Agendum
Oakland University
Board of Trustees Formal Session
April 1, 2009

IDENTITY THEFT PREVENTION PROGRAM POLICY

A Recommendation

1. **Division and Department:** Finance and Administration

2. **Introduction:** The attached proposed Identity Theft Prevention Program Policy (Attachment A) was developed to comply with the Federal Trade Commission's (FTC) Red Flags Rule (Rule), which implements sections of the Fair and Accurate Credit Transactions Act.

The Rule requires entities that offer or maintain "covered accounts" to develop and implement an identity theft prevention program designed to detect, prevent, and mitigate identity theft in connection with the opening of a covered account or any existing covered account. "Covered accounts" include the acceptance of deferred payment for goods and services, and as such, the Rule is applicable to Oakland University's operations. The Rule provides that such program be appropriate to the size and complexity of the creditor and the nature and scope of its activities, and the FTC will begin enforcement of the Rule on May 1, 2009.

To comply with the Rule, the University developed the attached policy and procedures to detect or mitigate identity theft through the identification of; detection of; and response to; relevant "red flags". "Red flags" are a "pattern, practice, or specific activity that indicates the possible existence of identity theft. The Rule also requires the University to update the program periodically to reflect changes in risks and to train staff, as necessary, to effectively implement the program.

The Rule requires that the Board of Trustees (Board) approve an initial written program for the University that will then be implemented by the administration. In that regard, the administration, under the auspices of the Vice President for Finance and Administration and his designees, will update the program periodically to reflect changes in risks and to train staff, as necessary, to run the program effectively.

3. **Previous Board Action:** None.

4. **Budget Implications:** None.

5. **Educational Implications:** None.

6. **Personnel Implications:** None.

7. University Reviews/Approvals: The attached proposed Identity Theft Prevention Program Policy was prepared by the Assistant Vice President and Controller and an Assistant General Counsel, and reviewed by the Vice President for Finance and Administration and the Chief Information Officer.

8. Recommendation:

WHEREAS, the Federal Trade Commission promulgated the Red Flags Rule implementing sections of the Fair and Accurate Credit Transactions Act; and

WHEREAS, the University is required to comply with the Red Flags Rule; now, therefore be it

RESOLVED, that the Board of Trustees approves the attached Identity Theft Prevention Program Policy.

9. Attachments:
A. Identity Theft Prevention Program Policy.

Submitted to the President
on 3/26, 2009 by

John W. Beaghan
Vice President for Finance and Administration
and Treasurer to the Board of Trustees

Recommended on 3/26, 2009
to the Board for approval by

Gary D. Russi
President

Attachment A

Oakland University
Identity Theft Prevention Program Policy

Rationale

Oakland University shall comply with the applicable requirements of 16 C.F.R. 681, regulations issued by the Federal Trade Commission (FTC) which implement sections of the Fair and Accurate Credit Transaction (FACT) Act of 2003.

The Program

Oakland University establishes an Identity Theft Prevention Program (Program) to detect, prevent, and mitigate identity theft. The Program includes reasonable policies and procedures to:

A. Identify Red Flags relevant to University business for covered accounts it offers or maintains and incorporate those Red Flags into the Program.
B. Detect Red Flags that have been incorporated into the Program.
C. Respond appropriately to any Red Flags that are detected to prevent and mitigate identity theft.
D. Ensure the Program is updated periodically to reflect changes in identity theft risks to customers and to the safety and soundness of the University in its role as a creditor.

Scope and Applicability

This policy is applicable to all University faculty and staff.

Definitions

Account – a continuing relationship established by a person, with the University, to obtain a product or service for personal, family, household or business purposes. Account includes:

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

A. credit or insurance to be used primarily for personal, family, or household purposes;
B. employment purposes; or
C. any other purpose authorized under US Code: Title 15, 1681b.

Covered Accounts –

A. Any account the University offers or maintains primarily for personal, family or household purposes, that involves multiple payments or transactions.
B. Any other account the University offers or maintains for which there is a reasonably foreseeable risk to customers or to the safety and soundness of the University from identity theft.

Creditor – an entity that regularly extends, renews, or continues credit.

Customer – person that has a covered account with the University.

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 University.

Red Flags

Red Flags may be detected as University employees interact with customers and consumer reporting agencies. The following Red Flags (I – IV below) are potential indicators of fraud. Any time a Red Flag is identified, it should be investigated.

I. Alerts, Notifications or Warnings from a Consumer Reporting Agency.

Examples of these Red Flags include the following:

A. A fraud or active duty alert included with a consumer report;
B. A notice of credit freeze in response to a request for a consumer report;
C. A Notice of Address Discrepancy, as defined in §334.82(b) of the Fairness and Accuracy in Credit Transactions Act; and
D. A consumer report indicating a pattern of activity that is inconsistent with the history and usual pattern of activity of an applicant or customer, such as:
    1. A recent and significant increase in the volume of inquiries;
    2. An unusual number of recently established credit relationships;

3. A material change in the use of credit, especially with respect to recently established credit relationships; or
4. An account closed for cause or identified for abuse of account privileges by a financial institution or creditor.

II. Suspicious Documents. Examples of these Red Flags include the following:

A. Documents provided for identification that appear to have been altered or forged;
B. The photograph or physical description on the identification is not consistent with the appearance of the person presenting the identification;
C. Other information on the identification is not consistent with information provided by the person opening a new covered account or person presenting the identification;
D. Other information on the identification is not consistent with readily accessible information that is on file with the University; and
E. An application that appears to have been altered or forged, or gives the appearance of having been destroyed and reassembled.

III. Suspicious Personal Identifying Information. Examples of these Red Flags include the following:

A. Personal identifying information provided is inconsistent when compared against external information sources used by the University. For example:
    1. The address does not match any address in the consumer report; or
    2. The Social Security Number (SSN) has not been issued, or is listed on the Social Security Administration's Death Master File.
B. 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;
C. Personal identifying information provided is associated with known fraudulent activity as indicated by internal or third-party sources used by the University. For example:
    1. The address on an application is the same as the address provided on a fraudulent application; or
    2. The phone number on an application is the same as the number provided on a fraudulent application.
D. Personal identifying information provided is of a type commonly associated with fraudulent activity as indicated by internal or third-party sources used by the University. For example:
    1. The address on an application is fictitious, a mail drop, or a prison; or
    2. The phone number is invalid, or is associated with a pager or answering service.
E. The SSN provided is the same as that submitted by another customer;
F. 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 customers or other persons opening accounts;

G. 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;
H. Personal identifying information provided is not consistent with personal identifying information that is on file with the University; and
I. When using security questions (mother's maiden name, pet's name, etc), the person opening the covered account cannot provide authenticating information beyond that which would be available from a wallet or consumer report.

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

Examples of these Red Flags include the following:

A. Shortly following the notice of a change of address for a covered account, University receives a request for new, additional, or replacement goods or services, or for the addition of authorized users on the account;
B. A covered account is used in a manner that is not consistent with established patterns of activity on the account. There is, for example:
    1. Nonpayment when there is no history of late or missed payments; or
    2. A material change in purchasing or usage patterns;
C. 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);
D. Mail sent to the customer is returned repeatedly as undeliverable although transactions continue to be conducted in connection with the covered account;
E. The University is notified that the customer is not receiving paper account statements;
F. The University is notified of unauthorized charges or transactions in connection with a covered account.
G. The University receives 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 University; and
H. The University 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.

Responses to Red Flags

In the event University personnel detect an identified Red Flag, such personnel shall take appropriate steps to respond and mitigate against identity theft depending on the nature and degree of risk posed by the Red Flag, including but not limited to:

- Continue to monitor an account for evidence of identity theft;
- Contact the customer;
- Change any passwords or other security devices that permit access to accounts;
- Not open a new account;
- Close an existing account;
- Reopen an account with a new number;

- Notify law enforcement; or;
- Determine that no response is warranted under the particular circumstances.

PROGRAM ADMINISTRATION

A. Oversight

The initial written Theft Prevention Program Policy must be approved by the University's Board of Trustees. The Board's approval of the initial plan must be appropriately documented and maintained.

Operational responsibility of the Program, including but not limited to the oversight, development, implementation, and administration of the Program, is delegated to the Vice President for Finance and Administration and his designees.

B. Training

University Human Resources Department will conduct training for employees who will regularly perform duties involving accounts or personal indentifying information that may present Red Flags.

C. Service Provider Arrangements

In the event the University engages a service provider to perform an activity in connection with one or more Covered Accounts, the University will take the following steps to ensure the service provider performs its activity in accordance with reasonable policies and procedures designed to detect, prevent and mitigate the risk of Identity Theft.

1. Require, by contract, that service providers have such policies and procedures in place; and
2. Require, by contract, that service providers review the University's Program and report any Red Flags to the University

D. Program Updates

At periodic intervals as deemed necessary by the University, the Program will be re-evaluated to determine whether all aspects of the Program are up to date and applicable in the current operational environment.

Periodic reviews will include an assessment of which accounts and activities are covered by the Program.

As part of the review, Red Flags may be revised, replaced or eliminated. Defining new Red Flags may also be appropriate.

Actions to take in the event that fraudulent activity is discovered may also require revision to reduce damage to the University and its students, faculty, staff and other constituents.