CLARKE UNIVERSITY
IDENTITY THEFT PREVENTION PROGRAM

This policy was developed by Clarke University in order to comply with the regulations of the Federal Trade Commission pertaining to the detection and prevention of identity theft, the Red Flags Rule, which becomes effective December 31, 2010.

POLICY DETECTION AND PREVENTION OF IDENTITY THEFT

A. Program Application

This policy applies to Clarke University because it offers covered accounts as defined by the Fair & Accurate Credit Transaction Act ("FACTA") and this policy. In accordance with FACTA, Clarke University has developed and implemented a written Identity Theft Prevention Program ("Program") that is designed to detect, prevent, and mitigate identity theft in connection with the opening of a covered account or any existing covered account.

B. Definitions

Covered account means:

1. An account that Clarke University offers or maintains that involves or is designed to permit multiple payments or transactions, such as a student loan or a student account making multiple payments on a payment plan.

2. Any other account that the University offers or maintains for which there is a reasonably foreseeable risk to customers or to the safety and soundness of Clarke University from identity theft, including financial, operational, compliance, reputation, or litigation risks.

C. Identifying Red Flags

Clarke University is dedicated to the identification and prosecution of potential identity theft attempts with the incorporation of the following Red Flag actions. Red Flags are patterns, practices or specific activities that indicate the possible existence of identity theft in connection with Clarke students, employees and vendors. Below are examples of red flags:

1. A student application appears to have been forged, altered, or destroyed and reassembled
2. Documents provided for identification of students or employees appearing altered or forged
3. A photograph or information on an ID is inconsistent with appearance or information provided by a student or employee
4. The Social Security number supplied by a student or employee is the same as that submitted by another person, or does not agree with the Social Security Administration Verification Webpage
5. The address or telephone number supplied by a student applicant is the same or similar to the account number or telephone number submitted by an unusually large number of other persons

6. Clarke University is notified that the student is not receiving account statements.

D. Detecting Red Flags

In order to detect Red Flags in connection with the opening of covered accounts and existing covered accounts, it is the policy of Clarke University to:

1. Obtain identifying information about, and verify the identity of, a person opening a covered account, and
2. Authenticate covered account holders, monitor transactions, and verify the validity of change of address requests, in the case of existing covered accounts.

E. Responding to Detected Red Flags

If Clarke should identify a Red Flag issue when a student account or employee personnel record is established in its database, an investigation should immediately occur by the office obtaining the information. If the information appears to be fraudulent, the office should notify the Vice President for Business & Finance. The Vice President for Business & Finance, with the help of his/her staff, will investigate the matter and then determine one of the following actions to be considered:

1. Monitoring a covered account for evidence of identity theft;
2. Contacting the covered account holder;
3. Changing any passwords, security codes, or other security devices that permit access to a covered account;
4. Reopening a covered account with a new account number;
5. Not opening a new covered account;
6. Closing an existing covered account;
7. Not attempting to collect on a covered account or not selling a covered account to a debt collector;
8. Notifying law enforcement; or
9. Determining that no response is warranted under the particular circumstances.

F. Updating the Program

Clarke University shall update the Program (including the Red Flags determined to be relevant) periodically, to reflect changes in risks to covered account holders or to the safety and soundness of Clarke University from identity theft, based on factors such as:

1. The experiences of the University with identity theft;
2. Changes in methods of identity theft;
3. Changes in methods to detect, prevent, and mitigate identity theft;
4. Changes in the types of accounts that Clarke University offers; and
5. Changes in the business arrangements of Clarke University, including changes in service provider agreements.

G. Administration & Oversight of the Program

In order to comply with its obligations under FACTA, Clarke University shall:

1. Obtain approval of the initial written Program from the University's board of trustees;

2. Involve the Vice President for Business & Finance of the University in the oversight, development, implementation and administration of the Program;
3. Train staff, as necessary, to effectively implement the Program; and
4. Exercise appropriate and effective oversight of service provider arrangements.

Appropriate and effective oversight of the Program shall include oversight by the Vice President for Business & Finance of the University who is:

1. Assigned specific responsibility for the Program's implementation;
2. Responsible for reviewing reports prepared by staff regarding compliance by the University;
3. Approving material changes to the Program as necessary to address changing identity theft risks.

H. Annual Assessment of Covered Accounts

Clarke University shall annually determine whether it offers or maintains covered accounts. As a part of this determination, the University shall conduct a risk assessment to determine whether it offers or maintains covered accounts, taking into consideration:

1. The methods it provides to open its accounts;
2. The methods it provides to access its accounts; and
3. Its previous experiences with identity theft.
4. Any new or expanded credit or debit activities covered under the FACTA guidelines.

I. Annual Report to Board

The Vice President for Business & Finance should report to the board of trustees at least annually, on compliance by Clarke University with this policy.

The report should 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 the University's response; and recommendations for material changes to the Program.

Approved April 13, 2009
Revised August 19, 2010