GCSU Red Flags Rule Policy

The US Federal Trade Commission's ("FTC") has established the "Red Flags Rule", which implements Section 114 of the Fair and Accurate Credit Transactions Act of 2003. Pursuant to the requirements of the "Red Flags Rule", GCSU shall establish procedures within each relevant department and/or division to implement the rule.

A. Red Flags Rule Definitions Used in this Program

- "Identity Theft" is a "fraud committed or attempted using the identifying information of another person without authority."
- A "Red Flag" is a "pattern, practice, or specific activity that indicates the possible existence of Identity Theft."
- A "Covered Account" includes all student accounts or loans that are administered by the University.
- "Program Administrator" is the individual designated with primary responsibility for oversight of the program.
- "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: name, address, telephone number, social security number, date of birth, government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number, student identification number, computer's Internet Protocol address, or routing code.

B. Fulfilling Requirements of the Red Flags Rule

Under the Red Flags Rule, the University is required to establish an "Identity Theft Prevention Program" tailored to its size, complexity and the nature of its operation. Each program must contain reasonable policies and procedures to:

1. Identify relevant Red Flags for new and existing covered accounts and incorporate those Red Flags into the Program;
2. Detect Red Flags that have been incorporated into the Program;
3. Respond appropriately to any Red Flags that are detected to prevent and mitigate Identity Theft; and
4. Ensure the Program is updated periodically to reflect changes in risks to students or to the safety and soundness of the student from Identity Theft.

C. Responsibility

Each department is responsible for the development and implementation of their departmental program including training personnel on those procedures. Responsibility for the oversight of the development and implementation of departmental programs and updating the GCSU Program lies with an Identity Theft Administrator for the University as appointed by Chief Academic Officer. The Administrator will be responsible for ensuring appropriate training of University employees 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.

So what is the Red Flags Rule?

In short it requires universities to develop and implement a program that will identify potential identity theft through suspicious activities. These patterns of suspicious activities are called "red flags." Every institution must create a compliance program to identify and respond to red flags. Once developed, employees must be trained on the program. The deadline for the red flag rules has been pushed back several times and the current deadline is ***December 31, 2010***. The delays have come from congress that is now looking at legislation that would affect the scope of the rules.

Red Flags mean a pattern, practice or specific activity that indicates the possible existence of identity theft. The Red Flags Rule was enacted by the Federal Trade Commission to help deter identity theft, and is implemented at institutions for that reason. Application of this rule is meant to fill any cracks that exist, that allow identity thieves to pilfer the identities of other for their own personal gain. The Red Flags Rule extends to any institution that is considered a "financial institution" or "creditor". This includes any institution that hold directly or indirectly a transaction account for a "consumer". As one such institution we are required to conduct a periodic risk assessment to assess whether we have any covered accounts. Covered accounts are those which are designed to permit multiple payments and transactions, or are assessed to have a reasonably foreseeable risk to identity theft. Each department within the institutions must then develop a written plan to detect, mitigate, and prevent identity theft in connection with those covered accounts. This can be as simple as library fines or as complex as student debit cards such as the Bobcat card or dining cards.

The FTC mandates these four parts:

1. **Identity relevant red flags. –** Identify the warning signs of identity theft that are specific to your business. Some common ones are suspicious documents, changes of address, warnings from credit agencies, and notices from victims or law enforcement.
2. **Detect red flags.** – Put in procedures that will detect the red flags in the day-to-day business.
3. **Prevent and mitigate identity theft.** – Put in reasonable responses when red flags are detected. This includes monitoring or closing accounts, not opening an account or notifying potential victims of a problem.
4. **Update your program periodically.** – Every program should be evaluated and updated for business practice changes and identity theft trends.

Once a compliance program is created, the University will need to educate your employees. This means more than just handing out a document such as this one but also working with them to protect all the private information in our care. All training should be documented for compliance records.

Training will be implemented by Hance Patrick and his people. Point of contact handouts will be provided for quick assessment and guidelines will be developed and reviewed annually.