The University of North Carolina at Chapel Hill

Identity Theft Prevention Program

The Board of Trustees of The University of North Carolina at Chapel Hill (the "University") adopts this Identity Theft Prevention Program (the "Program") pursuant to the Federal Trade Commission's Identity Theft Red Flags and Address Discrepancies Under the Fair and Accurate Credit Transactions Act of 2003 (the "Rule"). The University is covered by the Rule as a creditor because it offers or maintains accounts:

- That involve or are designed to permit multiple payments or transactions, deferred payment arrangements, and extensions of credit, loans, or deposit accounts which establish a continuing relationship with consumers;
- For which there is a reasonably foreseeable risk of Identity Theft to consumers or to the safety and soundness of the University, including financial, operational, compliance, reputational, or litigation risks; or
- That utilize credit checks.

Enforcement of the Rule begins May 1, 2009.

I. PURPOSE

The purpose of the Program is to:

- Identify, detect and respond to Red Flags;
- Prevent and mitigate Identity Theft; and
- Develop departmental protocols for compliance with the Rule.

II. DEFINITIONS

For purposes of the Program, the following definitions apply:

"**Covered Account**" includes those offered or maintained by the University:

- That involve or are designed to permit multiple payments or transactions, deferred payment arrangements, or extensions of credit, loans, or deposit accounts which establish a continuing financial relationship with individual consumers;
- For which there is a reasonably foreseeable risk of Identity Theft to consumers or to the safety and soundness of the University, including financial, operational, compliance, reputational, or litigation risks; or
- That utilize credit checks.

"**Identity Theft**" is a fraud committed using the Identifying Information of another person, subject to such further definition as the Federal Trade Commission may prescribe, by regulation.

"**Identifying Information**" is any name or number that may be used, alone or in conjunction with any other information, to identify a specific person, including any:

- Name, Social Security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number;
- Unique biometric data, such as fingerprint, voice print, retina or iris image, or other unique physical representation;
- Unique electronic identification number, address, or routing code; or
- Access device, including any card, plate, code, account number, electronic serial number, mobile identification number, personal identification number, or other telecommunications service, equipment, or instrument identifier, or other means of account access that can be used, alone or in conjunction with another device, to obtain money, goods, services, or any other thing of value, or that can be used to initiate a transfer of funds.

"**Program Administrator**" is the Chair of the University Committee on the Protection of Personal Data ("UCPPD") and is responsible for the oversight, development, implementation, and administration of the Program as outlined in the sections below. The Program Administrator shall consult with the UCPPD on implementation and maintenance of the Program.

"**Program Contact Person**" is the employee designated by a University department to act as a liaison between the department's management and the Program Administrator and to assume responsibility for Program duties as outlined in the sections below.

"**Red Flag**" is a pattern, practice, or specific activity that indicates the possible risk of Identity Theft.

"**Service Provider**" is an outside entity engaged by the University to perform an activity in connection with one or more Covered Accounts.

III. PROGRAM COMPONENTS

The University's Program consists of the following components:

- Identifying Covered Accounts;
- Identifying relevant Red Flags for new and existing Covered Accounts and incorporating those Red Flags into the Program;
- Detecting Red Flags that have been incorporated into the Program;
- Responding appropriately to any Red Flags that are detected to prevent and mitigate Identity Theft;
- Training employees regarding the Program;
- Reviewing Service Provider agreements for compliance with the Program; and
- Ensuring the Program is updated periodically to reflect changes in risks to consumers or to the University from Identity Theft.

A. Identifying Covered Accounts

In order to identify Covered Accounts, each University department shall make a risk determination of its financial transactional, credit, or loan accounts considering:

1. Methods used to open and access the account, especially those that do not require face-to-face contact, such as through the Internet or by telephone;
2. Whether the account has been the target of Identity Theft attempts in the past;
3. Technological risks (for example, password protection, use of mobile devices, computer controls such as locking screens, automatic logoffs, and physical security measures for work areas both during the workday and during nights/weekends), and
4. Other accounts if there is a reasonably foreseeable fraud or Identity Theft risk to consumers or to the University.

On or before May 1, 2009, each University department having Covered Accounts shall compile a list of Covered Accounts for which it has oversight and incorporate the list into a written Departmental Red Flags Rule Protocol ("Protocol") to be submitted to the Program Administrator (see Section IV).

B. Identifying Red Flags

As set forth in the Rule, Red Flags include but are not limited to:

1. The presentation of suspicious documents;
2. The presentation of suspicious Identifying Information;
3. The unusual use of, or other suspicious activity related to, a Covered Account;
4. Alerts, notifications, or other warnings received from consumer reporting agencies or service providers, such as fraud detection services; and
5. Notices from consumers, victims of Identity Theft, law enforcement authorities, or other persons regarding possible Identity Theft in connection with Covered Accounts held by the University.

Each University department having Covered Accounts shall compile a list of Red Flags relevant to its covered transactions and incorporate the list into its Protocol. Appendix A contains examples of Red Flags provided in the Rule but is not an exhaustive list for the purpose of this Program.

C. Detecting Red Flags

Each University department having Covered Accounts shall endeavor to detect Red Flags by developing internal procedures to obtain, verify, and monitor personal Identifying Information of account holders on file with the University. These procedures shall be set forth in the department's Protocol.

D. Responding to Detected Red Flags

Each University department having Covered Accounts shall endeavor to prevent and mitigate Identity Theft associated with its Covered Accounts by developing internal procedures to appropriately respond to detected Red Flags. Appropriate responses may include:

- Monitoring accounts;
- Contacting consumers;
- Changing passwords;
- Closing and reopening accounts;
- Refusing to open an account;
- Notifying the University's Department of Public Safety;
- Refusing to collect on or "sell" an account;
- Other responses as determined by the department; or
- Determining that no response is warranted.

These procedures shall be set forth in the department's Protocol.

Additionally, employees of departments having Covered Accounts are expected to notify their department's Program Contact Person once they become aware of an incident of Identity Theft or of the University's failure to comply with this Program (see also, Section IV). The departmental Program Contact Person shall in turn report the incident to his/her supervisor and the Program Administrator.

E. Training Employees

Each University department having Covered Accounts shall develop a training program and ensure that appropriate employees receive training regarding this Program and the department's Protocol. Names of employees who initially receive training shall be included in the department's Protocol. Thereafter, names of trained employees shall be submitted by the department's Program Contact Person to the Program Administrator on a continuous basis.

F. Reviewing Service Provider Arrangements

In the event that a University department engages a Service Provider to perform an activity in connection with Covered Accounts, the department will ensure the Service Provider's compliance with this Program by contractually requiring that Service Providers:

1. Have Identity Theft prevention policies and procedures in place;
2. Review the University's Identity Theft Prevention Program and the department's Protocol; and
3. Report detected Red Flags to the department's Program Contact Person and the Program Administrator.

Each University department having Covered Accounts shall identify such Service Providers. The department's Program Contact Person shall submit the Service Providers' names and contact information in writing to the Program Administrator on a continuous basis.

G. Updating the Program

Upon request by the Program Administrator, each department having Covered Accounts shall periodically review its Protocol to ensure its effectiveness. Consideration for updating Protocols shall be given to:

1. The department's experiences with Identity Theft;
2. Changes in or new methods of Identity Theft;
3. Changes in or new methods of detecting, mitigating, and preventing Identity Theft;
4. Changes in the types of Covered Accounts offered or maintained by the department; and
5. Changes in the University's business arrangements and Service Provider arrangements.

Written reports of Protocol reviews, including any updates made, shall be submitted by the department's Program Contact Person to the Program Administrator in a timely fashion.

IV. DEPARTMENTAL RED FLAGS RULE PROTOCOL

On or before May 1, 2009, each department having Covered Accounts shall use the template attached as Appendix B to prepare a Protocol containing:

1. The department name and number,
2. The name of and contact information for the person designated as its Program Contact Person;
3. The name of and contact information for the person responsible for Program training within the department (if different from above);
4. A list and description of Covered Accounts;
5. For each Covered Account:
    a. A list and description of relevant Red Flags;
    b. Internal procedures to obtain, verify, and monitor Identifying Information on file with the University; and
    c. Internal procedures to detect and respond to Red Flags; and
6. The names of employees who have received training regarding this Program and the department's Protocol.

Each Protocol will be submitted to the Program Administrator who will append the Protocols to this Program.

V. PROGRAM ADMINISTRATION

The Program Administrator in consultation with the UCPPD shall be responsible for the implementation, oversight, and continued development of the Program. The appointed Program Administrator shall chair the UCPPD and have responsibility for:

- Acting as the University's primary contact person for the Program;
- Providing general support and guidance to departments with Covered Accounts;
- Oversight of Program training;

- Prompting and approving Protocol reviews and other Program reports;
- Working with departments to help ensure Service Providers' compliance with the Program; and
- At least annually, reporting to the UCPPD on matters related to the Program, including:
    - An evaluation of the effectiveness of the current Program;
    - Significant instances of Identity Theft that occurred during the reporting period and actions taken in response;
    - Status of ongoing monitoring of Service Provider agreements; and
    - Any recommendations for material changes to the Program.

Program Administrator Name: Juliann (Juli) Tenney

Title: University Research Compliance Officer and HIPAA Privacy Officer

Telephone: 919-843-9953 Email: juliann_tenney@unc.edu

VI. AMENDMENTS & UPDATES

This Program may be amended or updated as needed by the Chancellor.

VII. EFFECTIVE DATE

This Program is effective upon approval by the Board of Trustees.

The University's Board of Trustees adopted this Program on March 26, 2009.

This Program is maintained by the Program Administrator.

APPENDIX A

FTC Red Flags Rule
Sample Red Flags

Departments with Covered Accounts may consider using the following examples of Red Flags in connection with Covered Accounts.

Alerts, Notifications or Warnings from a Consumer Reporting Agency

1. A fraud or active duty alert is included with a consumer report.

2. A consumer reporting agency provides a notice of credit freeze in response to a request for a consumer report.

3. A consumer reporting agency provides a notice of address discrepancy.

4. A consumer report indicates a pattern of activity that is inconsistent with the history and usual pattern of activity of an applicant or consumer, such as:

    a. A recent and significant increase in the volume of inquiries;
    b. An unusual number of recently established credit relationships;
    c. A material change in the use of credit, especially with respect to recently established credit relationships; or
    d. An account that was closed for cause or identified for abuse of account privileges by a financial institution or creditor.

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 applicant or consumer presenting the identification.

7. Other information on the identification is not consistent with information provided by the person opening a new Covered Account or consumer presenting the identification.

8. Other information on the identification is not consistent with readily accessible information that is on file with the financial institution or creditor, such as a signature card or a recent check.

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 financial institution or creditor. For example:

    a. The address does not match any address in the consumer report; or
    b. The Social Security number (SSN) has not been issued, or is listed on the Social Security Administration's Death Master File.

11. Personal Identifying Information provided by the consumer is not consistent with other personal Identifying Information provided by the consumer. For example, there is a lack of correlation between the SSN range and date of birth.

12. Personal Identifying Information provided is associated with known fraudulent activity as indicated by internal or third-party sources used by the financial institution or creditor. For example:

    a. The address on an application is the same as the address provided on a fraudulent application; or
    b. The phone number on an application is the same as the number provided on a fraudulent application.

13. Personal Identifying Information provided is of a type commonly associated with fraudulent activity as indicated by internal or third-party sources used by the financial institution or creditor. For example:

    a. The address on an application is fictitious, a mail drop, or prison; or
    b. The phone number is invalid, or is associated with a pager or answering service.

14. The SSN provided is the same as that submitted by other persons opening an account or other consumers.

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 consumers.

16. The person opening the Covered Account or the consumer 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 financial institution or creditor.

18. For financial institutions and creditors that use challenge questions, the person opening the Covered Account or the consumer 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 for a Covered Account, the institution or creditor receives a request for new, additional, or replacement cards or a cell phone, or for 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. For example:

    a. The majority of available credit is used for cash advances or merchandise that is easily convertible to cash (e.g., electronics equipment or jewelry); or
    b. The consumer fails to make the first payment or makes an initial payment but no subsequent payments.

21. A Covered Account is used in a manner that is not consistent with established patterns of activity on the account. There is, for example:

    a. Nonpayment when there is no history of late or missed payments;
    b. A material increase in the use of available credit;
    c. A material change in purchasing or spending patterns;
    d. A material change in electronic fund transfer patterns in connection with a deposit account; or
    e. A material change in telephone call patterns in connection with a cellular phone account.

22. 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).

23. Mail sent to the consumer is returned repeatedly as undeliverable although transactions continue to be conducted in connection with the consumer's Covered Account.

24. The financial institution or creditor is notified that the consumer is not receiving paper account statements.

25. The financial institution or creditor is notified of unauthorized charges or transactions in connection with a consumer's Covered Account.

Notice from Consumers, Victims of Identity Theft, Law Enforcement Authorities, or Other Persons Regarding Possible Identity Theft in Connection with Covered Accounts Held by the Financial Institution or Creditor

26. The financial institution or creditor is notified by a consumer, 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.

APPENDIX B

The University of North Carolina at Chapel Hill
Identity Theft Prevention Program

Departmental Red Flags Rule Protocol

Date Submitted:
Department Name:
Department Number:

Contact information for the employee designated as the department's Identity Theft Prevention Program Contact Person:

Name:
Title:
Telephone:
Email:

If different than the department's Program Contact Person, contact information for the employee responsible for Identity Theft Prevention Program training within the department:

Name:
Title:
Telephone:
Email:

Names of employees who have received training by reviewing the University's Identity Theft Prevention Program, and who will be responsible for following the department's Red Flags Rule Protocol:

Names of Service Providers engaged by the department to perform an activity in connection with Covered Accounts:

Please provide the following information for each Covered Account:

Name of Account #1:

Description of Account:

Relevant Red Flags:

Description of Red Flags:

Internal Procedures to Detect Red Flags (obtain, verify, and monitor personal Identifying Information of account holders on file with the University.):

Internal Procedures to Respond to Detected Red Flags:

Name of Account #2:

Description of Account:

Relevant Red Flags:

Description of Red Flags:

Internal Procedures to Detect Red Flags (obtain, verify, and monitor personal Identifying Information of account holders on file with the University.):

Internal Procedures to Respond to Detected Red Flags:

Name of Account #3:

Description of Account:

Relevant Red Flags:

Description of Red Flags:

Internal Procedures to Detect Red Flags (obtain, verify, and monitor personal Identifying Information of account holders on file with the University.):

Internal Procedures to Respond to Detected Red Flags:

Please continue with this format for Account #4 and above.

The department's Identity Theft Prevention Program Contact Person should submit a copy of the completed Protocol to the Committee representative with whom they are working and distribute copies to appropriate employees for training purposes.