RED FLAGS RULE PROGRAM

CLEMSON UNIVERSITY

RED FLAGS RULE PROGRAM

I. BACKGROUND

In response to the growing threats of identity theft in the United States, Congress passed the Fair and Accurate Credit Transactions Act of 2003 (FACTA), which amended a previous law, the Fair Credit Reporting Act (FCRA). This amendment to FCRA charged the Federal Trade Commission (FTC) and several other federal agencies with promulgating rules regarding identity theft. On November 7, 2007, the FTC, in conjunction with several other federal agencies, promulgated a set of final regulations known as the "Red Flags Rule". The Red Flags Rule became effective November 1, 2008, however, the FTC has deferred its enforcement of the rule through December 1, 2010 in order to permit institutions additional time in which to develop and implement the written identity theft prevention programs required by the Red Flags Rule regulations. An appropriate identity theft prevention program does not have to be very detailed or complex, but does need to be written, duly approved and implemented.

The Red Flags Rule is actually three different but related rules, parts of which apply to many colleges and universities. The elements consist of the following:

1. Debit and credit card issuers must develop policies and procedures to assess the validity of a request for a change of address that is followed closely by a request for an additional or replacement card. This provision will not likely affect colleges and universities, as the definition of debit card does not include stored value cards.

2. Users of consumer reports must develop reasonable policies and procedures to apply when they receive notice of an address discrepancy from a consumer reporting agency, i.e. credit or background checks for loan issuance or collection purposes, or for new hire applicants, etc.

3. Financial institutions and creditors holding "covered accounts" must develop and implement a written identity theft prevention program for both new and existing accounts. The creditor provision applies to areas of Clemson University that issue any type of credit, i.e. Perkins Loans, Short Term Loans for Students or Faculty/Staff, Housing Payment Plans, Transportation Payment Plans, Student Tuition/Fee Deferred Payment Plans, etc.

The regulations require entities that are considered "financial institutions" or "creditors" to determine if any of its extensions of credit are "covered accounts". It is mandatory for a college or university that holds covered accounts to implement a written Identity Theft Prevention Program for combating identity theft in their day-to-day operations in connection with covered accounts. The Program must develop reasonable policies and procedures for

detecting, preventing and mitigating identity theft and enable the departments with covered accounts to:

1. Identify relevant patterns, practices, or specific activities, signaling possible identity theft.

2. Detect Red Flags by implementing procedures to identify University specific red flags in the day-to-day operations.

3. Respond appropriately to any red flags that are detected to prevent and mitigate identity theft; and

4. Periodically review and update your program to keep it current as risks for identity theft can change rapidly. Educate and train staff as necessary.

II. PURPOSE

The purpose of this Program is to identify, detect, and appropriately respond to Red Flags which may indicate suspected or real incidents of identity theft upon the University, its employees, its students, its constituents and its customers and to ensure the compliance with the Federal Trade Commission's Red Flags Rule regulations. The requirements of this Program apply to Clemson University, to the employees and the third parties with whom Clemson contracts to perform certain functions on its behalf for covered accounts, such as student payment plans, federal loan programs and background checks for employment.

III. DEFINITIONS

Identity theft is defined as fraud committed or attempted using the identifying information of another person without authority. 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, but not limited to:

- Name
- Address
- Telephone number
- Social security number
- Date of Birth
- Government-issued driver's license or identification number

- Alien registration number
- Government passport number
- Individual identification number
- Bank or other financial account routing code

Financial Institution:
The Red Flags Rule defines a "financial institution" as a state or national bank, a state or federal savings and loan association, a mutual savings bank, a state or federal credit union, or any other entity that holds a "transaction account" belonging to a consumer.

Creditor:
This is a broad definition that includes a business or person who regularly defers payment for goods or services and bills customers later. The Rule also defines a "creditor" as one who regularly grants loans, arranges for loans or the extension of credit, or makes credit decisions.

Covered Accounts:
Includes both existing and new accounts that a financial institution or creditor 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. This includes small business accounts as well as personal accounts.

Transaction Account:
A deposit or other account from which the owner makes payments or transfers. Transaction accounts include checking accounts, negotiable order of withdrawal accounts, savings deposits subject to automatic transfers, and share draft accounts.

Customer:
A person that has a covered account with a financial institution or creditor.

Service Provider:
A person that provides a service directly to the financial institution or creditor.

IV. IDENTIFICATION & DETECTION OF RED FLAGS

A "Red Flag" is a pattern, practice, or specific activity that indicates the possible existence of identity theft. Any time a Red Flag, or a situation resembling a Red Flag, is apparent, it

should be investigated for verification. Potential indicators or warning signs of potential or actual identity theft or similar fraud:

Alerts, Notifications, and Warnings from a Credit Reporting Company

- Fraud or active duty alert on a credit report.
- Notice of a credit freeze in response to a request for a credit report.
- Notice of an address discrepancy provided by a credit-reporting agency.
- A credit report indicating a pattern of activity inconsistent with the person's history such as:
    1. A big increase in the volume of inquiries or the use of credit, especially on new accounts.
    2. An unusual number of recently established credit relationships; or
    3. An account that was closed because of an abuse of account privileges.

Suspicious Documents

- Identification that looks altered or forged.
- The person presenting the identification doesn't look like the photo or match the physical description.
- Information on the identification that differs from what the person presenting the identification is telling you or doesn't match with other information, like a signature card or recent check.
- An application that looks like it's been altered, forged, or torn up and reassembled.

Suspicious Personal Identifying Information

- Inconsistencies with what else you know – for example, an address that doesn't match the credit report, the use of a Social Security number that's listed on the Social Security Administration Death Master File, or a number that hasn't been issued, according to the monthly issuance tables available from the Social Security Administration.
- Inconsistencies in the information the customer has given you – say, a date of birth that doesn't correlate to the number range on the Social Security Administration's issuance tables.
- An address, phone number, or other personal information that's been used on an account you know to be fraudulent.
- A bogus address, an address for a mail drop or prison, a phone number that's invalid, or one that's associated with a pager or answering service.
- A Social Security number that's been used by someone else opening an account.
- An address or telephone number that's been used by many other people opening accounts.

- A person who omits required information on an application and doesn't respond to notices that the application is incomplete.
- A person who can't provide authenticating information beyond what's generally available from a wallet or credit report – for example, a person who can't answer a challenge question.

Suspicious Account Activity

- After you're notified of a change of address, you're asked for new or additional credit cards, cell phones, etc., or to add users to the account.
- A new account that's used in ways associated with fraud.
- An account that's used in a way inconsistent with established patterns – for example, nonpayment when there's no history of missed payments, a big increase in the use of available credit, a major change in buying or spending patterns or electronic fund transfers, or a noticeable change in calling patterns for a cell phone account.
- An account that's been inactive for a long time is suddenly used again.
- Mail sent to the customer that's returned repeatedly as undeliverable although transactions continue to be conducted on the account.
- Information that the customer isn't receiving their account statements in the mail.
- Information about unauthorized charges on the account.

Notice from Other Sources

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.

V. RESPONDING TO RED FLAGS

If a Red Flag is identified, Clemson University shall act quickly, as a rapid appropriate response can protect customers, employees, students and the institution from damages and loss. The Chief Financial Officer, the Program Coordinator and the Red Flag Committee shall be responsible for developing policies and procedures to ensure that when a Red Flag, or a situation resembling a Red Flag is apparent, it is investigated and an appropriate response is implemented.

The appropriate response will be dependent on the type of Red Flag identified, type of transaction, relationship with the victim of the fraud, availability of contact information for the victim of the fraud, and numerous other factors. However, by way of example, appropriate actions may include, but are not limited to:

- Monitoring a covered account for evidence of identity theft.

- Contacting the customer.
- Changing passwords, security codes, or other ways to access a covered account.
- Closing an existing account.
- Reopening an account with a new account number.
- Not opening a new account.
- Not trying to collect on an account.
- Notifying law enforcement.
- Determining that no response is warranted under the particular circumstances.

A. CONSUMER REPORTS—ADDRESS VERIFICATION

Any University office that obtains or receives notice from a consumer reporting agency or credit bureau stating the address furnished is different from the one in the agencies files must ensure that it has reasonable policies and procedures in place to enable the office to form a reasonable belief that the report is for the person intended. The office may reasonably confirm the accuracy of the consumer's address by:

- Verifying the address with the consumer about whom it has requested the report.
- Reviewing its own records (e.g., job applications, change of address notification forms other customer account records) to verify the address of the consumer.
- Verifying the address through third-party sources; or
- Using other reasonable means.

The office must provide the consumer's address that it has reasonably confirmed to be accurate, to the Consumer Reporting Agency.

B. THIRD PARTY SERVICE PROVIDERS

It is the responsibility of the University to ensure that the activities of any third service provider that is utilized in processing or establishing covered accounts, conducts their business in accordance with reasonable policies and procedures designed to detect, prevent, and mitigate the risk of identity theft. Before the University engages a service provider to perform an activity in connection with one or more of the University's covered accounts,
(i.e. offering students the option of having their student ID also operate as a Visa or MasterCard debit card should coordinate with the bank to ensure the bank has an adequate

identity theft program in place), the University must take the following steps to ensure the service provider performs its activities in accordance with reasonable policies and procedures designed to detect, prevent and mitigate the risks of identity theft:

- The University must require by contract that the service provider has such policies and procedures in place; and

- The University must require by contract that the service provider is aware of the University's Identity Theft Program, and will report any Red Flags it identifies as soon as possible to the department Supervisor.

VI. PROGRAM ADMINISTRATION

As part of the University's Compliance Monitoring Plan, a Red Flag Committee for the University will be established and consist of departmental representatives from Human Resources, Student Services, Admissions, Procurement, Student Affairs, Computing and information Technology and Financial Service Divisions. A representative from General Counsel and Internal Audit will serve on an ad hoc basis. A Program Coordinator in collaboration with the Red Flag Committee members will be identified and will be responsible for reviewing staff reports regarding detection of Red Flags, monitoring the response procedures to prevent and mitigate identity theft, and interpreting regulatory correspondence from the Federal Trade Commission and federal agencies. The Identity Theft Committee will identify and define Red Flags and periodically review procedures and actions required for the detection of Red Flag issues. The Identity Theft Committee and Program Coordinator will meet at least annually to review and discuss any changes, updates or compliance issues that may arise.

A. UPDATING THE PROGRAM

Departmental representatives will maintain responsibility for the implementation and ongoing support of this regulation in their respective department(s). On at least an annual basis the departmental representative will re-evaluate all aspects of the program to determine if they are up to date and applicable in the current business environment. In addition, they will audit compliance within the department to the Program and submit a written report to the Red Flag Committee. Periodic reviews will include an evaluation of which accounts are covered by the program.

B. STAFF TRAINING

The departmental representative will maintain responsibility for training staff responsible for

implementing the program in their respective department(s) as necessary. Only those staff members charged with effectively implementing the identification, detection and responsive steps to be taken when a Red Flag is detected, should be trained. Otherwise, any documents that have been produced to develop and implement this program are considered confidential and should not be shared with other University employees or the public.

VII. BOARD APPROVAL

Under the Red Flags Regulations, it is mandatory that the initial written Program be subject to Board, (or an appropriate committee of the board) approval. Once the initial written program is approved, The Board of Trustees will hereby delegate responsibility to oversee, implement and administer this Red Flag Program to the Clemson University Chief Financial Officer including the creation of appropriate policies and procedures.

VIII. RESOURCES

Federal Trade Commission. *Fighting Fraud with the Red Flags Rule: A How-To Guide for Business.*
http://www.ftc.gov/redflagsrule

Federal Trade Commission. *FTC Business Alert.*
http://www.RedFlags@ftc.gov

Federal Trade Commission. *Federal Register*. November 9, 2007, p. 63771 – 63773, 16 CFR Part 681

Federal Trade Commission. *Fighting Fraud with the Red Flags Rule:* Frequently Asked Questions.
http://www.ftc.gov/redflagsrule

Federal Trade Commission. Guidelines to FTC Red Flag Rule. *Interagency Guidelines on Identity Theft Detection, Prevention, and Mitigation.* Appendix J to Part 681-

NACUBO: *FTC'S Red Flag Rule Likely to Affect Colleges*
http://www.nacubo.org/Initiatives/News/FTCs_Red_Flag_Rule_Likely_to_Affect_Colleges.html

National Archives and Records Administration: *Federal Register*. November 9, 2007

IX. APPENDIX

Some Examples of Departments Impacted by the Policy

- Human Resources
  - Training
  - Address changes, presentation of identification
  - Background checks
  - Requests for payroll documents

- Financial Services
  - Address changes
  - Financial Aid document verification
  - Requests for 1098-T documents

- Office of the Registrar
  - Address changes
  - Requests for transcripts

- Admission
  - Changes to applicant information

- Technology Services
  - Assessment of risk and prevention
  - Password/ system access
  - Possible implementation of process to include recording and reporting

- Student Affairs
  - Changes to applicant information
  - Address changes
  - Presentation of identification

- Procurement
  - Address changes

Third party transactions
Requests for 1099 documents