THE LUTHERAN UNIVERSITY ASSOCIATION, INC.
d/b/a Valparaiso University

IDENTITY THEFT PREVENTION PROGRAM

SECTION 1: BACKGROUND

The risk to Valparaiso University ("University"), its employees, students (in each instance, current and former) and other affected third parties from data loss and identity theft is of significant concern to the University and can be reduced only through the diligent efforts of every employee.

The University developed this Identity Theft Prevention Program ("Program") pursuant to the Federal Trade Commission's Red Flags Rule ("Rule"), which implements Section 114 of the Fair and Accurate Credit Transactions Act of 2003. This Program was developed with oversight and approval of the Administration and Finance Committee of the Board of Directors. After consideration of the size of the University's operations and account systems, and the nature and scope of the University's activities, the Board of Directors determined that this Program was appropriate for the University, and therefore approved this Program on May 2, 2009.

SECTION 2: PURPOSE

The University adopts this Program to help protect employees, students, all other affected third parties and the University from damages related to the loss or misuse of sensitive information.

This Program will:

A. Define sensitive information;

B. Describe the physical security of data when it is printed on paper;

C. Describe the electronic security of data when stored and distributed; and

D. Place the University in compliance with state and federal law regarding identity theft protection.

This Program enables the University to protect employees, students and affected third parties, reduce risk from identity fraud, and minimize potential damage to the University. The Program will help the University:

A. Identify risks that signify potentially fraudulent activity within new or existing covered accounts;

B. Detect risks when they occur in covered accounts;

C. Respond to risks to determine if fraudulent activity has occurred, and act if fraud has been attempted or committed; and,

D. Update the Program periodically, including reviewing the accounts that are covered and the identified risks that are part of the Program.

SECTION 3: SCOPE

This Program applies to the University employees, students and all other affected parties, both current and former.

SECTION 4: IDENTITY THEFT PREVENTION PROGRAM: SENSITIVE INFORMATION

i) Definition of Sensitive Information - Sensitive information includes the following items whether stored in electronic or printed format:

(1) Credit card information, including any of the following:

(a) Credit card number (in whole or part)
(b) Credit card expiration date
(c) Cardholder name
(d) Cardholder address

(2) Tax identification numbers, including:

(a) Social Security number
(b) Business identification number
(c) Employer identification numbers

(3) Payroll information, including, among other information:

(a) Direct Deposit data
(b) Pay Advices
(c) Pay reports

(4) Medical information for any employee or student, including but not limited to:

(a) Doctor names and claims
(b) Insurance claims
(c) Prescriptions
(d) Any related personal medical information

(5) Other personal information belonging to any employee, student or other affected party, examples of which include:

(a) Date of birth
(b) Address
(c) Phone numbers
(d) Maiden Name
(e) Names

(6) University personnel are encouraged to use common sense judgment in securing confidential information to the proper extent. If an employee is uncertain of the sensitivity of a particular piece of information, he/she should contact his/her supervisor.

ii) Hard Copy Distribution - Each employee performing work for the University will comply with the following policies:

(1) File cabinets, desk drawers, overhead cabinets, and any other storage space containing documents with sensitive information will be locked when not in use.

(2) Storage rooms containing documents with sensitive information and record retention areas will be locked at the end of each workday or when unsupervised.

(3) Desks, workstations, work areas, printers and fax machines, and common shared work areas will be cleared of all documents containing sensitive information when not in use.

(4) Whiteboards, dry-erase boards, writing tablets, etc. in common shared work areas will be erased, removed, or shredded when not in use.

(5) When documents containing sensitive information are discarded they will be placed inside a locked shred bin or immediately shredded using a mechanical cross cut or Department of Defense (DOD) – approved shredding device. Locked shred bins are labeled "*Confidential paper shredding and recycling*."

iii) Electronic Distribution - Each employee and contractor performing work for the University will comply with the following policies:

(1) Internally, sensitive information may be transmitted using approved the University e-mail. All sensitive information must be encrypted when stored in an electronic format.

(2) Any sensitive information sent externally must be encrypted and password protected and sent only to approved recipients. Additionally, a statement such as this should be included in the e-mail:

"This message may contain confidential and/or proprietary information and is intended for the person/entity to whom it was originally addressed. Any use by others is strictly prohibited."

SECTION 5: ADDITIONAL IDENTITY THEFT PREVENTION PROGRAM

A. COVERED ACCOUNTS

A covered account includes any account that involves or is designed to permit multiple payments or transactions. Every new and existing employee or student account that meets the following criteria is also covered by this Program:

i) Business, personal and household accounts for which there is a reasonably foreseeable risk of identity theft; or

ii) Business, personal and household accounts for which there is a reasonably foreseeable risk to the safety or soundness of the University from identity theft, including financial, operational, compliance, reputation, or litigation risks.

B. RED FLAGS

Red flags are potential indicators of fraud. Any time a red flag, or a situation closely resembling a red flag, is apparent, it should be investigated for verification. Sections 5.C.1 - 5.F.5 identify various red flags applicable to the University's covered accounts.

C. RED FLAGS – NOTIFICATIONS OR WARNINGS FROM A CONSUMER REPORTING AGENCY

i) Alerts, notifications or warnings from a consumer reporting agency;

ii) A fraud or active duty alert included with a consumer report;

iii) A notice of credit freeze from a consumer reporting agency in response to a request for a consumer report; or

iv) A notice of address discrepancy from a consumer reporting agency.

v) Red flags also include consumer reports that indicate a pattern of activity inconsistent with the history and usual pattern of activity of an individual, 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 that was closed for cause or identified for abuse of account privileges by a financial institution or creditor.

D. SUSPICIOUS DOCUMENTS

Red flags may also include the following:

i) Documents provided for identification that appear to have been altered or forged.

ii) The photograph or physical description on the identification is not consistent with the appearance of the person presenting the identification.

iii) Other information on the identification is not consistent with information provided by the person opening a new covered account or presenting the identification.

iv) Other information on the identification is not consistent with readily accessible information that is on file with the University.

v) An application appears to have been altered or forged, or gives the appearance of having been destroyed and reassembled.

E. SUSPICIOUS PERSONAL IDENTIFYING INFORMATION

The following items may be red flags:

i) 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;

(2) The Social Security number (SSN) has not been issued or is listed on the Social Security Administration's Death Master File; or

(3) Personal identifying information provided by the employee or student is not consistent with other personal identifying information provided by the person. For example, there might be a lack of correlation between the SSN range and date of birth.

ii) Personal identifying information provided is associated with known fraudulent activity as indicated by internal or third-party sources used by the University. For example, an address provided on one document is the same as the address provided on a different, but fraudulent, document.

iii) 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 a document is fictitious or a mail drop;
(2) The phone number is invalid or is associated with a pager or answering service; or

(3) The request was made from a non-University issued e-mail account.

iv) The SSN provided is the same as that submitted by other employees, students or other affected parties.

v) The address or telephone number provided is the same as or similar to the address or telephone number submitted by an unusually large number of other employees, students or other affected parties.

vi) The person opening the covered account fails to provide all required personal identifying information.

vii) Personal identifying information provided is not consistent with personal identifying information that is on file with the University.

viii) When using security questions (mother's maiden name, etc.), the person opening the covered account cannot provide authenticating information beyond that which generally would be available from a wallet or consumer report.

F. UNUSUAL USE OF, OR SUSPICIOUS ACTIVITY RELATED TO, THE COVERED ACCOUNT.

Red flags may further include the following:

i) Mail sent to the employee, student or other affected party is returned repeatedly as undeliverable although transactions continue to be conducted in connection with the covered account.

ii) The University is notified that the employee or student is not receiving paper or electronic account statements.

iii) The University is notified of unauthorized activity in connection with an employee's or student's covered account.

iv) The University receives notice from employees, students, victims of identity theft, law enforcement authorities, or other persons regarding possible identity theft in connection with covered accounts held by the University.

v) The University is notified by an employee, student, a victim of identity theft, a law enforcement authority, or any other person that the University has opened a fraudulent account for a person engaged in identity theft.

SECTION 6: RESPONDING TO RED FLAGS

Once potentially fraudulent activity is detected, the University employee must act quickly as a rapid appropriate response can protect the University and any affected person from damages and loss.

A. Once potentially fraudulent activity is detected, the employee must gather all related documentation, write a description of the situation and present this information to the designated authority for determination.

B. The University's legal counsel will complete additional authentication to determine whether the attempted transaction was fraudulent or authentic.

If a transaction is determined to be fraudulent, appropriate actions must be taken immediately. Actions may include:

A. Denying access to the covered account until other information is available to eliminate the red flag;

B. Canceling the transaction;

C. Notifying and cooperating with appropriate law enforcement;

D. Determining the extent of liability of the University;

E. Notifying the affected person that fraud has been attempted;

F. Changing any passwords, security codes, or other security devices that permit access to a covered account; and,

G. Determining that no response is warranted under the particular circumstances.

SECTION 7: PERIODIC UPDATES TO THE PROGRAM

A. At periodic intervals or as required, this Program will be re-evaluated to determine whether all aspects of the Program are up to date and applicable in the current business environment. The following factors may lead to a re-evaluation or review:

   i) The experiences of the University with identity theft;

   ii) Changes in methods of identity theft;

   iii) Changes in methods to detect, prevent, and mitigate identity theft;

   iv) Changes in the types of accounts that the University offers or maintains; and

v) Changes in the business arrangements of the University, including service provider arrangements.

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

C. As part of the review, red flags may be revised, replaced or eliminated. Defining new red flags may also be appropriate.

D. Actions to take in the event that fraudulent activity is discovered may also require revisions to the Program to reduce damage to the University and its customers.

SECTION 8: PROGRAM ADMINISTRATION

A. INVOLVEMENT OF MANAGEMENT

i) The Program shall not be operated as an extension to existing fraud prevention programs, and its importance warrants the highest level of attention.

ii) Approval of the Program is the responsibility of the Board of Directors and will be appropriately documented and maintained.

iii) Operational responsibility of the Program shall be delegated to an appropriate Executive Officer ("Executive Officer") of the University.

B. REPORTS

i) The Executive Officer shall report to the Board of Directors at least annually, on compliance by the University with its obligations under applicable law.

ii) The report will address material matters related to the Program and evaluate issues such as: the effectiveness of the policies and procedures of the University in addressing the risk of identity theft in connection with the opening of covered accounts and with respect to existing covered accounts; service provider arrangements; significant incidents involving identity theft and management's response; and recommendations for material changes to the Program.

C. STAFF TRAINING

i) Staff training shall be conducted for all employees, officials and contractors for whom it is reasonably foreseeable that they may come into contact with accounts or personally identifiable information that may constitute a risk to the University or its employees, students or other affected parties.

ii) The Provost and the Executive Officer are responsible for ensuring identity theft training for all requisite employees and contractors.

iii) Employees must receive annual training in all elements of this Program.

iv) To ensure maximum effectiveness, employees may continue to receive additional training as changes to the Program are made.

D. OVERSIGHT OF SERVICE PROVIDER ARRANGEMENTS

i) It is the responsibility of the University to ensure that the activities of all service providers are conducted in accordance with reasonable policies and procedures designed to detect, prevent, and mitigate the risk of identity theft.

ii) A service provider that maintains its own identity theft prevention program, consistent with the guidance of the red flag rules and validated by appropriate due diligence, may be considered to be meeting these requirements.

iii) Any specific requirements should be specifically addressed in the appropriate contract arrangements.

The Program will take effect immediately upon its passage by the Board of Directors.