

**WESTERN WASHINGTON UNIVERSITY'S
RED FLAGS IDENTITY THEFT PREVENTION PROGRAM
IMPLEMENTING SECTIONS 114 AND 315 OF THE
FAIR AND ACCURATE CREDIT TRANSACTIONS ACT OF 2003**

**David Coble
Internal Control Officer**

TABLE OF CONTENTS

- 1) Introduction**
- 2) Scope of Covered Accounts**
- 3) Existing Policies and Procedures and Best Practices**
 - a) Policies
 - b) Procedures
 - c) Best Practices
- 4) Identifying Relevant Red Flags**
 - a) The Methods Provided to Open Covered Accounts
 - i) Federal Perkins Loan Program
 - ii) Federal Direct Student Loan Program
 - iii) Federal Direct Plus Loan Program
 - iv) WWU Institutional Loan Program
 - v) WWU Short-Term Emergency Loan Program
 - vi) Payment Plan for Student Covered Account
 - b) The Methods Provided to Access Covered Accounts
 - i) Federal Perkins Loan Program
 - ii) Federal Direct Student Loan Program
 - iii) Federal Direct Plus Loan Program
 - iv) WWU Institutional Loan Program
 - v) WWU Short-Term Emergency Loan Program
 - vi) Payment Plan For Student Covered Account
 - c) Sources of Red Flags
 - i) University Previous Identity Theft Experience
 - ii) University Opportunities that Reflect Future Changes in Identity Theft Risk
 - iii) Applicable Supervisory Guidance
 - d) Categories of Red Flags
 - i) Alerts, Notifications and Warnings from Credit Agencies
 - ii) The Presentation of Suspicious Documents
 - iii) The Presentation of Suspicious Personal Identification Information
 - iv) The Unusual Use of, or Suspicious Activity Related to the Covered Account
 - v) Alerts from Others Regarding Possible Identity Theft in Connection with Covered Accounts
- 5) Detecting Red Flags**
 - a) Opening a New Covered Account
 - b) Existing Covered Account
 - c) Notice of Address Discrepancy

6) Preventing and Mitigating Identity Theft

- a) Aggravating Factors that May Heighten the Risk of Identity Theft
- b) Steps Taken Following the Detection of Red Flags
- c) Steps Taken Under Internal Operating Procedures to Protect Student Identifying Information

7) Updating the University's Identity Theft Red Flags Program

8) Methods for Administering the Program

- a) Oversight of Program
- b) Reporting
- c) Training Requirements
- d) Service Provider Arrangements

9) Other Applicable Legal Requirements

1) INTRODUCTION

In late 2007, the Federal Trade Commission (FTC) and Federal banking agencies issued a regulation known as the Red Flags Rule under sections 114 and 315 of the Fair and Accurate Credit Transactions Act of 2003 (FACT Act). The regulation is intended to detect, prevent and mitigate opportunities for identity theft at Western Washington University to commit fraud. The regulation applies to any organization that offers credit or maintains a “covered account”. The Red Flags Rule requires any organization that offers or maintains a “covered account” to develop and provide a written identity theft prevention program to detect, prevent, and mitigate identity theft in connection with the opening of a covered account or any existing covered account.

2) SCOPE OF COVERED ACCOUNT ACTIVITIES

“Covered Accounts” are described as an account that a creditor holds that is designed to allow multiple payments or transactions after services have been delivered. Western Washington University is subject to the Red Flags Rule because we participate in the Federal Perkins Loan Program, Federal Direct Student Loan Program, Federal Direct Plus Loan Program, Western Washington University Institutional Loan Program, Western Washington University Short-Term Emergency Loan Program, and payment plan for covered student accounts.

3) EXISTING POLICIES AND PROCEDURES

The following items listed below are policies and procedures for University departments and business units and other arrangements that already exist at Western Washington University that control reasonable foreseeable risks to students or to the safety and soundness of the University from identity theft:

a) Policies

- POL-U5300.01 Safeguarding Non-Public Financial Information (Ensures compliance with Gramm-Leach-Bliley Act –GLBA, Family Education Rights and Privacy Act –FERPA)
- POL-U5351.01 Accepting and Maintaining Cash Receipting Locations
- POL-U5351.02 Training Cash Handlers
- POL-U5351.03 Supervising Cash Handling Activities
- POL-U5351.06 Accepting Cash
- POL-U5351.10 Maintaining Physical Control Over Cash
- POL-U5351.14 Accepting, Processing and Securing Payments through the Internet
- POL-U5352.03 Applying Credit to Students’ and General Receivable Accounts
- POL-U5352.08 Collecting Accounts owed to the University
- POL-U5352.09 Collecting Long Term Student Loans
- POL-U7100.01 Student Records Policy
- POL-U7100.02 Using Email for Official Correspondence with Students
- POL-U5400.08 Conducting Background Checks
- POL-U5400.11 Verifying Employment Eligibility
- POL-U5950.19 Reporting Loss of University Funds or Property

b) Procedures

- PRO-U5352.03C Billing Third Parties to Pay Charges on Students’ Accounts
- PRO-U5352.03H Processing Direct and Plus Loan Paper Promissory Notes
- PRO-U5352.03I Processing Perkins Loan Promissory Notes

- PRO-U5950.19A Reporting Loss of University Funds
- c) Best Practices
- Security and Data Management WWU Best Practices and Policies
 - Code of Responsibility for Security and Confidentiality of Records and Files
 - Ethical Conduct; WWU User Agreement for WWU Network and Computer Resources
 - Remote Access Policy
 - WWU Technology Security Incident Response Program
 - Financial Information Security Program
 - Data Security, Passwords, and WWU Computer Use
 - Maintaining Privacy and Security and University Computers
 - Password Aging for All University Accounts
 - WWU ‘Safeguarding Non-Public Financial Information’ Training Flyer

4) **IDENTIFYING RELEVANT RED FLAGS**

The following items listed below are risk factors that Western Washington University considers in identifying relevant Red Flags for Covered Accounts in its departments or business units:

a) The Methods Provided to Open Covered Accounts:

i) Federal Perkins Loan Program. Federal Direct Student Loan Program. Federal Direct Plus Loan Program

- (1) Student visits online Federal Student Aid (FSA) website and requests PIN (Personal Information Number)
- (2) Student applies for financial aid by submitting their FAFSA online at: www.fafsa.ed.gov
- (3) FSA validates student covered data reported in FAFSA and matches student data with Social Security Administration
- (4) FSA sends an electronic record to University Financial Aid Department
- (5) The Financial Aid Department determines the student’s eligibility for financial aid
- (6) The Financial Aid Department awards the loan and mails the award letter to the student for their signature and acceptance of their financial aid

ii) WWU Institutional Loan Program. WWU Short-Term Emergency Loan Program

(WWU offers two types of emergency loans to assist students with short term cash needs. An emergency loan for a maximum of \$250.00 that is due in 30 days or an institutional loan for a maximum of \$600.00 that is due in 90 days. Both loans require the parent’s address and two references with complete addresses and phone numbers. References cannot include parents, room mates, spouse or anyone affiliated with Western. The student must be enrolled at least half-time to be eligible for either loan)

- (1) Student visits WWU website and follows to Financial Aid webpage
- (2) Student completes loan application online and signs with their Western ID and PIN
- (3) Student is required to report parents’ address and two references with complete addresses and phone numbers
- (4) The Financial Aid Department will send two emails notifying receipt of application and process acceptance or rejection

- ii) Payment Plan for Student Covered Account
 - (1) Student enrolls at University and debt to institution is incurred
 - (2) A student with outstanding debt who is no longer actively attending the University may enroll in a monthly payment agreement
- b) The Methods Provided To Access Covered Accounts
 - i) Federal Perkins Loan Program
 - (1) Student signs University Award Letter and sends back to the University Financial Aid Department
 - (2) The Financial Aid Department prepares a promissory note and other required support documents and mails to student for signature
 - (3) Student returns signed promissory note and required support documents to the Financial Aid Department
 - (4) Student visits Web4U to review status of loan
 - ii) Federal Direct Student Loan Program. Federal Direct Plus Loan Program.
 - (1) Student signs University Award Letter and sends back to the Financial Aid Department
 - (2) Student signs the Master Promissory Note (MPN) online at www.dlenote.ed.gov
 - (3) Student parent completes and sign the Plus loan addendum accepting the loan
 - (4) The parent borrower of the Plus loan signs their MPN online at www.dlenote.ed.gov
 - (5) If E-Signature process is not available, then follow steps 2 – 4 in Federal Perkins Loan Program
 - iii) WWU Institutional Loan Program
 - (1) The Financial Aid Department processes loan with determination of how funds are applied to existing student account
 - (2) Student visits Web4U to access account to confirm how loan was applied
 - iv) WWU Short-Term Emergency Loan Program
 - (1) The Financial Aid Department processes loan and notifies University Cashier to perform their student eligibility checks and release cash to the student with picture ID
 - (2) Student visits Web4U to access account
 - (3) Student physically collects cash with picture ID verification
 - v) Payment Plan for Student Covered Account
 - (1) 120 days following separation from University electronic access (Web4U) is terminated and access to account is managed by mail, email or telephone
- c) Sources of Red Flags
 - i) Western Washington University departments or business units have no previous experience with identity theft regarding the opening and access to its Covered Accounts.

ii) Western Washington University has identified three specific opportunities that reflect future changes in identity theft risk.

- (1) A default PIN (Personal Identification Number) should be changed every 120 days as required by University Best Practice.
- (2) A universal screen should be assigned for all University students enrolled or enrolling at the University that will define four (4) standard security questions and one (1) security question defined solely by the user. These security questions will be used by University personnel when covered accounts are opened and accessed.
- (3) If the University should ever become an 'Issuer' of a credit or debit card for its students, additional policies and procedures will be required for this Program and its related Policy in the event that the cardholder sends a notice of change of address for an existing account followed within 30 days by a request for an additional or replacement card for the same account.

iii) Applicable Supervisory Guidance

- (1) Western Washington University will incorporate applicable supervisory guidance for this program through the services and mechanisms of the WWU Chief Information Officer, WWU Technology Security Incident Response Program, the Financial Information Security Program, the University's Identity Theft Prevention Program Coordinator and University's Identity Theft Prevention Program Oversight Committee. Mechanisms will include identifying and assessing the risk factors related to Covered Accounts, written procedures to manage and control these risks, training staff in program activities, adjusting program factors reflected by University experience, changes in risk to students, or changes Covered Accounts offered or maintained by the University.

d) Categories of Red Flags

i) Alerts, Notifications and Warnings from Credit Reporting Agencies

- (1) Report of fraud accompanying a credit report
- (2) Credit agency report of a credit freeze on an applicant
- (3) Credit agency report of an address discrepancy
- (4) Credit agency report of activity that is inconsistent with an applicant's usual pattern of activity

ii) The Presentation of Suspicious Documents

- (1) Documents provided for identification that appear to have been altered or forged, or give an appearance of having been destroyed and reassembled
- (2) A photograph or physical description on an identification document or card that is not consistent with the appearance of the student applicant presenting the identification
- (3) Information on the identification document or card that is not consistent with information provided by the person opening a new covered account or presenting the identification
- (4) Information on the identification that is not consistent with readily accessible information that is on file with the University, such as a signature on an application or recent check

iii) The Presentation of Suspicious Personal Identification Information

- (1) Identifying information presented that is inconsistent with other information the student provides i.e. inconsistent birth dates
- (2) Identifying information presented that is inconsistent with other sources of information i.e. address does not match address on loan application
- (3) Identifying information presented that is the same information shown on other applications that were found to be fraudulent
- (4) Identifying information presented that is consistent with fraudulent activity as indicated by a credit agency or internal source
- (5) The Social Security Number presented that is the same as that of another student
- (6) An address or phone number presented that is the same as that of another student
- (7) A student fails to provide complete personal identifying information on an application when reminded to do so
- (8) A person's identifying information is not consistent with the information that is on file for the student

iv) The Unusual Use of or Suspicious Activity Related to the Covered Account

- (1) Change of address for an account followed by a request to change the student's name, or add authorized users on the account
- (2) Student fails to make the first payment
- (3) Account is inactive for a reasonably lengthy period of time in use
- (4) Mail sent to the student is repeatedly returned as undelivered
- (5) Notice to the University that an account has unauthorized activity
- (6) Breach in the University's computer security
- (7) Unauthorized access to or use of student account information

v) Alerts from Others Regarding Possible Identity Theft in Connection with Covered Accounts

- (1) Notice to the University student, Identity Theft victim, law enforcement or any other person that the University has opened a fraudulent account for a person engaging in Identity Theft

5) DETECTING RED FLAGS

The Western Washington University Identity Theft Prevention Coordinator in collaboration with departmental managers of Covered Accounts will implement and comply with each specific method appropriate to addressing the detection of Red Flags in connection with the opening of Covered Accounts and existing Covered Accounts:

a) Opening a New Covered Account

- i) Verify the identification of students if they request information (in person, telephone, email, application), such as name, date of birth, home address or other identification
- ii) Verify the validity of billing address by reviewing a driver's license or other government issued photo identification
- iii) Independently contact the student or payment borrower

- iv) Prohibit release of loan information without available Information Release form and/or established authorized pay-or identification
- b) Existing Covered Account
 - i) Verify the identification of students if they request information (in person, telephone, email)
 - ii) Verify the validity of requests to change billing addresses
 - iii) Monitor transactions
- c) Notice of Address Discrepancy
 - i) Compare the information reported by the Credit Agency of the student to University records such as applications, change of address notifications, or other student account records
 - ii) Verify accuracy of address change by requesting in person proof of address change from the student
 - iii) Furnish accuracy of information to the Credit Agency from which the address discrepancy report relating to the student was obtained
 - iv) Validate address discrepancy with the Credit Agency within a reasonable time where the relationship with the student is active

6) PREVENTING AND MITIGATING IDENTITY THEFT

- d) Aggravating Factors that May Heighten the Risk of Identity Theft
 - i) Data security breach
(Per RCW 42.56.590, notification or disclosure shall be made in the most expedient time possible, without unreasonable delay. Exemptions include encrypted data, publicly available government data and immaterial breaches)
 - ii) Third Party Service Provider Notice of fraudulent activity
 - iii) Student Notice of suspicious fraudulent activity

b) Steps Taken Following the Detection of Red Flags

In the event University Personnel detects any identified Red Flags with respect to Covered Accounts, such personnel shall take one or more of the following steps depending on the degree of risk posed by the Red Flag

- i) Notify the Program Coordinator and/or Chief Information Officer for determination of the appropriate step(s) to take
 - ii) Continue to monitor a Covered Account for evidence of Identity Theft
 - iii) Contact the student or applicant (for which a credit report was run)
 - iv) Change passwords or other security devices that permit access to Covered Accounts
 - v) Not open a new Covered Account
 - vi) Provide the student with a new student identification number
 - vii) Notify law enforcement
 - viii) Determine that no response is warranted under the particular circumstances
- c) Steps Taken Under Internal Operating Procedures to Protect Student Identifying Information

- i) Ensure that any University website that is used to access Covered Accounts is secure or provide clear notice to all users that the website is not secure
- ii) Secure University websites must be tested based on the University's information security program to ensure that they remain secure
- iii) Ensure that paper documents which contain personal identifying information are maintained in a secure environment, and that such documents are shredded and recorded on file when the University no longer needs to retain them
- iv) Ensure that office computers with access to Covered Account information are password protected and the only individuals who have access to such files are those with a need to access the files in order to perform their job duties
- v) Ensure computer virus protection is up to date
- vi) Require and keep only the kinds of student information that is necessary for University purpose
- vii) Periodic audits should be performed within the departments offering or maintaining Covered Accounts to ensure that individuals who should not have access to such files are not accessing them
- viii) Each department or business unit who offers or maintains Covered Accounts must perform a WISR Enterprise Risk Management (ERM) risk assessment to ensure low risks or risk likelihood of identity theft opportunities
- ix) All incidents of identity theft must be reported to the University Identity Theft Program Coordinator and/or Chief Information Officer
- x) A contracted IT Security Audit every seven (7) years

7) UPDATING THE UNIVERSITY'S IDENTITY THEFT RED FLAGS PROGRAM

The Identity Theft Program Coordinator will be responsible for periodically updating the Red Flags Program to reflect changes in risk to students, or the safety and soundness of the University from identity theft. The following risk factors guiding program change may include:

- a) Identity theft experience at the University
- b) Changes in methods of identity theft
- c) Changes in methods to detect, prevent, and mitigate identity theft
- d) Changes in Covered Accounts that the University offers or maintains
- e) Changes in Service Provider arrangements.

8) METHODS FOR ADMINISTERING THE PROGRAM

a) Oversight of Program

The responsibility for developing, implementing and updating the University Identity Theft Red Flags Program lies with the Identity Theft Program Coordinator who is appointed by the Chief Information Officer in consultation with the Vice President for Business and Financial Affairs. The Chief Information Officer (CIO) will appoint managers from relevant University departments to serve on the Oversight Committee. These departments may include Student Financial Affairs, Financial Aid, Administrative Computing Services, Internal Audit, and Business and Financial Affairs Internal Control Officer. The Identity Theft Oversight Committee will be responsible for ensuring that University personnel are appropriately trained on this Program. All possible identity theft instances will be reported to the Chief Information Officer (CIO). The CIO will call the WWU Security Instance Response Team together for review and designated action, and reviewing any reports regarding the detection of possible identity theft and steps for preventing and mitigating identity theft.

b) Reporting

The Identity Theft Program Coordinator will present a written report of material program matters to the Board of Trustees Audit Committee, Vice President of Business and Financial Affairs, the Chief Information Officer (CIO), the Security Incident Response Team, and the Oversight Committee periodically.

- i) The activities of the program
- ii) The effectiveness of the program in addressing the risk of identity theft
- iii) Service provider arrangements
- iv) Significant incidents involving identity theft and management's response

c) Training Requirements

University employees responsible for the creation, modification or administration of Covered Accounts shall be trained to effectively to comply with the Identity Theft Prevention Program under the direction of the University's Identity Theft Prevention Program Coordinator in collaboration with the University's Identity Theft Prevention Program Oversight Committee in the detection, prevention, and mitigation of identity theft in connection with the opening of a Covered Account or any existing Covered Account.

d) Service Provider Arrangements

The University remains responsible for compliance with the Red Flags Rule even if it outsources operations to a third party service provider. Contract language between the University and the third party provider shall require the third party to have no later than May 1, 2009, policies and practices in place to detect identity theft in compliance with the Federal Trade Commission's Red Flags Rule (Sections 114 and 315 of the Fair and Accurate Credit Transactions Act of 2003) that may arise in the performance of their service provider's activities. The Contract Administrator will ensure Service Provider bid documents and contracts comply with FTC Red Flags Rule.

9) OTHER APPLICABLE LEGAL REQUIREMENTS

In the event University Personnel detects any 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:

- a) File or assist in filing a Suspicious Activities Report ("SAR") with a Credit Agency in accordance with applicable law and regulation
- b) Furnish information to a Credit Agency to correct or update inaccurate or incomplete information, and to not report information that the University has reasonable cause to believe is inaccurate
- c) Implement requirements for students who under circumstances detects a fraud or receives an active alert, notification or warning from a Credit Agency for fraud, to extend credit
- d) Comply with applicable law and regulation on the sale, transfer and placement for collection of certain debts resulting from identity theft