IDENTITY THEFT PREVENTION PROGRAM

This program is launched in response to the Federal Trade Commission Red Flag Rules and Address Discrepancy Rules in conjunction with the Fair and Accurate Credit Transaction (FACT) Act of 2003.

Launch Date – May 1, 2009

Identity Theft Prevention Program (ITPP) and the "Red Flags Rule"

Purpose:
ACC is launching this ITPP because we are committed to protecting our students and associates from identity theft. We have long safeguarded our student records pursuant to FERPA and both student and associate records pursuant to the Gramm Leach Bliley Act (GLBA), as well as our student and associate health information pursuant to HIPAA. Now the Federal Trade Commission has mandated that we implement a new program intended to detect and respond to activities that could be "red flags" for identity theft.

This program is adopted to establish and implement policies and procedures to identify patterns, practices or specific activities that indicate the possible existence of identity theft ("red flags") and to detect and respond to these "red flags" to prevent and mitigate the risks of identity theft at our campuses and corporate office.

How is ACC covered by this new regulation?

The Red Flags Rule is actually three different but related rules, two of which apply to ACC:

(1) Users of consumer reports (for background checks in hiring or admissions) must develop reasonable policies and procedures to apply when they receive notice of an address discrepancy from a consumer reporting agency.

(2) Financial institutions and creditors holding "covered accounts" must develop and implement a written identity theft prevention program for both new and existing accounts. The "Red Flags Rule" defines the terms "creditor" and "covered accounts" broadly. A "creditor" under the rule includes 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. So, since ACC allows students to enter a payment plan in conjunction with signing their enrollment agreement, we are potentially creating a "covered account" with each enrollment. (Even if the student doesn't enter into a payment plan, we will still use the same process to identify red flags.)

Because ACC falls into both of these categories, we are covered by the FTC Red Flag Rules.

Responsibilities:
Our ITPP program has been developed with the input of the IT department, the HR department, the FA department and General Counsel/Vice President of Compliance. The program will be monitored and maintained under the guidance of General Counsel. After assessing the company's risk, we believe that Human Resources and Financial Aid are most likely to encounter the types of accounts covered by the FTC regulations, but we believe all associates should be on alert for these "red flags" so that we can provide the highest level of identity theft protection.

How does it work?
The FTC requires that we identify the likely "red flags" we might encounter using our experience as a school/company, the FTC suggested "flags" and using guidance from governmental agencies. Once we have established the "red flags", we must develop procedures for detecting and responding to them. ACC will provide training on our ITPP and we will update our ITPP to keep pace with changing technologies, and changing criminal activities. At least once per year, we will evaluate the program and make recommendations for updates. Your feedback is valuable, so please let us know if you have thoughts on how the program can be improved.

If, after training, you still have questions about the ITPP, please contact Kate Carey at ext. 14922.

DETECTING THE RED FLAGS

Alerts, Notifications or Warnings from a Consumer Reporting Agency

1. A fraud or active duty alert is included with a consumer report.
    a. A fraud alert is put on an account by the account holder when fraud has been detected or when the account holder has reason to believe someone might have accessed the account holder's information.
    b. An active duty alert is posted on a serviceman/woman's account when they are commissioned on active duty and want to protect their accounts while they are out of the country.
2. A consumer reporting agency provides a notice of credit freeze in response to a request for a consumer report.
    a. When a customer "freezes" his/her credit record, s/he prevents lenders from seeing his/her credit report unless s/he specifically grants them access. This can prevent identity thieves from taking out new credit in the customer's name, even if they have his/her Social Security number and other personal information.
    b. Current creditors are exempt from the freeze, and customers can use a PIN or password to open their file for certain lenders or for a certain time period if they plan to apply for credit.
3. A consumer reporting agency provides a notice of address discrepancy, as defined in Sec. 681.1(b) of the FTC regulations.
    a. For purposes of this section, a *notice of address discrepancy* means a notice sent to a user by a consumer reporting agency pursuant to 15 U.S.C. 1681c(h)(1), that informs the user of a substantial difference between the address for the consumer that the user provided to request the consumer report and the address(es) in the agency's file for the consumer.
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. A recent and significant increase in the volume of inquiries;
    b. An unusual number of recently established credit relationships;
    c. A material change in the use of credit, especially with respect to recently established credit relationships; or
    d. An account that was 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 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:
    a. The address does not match any address in the consumer report; or
    b. 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:
    a. The address on an application is the same as the address provided on a fraudulent application; or
    b. 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:
    a. The address on an application is fictitious, a mail drop, or a prison; or
    b. 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 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.

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

19. 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.

RESPONSE, PREVENTION AND MITIGATION

Now that you know the Red Flags to look for, you must be ready to respond. Note that your response must take into account the total circumstances and any aggravating factors that might make the situation more problematic. Make sure you work with your supervisor to assess all the information before responding.

Response techniques if a Red Flag is detected:

1. Do not proceed with the transaction until further reasonable procedures are taken to determine the identity of the person.
2. Request additional identification information, and go to third party sources if need be (such as the Social Security Administration).
3. Fully assess the risk presented by the Red Flag – discuss the situation with your supervisor.
4. Satisfy yourself that there is no reasonable basis to believe that identity theft is involved. If satisfied, no further response is needed.
5. If there is a continuing concern, contact General Counsel or the Chief Compliance Officer to discuss next steps.
6. Do not complete the transaction unless you and your supervisor (or GC or CCO) have a reasonable basis to believe identity theft is not involved.

If believe that identity theft may have occurred on an existing account, you should consider the following actions:

7. Notify your supervisor, or the GC.
8. Notify the customer.
9. Notify law enforcement.
10. Notify any creditor to whom the account has been assigned.
11. Suspend any further activity.
12. Stop collection action, if such action has proceeded.
13. Notify other potentially affected departments.

Response in the event of a fraud or active duty alert:

14. Take all appropriate steps to confirm the customer's identity and confirm that the application is not the result of identity theft (using the general response techniques outlined in numbers 1 – 6 in this section.)
15. In the event of a notification that requires you to contact the customer, be sure to use the phone number or other contact information provided in the alert to obtain authorization to proceed.

In the event that you receive a notice of credit freeze:

16. Follow the general response techniques outlined in numbers 1 – 6 in this section.
17. Do not proceed with the planned transaction.
18. Proceed only when you have received notification that the freeze has been lifted and credit report has been obtained.

In the event of notice of address discrepancy on a consumer report:

19. Follow the general response techniques outlined in numbers 1 – 6 in this section.
20. Do not proceed until you have verified the address and you have a reasonable belief that you are dealing with the consumer whose report was requested.

MAINTAINING APPROPRIATE DOCUMENTATION

For any situation where a Red Flag is detected and follow up is required, be sure to maintain a file for that individual, showing the steps taken and containing any documentation gathered in an effort to clear up the flag. If the FTC ever audited us on this program, we would want to have solid record keeping practices to show that we are complying with our policy, and this law.