

**THREE RIVERS COLLEGE  
FINANCIAL REGULATION**

Section: 3000 Financial	
Sub Section: 3100 Financial Management	
Title: FR 3105 Protection, Prevention, and Mitigation of Identity Theft	Page 1 of 14
Primary Policy: FP 3105 Risk Management	
References: 16 CFR 681.1; 16 CFR 603.2; 18 U.S.C. 1029(e); Missouri State Statute Section 174.130; FERPA; HIPAA; 15 U.S.C. 1681c-1(h); 15 U.S.C. 1681s-2; 15 U.S.C. 1681m	
Supersedes: NA	
Responsible Administrator: Chief Financial Officer	
Initial Approval: 12-16-2009	Last Revision: 09-21-2016

**Authority**

Due to the increased threat of identity theft, Code of Federal Regulations, Title 16, Chapter I, Subchapter F (The Fair Credit Reporting Act), Part 681.1, entitled “Duties regarding the detection, prevention, and mitigation of identity theft,” and otherwise known as the Federal Trade Commission’s “Red Flags Rules,” (the “Red Flag Rules”) was adopted and shall be effective as of November 1, 2009.

The Red Flag Rules require each financial institution and creditor that offers or maintains one or more covered accounts, as defined in 16 CFR 681.1), to develop and provide for the continued administration of a written program to detect, prevent, and mitigate identity theft in connection with the opening of a covered account or any existing covered account. Three Rivers College, because it is a creditor as defined by 16 CFR 681.1(b)(5) which opens and maintains covered accounts for its customers, is subject to the Red Flags Rules, and, therefore, hereby establishes an Identity Theft Prevention Program (the “Identity Theft Prevention program” or the “program”) by this written instrument. The Identity Theft Prevention program is intended to satisfy and fulfill the requirements of 16 CFR 681.1. The program is designed with consideration of the size and complexity of Three Rivers College and the nature and scope of its activities.

**Definitions**

Definitions for the purposes of this instrument are as follows:

- A. An “account,” as defined under 16 CFR 681.1(b)(1), is “a continuing relationship established by a person with a financial institution or creditor to obtain a product or service for personal, family, household, or business purposes.” This includes extensions of credit.
- B. A “covered account,” as defined under 16 CFR 681.1(b)(3), is “an account that a financial institution or creditor offers or maintains, primarily for personal, family, or household purposes, that involves or is designed to permit multiple payments or transactions.” This includes the college’s student accounts receivable, employee expense accounts, employee health reimbursement accounts, employee flexible spending accounts, other

**THREE RIVERS COLLEGE  
FINANCIAL REGULATION**

Section: 3000 Financial	
Sub Section: 3100 Financial Management	
Title: FR 3105 Protection, Prevention, and Mitigation of Identity Theft	Page 2 of 14
Primary Policy: FP 3105 Risk Management	
References: 16 CFR 681.1; 16 CFR 603.2; 18 U.S.C. 1029(e); Missouri State Statute Section 174.130; FERPA; HIPAA; 15 U.S.C. 1681c-1(h); 15 U.S.C. 1681s-2; 15 U.S.C. 1681m	
Supersedes: NA	
Responsible Administrator: Chief Financial Officer	
Initial Approval: 12-16-2009	Last Revision: 09-21-2016

employee and student accounts for such purposes as insurance, retirement, etc., and other accounts of a similar nature. This definition of a “covered account” also includes “any other account that the financial institution or creditor offers or maintains for which there is a reasonably foreseeable risk to customers or to the safety and soundness of the financial institution or creditor from identity theft, including financial, operational, compliance, reputation, or litigation risks.” This includes certain accounts payable accounts in conjunction with small businesses, sole proprietorships, etc. and other sensitive accounts which may be vulnerable to identity theft, and therefore, should be considered.

- C. A “Red Flag,” as defined under 16 CFR 681.1(b)(9), is a “pattern, practice, or specific activity that indicates the possible existence of identity theft.
- D. The “Red Flag Rules Compliance Officer” is the individual who is responsible for the oversight of the program, including the development, implementation, and maintenance of the program.
- E. “Identity theft,” as defined under 16 CFR 603.2(a), is “a fraud committed or attempted using the identifying information of another person without authority.”
- F. “Identifying information,” as defined under 16 CFR 603.2(b) and 18 USC 1029(e), is “any name or number that may be used, alone or in conjunction with any other information, to identify a specific person, including any— (1) Name, social security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number; (2) Unique biometric data, such as fingerprint, voice print, retina or iris image, or other unique physical representation; (3) Unique electronic identification number, address, or routing code; or (4) Telecommunication identifying information or access device.”).
- G. A “service provider,” as defined under 16 CFR 681.1(b)(10) is a person, organization, etc. “that provides a service directly to the financial institution or creditor” (such as auditors, collectors, etc.)

**THREE RIVERS COLLEGE  
FINANCIAL REGULATION**

Section: 3000 Financial	
Sub Section: 3100 Financial Management	
Title: FR 3105 Protection, Prevention, and Mitigation of Identity Theft	Page 3 of 14
Primary Policy: FP 3105 Risk Management	
References: 16 CFR 681.1; 16 CFR 603.2; 18 U.S.C. 1029(e); Missouri State Statute Section 174.130; FERPA; HIPAA; 15 U.S.C. 1681c-1(h); 15 U.S.C. 1681s-2; 15 U.S.C. 1681m	
Supersedes: NA	
Responsible Administrator: Chief Financial Officer	
Initial Approval: 12-16-2009	Last Revision: 09-21-2016

H. "Three Rivers College" shall herein be called "Three Rivers College" or "college."

I. Three Rivers College is herein regarded as a "financial institution" or "creditor, as defined under 16 CFR 681.1(b)(5) and 681.1(b)(7) for certain financial functions and/ or roles which it fills.

**Requirements of the program**

The following are specifications for the Identity Theft Prevention program:

- A. The program shall contain guidelines to:
  - a. Identify relevant Red Flags for covered accounts and incorporate those Red Flags into the program;
  - b. Detect Red Flags that have been incorporated into the program;
  - c. Respond appropriately to any Red Flags that are detected to prevent and mitigate identity theft; and
  - d. Ensure the program is updated periodically, to reflect changes in risks to customers or to the safety and soundness of the college from identity theft.
- B. The program shall implement reasonable policies and procedures to address the risk of identity theft to college's customers and the safety and soundness of the college, including financial, operational, compliance, reputation, and litigation risks.
- C. The program shall be appropriate for the size and complexity of the college and the nature and scope of its activities.
- D. The program shall be designed to address the experiences the college has with identity theft, the changes in the methods of identity theft, the methods to detect, prevent, and mitigate identity theft, the types of accounts the college offers and/or maintains, and the business arrangements of the financial institution, including service provider arrangements.

**THREE RIVERS COLLEGE  
FINANCIAL REGULATION**

Section: 3000 Financial	
Sub Section: 3100 Financial Management	
Title: FR 3105 Protection, Prevention, and Mitigation of Identity Theft	Page 4 of 14
Primary Policy: FP 3105 Risk Management	
References: 16 CFR 681.1; 16 CFR 603.2; 18 U.S.C. 1029(e); Missouri State Statute Section 174.130; FERPA; HIPAA; 15 U.S.C. 1681c-1(h); 15 U.S.C. 1681s-2; 15 U.S.C. 1681m	
Supersedes: NA	
Responsible Administrator: Chief Financial Officer	
Initial Approval: 12-16-2009	Last Revision: 09-21-2016

The program shall be implemented and be continuously administered and updated.

**Identifying Relevant Red Flags**

- A. In determining which Red Flags are relevant to the prevention of identity theft for the college, the college shall examine the following risk factors: the types of covered accounts offered and/or maintained, methods for opening and providing access to covered accounts, previous experience with identity theft, and its size, location, and customer base.
- B. The following items represent the relevant Red Flags the college is to detect:
  - a. Suspicious documents consisting of:
    - i. Identification documents, which appear to be altered, forged, or inauthentic.
    - ii. Identification documents, which contain photographs, or physical descriptions, which are inconsistent with the appearance of the person presenting the identification.
    - iii. Documents with information inconsistent with current student or other account records.
    - iv. Application documents which appear to have been altered or forged, or give the appearance of having been destroyed and reassembled.
  - b. Suspicious personal identifying information consisting of:
    - i. Personal identifying information provided which is inconsistent with other information the person provides, or is internally inconsistent (for example, there is a lack of correlation between the Social Security Number range and date of birth).
    - ii. Personal identifying information provided which is inconsistent with other, external sources of information used by the college.

**THREE RIVERS COLLEGE  
FINANCIAL REGULATION**

Section: 3000 Financial	
Sub Section: 3100 Financial Management	
Title: FR 3105 Protection, Prevention, and Mitigation of Identity Theft	Page 5 of 14
Primary Policy: FP 3105 Risk Management	
References: 16 CFR 681.1; 16 CFR 603.2; 18 U.S.C. 1029(e); Missouri State Statute Section 174.130; FERPA; HIPAA; 15 U.S.C. 1681c-1(h); 15 U.S.C. 1681s-2; 15 U.S.C. 1681m	
Supersedes: NA	
Responsible Administrator: Chief Financial Officer	
Initial Approval: 12-16-2009	Last Revision: 09-21-2016

- iii. Personal identifying information provided is associated with known fraudulent activity as indicated by internal or third-party sources used by the college (for example, contact information presented is the same as that on a fraudulent application).
  - iv. Personal identifying information provided is of a type commonly associated with fraudulent activity (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).
  - v. Social Security Number presented is the same as that submitted by other persons opening an account or other customers.
  - vi. Address or phone number presented is the same as that submitted by other persons opening an account or other customers.
  - vii. The person opening the covered account or the customer fails to provide all required personal identifying information on an application or form or in response to notification that the application or form is incomplete.
  - viii. The person opening the account or the customer cannot provide authenticating personal identifying information beyond that which generally would be available from a wallet or consumer report.
- c. Suspicious account activity on a covered account consisting of:
- i. Change of address for an account followed shortly by a request for name change, or vice versa.
  - ii. Payments stop on an otherwise consistently up-to-date account.
  - iii. A transaction that occurs with respect to a credit or deposit account that has been inactive for more than 2 years.
- d. Alerts, notifications, or other warnings from customers, victims of identity

**THREE RIVERS COLLEGE  
FINANCIAL REGULATION**

Section: 3000 Financial	
Sub Section: 3100 Financial Management	
Title: FR 3105 Protection, Prevention, and Mitigation of Identity Theft	Page 6 of 14
Primary Policy: FP 3105 Risk Management	
References: 16 CFR 681.1; 16 CFR 603.2; 18 U.S.C. 1029(e); Missouri State Statute Section 174.130; FERPA; HIPAA; 15 U.S.C. 1681c-1(h); 15 U.S.C. 1681s-2; 15 U.S.C. 1681m	
Supersedes: NA	
Responsible Administrator: Chief Financial Officer	
Initial Approval: 12-16-2009	Last Revision: 09-21-2016

theft, law enforcement authorities, service providers, or other persons regarding possible identity theft in connection with covered accounts held by the college consisting of:

- i. The college is notified of unauthorized charges or transactions in connection with a customer's account.
  - ii. The college is notified that it has opened, or is maintaining, a fraudulent account for a person engaged in identity theft.
  - iii. The college is notified that the accountholder is not receiving account statements or other college mail.
  - iv. The college is notified that its customer has provided information to someone fraudulently claiming to represent Three Rivers College or to a fraudulent web site appearing as that of Three Rivers College.
- e. Other Red Flags:
- i. The college detects, or is informed of; attempted or actual unauthorized access to a customer's personal identifying information, whether through computer system, records, or other means.

**Detecting Red Flags**

In order to detect Red Flags in connection with opening an account or with any existing account college employees shall take the following measures:

A. In regard to opening accounts:

- a. Obtain identifying information about, and verify the identity of, a person opening an account (for example, registering a student, hiring an employee, creating certain business relationships, etc.) or issuing a student identification card
- b. Pursuant to Missouri State Statute Section 174.130, Three Rivers College will

**THREE RIVERS COLLEGE  
FINANCIAL REGULATION**

Section: 3000 Financial	
Sub Section: 3100 Financial Management	
Title: FR 3105 Protection, Prevention, and Mitigation of Identity Theft	Page 7 of 14
Primary Policy: FP 3105 Risk Management	
References: 16 CFR 681.1; 16 CFR 603.2; 18 U.S.C. 1029(e); Missouri State Statute Section 174.130; FERPA; HIPAA; 15 U.S.C. 1681c-1(h); 15 U.S.C. 1681s-2; 15 U.S.C. 1681m	
Supersedes: NA	
Responsible Administrator: Chief Financial Officer	
Initial Approval: 12-16-2009	Last Revision: 09-21-2016

not knowingly admit any aliens unlawfully present in the United States. Proof of legal residency may be required at the time of application. International Students are required to be fully identified according to applicable laws and college policies.

- c. Follow any applicable state or federal regulations in conjunction with verifying the identity of new employees, students, vendors, or other accountholders.
- d. Be aware of any suspicious documents or suspicious personal identifying information.

B. In regard to monitoring existing accounts:

- a. Verify the identification of any person performing an account transaction or requesting information regarding an account (whether in person, over the telephone, via fax or email).
- b. Verify the validity of requests to change billing addresses by mail or email and provide the accountholder a reasonable means of promptly reporting incorrect billing address changes.
- c. Verify changes in banking information given for billing and payment purposes.
- d. Be aware of unusual account activities.

**Preventing Identity Theft**

Three Rivers College shall respect and protect the confidentiality and privacy of its student's, employees, and other accountholder's non-public, personal information. Appropriate protective measures, set in place to prevent identity theft, include the following:

A. Privacy Regulations:

- a. College personnel shall comply with the following regulations relating to privacy and information security: the Red Flag Rules, the Family Educational Rights and Privacy Act (FERPA), the Health Insurance Portability and

**THREE RIVERS COLLEGE  
FINANCIAL REGULATION**

Section: 3000 Financial	
Sub Section: 3100 Financial Management	
Title: FR 3105 Protection, Prevention, and Mitigation of Identity Theft	Page 8 of 14
Primary Policy: FP 3105 Risk Management	
References: 16 CFR 681.1; 16 CFR 603.2; 18 U.S.C. 1029(e); Missouri State Statute Section 174.130; FERPA; HIPAA; 15 U.S.C. 1681c-1(h); 15 U.S.C. 1681s-2; 15 U.S.C. 1681m	
Supersedes: NA	
Responsible Administrator: Chief Financial Officer	
Initial Approval: 12-16-2009	Last Revision: 09-21-2016

Accountability Act (HIPAA), other state and federal regulations regarding the same, and all policies, regulations, and procedures of the college. When there is a matter of conflict between these items, the stricter shall be followed.

- b. According to FERPA, when a student is admitted to the college, regardless of age, all rights afforded to parents under FERPA are transferred to that student. In summary, these regulations do not allow the release of any personally identifiable information to anyone but that same person. In order to release personally identifiable information to a student's parent, guardian, or any other party, that party must have a written release from the student. Directory information, as defined by FERPA, may be released by the college to interested parties unless the student files a written request to withhold information. Certain exceptions and details to this are contained within the FERPA regulations.
- c. The internal or external release of personal information throughout the college should only be released on a "need to know" basis and within the guidelines established by applicable laws and regulations. This affords officers of the college, with legitimate interest, access to information, and also affords access, upon disclosure to the student, to nonaffiliated third parties to perform services for the institution, under a non-disclosure contract. There are also certain exceptions to these regulations contained within these and other regulations. In any release of student's private information, business office personnel shall exercise professional judgment and discretion.

**B. Information storage and retrieval systems:**

- a. Information storage and retrieval systems consist of all records and archives whether physical or electronic. Access to the college's information storage and retrieval systems is granted to college employees only, on a "need-to-know" basis, which should be directly related to that employee's job



**THREE RIVERS COLLEGE  
FINANCIAL REGULATION**

Section: 3000 Financial	
Sub Section: 3100 Financial Management	
Title: FR 3105 Protection, Prevention, and Mitigation of Identity Theft	Page 9 of 14
Primary Policy: FP 3105 Risk Management	
References: 16 CFR 681.1; 16 CFR 603.2; 18 U.S.C. 1029(e); Missouri State Statute Section 174.130; FERPA; HIPAA; 15 U.S.C. 1681c-1(h); 15 U.S.C. 1681s-2; 15 U.S.C. 1681m	
Supersedes: NA	
Responsible Administrator: Chief Financial Officer	
Initial Approval: 12-16-2009	Last Revision: 09-21-2016

responsibility. Certain college positions are assigned access on a permanent and continuing basis.

- b. College employees who have access to information storage and retrieval systems are responsible for the security of that information and must follow the information control measures established above.
- c. Employees shall promptly report to their supervisors the loss or mutilation of any official college records or documents. The records and documents in the custody of college employees are for official purposes only (employees shall not use the information for personal gain). It is unlawful to remove or conceal, alter, mutilate, obliterate, or destroy records and documents from files without approval from proper authority. Authorized disposal of documents or files containing identifying information, whether physical or electronic, shall be secure and complete.
- d. Access to college information systems containing accountholder's identifying information shall be password protected.
- e. The college shall only require and keep such accountholder identifying information as is necessary for its essential purposes.
- f. College staff avoid the use of Social Security Numbers whenever possible and encourage the use of student identification numbers and cards when students are conducting business.
- g. The college shall ensure that its website is secure, or provide clear notification that it is not, and shall employ and maintain anti-virus software and /or other protective measures to ensure the integrity of the college's information systems.

**Responding to Prevent & Mitigate Identity Theft**

In the case Red Flags are detected, officers and employees of the college shall assess whether

**THREE RIVERS COLLEGE  
FINANCIAL REGULATION**

Section: 3000 Financial	
Sub Section: 3100 Financial Management	
Title: FR 3105 Protection, Prevention, and Mitigation of Identity Theft	Page 10 of 14
Primary Policy: FP 3105 Risk Management	
References: 16 CFR 681.1; 16 CFR 603.2; 18 U.S.C. 1029(e); Missouri State Statute Section 174.130; FERPA; HIPAA; 15 U.S.C. 1681c-1(h); 15 U.S.C. 1681s-2; 15 U.S.C. 1681m	
Supersedes: NA	
Responsible Administrator: Chief Financial Officer	
Initial Approval: 12-16-2009	Last Revision: 09-21-2016

such Red Flags evidence a risk of identity theft (the college must have a reasonable basis for concluding that a Red Flag does not evidence a risk of identity theft). If the college determines that a risk of identity theft exists, such risk shall be addressed in accordance with the degree of risk posed. The officers and employees of the college shall determine and enact the appropriate response, considering aggravating factors that could heighten the risk of identity theft. Such responses can include one or more of 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 and/or student I.D. number;
- E. Not opening a new covered account;
- F. Closing an existing covered account;
- G. Notifying the Red Flags Rules Compliance Officer;
- H. Notifying law enforcement;
- I. Implementing requirements applicable to the college, if any, regarding limitations on credit extensions under 15 U.S.C. 1681c–1(h), such as declining to issue a grade(s) and/or disallowing re-enrollment into a class(es) when the college detects a fraud or active duty alert associated with the opening of an account, or an existing account.

**Administration of the program**

The college shall provide for the implementation and the continued administration of the program as follows:

- A. The board of trustees shall approve applicable policy regarding this program.
- B. The college president, or his or her designee at the level of senior management, shall fulfill

**THREE RIVERS COLLEGE  
FINANCIAL REGULATION**

Section: 3000 Financial	
Sub Section: 3100 Financial Management	
Title: FR 3105 Protection, Prevention, and Mitigation of Identity Theft	Page 11 of 14
Primary Policy: FP 3105 Risk Management	
References: 16 CFR 681.1; 16 CFR 603.2; 18 U.S.C. 1029(e); Missouri State Statute Section 174.130; FERPA; HIPAA; 15 U.S.C. 1681c-1(h); 15 U.S.C. 1681s-2; 15 U.S.C. 1681m	
Supersedes: NA	
Responsible Administrator: Chief Financial Officer	
Initial Approval: 12-16-2009	Last Revision: 09-21-2016

the duties of the red flags rules compliance officer including:

- a. Assigning specific responsibility for the implementation of the program.
- b. Approving material changes to the program, as necessary, to address changing identity theft risks, including mandatory updates to the program as provided in paragraph 3 of this Section H.
- c. Reviewing annual reports prepared by key staff regarding compliance by the college with this program. Such reports 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 administration's response; and recommendations for material changes to the program.
- d. Periodically determining whether the college offers or maintains covered accounts, as defined herein, including performing the risk assessment associated with certain types of covered accounts, taking into consideration the methods the college provides to open accounts, the methods the college provides for customers to access their accounts, and the college's previous experiences with identity theft.
- e. Providing oversight of the college's service provider arrangements. Whenever the college engages a service provider to perform an activity in connection with one or more covered accounts, the college shall take steps to ensure that the activity of the service provider is conducted in accordance with reasonable policies and procedures designed to detect, prevent, and mitigate the risk of identity theft. For example, requiring the service provider, by contract, to have policies and procedures to detect relevant Red Flags that may arise in the performance of the service provider's activities, and either report the Red Flags to the college, or to take

**THREE RIVERS COLLEGE  
FINANCIAL REGULATION**

Section: 3000 Financial	
Sub Section: 3100 Financial Management	
Title: FR 3105 Protection, Prevention, and Mitigation of Identity Theft	Page 12 of 14
Primary Policy: FP 3105 Risk Management	
References: 16 CFR 681.1; 16 CFR 603.2; 18 U.S.C. 1029(e); Missouri State Statute Section 174.130; FERPA; HIPAA; 15 U.S.C. 1681c-1(h); 15 U.S.C. 1681s-2; 15 U.S.C. 1681m	
Supersedes: NA	
Responsible Administrator: Chief Financial Officer	
Initial Approval: 12-16-2009	Last Revision: 09-21-2016

appropriate steps to prevent or mitigate identity theft.

- f. Ensuring that the college trains relevant staff, as necessary, to effectively implement this program.
  - g. Ensuring the effectiveness of this program by keeping its disclosure limited. Disclosure of this program shall only be made to the board of trustees, the Red Flags Compliance Officer and his or her official designee at a level of senior management, and those key employees, on a “need-to-know” basis, who are responsible for its implementation. Disclosure of this program, related reports, and similar documents to other non-classified staff, accountholders, or other individuals, constitutes a potential breach in security and a hazard of identity theft. Therefore, this instrument or any communication concerning this instrument should be classified as confidential in regards to publication in any public document or posting, or in relation to the Missouri Sunshine Law, and should be protected.
- C. The college shall update the program periodically (including the relevant Red Flags to be identified) to reflect changes in risks to customers or to the safety and soundness of the college from identity theft, based on factors such as:
- a. The experiences of the college with identity theft
  - b. Changes in methods of identity theft
  - c. Changes in methods to detect, prevent, and mitigate identity theft
  - d. Changes in the types of accounts that the college offers and /or maintains
  - e. Changes in the business arrangements of the college, including service provider arrangements.
  - f. Applicable supervisory guidance.

**THREE RIVERS COLLEGE  
FINANCIAL REGULATION**

Section: 3000 Financial	
Sub Section: 3100 Financial Management	
Title: FR 3105 Protection, Prevention, and Mitigation of Identity Theft	Page 13 of 14
Primary Policy: FP 3105 Risk Management	
References: 16 CFR 681.1; 16 CFR 603.2; 18 U.S.C. 1029(e); Missouri State Statute Section 174.130; FERPA; HIPAA; 15 U.S.C. 1681c-1(h); 15 U.S.C. 1681s-2; 15 U.S.C. 1681m	
Supersedes: NA	
Responsible Administrator: Chief Financial Officer	
Initial Approval: 12-16-2009	Last Revision: 09-21-2016

**Other Applicable Legal Requirements**

The college shall be mindful of other related legal requirements that may be applicable, if any, to the college, such as:

- A. Implementing any requirements for furnishers of information to consumer reporting agencies under 15 U.S.C. 1681s–2, for example, to correct or update inaccurate or incomplete information, and to not report information that the furnisher has reasonable cause to believe is inaccurate; and
- B. Complying with the prohibitions in 15 U.S.C. 1681m on the sale, transfer, and placement for collection of certain debts resulting from identity theft.

**THREE RIVERS COLLEGE  
FINANCIAL REGULATION**

Section: 3000 Financial	
Sub Section: 3100 Financial Management	
Title: FR 3105 Protection, Prevention, and Mitigation of Identity Theft	Page 14 of 14
Primary Policy: FP 3105 Risk Management	
References: 16 CFR 681.1; 16 CFR 603.2; 18 U.S.C. 1029(e); Missouri State Statute Section 174.130; FERPA; HIPAA; 15 U.S.C. 1681c-1(h); 15 U.S.C. 1681s-2; 15 U.S.C. 1681m	
Supersedes: NA	
Responsible Administrator: Chief Financial Officer	
Initial Approval: 12-16-2009	Last Revision: 09-21-2016

**DOCUMENT HISTORY:**

- 12-16-2009:** Initial approval of regulation FR 3105 Protection, Prevention, and Mitigation of Identity Theft.
- 09-21-2016:** The College Board of Trustees approved the name change of the college from Three Rivers Community College to Three Rivers College.