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

Overview

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 and pursuant to the Federal Trade Commission's Red Flags Rule (“Rule”), the University of California Board of Regents has adopted the following Identity Theft Prevention Implementation Plan (“Implementation Plan”) as developed by the Office of Ethics, Compliance and Audit Services (“ECAS”) with support from the Office of General Counsel and integrated into the University of California (“UC”) Ethics and Compliance Program Plan (“Program”). The objective of this Implementation Plan is to establish processes at the campuses and UC Office of the President (“UCOP”) to:

- Identify relevant Red Flags applicable to UC accounts and incorporate those into this Implementation Plan;
- Continually review UC accounts to detect those Red Flags that have been incorporated into the Implementation Plan;
- Respond appropriately to any Red Flags that have been identified to prevent and mitigate identity theft; and
- Ensure the Implementation Plan is periodically updated to identify new or changed risks to our relevant constituents.

This Implementation Plan has been designed to include, as appropriate, any existing UC systemwide and campus-specific policies and procedures currently in place that control reasonably foreseeable risks associated with identify theft.

Actions

Each campus and UCOP will be responsible for implementing the following:

I. Identify Covered Accounts - ECAS developed and disseminated a Red Flags Rule Inventory Grid (“Grid”) to the campuses and UCOP to use as a tool for documenting applicable covered accounts across the UC system. It is the campuses’ and UCOP’s responsibility to:

   A. Ensure the information contained within the Grid is accurate; and

   B. Update the Grid quarterly to reflect current campus practices and activities to highlight evolving account activity risks.

II. Identify Relevant Red Flags - In an effort to identify relevant Red Flags which may include, but not be limited to a pattern, practice or specific activity that indicates the possible
Identity Theft Prevention Implementation Plan

existence of identity theft, campuses should consider a) the types of accounts it offers and maintains, b) methods to open and/or access accounts, and c) previous experiences with identity theft. The following list outlines several examples of potential sources to identify Red Flags:

A. notifications and warnings from credit reporting agencies and other third parties;
B. suspicious documents;
C. unusual use of accounts; and
D. Suspicious identifying information.

III. Review Mechanisms for Detection of Red Flags - Campuses will review their current policies/procedures and systems to address detection of Red Flags for each covered account and/or processes within a identified account with a key focus on verifying identity, authenticating customers, monitoring transactions, and verifying the validity of address changes.

IV. Review Mechanisms for Responses to Identity Theft - Campuses will establish processes to periodically review control mechanisms put into place to prevent and mitigate identity theft. These reviews will be reported to the Campus Ethics and Compliance Risk Committees in a timeframe defined by the campuses.

V. Integrate Red Flags Rule into Current Compliance Program Activities - Once campuses have completed the steps above, here forward the campuses’ activities around this area will be integrated into their compliance program efforts on an ongoing basis. At a minimum, quarterly monitoring on the Rule will occur on each campus through the Campus Ethics and Compliance Risk Committee to identify detection, prevention and mitigation efforts. The Systemwide Ethics and Compliance Risk Council will periodically review the monitoring efforts and identify trends related to these areas.

VI. Ensure Contract Compliance. Campuses will review their current policies/procedures and systems to ensure appropriate and effective oversight of service providers. Each campus must further verify that vendors providing services in connection with covered accounts have established their own identity theft prevention programs and that such programs shall be subject to the campuses’ periodic review and reporting requirements.

VII. Provide Employee Training - Campus management and staff responsible for the covered accounts will be trained at the campus department level through their normal compliance training efforts related to their specific processes for the prevention, detection and response to identity theft issues, and contracting with vendors providing services in connection with covered accounts.

VIII. Provide Oversight and Review of the Program - The UC Ethics and Compliance Program at the campus and system levels will provide oversight and assurance that these activities are
occurring (assurance activities may be delegated but the Campus Ethics and Compliance Risk Committee will maintain oversight):

A. Administering the Implementation Plan on their respective campus;

B. Ensuring appropriate training of campus staff on the Implementation Plan;

C. Reviewing any staff reports regarding the detection of Red Flags and the steps for preventing and mitigating identity theft;

D. Determining which steps of prevention and mitigation should be taken in particular circumstances and considering periodic changes to the Implementation Plan; and

E. At a minimum, evaluating the effectiveness of their policies and procedures in addressing the risk of identity theft in connection with covered accounts. Recommendations for material changes will be provided and considered in this area as determined by each Campus Ethics and Compliance Risk Committee.

The UC Systemwide Ethics and Compliance Risk Council will periodically validate with the campus level oversight, progress and efforts made related to compliance with these rules. The Office of Ethics, Compliance and Audit Services will provide the status of system compliance with the Rule in the Annual Report to The Board of Regents through the Committee on Compliance and Audit.