



Medical College of Georgia

Administrative
Policy Library

**Identity Theft Program
Policy**
(FTC Red Flag & Address Rules)

CITATION REFERENCE

Official Title: Identity Theft Program Policy (FTC Red Flag & Address Rules)

Abbreviated Title: Identity Theft Program

Volume: Finance & Administration

Responsible Office: Controller's Office

Originally issued: April 2009

Revised: Not applicable

Policy Statement

This policy applies to any department or individual reviewing consumer credit or criminal background reports on employees, students or other customers.

This policy also applies to anyone on campus who may receive address, name or bank information change requests from such parties.

This Identity Theft Program (The Program) was developed under the oversight of Finance Administration based upon consideration of the nature and scope of the College's activities. On the recommendation of the Senior Vice President for Finance and Administration, this program has been duly approved by the President's Cabinet.

Reason for Policy

The Office of Consumer Credit and various Federal Agencies have jointly issued final rules and guidelines implementing section 114 and 315 of the Fair and Accurate Credit Transactions Act of 2003 (FACT Act.)

This Program is developed pursuant to the section 114 rules which require each financial institution or creditor to develop and implement a written Identity Theft Prevention Program to detect, prevent, and mitigate identity theft in connection with the opening of certain accounts or certain existing accounts.

The section 114 rules require the assessment of the validity of notifications of changes of address under certain circumstances, and the section 315 rules provide guidance regarding reasonable policies and procedures that a user of consumer reports must employ when a consumer reporting agency sends the user a notice of address discrepancy.

Entities Affected By This Policy / Who Should Read This Policy

All departments or individuals who may have the occasion to receive address, name or bank information change requests from employees, students or other MCG customers, or who may review consumer credit or criminal background reports on the same must comply with this policy.

Any and all personnel who have security access to personal information databases (student, employee or customer records) are responsible for the application of this and related policies.

Contacts

Contact	Phone	e-mail/URL
Human Resources	706-721-7905	dpickett@mcg.edu
Public Security	706-721-8106	wmcbride@mcg.edu
Controller's Division	706-721-4116	krust@mcg.edu

Website Address for This Policy

www.mcg.edu/policies/documents/identitytheftprogram.pdf

Related Documents

None

Definitions

Red Flags Rule: A regulation issued in 2007 by the Federal Trade Commission (FTC) and Federal banking agencies intended to reduce the risk of identify theft. Mandatory compliance with the Red Flags Rule for "creditors" or "financial institutions" that provide "covered accounts" begins on May 1, 2009. The FTC has stated that nonprofit and government entities can be subject to parts of the rule.

The Red Flags Rule is actually three different but related rules, one or two of which apply to many colleges and universities. There are 26 detailed rules which fall under the three general categories and which are detailed below:

(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 is likely not applicable to colleges and universities, because, as discussed in the preamble to the Red Flags Rule, the definition of "debit card" specifically does not include stored value cards. However, this provision could implicate student ID's that can also be used as part of a national debit card network, such as Visa or MasterCard.)*

(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. *(This provision applies to colleges and universities when they use consumer reports to conduct credit or background checks on prospective employees or applicants for credit.)*

(3) Financial institutions and creditors holding "covered accounts" must develop

and implement a written identity theft prevention program for both new and existing accounts. *(This provision likely applies to many colleges and universities).*

Identity Theft: Fraud committed using the identifying information of another person.

Creditor: The Red Flags Rule defines the terms "creditor" broadly, including any person who defers payment for services rendered, such as an organization that bills at the end of the month for services rendered the previous month. In its July 2008 guidance, the FTC stated "where non-profit and government entities defer payment for goods or services, they too are to be considered creditors."

Activities that could cause colleges and universities to be considered "creditors" under the Red Flags Rule may include

- Participating in the Federal Perkins Loan program
- Participating as a school lender in the Federal Family Education Loan or Direct Lending Programs
- Offering institutional loans to students, faculty, or staff (e.g. MCG's emergency loans for students)
- Offering a plan for payment of tuition throughout the semester (disallowed by the Board of Regents)

Covered Accounts: A consumer account that involves multiple payments or transactions, such as a loan that is billed or payable monthly, and which includes certain types of arrangements in which an individual establishes a "continuing relationship" with the enterprise, including billing for previous services rendered. The rules specifically exclude "stored value cards" (prepaid cards), such as the "debit express" cards issued to students and employees for use on campus to purchase goods and services. Covered accounts at MCG would include student loans granted or administered by the College.

Address Rules: Issued by the FTC at the same time as the "Red Flags Rule," and effective November 1, 2008, the rules (16 C.F.R. §681.1) apply not only to financial institutions and creditors but potentially to all employers that use consumer reporting agencies to conduct background checks on applicants and employees.

The Address Discrepancy rules provide specific guidelines to enable an employer to establish practices that will permit it to form a reasonable belief as to whether a consumer report relates to the person on whom the report was obtained. Those rules also provide criteria for when employers have an obligation to provide confirmed addresses to the nationwide CRA. In a nutshell, the Address Discrepancy rules require the nationwide consumer reporting agencies to provide users of consumer reports (including employers) with a notice of address discrepancy when there is a "substantial difference" between the address the agency has on file for a consumer and the address provided by the employer when requesting the report. The regulation also requires users of consumer reports

(including employers doing background checks on applicants) to establish policies that permit them to form a reasonable belief as to whether addresses provided by applicants are correct and to notify the CRA when they have confirmed applicant addresses.

Red Flags: A pattern, practice, or specific activity that indicates the possible existence of Identity Theft. These flags are circumstantial factors identified to indicate potential identity theft. While the majority of these flags pertain exclusively to a traditional creditor/customer or financial institution (banking)/customer relationship, many may still apply to the College in certain situations. The 26 flags identified are:

Alerts, Notifications or Warnings from a Consumer Reporting Agency

1. A fraud or active duty alert is included with a consumer report.
2. A consumer reporting agency provides a notice of a credit freeze in response to a request for a consumer report.
3. A consumer-reporting agency provides a notice of address discrepancy
4. A consumer report indicates a pattern of activity that is inconsistent with the history and usual pattern of activity of an applicant or customer, such as
 - A recent and significant increase in the volume of inquiries;
 - An unusual number of recently established credit relationships;
 - A material change in the use of credit, especially with respect to recently established credit relationships;
 - An account closed for cause or identified for abuse of account privileges by a financial institution or creditor.

Suspicious Documents

5. Documents provided for identification appear to have been altered or forged.
6. The photograph or physical description on the identification is not consistent with the appearance of the applicant or customer presenting the identification.
7. Other information on the identification is not consistent with information provided by the person opening a new covered account or customer presenting the identification.
8. Other information on the identification is not consistent with readily accessible information that is on file with the financial institution or creditor, such as a signature card or a recent check.
9. An application appears to have been altered or forged, or gives the appearance of having been destroyed and reassembled.

Suspicious Personal Identifying Information

10. Personal identifying information provided is inconsistent when compared against external information sources used by the financial institution or creditor. For example: The address does not match any address in the consumer report or the Social Security Number (SSN) has not been issued or is listed on the Social Security Administration's Death Master File.

11. Personal identifying information provided by the customer is not consistent with other personal identifying information provided by the customer. For example, there is a lack of correlation between the SSN range and date of birth.

12. Personal identifying information provided is associated with known fraudulent activity as indicated by internal or third-party sources used by the financial institution or creditor. For example: The address on an application is the same as the address provided on a fraudulent application or the phone number on an application is the same as the number provided on a fraudulent application.

13. Personal identifying information provided is of a type commonly associated with fraudulent activity as indicated by internal or third-party sources used by the financial institution or creditor. For example: The address on an application is fictitious, a mail drop, or a prison or the phone number is invalid or is associated with a pager or answering service.

14. The SSN provided is the same as that submitted by other persons opening an account or other customers.

15. The address or telephone number provided is the same as or similar to the account number or telephone number submitted by an unusually large number of other persons opening accounts or other customers.

16. 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.

17. Personal identifying information provided is not consistent with personal identifying information that is on file with the financial institution or creditor.

18. For financial institutions and creditors that use 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.

19. Shortly following the notice of a change of address for a covered account, the institution or creditor receives a request for a new, additional, or replacement card or a cell phone, or for the addition of authorized users on the account.

20. A new revolving credit account is used in a manner commonly associated with known patterns of fraud patterns. For example: The majority of available credit is used for cash advances or merchandise that is easily convertible to cash (e.g., electronics equipment or jewelry) or the customer fails to make the first payment or makes an initial payment but no subsequent payments.

21. A covered account is used in a manner that is not consistent with established patterns of activity on the account. There is, for example: Nonpayment when there is no history of late or missed payments; a material increase in the use of available credit; a material change in purchasing or spending patterns; a material change in electronic fund transfer patterns in connection with a deposit account; or a material change in telephone call patterns in connection with a cellular phone account.

22. A covered account that has been inactive for a reasonably lengthy period of time is used (taking into consideration the type of account, the expected pattern of usage and other relevant factors).

23. Mail sent to the customer is returned repeatedly as undeliverable although transactions continue to be conducted in connection with the customer's covered account.

24. The financial institution or creditor is notified that the customer is not receiving paper account statements.

25. The financial institution or creditor is notified of unauthorized charges or transactions in connection with a customer's covered account (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 Financial Institution or Creditor).

26. The financial institution or creditor 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.

Overview

With respect to the Address Rules, the College conducts criminal background checks on employees when being promoted into positions, candidate(s) being selected as finalists, temporary employees, consultants, and contractors. Additionally, credit checks are conducted for financially sensitive positions and for issuance of purchasing card (P-card) privileges.

With Respect to the Red Flags Rule, the College does not generally permit services to be rendered prior to payment; therefore, the following are paid in advance and do not constitute “covered accounts”:

- Student Tuition and Fees Receivables (BOR disallows payment plans)
- Wellness Center Memberships
- Student Residence Hall Rents
- Bookstore Purchases (Charges only permitted to a student’s account when a student has a pending financial aid award)

However, the College does conduct certain activities representing “covered accounts” under the Red Flags Rule. The College

- Grants emergency loans to students
- Participates in the Direct Lending Program
- Issues Perkins Loans to students
- Hires a third-party loan servicer to manage student loan accounts
- Provides Student Health services on “credit” to student, pending insurance claim settlements
- Provides Dental Clinic services on “credit” to patients, pending insurance claim settlements

In all but the last “covered account” scenarios listed above, customers are exclusively students. Therefore, the great majority of the 26 Red Flag Rules are not applicable.

COVERED ACCOUNTS PERTAINING TO STUDENTS:

Banner access is strictly controlled. Only duly enrolled students are assigned Banner IDs and passwords. Address and bank account changes may only be changed directly by a student with appropriate log-in to his or her Banner account. Students are not permitted to direct Banner correspondence to an external e-mail address; the College uses the student’s campus-issued Novell e-mail account to address all official correspondence. Upon making an address or bank account change in Banner, Banner automatically issues an e-mail notification to the student’s campus e-mail account confirming the legitimacy of the submitted change. Student service areas will not make changes to Banner on behalf of a student (the student is instructed to log in to Banner), except for name changes, which may not be made by the student. Students must appear in person at the Office of the Registrar to request name changes. Appropriate legal documentation of the name change or correction must be presented before the change will be effected.

Issuance of student loans involves an entrance interview in the Student Loan Office. Students must log in to the third party servicer website (ACS) to electronically sign a promissory note. ACS has a suitable Identity Theft Program in place and has provided us with the Program details.

Emergency Loans are not disbursed in person but are disbursed only to the student’s official address or bank account of record, as contained in the Banner records.

Neither the Student Loan Office nor the Financial Aid Office have occasion to request consumer credit reports on students. As relating to the Direct Lending Program, the Department of Education is responsible for any credit checks to be performed with respect to student loan applications. The Financial Aid Office would not, therefore, be the recipient of any credit bureau notices of address discrepancy.

Students obtaining services at Student Health must provide a student ID and insurance card to obtain services.

COVERED ACCOUNTS PERTAINING TO DENTAL CLINIC PATIENTS:
The Dental Clinic requires proof of insurance to be presented before providing services. Photo identification is also required. Name discrepancies on identification and insurance information must be adequately explained and documented. Suspicious documents will not be accepted.

COVERED ACCOUNTS PERTAINING TO EMPLOYEES: (ADDRESS RULE CONSIDERATIONS):
MCG does not extend credit to employees so there are no “covered accounts” under the meaning of the Red Flag Rule. However, in connection with extending P-card privileges to an employee, MCG requests and screens credit reports. There are also address rule considerations to be addressed.

Human Resources obtains comprehensive employee documentation within 3 days of hire, to include copies of social security cards, driver’s licenses, or other legal identification permitted by the Federal I-9 form. All information is keyed into the employees records based on the physical documentation presented. Should the employee (new hire or existing employee) communicate a name discrepancy, the employee is directed to apply for a replacement social security card. Human Resources will only make name changes in the system when presented with a Social Security Administration receipt which includes the employee’s social security number as verification.

The candidate must sign a *Consent to Conduct a Criminal Background Check* (and credit check if required by the position). This may apply to a job candidate who is an existing employee as well as to new hires. Any discrepancy, to include, but not limited to, a name or address discrepancy, is communicated in writing to the candidate. The candidate must respond and resolve the discrepancy to the satisfaction of the Human Resources Department. In the event of unusual circumstances or the presence of “Red Flags” (as defined previously), a Background Investigation Committee will make a joint determination whether the hire can proceed. The Committee consists of members from Human Resources, Public Safety, and the Legal Office. As it relates to credit checks, the Committee consists of Human Resources and Financial Division personnel, such as from the P-Card Office or Accounts Payable. Adverse hiring decisions are also communicated in writing. Should an employee or candidate claim that a misidentification has occurred, the burden of proof is on the individual to prove the misidentification to the satisfaction of the Committee.

There may be occasions when “Red Flags” are present which do not relate to either a decision to promote, hire or issue a P-card to an employee. Examples are notice taken of an unusual number of credit inquiries on an employee’s credit report or a large number of recently opened accounts. In this case, there is no “covered account” involved and MCG does not have the responsibility to notify the employee of these flags. If the information is used to make a decision to withhold P-card privileges, on the other hand, MCG would be required to notify the employee in writing of the basis for declining the privilege. The letter should very generally state that, based on information contained in the employee’s credit report, P-card privileges could not be extended. The employee should then be advised that they are entitled to request an annual free copy of their credit report and have the right to dispute the information contained therein with their creditors and with the credit reporting agency. Specifics (creditor names, etc.) should not be mentioned in the letter.

ANNUAL REPORTING TO SENIOR MANAGEMENT AND THE BOARD OF REGENTS:

Annually, on April 15th, each office addressed under the Responsibilities Section below shall send a brief report stating whether the responsibilities assigned to it were accomplished during the period May 1 of the prior year through April 30 of the current year. Any exceptions should be addressed. This report shall be sent to the Office of the Controller for accumulation and submission to the Senior Vice President for Finance and Administration.

Upon approval of this report, the Senior Vice President for Finance and Administration will, by May 1, submit a summary report to the Vice Chancellor of Fiscal Affairs of the Board of Regents for presentation to the Board.

Process/Procedures

No specific procedures apply to this policy.

Responsibilities

The responsibilities each party has in connection with the *Credit Card Processing Policy* are:

Human Resources Division	Develop and consistently apply detailed business processes to identify and respond to “red flags” associated with <i>personally identifiable information of employees and potential employees</i> , including but not limited to name and address discrepancies.
Public Safety Division	Apply similar processes to <i>contractors, temporary agency staff and consultants</i> applying for clearance to work on the MCG campus, which may not have come through Human Resources for the prescreening or payroll processing.

<p>Criminal Background Check Committee (HR and Public Safety)</p> <p>Credit Checks Committee (HR/Accounts Payable Manager and P-Card Manager)</p>	<p>Develop and consistently apply detailed business processes to identify and respond to “red flags” associated with <i>credit checks and criminal background checks for current or potential employees.</i></p>
<p>Student Services Areas (primarily the Office of the Registrar)</p> <p>Cashier’s Office, Controller’s Division</p>	<p>Develop and consistently apply detailed business processes to identify and respond to “red flags” associated with <i>personally identifiable information of students.</i></p>
<p>Student Loan Office, Controller’s Division</p>	<p>Develop and consistently apply detailed business processes to identify and respond to “red flags” associated with <i>Student Loan activities.</i></p> <p>Ensure that MCG’s <i>third party servicer of student loans (ACS)</i> has a suitable Identify Theft Program in place.</p>
<p>Information Technology Security Division</p>	<p>Assure that the <i>personally identifiable information of both employees and students is secured</i> and that access rights are strictly regulated and password protected.</p>
<p>School of Dentistry Dental Clinic</p>	<p>Develop and consistently apply detailed business processes to identify and respond to “red flags” associated with <i>personally identifiable information of patients</i>, including but not limited to name, address and insurance information changes.</p>
<p>Student Health Office</p>	<p>Develop and consistently apply detailed business processes to identify and respond to “red flags” associated with <i>personally identifiable information of students</i>, including but not limited to name, address and insurance information changes.</p>
<p>All Departments and Divisions</p>	<p>In addition to addressing relevant "red flags," ensure relevant staff are adequately trained to identify red flags and to execute the Program effectively.</p>

Forms

None

Appendices

None