or physical description is inconsistent with the person presenting the document;
3. Other document with information inconsistent with account holder information on file;
4. Application for service that appears to have been altered or forged.

C. Suspicious Personal Identifying Information

1. Identifying information inconsistent with identifying information on file;
2. Identifying information inconsistent with other information provided by the account holder (example: inconsistent birth dates);
3. Identifying information inconsistent with other sources of information (for instance, giving an address that does not match the address on a loan application);
4. Identifying information the same as identifying information on other documents found to be fraudulent;
5. Identifying information typical of fraudulent activity (such as an invalid phone number or non-existent billing address);
6. Social security number the same as that of another person;
7. Address or phone number the same as that of another person;
UNIVERSITY OF CALIFORNIA, BERKELEY
Policy on Identity Fraud Prevention and Response

8. Failure to provide complete personal identifying information on an application when reminded to do so.

D. Suspicious Account Activity or Unusual Use of Account

1. Change of address for an account followed by a request to change the account holder’s name;
2. Payment stop on an otherwise consistently up-to-date account;
3. Account used in a way that is not consistent with prior use;
4. Mail to the account holder repeatedly returned as undeliverable;
5. The account holder reports to the campus that he or she is no longer receiving mail sent by the campus;
6. Notice to the campus that an account has unauthorized activity;
7. Breach in the campus’s computer system security;
8. Unauthorized access to or use of account information.

E. Notifications and Warnings from Credit Reporting Agencies

1. Report of fraud accompanying a credit report;
2. Notice or report from a credit agency of a credit freeze on an applicant;
3. Notice or report from a credit agency of an active duty alert for an applicant;
4. Receipt of a notice of address discrepancy in response to a credit report request;
5. Indication from a credit report of activity inconsistent with an applicant’s usual pattern of activity.

F. Additional Red Flags

The campus recognizes that additional red flags may be identified for specific types of accounts.

II. Detecting Red Flags

A. Establishing an Individual’s Identity

A student’s identification is established during the admission process and culminates in an official identification card containing the student’s picture, identification number, and signature sample.

An employee’s identification is established through the I-9 process and culminates in an official identification card containing the employee’s picture, identification number, and signature sample.

B. Checking an Individual’s Identity

Each unit develops its own methodology to detect red flags based upon its business needs and the nature of its interactions with students and employees.
To maintain this policy’s effectiveness, knowledge about specific red flag identification, detection, mitigation, and prevention practices are limited to employees with a need to know them. The contents of documents that list or describe such practices should not be shared with other campus employees or the public.

III. Preventing and Mitigating Identity Fraud

Campus personnel who detect red flags must take one or more of the following steps, depending on the degree of risk posed by the red flag:

1. Request additional documentation to validate identity;
2. Continue to monitor the covered account for evidence of identity fraud;
3. Contact the account holder or applicant;
4. Change passwords or other security features that permit access to the account;
5. Not open a new account;
6. Close an existing account;
7. Provide the account holder with a new student or staff identification number;
8. Notify the program administrator for determination of the appropriate step(s) to take;
9. Notify law enforcement;
10. File or assist in filing a Suspicious Activities Report ("SAR") with the Campus Representative for Red Flags Rule; or
11. Determine that no response is warranted under the circumstances.

IV. “Service Provider” Compliance

In the event a campus unit engages a service provider to perform an activity in connection with one or more accounts, the campus unit takes the following steps to ensure that the service provider performs its activity in accordance with this policy:

1. Require, by contract, that service providers have their own policies and procedures in place to respond to red flags; and
2. Require, by contract, that service providers review the University’s Identity Fraud Prevention Program and report any real or suspected red flags to the appropriate campus office.

V. Training

The Campus Representative for Red Flags will ensure that campus staff is trained to prevent, detect, and respond to identity fraud. Red flag training should be incorporated into existing training programs for personnel who work with accounts or account holders.

VI. Reporting

Attempts at identity fraud should be reported immediately to the Campus Representative for Red Flags Rule.
At least quarterly, or as otherwise requested by the Chief Ethics and Compliance Officer (CECO), the Campus Representative for Red Flags reports to the CECO on compliance with this policy. The report must address such issues as:

1. Effectiveness of the policies and procedures in addressing the risk of identity fraud;
2. Significant incidents involving identity fraud and the response;
3. Recommendations for changes to the program.

**Web Site Address for This Policy**

http://campuspol.chance.berkeley.edu/policies/identityfraud.pdf

**Glossary**

**Covered Account:** an account that involves multiple payments or transactions, such as a loan or account that is billed or payable monthly. At UC Berkeley this definition would include student accounts and loans and employee loans.

**Fraud:** a false representation of a matter of fact intended to deceive another.

**Identity Fraud:** fraud committed or attempted using the identifying information of another person without authority.

**Identity Theft:** taking a person’s identifying information without permission.

**Identifying Information:** any name or number that may be used, alone or in conjunction with 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, government passport number, employer or taxpayer identification number, student identification number, computer Internet Protocol address, or routing code.

**Red Flag:** a pattern, practice, or specific activity that indicates the possible existence of identity fraud.

**Related Documents**

[Fair and Accurate Credit Transactions Act of 2003](http://campuspol.chance.berkeley.edu/policies/identityfraud.pdf)

The University of California Identity Theft Prevention “Red Flags Rule” Implementation Plan