IDENTITY THEFT PREVENTION PROGRAM

Concordia Board of Regents	May 2009

A Resolution Adopting the Identity Theft Prevention Program

WHEREAS, The Federal Trade Commission, under Part 681 of Title 16 in the Code of Federal Regulations, Identity Theft Rules, requires the university to implement an identity theft program, and

WHEREAS, The Board of Regents has determined that the attached *Identity Theft Prevention Program* is in the best interest of the university and its students. NOW, THEREFORE,

BE IT RESOLVED by the Board of Regents of Concordia University Texas that the *Identity Theft Prevention Program* dated May 1, 2009 is hereby approved.

Identity Theft Prevention Program
Effective May 1, 2009
Revised October 20, 2009

I. Purpose

The purpose of this program is to comply with a new federal mandate relating to identity theft. Although we believe the risk of identity theft is low at Concordia University Texas, we believe implementation of a prevention program is in the best interest of our students and those that we serve.

II. Definitions

A. **"Identity Theft"** means a fraud committed or attempted using the identifying information of another person without authority.

B. **"Identifying Information"** means 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;
- 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; and
- Telecommunication identifying information or access device (as defined in 18 USC 1029(e)).

C. **"Account"** means 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 1) an extension of credit, such as the purchase of property or services involving a deferred payment, and 2) a deposit account.

D. **"Covered Account"** means:
- An account that the university offers or maintains, primarily for personal, family, or household purposes, that involves or is designed to permit multiple payments or transactions; and

- 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.

E. **"Customer"** means a person that has a covered account with the financial institution or creditor.

F. **"Red Flag"** means a pattern, practice, or specific activity that indicates the possible existence of identity theft.

G. **"Service Provider"** means a person that provides a service directly to the financial institution or creditor.

III. Administering the Program

A. *Approval and Management.* The Concordia Board of Regents approves the initial written Identity Theft Prevention Program. Thereafter, the President of the institution has the responsibility for oversight of the Program, including delegating the implementation and administration of the Program, reviewing reports, and approving material changes to the Program as necessary to address changing identity theft risks.

B. *Program Administration and Training.* Administration of the Program includes:
   1. Providing training for relevant university employees to effectively implement the Program; and
   2. Reviewing the Program and providing reports to the President on at least an annual basis.
      a. The review will evaluate issues such as:
         i. The effectiveness of the policies and procedures addressing the risk of identity theft with respect to covered accounts;
         ii. Oversight of service providers;
         iii. Significant incidents involving identity theft and Concordia's response; and
         iv. Any recommendations for material changes to the program.
      b. As part of the review, red flags may be revised, replaced, or eliminated. Defining new red flags may also be appropriate.

IV. Transactions at Risk

Concordia has reviewed its transactions and determined that student accounts for tuition, fees, and other charges are "covered accounts" and thus subject to the identity theft prevention policy. In addition, Concordia intends to apply the guidelines to other institutional accounts including faculty and staff accounts and donor accounts, as appropriate.

Concordia has also reviewed the guidelines that contain potential red flags in Appendix A to part 681 of Title 16 in the Code of Federal Regulations implementing Sections 114 and 315 of the Fair and Accurate Credit Transactions Act (FACTA) of 2003. Concordia has existing policies, procedures, and other arrangements to ameliorate the risk to customers, with particular emphasis on those customers who are students or former students, of identity theft. Concordia intends to utilize those current policies in addition to the new requirements of this identity theft prevention program.

V. **Risk Assessment**

A. *Risk Factors.* Concordia will consider the following risk factors in identifying red flags for covered accounts, if appropriate:
   1. The types of covered accounts we offer or maintain;
   2. The methods we provide to open covered accounts;
   3. The methods we provide to access covered accounts; and
   4. Concordia's previous experience with identity theft.

B. *Sources of Red Flags.* Concordia will incorporate relevant red flags from sources such as:
   1. Incidents of identity theft that we have experienced;
   2. Methods of identity theft we have identified that reflect changes in identity theft risks; and
   3. Applicable supervisory guidance.

C. *Categories of Red Flags.* Concordia will include relevant red flags from the following categories, if appropriate:
   1. Alerts, notifications, or other warnings received from consumer reporting agencies or service providers, such as fraud detection services;
   2. The presentation of suspicious documents;
   3. The presentation of suspicious personal identifying information, such as a suspicious address change;
   4. The unusual use of a covered account or other suspicious activity related to a covered account; and
   5. 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.

VI. **Detecting Red Flags**

Concordia will attempt to detect relevant red flags in connection with the opening of covered accounts and existing covered accounts, such as by:
- Obtaining identifying information about, and verifying the identity of, a person opening a covered account; and
- Authenticating customers, monitoring transactions, and verifying the validity of change of address requests, in the case of existing covered accounts.

VII. **Red Flags Identified**

Concordia will consider the following instances as Red Flags (listed by category)—

A. Alerts, Notifications, or Other Warnings received from consumer reporting agencies or service providers, such as fraud detection services.

B. The Presentation of Suspicious Documents
   1. Documents provided for identification appear to have been altered or forged.
   2. The photograph or physical description on the identification is not consistent with the appearance of the applicant or customer presenting the identification.
   3. Other information on the identification is not consistent with information provided by the person opening a new covered account or customer presenting the identification.

4. Other information on the identification is not consistent with readily accessible information that is on file with us.
5. An application appears to have been altered or forged, or given the appearance of having been destroyed and reassembled.

C. The Presentation of Suspicious Personal Identifying Information
1. Personal identifying information is not consistent with other personal identifying information provided by the customer.
2. Personal identifying information provided is associated with known fraudulent activity as indicated by internal or third-party sources used by the university.
3. The Social Security Number provided is the same as that submitted by other persons opening an account or is the same as other customers.
4. 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.
5. Personal identifying information provided is not consistent with personal identifying information that is on file at the university.
6. If the university uses challenge questions, the person opening the covered account or the customer cannot provide authenticating information beyond that which generally would be available from a wallet or consumer report.

D. Unusual use of, or Suspicious Activity Related to, the Covered Account
1. Mail sent to the customer is returned repeatedly as undeliverable although transactions continue to be conducted in connection with the customer's covered account.
2. The university is notified that the customer is not receiving paper account statements.
3. The university is notified of unauthorized charges or transactions in connection with a customer's covered account.
4. *A covered account is opened and financial aid is applied to the covered account, but the account owner does not attend classes during the term and does not provide a reason for their absence.**
5. *A person attempts to access a covered account and is able to provide correct personally identifiable information for that account, but does not identify themselves as the account holder.**

E. Notice from Customers and Others Regarding Possible Identity Theft In Connection with Covered Accounts Held by the University
1. 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.

F. *Other unusual account activity*
1. *University personnel notice evidence of tampering with records stored physically within secured filing cabinets or other physical storage mediums or office areas.**

**Italicized items are recommendations from the Red Flags Task Force which have been approved by the Ad Council, but are pending final approval from the Board of Regents.*

VIII. **Response to Detected Red Flags**

The program shall provide for appropriate responses to detected red flags in order to prevent and mitigate identity theft. The response of the university shall be commensurate with the degree of risk posed. Appropriate responses may include, but not be limited to:

- Monitoring a covered account for evidence of identity theft;
- Contacting the customer;
- Changing any passwords, security codes, or other security devices that permit access to a covered account;
- Canceling the transaction;
- Reopening a covered account with a new account number;
- Not opening a new covered account;
- Closing an existing covered account;
- Notifying and cooperating with appropriate law enforcement; or
- Determining no response is warranted under the particular circumstances.

IX. **Updating the Program**

A. The program shall be re-evaluated and updated periodically to reflect changes in risks to customers or the safety and soundness of the university based on factors such as:
   - The experiences of the university with identity theft;
   - Changes in methods of identity theft;
   - Changes in methods to detect, prevent, and mitigate identity theft;
   - Changes in the types of accounts that the university offers or maintains; or
   - Changes in the business arrangements of the university, including cooperative agreements with other universities and service provider arrangements.

B. The reviews will include an assessment of which accounts are covered by the program, and the risk of identity theft with respect to each type of covered account.

X. **Oversight of Service Providers**

It will be the responsibility of the university to ensure that the activity of a service provider, who is engaged by the university to perform an activity in connection with covered accounts, is conducted with reasonable policies and procedures designed to detect, prevent, and mitigate the risk of identity theft. A service provider that maintains its own identity theft prevention program that is consistent with the policy of Concordia University Texas and the federal law and regulations may be considered to be meeting these requirements.