OAKLAND UNIVERSITY

ADMINISTRATIVE POLICIES AND PROCEDURES

412 DETECTION OF AND RESPONSE TO IDENTITY THEFT RED FLAGS

SUBJECT: DETECTION OF AND RESPONSE TO IDENTITY THEFT RED FLAGS

NUMBER: 412

AUTHORIZING BODY: STRATEGY COUNCIL

RESPONSIBLE OFFICE: FINANCE AND ADMINISTRATION

DATE ISSUED: OCTOBER 29, 2008

LAST UPDATE: APRIL 2017

RATIONALE:

Oakland University (University) shall comply with the applicable requirements of 16 C.F.R. 681, a federal regulation issued by the Federal Trade Commission (FTC) as part of the Fair and Accurate Credit Transaction (FACT) Act of 2003 requiring that financial institutions and Creditors implement written programs which provide for detection of and response to specific activities (Red Flags) that could be related to Identity Theft.

POLICY:

The University will implement and provide for the continued administration of programs in relation to:

1. Duties of users regarding address discrepancies.

2. Duties regarding the detection, prevention, and mitigation of Identity Theft.

3. Duties of Card Issuers regarding changes of address.

SCOPE AND APPLICABILITY:

This policy is applicable to all University faculty and staff.

DEFINITIONS:

Account: A continuing relationship established by a person with a financial institution or Creditor to obtain a product or service for personal, family, household or business purposes. Account includes:

I. An extension of credit, such as the purchase of property or services involving a deferred payment; and

II. A deposit Account.

Consumer Reporting Agency: Are entities that collect and disseminate information about consumers to be used for credit evaluation and certain other purposes.

Consumer Reports: Any written, oral, or other communication of any information by a Consumer Reporting Agency bearing on a consumer's credit worthiness, credit standing, credit capacity, character, general reputation, personal characteristics, or mode of living which is used or expected to be used or collected in whole or in part for the purpose of serving as a factor in establishing the consumer's eligibility for:

I. Credit or insurance to be used primarily for personal, family, or household purposes;

II. Employment purposes; or

III. Any other purpose authorized under US Code: Title 15, 1681b.

Covered Accounts:

I. An Account that a financial institution or Creditor offers or maintains, primarily for personal, family, or household purposes, that involves or is designed to permit multiple payments or transactions, such as a credit card Account, mortgage loan, automobile loan, margin Account, cell phone Account, utility Account, checking Account, or savings Account; and

II. Any other Account that the financial institution or Creditor offers or maintains for which there is a reasonably foreseeable risk to Customers or to the safety and soundness of the financial institution or Creditor from Identity Theft, including financial, operational, compliance, reputation, or litigation risks.

Creditor: Any person, corporation, government or governmental subdivision or agency, trust, estate, partnership, cooperative, or association who regularly extends, renews, or continues credit; any person who regularly arranges for the extension, renewal, or continuation of credit; or any assignee of an original Creditor who participates in the decision to extend, renew, or continue credit.

Customer: Person that has a covered Account with a financial institution or Creditor.

Debit Card: Any card issued by a financial institution to a consumer for use in initiating an electronic fund transfer from the Account of the consumer at such financial institution, for the purpose of transferring money between Accounts or obtaining money.

Notice of Address Discrepancy: A notice sent to a user by a Consumer Reporting Agency pursuant to 15 U.S.C. 1681c(h)(1), that informs the user of a substantial difference between the address for the consumer that the user provided to request the consumer report and the address(es) in the agency's file for the consumer.

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

Red Flag: A pattern, practice, or specific activity that indicates the possible existence of Identity Theft.

Service Provider: A person that provides a service directly to the financial institution or Creditor.

Card Issuer: Financial institution or Creditor that issues a debit or credit card

PROCEDURES:

Duties of Users Regarding Address Discrepancies

A. University departments which use Consumer Reports will form a reasonable belief that a consumer report relates to the consumer about whom it has requested the report when a Notice of Address Discrepancy is received by:

   i. Comparing the information in the consumer report provided by the Consumer Reporting Agency with information the department:

      1. Maintains in its own records, such as applications, change of address notifications, other Customer Account records; or

      2. Obtains from third-party sources; or

   ii. Verifying the information in the consumer report provided by the Consumer Reporting Agency with the consumer.

B. University departments which use Consumer Reports will furnish an address for the consumer that the department has reasonably confirmed is accurate to the Consumer Reporting Agency from whom it received the Notice of Address Discrepancy when the department:

i. Can form a reasonable belief that the consumer report relates to the consumer about whom the user requested the report;

ii. Established a continuing relationship with the consumer; and

iii. Regularly and in the ordinary course of business furnishes information to the Consumer Reporting Agency from which the Notice of Address Discrepancy relating to the consumer was obtained.

iv. The department may reasonably confirm an address is accurate by:

1. Verifying the address with the consumer about whom it has requested the report;

2. Reviewing its own records to verify the address of the consumer;

3. Verifying the address through third-party sources; or

4. Using other reasonable means.

v. If applicable, a department will furnish a consumer's address that the department has reasonably confirmed is accurate to the Consumer Reporting Agency as part of the information it regularly furnishes for the reporting period in which it establishes a relationship with the consumer.

Duties Regarding the Detection, Prevention, and Mitigation of Identity Theft

A. University departments will periodically determine whether they offer or maintain Covered Accounts and as part of the determination, departments will conduct a risk assessment to determine whether it offers or maintains Covered Accounts for which there is a reasonably foreseeable risk to Customers or to the safety and soundness of the University from Identity Theft, including financial, operational, compliance, reputation, or litigation risks, taking into consideration:

i. The methods it provides to open its Accounts;

ii. The methods it provides to access its Accounts; and

iii. Its previous experiences with Identity Theft.

B. Each University department which offers or maintains Covered Accounts will develop and implement a written procedure ("Program") that is designed to detect, prevent, and mitigate Identity Theft in connection with opening of a Covered Account and that is appropriate to the department's size, complexity, and the scope of its activities designed to:

i. Identify relevant Red Flags for the Covered Accounts that the department offers or maintains, and incorporate those Red Flags into its Program;

ii. Detect Red Flags that have been incorporated into the Program of the department;

iii. Respond appropriately to any Red Flags that are detected to prevent and mitigate Identity Theft; and

C. Each University department which offers or maintains Covered Accounts will update its Program periodically to reflect changes in risks to Customers and to the safety and soundness of the department from Identity Theft and will:

i. Involve the President and/or his designees, in the oversight development, implementation and administration of the Program;

ii. Train staff, as necessary, to effectively implement the Program; and

iii. Exercise appropriate and effective oversight of Service Provider arrangements.

iv. Consider guidelines included in Appendix A of 16 C.F.R. 681 and include in its Program those guidelines that are appropriate.

Duties of Card Issuers Regarding Changes of Address

A. University departments which are Card Issuers, if any, will assess the validity of a change of address if it receives notification of a change of address for consumer's Debit or Credit Card Account and, within a short period of time afterwards (during at least the first 30 calendar days after it receives such notification), the department receives a request for an additional or replacement card for the same Account. The department will not issue an additional or replacement card until the department:

i. Notifies the cardholder of the request:

1. At the cardholder's former address; or

2. By any other means of communication that the Card Issuer and the cardholder have previously agreed to use; and

ii. Provides to the cardholder a reasonable means of promptly reporting incorrect address changes; or

1. Otherwise assesses the validity of the change of address by reasonable means

B. A department may satisfy the requirements of the preceding section by validating an address when it receives an address change notification before it receives a request for an additional or replacement card. Any written or electronic notice that the department provides under the preceding section should be clear and conspicuous and be provided separately from its regular correspondence with the cardholder.

Conformity to Law

All programs implemented pursuant to this policy must be in compliance with the law and with University policies and regulations and shall conform to the legal standards and requirements of the University General Counsel.

RED FLAG Identity Theft Protection Program

In accordance with regulations, the University created a RED FLAG Identity Theft Protection Program which includes online training and a short exam on the content of the training. Finance & Administration strongly recommends that all employees review the training materials and take the exam on an annual basis.

RELATED POLICIES AND FORMS:

- Identity Theft Prevention Program: To login, use your NetID and Password. If you have never accessed the training before, enter the code "Enrollme" (case-sensitive) when prompted for the Enrollment key to access the training and test.

APPENDIX:

Copy