# Red Flag Regulation Implementation at UCLA
# Student Financial Services

In November 2007, final rules implementing section 114 of the Fair and Accurate Credit Transactions Act of 2003 were issued by the Federal Trade Commission ("FTC"), the federal bank regulatory agencies, and the National Credit Union Administration ("NCUA"). A joint notice of final rulemaking was published in the Federal Register (72 FR 63718) finalizing *the Identity Theft Red Flags Rule* ("the Rule"). The Rule was issued with the underlying goal of detecting, preventing, and mitigating identity theft "in connection with the opening of certain accounts or existing accounts," referred to as "*covered accounts*."

Red Flags are defined by the Rule as those events which should alert an organization that there is a risk of identity theft. The Rule supplements existing legislation aimed at preventing identify theft through tightened data security (e.g., Gramm-Leach-Bliley) by addressing situations where individuals are trying to use another person's identity in order to fraudulently obtain resources or services. Institutions are to identify Red Flags to alert to and intervene against the possibility of such attempts.

## UCLA as a Covered Entity

The Rule applies to financial institutions and creditors that offer or maintain accounts that provide for multiple transactions primarily for personal, family, or household purposes. The Rule defined 'account' as 'a continuing relationship established to provide a financial product or service that a financial holding company could offer by engaging in an activity that is financial in nature or incidental to such a financial activity under section 4(k) of the Bank Holding Company Act, 12 U.S.C. 1843(k).'
UCLA is considered a covered entity because we act as a "creditor" by:

- regularly extending, renewing, or continuing credit; or
- regularly arranging for the extension, renewal, or continuation of credit; or

- acting as an assignee of an original creditor who participates in the decision to extend, renew, or continue credit.

The Rule is actually three different but related rules, two of which will definitely apply to UCLA. The third rule should not apply as noted below:

- *(681.1) Users of consumer reports must develop reasonable policies and procedures to apply when they receive notice of an address discrepancy from a consumer reporting agency*. This provision would apply to any areas of UCLA that utilize consumer reporting agencies for any reason, i.e. credit or background checks for loan issuance or collection purposes, or for new hire applicants, etc.
- *(68.2) Financial institutions and creditors holding 'covered accounts' must develop and implement a written identity theft prevention program for both new and existing accounts.* This provision applies to any areas of UCLA that issue any type of credit, i.e. Perkins Loans, Short Term Loans for Students or Faculty/Staff, Housing Payment Plans, Transportation Payment Plans, Student Tuition/Fee Deferred Payment Plans, etc.
- *(681.3) Debit and credit card issuers must develop policies and procedures to assess the validity of a request for a change of address that is followed closely by a request for an additional or replacement card.* This provision does not apply as UCLA does not issue debit and/or credit cards. While the BruinCard has debit functionality, it is a closed loop system and cannot be processed through the regular debit/credit card network. Our customers are all known entities associated with the University and address updates are received only through uploads from either Payroll or Student systems. Additionally, addresses are not used in the BruinCard system. All refunds are generated through the University Billing and Receivable (BAR) system.

**Summary of the Rule Requirements and Implementation Deadline**

Covered entities under the Rule must adopt and implement a written Identity Theft Prevention Program to *detect*, *prevent*, and *mitigate* identity theft in connection with the opening of a covered account, or any existing covered account. The Identity Theft

Prevention Program may be integrated into the structure of an existing Compliance Program. However, the efforts and resources committed must be appropriate to the size and complexity of the organization and the nature and scope of its activities. Elements required by the Rule include:

- Identification of Red Flags – Policies and procedures to identify which Red Flags, singly or in combination, are relevant to detecting the possible risk of identity theft to customers using a risk evaluation method appropriate to the organization.
- Detection of Red Flags – Policies and procedures designed to prevent and mitigate identity theft in connection with opening an account or any existing account.
- Responding to Red Flags – Policies and procedures to assess whether the Red Flags detected evidence a risk of identity theft. There must also be a reasonable basis for concluding that a Red Flag does not evidence a risk of identity theft.
- Updating the Program – Policies and procedures in place to ensure the program is updated periodically to reflect changes in risks to the customer and institution.
- Administration of the Program – Involvement of senior management in development, implementation and oversight. Ongoing staff training is required. Also included is oversight of service provider arrangements to ensure they are in compliance.

The implementation date by which covered entities were to comply with the Rule was set at November 1, 2008. In October 2008, the FTC announced that they were delaying enforcement of the Rule as to the entities under its jurisdiction by six months, until May 1, 2009.

## Twenty-Six Red Flags Identified in the Rule

As an Appendix to the Rule, the FTC has identified twenty-six Red Flags that the University may consider incorporating into their program. These are subdivided into five sections, see below:

Alerts, Notifications or Warnings from a Consumer Reporting Agency

1. A fraud or credit alert is included with a consumer report.
2. A notice of credit freeze on a consumer report is provided from a consumer reporting agency.
3. A consumer reporting agency provides a notice of address discrepancy.
4. A consumer report indicates a pattern of activity inconsistent with the history and usual pattern of activity of a customer.

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 customer presenting the identification.
7. Other information on the identification is not consistent with information provided by the person opening an account or presenting the identification.
8. Other information on the identification is not consistent with readily accessibly information that is on file with the University.
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 University.
11. Personal identifying information provided by the customer is not consistent with other personal identifying information provided by the customer.
12. Personal identifying information provided is associated with known fraudulent activity as indicated by internal or third-party sources used by the University.
13. Personal identifying information provided is of a type commonly associated with fraudulent activity as indicated by the internal or third-party sources used by the University.
14. The social security number 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 account 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 University.
18. If the University uses a challenge question, 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, the University receives a request for a new or replacement card or cell phone, or 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.
21. An account is used in a manner that is not consistent with established patterns of activity on the account.
22. An account that has been inactive for a reasonably lengthy period of time is used.
23. Mail sent to the customer is returned repeatedly as undeliverable although transactions continue to be conducted in connection with the account.
24. The University is notified that the customer is not receiving paper account statements.
25. The University is notified of unauthorized charges or transactions in connection with a customer's account.

Notice from Customers, Victims of Identity Theft, Law Enforcement Authorities, or Other Persons Regarding Possible Identity Theft in Connection with Covered Accounts

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

## Student Financial Services Policy and Procedures for the Rule

It will be the policy of Student Financial Services to:

- Verify identification for any student, faculty, or staff requesting services. The identification should be scrutinized to verify that it has not been altered or forged.
- Verify that the picture on the identification provided matches the appearance of the customer presenting the identification.
- Verify that the information on the identification is consistent with other information on file at the University, particularly on the customer's account.
- Verify that requests for information updates, i.e. BruinDirect sign up forms, have not been altered or forged, or that the paperwork gives the appearance of having been destroyed and reassembled.
- Not share any more information with a customer than is documented in the student system if there is a full FERPA restriction on the account. If additional information is requested, the student should be forwarded to the Registrars office for assistance.
- Report to upper management without assisting the customer if the UID provided is the same as that submitted by another customer.
- Report to upper management if an account is used in a manner not consistent with regular patterns of activity, i.e. if a student receives more than one Short Term loan at a time, or over the period of one term.
- Call or email the customer if mail addressed to the customer is returned twice as undeliverable although transactions continue to be conducted with their account.
- Notify upper management if an account has three different address changes in the past ninety (90) days.
- Investigate and verify the correctness of unauthorized charges or transactions assessed by Student Financial Services in connection with a customer's account. If there are questions regarding the correctness of departmental charges, refer them on to the appropriate department for resolution.
- Notify the Director immediately if the University is notified by a customer, a victim of identity theft, a law enforcement authority, or any other person that it has opened, discovered, or manipulated a fraudulent account for a person engaged in identity theft.

- Not provide any information to an individual claiming to be the victim of identity theft without them providing evidence of a Police Case Number or an FTC affidavit of identity theft. If a customer needs assistance of this type, the request must be in writing with detailed information requested as well as proof of positive identification and proof of claim of identity theft (police report or FTC affidavit).
- Ensure that customers who call are not given information on an account if they cannot provide the UID and customer name. Be cautious about callers who attempt to get financial information without providing any substantive knowledge about the account.
- Student Financial Services staff should not respond to any questions from customers related to any medical type services, specifically the Ashe Center or Psychiatric Services. All calls of this type should be immediately referred to the phone number of the department in question.

**Oversight, Training, Third Party Compliance and Update**

Due to the sensitive nature of this topic, the Manager of each area within Student Financial Services will maintain responsibility for the implementation and ongoing support of this regulation. On a quarterly basis they will audit the procedures and report compliance to the Director.

Training for Red Flag will be conducted annually along with other compliance training affecting Student Financial Services. This training will be conducted at Staff Meeting and is mandatory for all staff. If students or staff are not able to attend in Staff Meeting, the Managers will update their staff when they are available.

Currently there are no Third Party contracts in Student Financial Services that need updating with compliance verbiage, nor are there vendors that need to report compliance.

This policy will be updated at least annually based on new processes and procedures.