ï»¿

Red Flag Rule

Purpose/Statement

In response to the growing threat of identity theft, the United States Congress passed the Fair and Accurate Credit Transactions Act of 2003 (FACTA). On November 9, 2007, the Federal Trade Commission circulated the final rules, known as the "Red Flag" rules, which have an effective date of November 1, 2008 and an enforcement date of November 1, 2009 that has now been extended to December 31, 2010. These rules, implementing sections 114 and 315 of FACTA, require "financial institutions" and "creditors" with "covered accounts" to enact certain policies and procedures that would enable the institution to mitigate, identify, detect, and respond to patterns, practices, or specific activities—known as "red flags"—that could indicate identity theft.

Reason for the Policy: The policy is designed to detect, prevent and mitigate identity theft in connection with the opening of a covered account or an existing covered account and to provide for continued administration of an Identify Theft Detection Program. The Program shall include reasonable policies and procedures to:

- Identify relevant red flags for covered accounts it offers or maintains and incorporate those red flags into the program;
- Detect red flags that have been incorporated into the Program;
- Respond appropriately to any red flags that are detected to prevent and mitigate identity theft; and
- Ensure the Program is updated periodically to reflect changes in risks to Students and to the safety and soundness of the creditor from identity theft.

The program shall, as appropriate, incorporate existing policies and procedures that control reasonably foreseeable risks.

Overview

Colleges and Universities that participate in federal or institutional loan programs, or make available payment plans and/or promissory notes (extending credit), or who generate credit report inquiries for loans are considered "**creditors**" with "**covered accounts**" and are therefore subject to the Red Flag regulations.

The Red Flag Rule applies to Clark due to our participation in the Perkins Loan program, our institutional loan program, and our extension of credit for student accounts. Our analysis of the type and scope of activity covered in the regulation, and our risk assessment of potential identity theft opportunities has resulted in a determination that there is a low level risk of possible identity theft at Clark University.

Entities Affected by this Policy

Primary Clark Departments

- Business and Financial Services—Students are extended credit that allows a balance to be paid in future installments. The University offers employees a loan for home purchase in the University neighborhood.

- Graduate School of Management—Students are extended credit that allows a balance to be paid in future installments.
- One Card Office—Students are given ID cards which serves as their cash card, which is a physical extension of their student account.

Other Departments that have access to and could obtain and/or retain data:

- Information Technology (IT)
- Human Resources
- University Advancement
- Registrar Office
- Payroll
- Accounts Payable
- Admissions
- Dean of Students
- University Police
- Academic Advising
- College of Professional and Continuing Education

Third-Party Service Providers

- Educational Computing Services Inc. (ECSI) - a Perkins Loan servicer for the purpose of billing and collection of Perkins and Clark institutional loan payments.
- Tuition Management Services - a payment plan company that collects monthly payments from our families.
- Delta Management - a collection agency that collects past due student receivables and defaulted Perkins and Clark Loans on behalf of Clark University.
- Windham Professionals - a collection agency that collects past due student receivables and defaulted Perkins and Clark Loans on behalf of Clark University.
- International and extended campus programs administered by COPACE

Who Should Read this Policy—All faculty, staff and students should be aware of the policy. Employees, students and service providers are responsible for reporting any suspicious changes in data (address discrepancies, presentation of suspicious documents, suspicious activity related to covered accounts, notification of fraudulent activity from a credit agency etc.

Definitions

Covered Account	A "**covered account**" is 1) an account primarily for personal, family or household purposes that involves or is designed to permit multiple payments or transactions or 2) any other account for which there is a foreseeable risk to customers or the safety and soundness of the "financial institution" or "**creditor**" from identity theft.Â At Clark, a

	"covered account" includes all student accounts and loans that are administered by the University.
Creditor	A "**creditor**" is an entity that 1) regularly extends, renews or continues credit; or 2) regularly arranges for the extension, renewal, or continuation of credit; or 3) is involved in the decision to extend, renew, or continue credit.
IndentifyingÂ Information	"Identifying information" is any name or number that may used, alone or in conjunction with any other information, to identify a specific person, including, name, social security number, date of birth, government issued driver's license or identification number, alien registration number, government passport number,Â employer orÂ taxpayer identification number, unique biometric data, unique electronic identification information of access device, orÂ telecommunication identifying information or access device.
Identity Theft	"Identity theft" is a fraud committed or attempted using information of another person without authority.
Red Flag	A "red flag" is a pattern, practice or specific activity that indicates the possible existence of identity theft.
Responsible Organization/Party	The "responsible organization/party" is the office or person at the University designated with primary responsibility for oversight of the regulation. Defined at Clark as the Data Manager.

Procedures

Under the Red Flags Rule, Clark is required to establish a written "Identity Theft Prevention Program" tailored to its size, complexity and the nature of its operation. The plan should include

procedures to detect, prevent, and respond to patterns, practices, or specific activities that may indicate identity theft. The designed program must be approved by the organization's board of directors or appointed committee, and it must be updated and monitored according to changes in risk. The University must assign a person or persons for specific oversight, train staff, and audit compliance to accomplish the following:

- **Identify Red Flags** for new and existing covered accounts and incorporate those Red Flags into the Program
- **Detect Red Flags** that have been incorporated into the Program
- **Respond to Red Flags** identified in the Program appropriately to prevent and mitigate identity theft.
- **Ensure the program is updated** periodically to reflect changes in risks to students and customers.

Identification of Red Flags

In order to identify relevant Red Flags, the University considers the types of accounts that it offers and maintains, methods it provides to open its accounts, methods it provides to access its accounts, and its previous experiences with Identity Theft. The University identifies the following Red Flags in each of the listed categories:

A. Suspicious Documents

Red Flags

- Identification document or card that appears to be forged, altered or inauthentic
- Identification document or card on which a person's photograph or physical description is not consistent with the person presenting the document
- Other document with information that is not consistent with existing student information
- Application for service that appears to have been altered or forged

B. Suspicious Personal Identifying Information

Red Flags

- Identifying information presented that is inconsistent with other information the student provides (example: inconsistent birth dates)
- Identifying information presented that is inconsistent with other sources of information (for instance, an address not matching an address on a loan application)
- Identifying information presented that is the same as information shown on other applications that were found to be fraudulent
- Identifying information presented that is consistent with fraudulent activity (such as an invalid phone number or fictitious billing address)
- Social security number presented that is the same as one given by another student
- An address or phone number presented that is the same as that of another person
- A person fails to provide complete personal identifying information on an application when reminded to do so
- A person's identifying information is not consistent with the information that is on file for the student.

C. Suspicious Covered Account Activity or Unusual Use of Account

Red Flags

- Change of address for an account followed by a request to change the student's name
- Payments stopped on an otherwise consistently up-to-date account
- Account used in a way that is not consistent with prior use
- Mail sent to the student is repeatedly returned as undeliverable
- Notice to the University that a student is not receiving mail sent by the University
- Notice to the University that an account has unauthorized activity
- Breach in the University's computer system security
- Unauthorized access to or use of student account information

D. Alerts from Others

Red Flag

Notice to the University from a student, Identity Theft victim, law enforcement, third-party service provider, or other person that the University has opened or is maintaining a fraudulent account for a person engaged in Identity Theft.

Detecting Red Flags

A. Student Enrollment
In order to detect any of the Red Flags identified above associated with the enrollment of a student, University personnel will take the following steps to obtain and verify the identity of the person opening the account:

Detect

- Require certain identifying information such as name, date of birth, academic records, home address or other identification
- Verify the student's identity at time of issuance of student identification card (review of driver's license or other government-issued photo identification).

B. Existing Accounts
In order to detect any of the Red Flags identified above for an existing Covered Account, University personnel will take the following steps to monitor transactions on an account:

Detect

- Verify the identification of students if they request information (in person, via telephone, via facsimile, via email)
- Verify the validity of requests to change billing addresses by mail or email and provide the student a reasonable means of promptly reporting incorrect billing address changes
- Verify changes in banking information given for billing and payment purposes

Preventing and Mitigating Identity Theft

In the event University personnel detect any identified Red Flags, such personnel shall take one or more of the following steps, depending on the degree of risk posed by the Red Flag:

Prevent and Mitigate

- Notify the Red Flag Data Manager for determination of the appropriate step(s) to take:
- Continue to monitor a Covered Account for evidence of Identity Theft
- Contact the student or employee
- Change any passwords or other security devices that permit access to Covered Accounts
- Not open a new Covered Account
- Provide the student with a new student identification number
- Notify law enforcement
- Determine that no response is warranted under the particular circumstances

Protect Student Identifying Information

In order to further prevent the likelihood of Identity Theft occurring with respect to Covered Accounts, the University will take the following steps with respect to its internal operating procedures to protect student identifying information:

- Ensure that its website is secure or provide clear notice that the website is not secure
- Ensure complete and secure destruction of paper documents and computer files containing student account information when a decision has been made to no longer maintain such information
- Ensure that office computers with access to Covered Account information are password protected
- Avoid use of social security numbers
- Ensure computer virus protection is up to date
- Require and keep only the kinds of student and employee information that are necessary for University purposes.

Program Administration

A. Oversight
Responsibility for developing, implementing and updating this Program lies with the Red Flag Data Manager. The Data Manager will be responsible for ensuring appropriate training of University staff on the Program, for reviewing any staff reports regarding the detection of Red Flags and the steps for preventing and mitigating Identity Theft, determining which steps of prevention and mitigation should be taken in particular circumstances and considering periodic changes to the Program.

B. Staff Training and Reports
University staff responsible for implementing the Program shall be trained either by or under the direction of the Red Flag Data Manager in the detection of Red Flags and the responsive steps to be taken when a Red Flag is detected. University staff shall be trained, as necessary, to effectively implement the Program. University employees are expected to notify the Program Administrator once they become aware of an incident of Identity Theft or of the University's failure to comply with this Program. At least annually, University staff responsible for development, implementation, and administration of the Program shall report to the Red Flag Data Manager on compliance with this

Program. The report should address such issues as effectiveness of the policies and procedures in addressing the risk of identity theft in connection with the opening and maintenance of Covered Accounts, service provider arrangements, significant incidents involving identity theft and management's response, and recommendations for changes to the Program.

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.
Â· Require, by contract, that service providers have such policies and procedures in place
Â· Require, by contract, that service providers review the University's Program and report any Red Flags to the Program Administrator or the University employee with primary oversight of the service provider relationship.

D. Program Updates
The Red Flag Data Manager will annually review and update this Program to reflect changes in risks to students and employees and the soundness of the University from Identity Theft. In doing so the Manager consider the University's experiences with Identity Theft situations, changes in Identity Theft methods, changes in Identity Theft detection and prevention methods, and changes in the University's business arrangements with other entities. After considering these factors, the Red Flag Data Manger will determine whether changes to the Program, including the listing of Red Flags, are warranted. If warranted, the Data Manger will update the Program.

Related Policies, Laws and Resources:
Red Flag Rule [PDF]

Date of Creation: October 24, 2008
Date of Last Revision: June 12, 2010