3.27 Identity Theft Prevention Program and Red Flag Rules Policy

PROGRAM ADOPTION

Piedmont College ("College") developed this Identity Theft Prevention Program ("Program") pursuant to the Federal Trade Commission's ("FTC") Red Flags Rule, which implements Section 114 of the Fair and Accurate Credit Transactions Act of 2003. After consideration of the size and complexity of the College's operations and account systems, and the nature and scope of the College's activities, the Piedmont College Board of Trustees determined that this Program was appropriate for the College, and therefore approved this Program.

PURPOSE:

To provide guidelines for the administration of an "Identity Theft Prevention Program" that detects, prevents, and mitigates identity theft in connection with covered accounts. In order to manage information exposure, the Program is centered on the following four FACTA Section 114 requirements: Under the Red Flags Rule, the College 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;
2. Incorporate business practices to detect Red Flags;
3. Prevent and mitigate identity theft with an appropriate response; 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.

DEFINITIONS

Identity Theft: a fraud committed or attempted using the identifying information of another person without authority.

Red Flag: a pattern, practice, or specific activity that indicates the possible existence of identity theft.

Covered Account: the FTC describes this as an account that a creditor offers or maintains for which there is a foreseeable risk to customers or to the safety and soundness of the financial institution or creditor from identity theft. This definition includes all student accounts.

Creditor: an organization that regularly defer payments for goods or services or one who grants loans, arranges for loans/extensions of credit, or makes credit decisions.

Program Administrator: the individual designated with primary responsibility for oversight of the program. See Section IV below.

Identifying Information: any name or number that may be used, alone or in conjunction with any other information, to identify a specific person (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).

I: IDENTIFICATION OF RED FLAGS

In order to identify relevant Red Flags, the College 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 College identifies the following Red Flags in each of the listed categories:

A. Notifications and warnings from Credit Reporting Agencies for purpose of background/credit checks

1. Name discrepancy on identification and insurance information;
2. Presentation of suspicious documents;
3. Personal information inconsistent with information already on file;
4. Unusual use or suspicious activity related to a covered account, and/or notice from customers, law enforcement or others of unusual activity related to that covered account;
5. Report of fraud accompanying a credit report;
6. Notice or report from a credit agency of a credit freeze or an active duty alert on an applicant;
7. Receipt of a notice of address discrepancy in response to a credit report request.

B. Suspicious Documents

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

C. Suspicious Personal Identifying Information

Identifying information presented that is inconsistent with other information the student provides (example: inconsistent birth dates);

1. Identifying information presented that is inconsistent with other sources of information (for instance, an address not matching an address on a loan application);
2. Identifying information presented that is the same as information shown on other applications that were found to be fraudulent;

3. Identifying information presented that is consistent with fraudulent activity (such as an invalid phone number or fictitious billing address);
4. Social Security number presented that is the same as one given by another student;
5. An address or phone number presented that is the same as that of another person;
6. A person fails to provide complete personal identifying information on an application when reminded to do so; and
7. A person's identifying information is not consistent with the information that is on file for the student.

D. Suspicious Covered Account Activity or Unusual Use of Account

1. Change of address for an account followed by a request to change the student's name;
2. Payments stop on an otherwise consistently up-to-date account;
3. Account used in a way that is not consistent with prior use;
4. Mail sent to the student is repeatedly returned as undeliverable;
5. Notice to the College that a student is not receiving mail sent by the College;
6. Notice to the College that an account has unauthorized activity;
7. Breach in the College's computer system security; and
8. Unauthorized access to or use of student account information.

E. Alerts from Others

Notice to the College from a student, identity theft victim, law enforcement or other person that the College has opened or is maintaining a fraudulent account for a person engaged in identity theft.

II: DETECTING RED FLAGS

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

Detect

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

3. Review and scrutinize all documents for identification of any possible Red Flags upon any receipt of electronic or non-electronic transmission containing student, parent or guarantor identifying information.

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

Detect

1. Verify the identification of students if they request information (in person, via telephone, via facsimile, via email);
2. Verify the validity of request to change billing addresses by mail or email and provide the student a reasonable means of promptly reporting incorrect billing address changes;
3. Verify changes in banking information given for billing and payment purposes; and
4. Review and scrutinize all documents for identification of any possible Red Flags upon any receipt of electronic or non-electronic transmission containing student, parent or guarantor identifying information.

C. Consumer ("Credit") Report Requests: in order to detect any of the Red Flags identified above for an employment or volunteer position for which a credit or background report is sought, College personnel will take the following steps to assist in identifying address discrepancies:

Detect

1. Require written verification from any applicant that the address provided by the applicant is accurate at the time the request for the credit report is made to the consumer reporting agency; and
2. In the event that notice of an address discrepancy is received, verify that the credit report pertains to the applicant for whom the requested report was made and report to the consumer reporting agency an address for the applicant that the College has reasonable confirmed is accurate.

III: PREVENTING AND MITIGATING IDENTIFY THEFT

In the event College personnel detect 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

1. Continue to monitor a Covered Account for evidence of identity theft;
2. Contact the student or applicant (for which a credit report was run);
3. Change any passwords or other security devices that permit access to Covered Accounts;

4. Not open a new Covered Account;
5. Provide the student with a new student identification number;
6. Notify the Program Administrator for determination of the appropriate step(s) to take;
7. Notify law enforcement;
8. File or assist in filing a Suspicious Activities Report; or
9. 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 College will take the following steps with respect to its internal operating procedures to protect student identifying information**:**

1. Ensure that its website is secure or provide clear notice that the website is not secure;
2. 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;
3. Ensure that office computers with access to Covered Account information are password protected;
4. Avoid use of social security numbers (or have a plan to limit exposure in departments where the use of the social security number is unavoidable);
5. Ensure computer virus protection is up to date;
6. Require and keep only the kinds of student information that are necessary for College purposes; and
7. Ensure data storage is secure.

IV: PROGRAM ADMINISTRATION

A. Oversight

Responsibility for developing, implementing and updating this Program lies with the Piedmont College Human Resources Office. This office is responsible for program administration, ensuring appropriate training of the College's staff on the Program, reviewing any staff reports regarding the detection of Red Flags on the identified covered accounts 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

Staff training is required for all employees, officials and contractors for whom it is reasonably foreseeable that they may come into contact with accounts or personally identifiable information that may constitute a risk to the College or its customers.

The Division or Department Head of each office that maintains a covered account under this Program is responsible for ensuring that appropriate identity theft training for all requisite employees, officials and contractors occurs at least annually.

As part of the training, all requisite employees, officials and contractors should be informed of the contents of the College's Identity Theft Program, and be provided with access to a copy of this document. In addition, all requisite employees, official and contractors should be trained how to identify Red Flags, and what to do should he/she detect a Red Flag or have similar concerns regarding an actual or potential fraud involving personal information. At the end of this policy is a Preventing Identity Theft at Piedmont College confirmation statement that is signed by all new employees to the college.

C. Service Provider Arrangements

In the event the College engages a service provider to perform an activity in connection with one of more Covered Accounts, the College 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.

1. Require that service providers have such policies and procedures in place; and
2. Require that service providers review the College's Program and report any Red Flags to the College employee with primary oversight of the service provider relationship.

D. Non-disclosure of Specific Practices

For the effectiveness of this program, knowledge about specific Red Flag identification, detection, mitigation and prevention practices will be limited to those employees with a need to know them. Any documents that may have been produced or are produced in order to develop or implement this program that list or describe such specific practices and the information those documents contain are considered "confidential" and should not be shared with other Piedmont College employees or the public.

E. Program Updates

On an annual basis, as part of the College's plan, the Program will be re-evaluated to determine whether all aspects of the Program are up to date and applicable. This review will include an assessment of which accounts and/or databases are covered by the program, whether additional Red Flags need to be identified as part of the Program, whether training has been implemented, whether training has been effective. In addition, the review will include an assessment of whether mitigating steps included in the program remain appropriate, and/or whether additional steps need to be defined.

Preventing Personal Identity Theft at Piedmont College Acknowledgement

(To comply with FTC Red Flag Rules)

Millions of Americans have their identities stolen each year, where thieves may drain consumer accounts, damage their credit, and even threaten their physical or medical safety. In response to the growing threat of identity theft, Congress passed the Fair and Accurate Credit Transactions Act of 2003 (FACTA) primarily targeting financial organizations that deal with individual credit accounts. The law was later expanded to include identity theft in any organization where personal information is used in the normal course of business.

In November 2007, the Federal Trade Commission finalized **Red Flag Rules** to encourage recognition and detection of warning signs of potential identity theft and take steps to prevent fraud from occurring.

In addition to data security practices and guidelines, Red Flag Rules are designed to enhance the prevention of identity theft by implementing policies to specifically help protect personal identifying information. Piedmont College aims to prevent identity theft and fraud on two fronts:

1. By implementing data security practices that make it more difficult to gain unauthorized access to personal or identifying information that may be used to open or access accounts, and
2. By teaching faculty and staff to recognize and detect Red Flags that may be warning signs of potential identity theft and take steps to prevent fraud from occurring.

Responsibility for administration of the Identity Theft Prevention and Red Flag Rules lies with the Office of Human Resources and the program administrator is Margie Means. College employees are expected to notify the program administrator immediately once they become aware of an incident of identity theft or of the college's failure to comply with the program so that immediate and appropriate action can be taken.

All Piedmont College employees must review the Identity Theft Prevention and Red Flag Rules policy annually. All new employees must confirm reviewing by signing below:

I have reviewed Piedmont College's Identity Theft Prevention Program and Red Flag Rules and understand my role to help prevent and stop theft and fraudulent use of personal data and to help protect students, faculty, staff, and other constituents from damages related to fraudulent activity.

Employee Name: _____ Signature: _____

Date: _____

<u>This document should be returned to HR when completed.</u>