

**WEST VIRGINIA UNIVERSITY
BOARD OF GOVERNORS
EMERGENCY POLICY 54**

Emergency Rule on Identity Theft Detection and Prevention Program

Section 1. General

- 1.1 Purpose: The purpose of this policy is to establish an Identity Theft Prevention 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 (FACT Act). West Virginia University Board of Governors' Identity Theft Detection and Prevention Program is designed to identify, detect, prevent, and mitigate "identity theft" in connection with any "covered account" and establish a system for reporting potential identity theft incidents.
- 1.2 Authority: WV Code § 18B-1-6 and 15 U.S.C. 1681 et seq., HEPC Series 4 (133 WVCSR 4) and WVU BOG Policy #45
- 1.3 Scope: This policy applies to all faculty, staff, and students, and to any service providers with whom the West Virginia University Board of Governors contracts to perform certain functions on its behalf.
- 1.4 Effective Date: November 1, 2009
- 1.5 Revision History: This is the first West Virginia University Board of Governors' Identity Theft Detection and Prevention Program.

Section 2. Definitions

- 2.1 Covered Account – A consumer account designed to permit multiple payments or transactions and any other account for which there is a foreseeable risk of identity theft. These include accounts where payments are deferred and made by a borrower periodically over time such as tuition or a fee installment payment plan. Such accounts can be maintained and administered by WVU or a service provider. Examples of covered accounts include:
- Refund of credit balances involving PLUS loans
 - Refund of credit balances without PLUS loans
 - Deferment of tuition payments
- 2.2 Creditor – Any entity that regularly extends, renews, or continues credit; any entity that regularly arranges for the extension, renewal, or continuation of credit; or any assignee of an original creditor who is involved in the decision to extend, renew, or continue credit. Examples of activities that indicate a college or university is a "creditor" are:

- Participation in the Federal Perkins Loan Program
 - Participation as a school lender in the Federal Family Education Loan Program
 - Offering institutional loans to students, faculty, or staff
 - Offering a plan for payment of tuition or fees throughout the semester, rather than requiring full payment at the beginning of the semester
 - Emergency loans
 - Bookstore charges
 - Student Health Center charges
- 2.3 Existing Account – An established continuing relationship with WVU that could result in the establishment of a Covered Account.
- 2.4 Identity Theft – Fraud committed or attempted using identifying information of another without authorization.
- 2.5 New Account – The beginning of any continuing relationship with WVU that could result in the establishment of a Covered Account.
- 2.6 Personally Identifiable Information (PII) – Any piece of information that may be used to uniquely identify, contact, or locate a specific person. PII includes but is not limited to the following: name, address, telephone number, social security number, date of birth, driver’s license number, alien registration number, passport number, employer or tax ID number, financial information, and/or any combination of information that will uniquely identify an individual.
- 2.7 Red Flag – A pattern, practice, or specific activity that indicates the possible existence of identity theft. Examples of Red Flags include:
- an application appears to have been forged, altered, or destroyed and reassembled;
 - a consumer report includes a fraud alert, credit freeze, or address discrepancy;
 - a change of address notice is followed shortly by a request for a new credit card, bank card, or cell phone;
 - the Social Security number supplied by an applicant is the same as that submitted by another person opening an account;
 - the address or telephone number supplied by an applicant is the same or similar to the account number or telephone number submitted by an unusually large number of other persons;
 - the financial institution or creditor is notified that the customer is not receiving account statements; and
 - an account that has been inactive for a reasonably long period of time is utilized

Section 3. Policy

As required by the FTC's Red Flags Rules, West Virginia University Board of Governors' Identity Theft Prevention Program shall include procedures for identifying, detecting, preventing, and responding to Red Flags.

3.1 Identification of Red Flags - any time a Red Flag or a situation resembling a Red Flag is apparent, it must be investigated for verification. Red Flags include but are not limited to the following examples in each of the listed categories:

3.1.1 Notifications and Warnings from Credit Reporting Agencies

Red Flags

- Report of fraud accompanying a credit report;
- Notice or report from a credit agency of a credit freeze on an applicant;
- Notice or report from a credit agency of an active duty alert for an applicant; and
- Indication from a credit report of activity that is inconsistent with an applicant's usual pattern or activity.

3.1.2 Suspicious Documents

Red Flags

- Identification document or card that appears to be forged, altered or inauthentic;
- Identification document or card on which a person's photograph or physical description is not consistent with the person presenting the document;
- Other document with information that is not consistent with existing applicant information (such as if a person's signature on a check appears forged); and
- Application for service that appears to have been altered or forged.

3.1.3 Suspicious "Personally Identifiable Information"

Red Flags

- Identifying information presented that is inconsistent with other information the applicant provides (example: Inconsistent birth dates);
- Identifying information presented that is inconsistent with other sources of information (for instance, an address not matching an address on a credit report);
- Identifying information presented that is the same as information shown on other applications that were found to be fraudulent;
- Identifying information presented that is consistent with fraudulent activity (such as an invalid phone number or fictitious billing address);

- Social security number presented that is the same as that of another person;
- An address or phone number presented that is the same as that of another person;
- A person fails to provide complete personally identifying information on an application when reminded to do so; or
- A person's identifying information is not consistent with the information that is on file for the applicant.

3.1.4 Suspicious Account Activity

Red Flags

- Change of address for an account followed by a request to change the account holder's name;
- Payments stop on an otherwise consistently up-to-date account;
- Account used in a way that is not consistent with prior use (example: very high activity);
- Mail sent to the account holder is repeatedly returned as undeliverable;
- Notice to West Virginia University that an applicant is not receiving mail sent by West Virginia University;
- Notice to West Virginia University that an account has unauthorized activity;
- Breach in West Virginia University's computer system security; and
- Unauthorized access to or use of applicant account information.

3.1.5 Notices from Other Sources

Red Flags

- Notice of possible identity theft from an applicant, identity theft victim, law enforcement, or other person.

3.2 Detection of Red Flags

3.2.1 New Accounts

In order to detect any of the Red Flags identified above associated with the opening of a ***New Account***, the following steps will be taken to obtain and verify the identity of the person opening the account:

1. Require certain identifying information such as name, date of birth, residential or business address, driver's license or other identification;
2. Verify the applicant's identity; and

3. Independently contact the applicant.

3.2.2 Existing Accounts

In order to detect any of the Red Flags identified above for an *Existing Account*, the following steps will be taken to monitor all contacts/transactions:

1. Verify the identification of applicants if they request information;
2. Verify the validity of requests to change billing addresses; and
3. Verify changes in banking information given for billing and payment purposes.

- 3.3 Preventing and Mitigating Identity Theft – In the event any person detects any identified Red Flags, such person shall follow the procedure for implementing this policy and notify the Office of the Associate Provost for Information Technology and Chief Information Officer.
- 3.4 Program Updates – The Program Procedures will be revisited on an annual basis and updated as needed to consider changes in experiences with identity theft situations, in identity theft methods, in identity theft detection and prevention methods, in types of accounts West Virginia University maintains, in West Virginia University’s business arrangements with other entities and/or changes in the law.
- 3.5 All employees who process information related to a Covered Account shall receive training on the procedures covered in the Identity Theft Detection and Prevention Program. Refresher training may be provided annually. The training will be revisited on an annual basis to assess the need for changes.

Section 4. Service Provider Arrangements

- 4.1 In the event the West Virginia University Board of Governors engages a service provider to perform an activity in connection with one or more Covered Accounts, the following steps will be taken to ensure that 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, by contract, that service providers have such policies and procedures in place; and
 2. Require, by contract, that service providers review West Virginia University Board of Governors’ Program and report any Red Flags to the Office of the Associate Provost for Information Technology and Chief Information Officer.

Section 5. Penalties

- 5.1 Noncompliance with this policy could result in a broad range of penalties up to and including civil fines.

Section 6. Responsibility for Interpretation

- 6.1 Responsibility for interpretation of this policy rests with the Office of the Vice President for Legal Affairs.

Section 7. Responsibility for Application/Development of Procedures

- 7.1 Responsibility for application of this policy and the development of procedures rests with the Office of the Associate Provost for Information Technology and Chief Information Officer, in consultation with the Office of the Vice President for Legal Affairs. Any procedures developed by the Office of the Associate Provost for Information Technology and Chief Information Officer or material changes thereto shall be posted for ten (10) working days before the procedures become effective.
- 7.2 For additional information regarding the application of this policy please refer to the [Emergency Identity Theft Detection and Prevention Program](#) procedure.

**WEST VIRGINIA UNIVERSITY
OFFICE OF INFORMATION TECHNOLOGY**

Identity Theft Detection and Prevention Program Procedure

Section 1. General

- 1.1 Purpose: To establish an official procedure for implementing an Identity Theft Prevention 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 (FACT Act). West Virginia University Board of Governors' Identity Theft Detection and Prevention Program is designed to identify, detect, prevent, and mitigate "identity theft" in connection with any "covered account" and establish a system for reporting potential identity theft incidents.
- 1.2 Authority: [WVU-BOG Policy # 54 – Emergency Rule on Identity Theft Detection and Prevention Program](#)
- 1.3 Scope: This procedure applies to all faculty, staff, and students, and to any service providers with whom the West Virginia University Board of Governors contracts to perform certain functions on its behalf.
- 1.4 Effective Date: November 1, 2009
- 1.5 Revision History: This is the first Office of Information Technology's Identity Theft Detection and Prevention Program Procedure.

Section 2. Definitions

- 2.1 Covered Account – A consumer account designed to permit multiple payments or transactions. These are accounts where payments are deferred and made by a borrower periodically over time such as tuition or a fee installment payment plan. Such accounts can be maintained and administered by WVU or a service provider. Examples of covered accounts include:
- Refund of credit balances involving PLUS loans
 - Refund of credit balances without PLUS loans
 - Deferral of tuition payments
- 2.2 Red Flag – A pattern, practice, or specific activity that indicates the possible existence of identity theft. Examples of Red Flags include:
- an application appears to have been forged, altered, or destroyed and reassembled;
 - a consumer report includes a fraud alert, credit freeze, or address discrepancy;

- a change of address notice is followed shortly by a request for a new credit card, bank card, or cell phone;
- the Social Security number supplied by an applicant is the same as that submitted by another person opening an account;
- the address or telephone number supplied by an applicant is the same or similar to the account number or telephone number submitted by an unusually large number of other persons;
- the financial institution or creditor is notified that the customer is not receiving account statements; and
- an account that has been inactive for a reasonably long period of time is utilized

Section 3. Procedure

- 3.1 Any Department engaged in contracting including the Department of Purchasing Contracts and Payment Services shall incorporate into all contracts with service providers, that maintain Covered Accounts, language requiring service providers to comply with WVU BOG Policy#54 and this procedure.
- 3.2 Any person who detects a Red Flag must immediately notify management within their unit.
- 3.3 Once a manager has confirmed the detection of a Red Flag, he or she will work in conjunction with the Office of the Associate Provost for Information Technology and Chief Information Officer to take one or more of the following steps, depending on the degree of risk posed by the Red Flag:
 - .1 Continue to monitor an account for evidence of identity theft;
 - .2 Contact the applicant;
 - .3 Change any passwords or other security devices that permit access to accounts;
 - .4 Not open a new account;
 - .5 Close an existing account;
 - .6 Reopen an account with a new number;
 - .7 Notify law enforcement; or
 - .8 Determine that no response is warranted under the particular circumstances.

Section 4. Service Provider Arrangements

- 4.1 Any service provider with whom the West Virginia University Board of Governors contracts to perform services related to any Covered Account shall have appropriate policies and procedures in place and must immediately notify the WVU unit it provides service for and the Office of the Associate Provost for Information Technology and Chief Information Officer of any Red Flag it detects. Such notification shall include all information regarding the Red Flag and the Service Provider's expected course of action.

Section 5. Training

- 5.1 Any person who processes information related to Covered Accounts shall be required to read and acknowledge their receipt of WVU BOG Policy #54 and this procedure prior to beginning work related to Covered Accounts. Refresher training may be provided annually by or under the direction of the Office of the Vice President for Legal Affairs.

Section 6. Program Updates

- 6.1 Any unit, college division or service provider that accepts applications for, opens, closes, or maintains any Covered Account shall participate in a yearly review process with the Associate Provost for Information Technology and Chief Information Officer to consider experiences with identity theft situations, changes in identity theft methods, changes in identity theft detection and prevention methods, and changes in the University's business methods. After considering information revealed in the yearly review, the Associate Provost for Information Technology and Chief Information Officer in conjunction with the Office of the Vice President for Legal Affairs will make appropriate changes to the Identity Theft Detection and Prevention Program Policy or Procedure, including the list of Red Flags as he or she deems necessary.

Section 7. Responsibility for Interpretation

- 7.1 Application of this procedure is the responsibility of the Associate Provost for Information Technology and Chief Information Officer.

Section 8. Responsibility for Interpretation

- 8.1 Responsibility for interpretation of this procedure rests solely with the Office of the Associate Provost for Information Technology and Chief Information Officer.