SOUTH TEXAS COLLEGE

Identity Theft Prevention Program and Guidelines

FTC Red Flags Rule

Issued
June 24, 2009

Table of Contents

Section 1: Program Background and Purpose

South Texas College ("College") developed the Identity Theft Program and Guidelines 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. The College's Board of Trustees approved the program policy and the initial guidelines on October 13, 2008.

Under the Red Flags Rule, the College is required to establish an "Identity Theft Program" tailored to its size, complexity and the nature of its operation.

The purpose of the Program is to detect identity theft attempts and stop identity thieves from using someone else's identifying information at the College to commit fraud.

The associated guidelines are designed to identify relevant red flags and incorporate them into the program; detect red flags that are part of the program; respond appropriately to any red flags that are detected; and ensure the program is updated periodically to address changing risks.

The college adopts these sensitive information guidelines to help protect students, employees, third party contractors, other appropriate individuals, and the college from damages related to the loss or misuse of sensitive information.

These guidelines:

1. Define sensitive information;
2. Describe the physical security of data when it is printed on paper;
3. Describe the electronic security of data when stored and distributed; and
4. Place the college in compliance with state and federal law regarding identity theft protection.

The program helps the college:

1. Identify red flags that signify potentially fraudulent activity within new or existing covered accounts;
2. Detect red flags when they occur in covered accounts;
3. Prevent and mitigate identity theft and respond to risks to determine if fraudulent activity has occurred and act if fraud has been attempted or committed;
4. Update the program periodically, including reviewing the accounts that are covered and the identified risks that are part of the program.
5. Improves program administration including involvement of management, staff training and oversight of service provider arrangements.

The risk to the college, its employees and customers from data loss and identity theft is of significant concern to the college and can be reduced only through the combined efforts of every employee and contractor.

Section 2: Definitions

"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 College.

"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 address, or routing code.

Section 3: Scope

These guidelines and protection program applies to students, employees, contractors, consultants, temporary workers, and other workers at the college, including all personnel affiliated with third parties.

Section 4: Guidelines

4A Sensitive Information

4A.1 Definition of Sensitive Information

Sensitive information includes the following items whether stored in electronic or printed format:

4A.1.a Credit card information, including any of the following:

1. Credit card number (in part or whole)
2. Credit card expiration date
3. Cardholder name
4. Cardholder address
5. Security Code
6. Substitute Social Security Number

4A.1.b Tax identification numbers, including:

1. Social Security number
2. Business identification number
3. Employer identification numbers

4A.1.c Payroll information, including, among other information:

1. Paychecks
2. Pay stubs

4A.1.d Cafeteria plan check requests and associated paperwork

4A.1.e Medical information for any employee or customer, including but not limited to:

1. Doctor names and claims
2. Insurance claims
3. Prescriptions
4. Any related personal medical information

4A.1.f Other personal information belonging to any customer, employee or contractor, examples of which include:

1. Date of birth
2. Address
3. Phone numbers
4. Maiden name
5. Names
6. Customer number
7. Driver license

4A.1.g College personnel are encouraged to use common sense judgment in securing confidential information to the proper extent. Furthermore, this section should be read in conjunction with the Texas Public Information Act and the College's open records policy. If an employee is uncertain of the sensitivity of a particular piece of information, he/she should contact their supervisor. In the event that the college cannot resolve a conflict between these guidelines and the Texas Public Records Act, the college will contact the Texas Office of Open Records.

4A.2 Hard Copy Distribution

Each employee and contractor performing work for the college will comply with the following guidelines:

1. File cabinets, desk drawers, overhead cabinets, and any other storage space containing documents with sensitive information will be locked when not in use.
2. Storage rooms containing documents with sensitive information and record retention areas will be locked at the end of each workday or when unsupervised.
3. Desks, workstations, work areas, printers and fax machines, and common shared work areas will be cleared of all documents containing sensitive information when not in use.
4. Whiteboards, dry-erase boards, writing tablets, etc. in common shared work areas will be erased, removed, or shredded when not in use.

5. When documents containing sensitive information are discarded they will be placed inside a locked shred bin or immediately shredded using a mechanical cross cut or Department of Defense (DOD)-approved shredding device. Locked shred bins are labeled "*Confidential paper shredding and recycling.*" College records, however, may only be destroyed in accordance with the College's records retention policy.

4A.3 Electronic Distribution

Each employee and contractor performing work for the college will comply with the following guidelines:

1. Internally, sensitive information may be transmitted using approved college e-mail. All sensitive information must be encrypted when stored in an electronic format.
2. Any sensitive information sent externally must be encrypted and password protected and only to approved recipients. Additionally, a statement such as this should be included in the e-mail:

"This message may contain confidential and/or proprietary information and is intended for the person/entity to whom it was originally addressed. Any use by others is strictly prohibited."

Section 5: Identify Relevant Red Flags

5A Covered accounts

A covered account includes any account that involves or is designed to permit multiple payments or transactions. Every new and existing customer account that meets the following criteria is covered by this program:

1. Business, personal and household accounts for which there is a reasonably foreseeable risk of identity theft; or
2. Business, personal and household accounts for which there is a reasonably foreseeable risk to the safety or soundness of the college from identity theft, including financial, operational, compliance, reputation, or litigation risks.

5B Identify Relevant Red Flags

5B.1 Risk Factors. The College will consider the following factors in identifying relevant Red Flags for covered accounts, as appropriate:

(1) The types of covered accounts it offers or maintains;
(2) The methods it provides to open its covered accounts;
(3) The methods it provides to access its covered accounts; and
(4) Its previous experiences with identity theft.

5B.2 Sources of Red Flags. The College will incorporate relevant Red Flags from sources such as:

(1) Incidents of identity theft that the College has experienced;
(2) Methods of identity theft that the College has identified that reflect changes in identity theft risks; and
(3) Applicable supervisory guidance.

5B.3 Categories of Red Flags. The Program includes relevant Red Flags from the following categories, as appropriate.

(1) Alerts, notifications, or other warnings received from consumer reporting agencies or service providers, such as fraud detection services;
(2) The presentation of suspicious documents;
(3) The presentation of suspicious personal identifying information, such as a suspicious address change;
(4) The unusual use of, or other suspicious activity related to, a covered account; and
(5) 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.

5C Alerts, Notifications or other warnings received from customer reporting agencies

5C.1 The following red flags are potential indicators of fraud. Any time a red flag, or a situation closely resembling a red flag, is apparent, it should be investigated for verification.

1. Alerts, notifications or warnings from a consumer reporting agency;
2. A fraud or active duty alert included with a consumer report;
3. A notice of credit freeze from a consumer reporting agency in response to a request for a consumer report; or
4. A notice of address discrepancy from a consumer reporting agency as defined in § 334.82(b) of the Fairness and Accuracy in Credit Transactions Act.

5C.2 Red flags also include consumer reports that indicate a pattern of activity 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; or
- An account that was closed for cause or identified for abuse of account privileges by a financial institution or creditor.

5D Suspicious documents

5D.1 Documents provided for identification that appear to have been altered or forged.
5D.2 The photograph or physical description on the identification is not consistent with the appearance of the applicant or customer presenting the identification.
5D.3 Other information on the identification is not consistent with information provided by the person opening a new covered account or customer presenting the identification.
5D.4 Other information on the identification is not consistent with readily accessible information that is on file with the college, such as a signature card or a recent check.
5D.5 An application appears to have been altered or forged, or gives the appearance of having been destroyed and reassembled.

5E Suspicious personal identifying information

5E.1 Personal identifying information provided is inconsistent when compared against external information sources used by the college. For example:

- The address does not match any address in the consumer report;
- The Social Security number (SSN) has not been issued or is listed on the Social Security Administration's Death Master File; or
- 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.

5E.2 Personal identifying information provided is associated with known fraudulent activity as indicated by internal or third-party sources used by the college. For example, the address on an application is the same as the address provided on a fraudulent application

5E.3 Personal identifying information provided is of a type commonly associated with fraudulent activity as indicated by internal or third-party sources used by the college. 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.

5E.4 The SSN provided is the same as that submitted by other persons opening an account or other customers.

5E.5 The address or telephone number provided is the same as or similar to the address or telephone number submitted by an unusually large number of other customers or other persons opening accounts.

5E.6 The customer or the person opening the covered account fails to provide all required personal identifying information on an application or in response to notification that the application is incomplete.

5E.7 Personal identifying information provided is not consistent with personal identifying information that is on file with the College.

5E.8 When using security questions (email address, last classes taken, etc.), 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.

5F Unusual use of, or suspicious activity related to, the covered account and notice from others

5F.1 Shortly following the notice of a change of address for a covered account, the college receives a request for new, additional, or replacement goods or services, or for the addition of authorized users on the account.

5F.2 A new revolving credit account is used in a manner commonly associated with known patterns of fraud patterns. For example, the customer fails to make the first payment or makes an initial payment but no subsequent payments

5F.3 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 change in purchasing or usage patterns

5F.4 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).

5F.5 Mail sent to the customer is returned repeatedly as undeliverable although transactions continue to be conducted in connection with the customer's covered account.

5F.6 The College is notified that the customer is not receiving paper account statements.

5F.7 The College is notified of unauthorized charges or transactions in connection with a customer's covered account.

5F.8 The College receives 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 college.

5F.9 The College 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.

Section 6: Detect Red Flags

Once the College has identified the red flags of identity theft as reflected above, the College will take the following steps to detect them in our day-to-day operation. Each organizational unit will develop and implement specific methods and protocols appropriate to meet the requirements of this Program.

6A New Accounts – Student Enrollment

6A.1 Requiring identifying information such as a name, address, and identification number and, for in-person verification, check a current government-issued identification cards, like a driver's license or passport.

6A.2 Compare the data received above with the information received from other sources, like a credit reporting company or data broker, the Social Security Number Death Master File, or publicly available information.

6A.3 Ask challenge questions based on information from other sources that can be another way of verifying someone's identity. Do not use information that may be found in a person's purse or wallet.

6B Existing Accounts

6B.1 Authenticate students, monitor transactions, and verify the validity of change-of-address requests.

6B.2 For on-line authentication, the College will consider the Federal Financial Institutions Examination Council's guidance which explores the application of multi-factor authentication techniques in high-risk environments, including using passwords, PIN numbers, smart cards, tokens, and biometric identification. The College will not use authenticators that are easily accessible such as a social security number, date of birth, mother's maiden name, or mailing address.

6B.3 The College will incorporate into the Program other procedures which are already being used to monitor transactions, identify behavior that indicates the possibility of fraud and identify theft, or validate changes of address.

Section 7: Prevent, Mitigate and Appropriately Respond to Identity Theft

7A Preventing and Mitigating Identity Theft

The Program's policies and procedures provides for appropriate responses to the Red Flags the College has detected that are commensurate with the degree of risk posed. In determining an appropriate response, the College should consider aggravating factors that may heighten the risk of identity theft. Appropriate responses may include the following:

(a) Monitoring a covered account for evidence of identity theft;
(b) Contacting the customer;
(c) Changing any passwords, security codes, or other security devices that permit access to a covered account;

(d) Reopening a covered account with a new account number;
(e) Not opening a new covered account; until further required information is received;
(f) Closing an existing covered account; until further required information is received;
(g) Not attempting to collect on a covered account or not selling a covered account to a debt collector;
(h) Notifying law enforcement; or
(i) Determining that no response is warranted under the particular circumstances.

7B Once potentially fraudulent activity is detected, an employee must act quickly as a rapid appropriate response can protect customers and the college from damages and loss.

7B.1 Once potentially fraudulent activity is detected, gather all related documentation and write a description of the situation. Present this information to the designated authority for determination.

7B.2 The designated authority will complete additional authentication to determine whether the attempted transaction was fraudulent or authentic.

7C If a transaction is determined to be fraudulent, appropriate actions must be taken immediately. Actions may include:

1. Canceling the transaction;
2. Notifying and cooperating with appropriate law enforcement;
3. Determining the extent of liability of the college; and
4. Notifying the actual customer that fraud has been attempted.

Section 8: Periodic Updates to Plan

8A At periodic intervals established in the program, or as required, the program will be re-evaluated to determine whether all aspects of the program are up to date and applicable in the current business environment.

8B Periodic reviews will include an assessment of which accounts are covered by the program.

8C As part of the review, red flags may be revised, replaced or eliminated. Defining new red flags may also be appropriate.

8D Actions to take in the event that fraudulent activity is discovered may also require revision to reduce damage to the college and its customers.

Section 9: Program Administration

9A Involvement of management

1. The Identity Theft Prevention Program shall not be operated as an extension to existing fraud prevention programs, and its importance warrants the highest level of attention.

2. The Identity Theft Prevention Program is the responsibility of the President or designee.
3. Approval of the initial plan must be appropriately documented and maintained.
4. Operational responsibility of the program is delegated to the President or designee.
5. The President or designee will approve material changes to the Program as necessary to address changing identity theft risks.
6. Staff responsible for development implementation, and administration of its Program should report to the Board of Trustees, and appropriate committee of the board, or a designated employee at the level of senior management, at least annually, on compliance by the College with the Program. The report should address material matters related to the Program and evaluate issues such as: the effectiveness of the policies and procedures of the College in addressing the risk of identity theft in connection with the opening of covered accounts and with respect to existing covered accounts; service provider arrangements; significant incidents involving identity theft and management's response; and recommendations for material changes to the Program.

9B Staff training

1. Staff training shall be conducted for all employees and third party 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.
2. Human Resource Department is responsible for ensuring identity theft training for all employees.
3. Employees must receive annual training in all elements of the guidelines.
4. To ensure maximum effectiveness, employees may continue to receive additional training as changes to the program are made.

9C Oversight of service provider arrangements

1. It is the responsibility of the college to ensure that the activities of all service providers are conducted in accordance with reasonable policies and procedures designed to detect, prevent, and mitigate the risk of identity theft.
2. A service provider that maintains its own identity theft prevention program, consistent with the guidance of the red flag rules and validated by appropriate due diligence, may be considered to be meeting these requirements.
3. Any specific requirements should be specifically addressed in the appropriate contract arrangements.

Version 2 - April 24, 2009, updated by ME with notes from PDG Bursar's Conference
Version 3 – April 24, 2009, review by RFR taskforce
Version 4 – June 1, 2009, updated by ME to agree with FTC RFR Appendix J requirements and issued to taskforce for review
Version 5 – June 24, 2009, updated by ME with Paul Varville's revisions and reviewed at AA Roundup
Version 6 – July 15, 2011, update by ME to include driver's license (4A.1f) as sensitive information and authentication information (5E.8).

MANUAL OF POLICY

Title	**Identity Theft Policy**	**5470**
Legal Authority	**Approval of the Board of Trustees**	
Date Approved by Board	**Board Minute Order dated October 13, 2008**	

It is the policy of the College to protect students, employees, consultants, third party contractors and other appropriate individuals from damages related to the loss or misuse of sensitive information. The College maintains guidelines regarding identity theft protection in compliance with the Red Flag Rules promulgated by the Federal Trade Commission.