Identity Theft Red Flags
Policies and Procedures

January 2014
1. PURPOSE

The purpose of these Identity Theft Red Flags Procedures is to detect, prevent, and mitigate loss due to errors or malicious behavior when working with consumers’ new and existing covered accounts. Bloomfield College recognizes that absolute security against all threats is an unrealistic expectation. Therefore, the goals of risk reduction and implementation of these procedures are based on:

- An assessment of the “covered accounts” handled by Bloomfield College.
- The cost of preventative measures designed to detect and prevent errors or malicious behavior.
- The amount of risk that Bloomfield College is willing to absorb.

These procedures were derived through a risk assessment of Bloomfield College’s methods of opening new or accessing existing accounts. Determination of appropriate security measures must be a part of all operations and shall undergo periodic evaluation.

2. BACKGROUND

In October 2007, the Joint Committee of the Office of the Comptroller of Currency (OCC), the Federal Reserve Board, the Federal Deposit Insurance Corporation (FDIC), the Office of Thrift Supervision (OTS), the National Credit Union Administration (NCUA), and the Federal Trade Commission passed final legislation for sections 114 and 315 of the Fair and Accurate Credit Transactions Act of 2003 (FACTA). They are known as Red Flag Regulations and Guidelines. Because Bloomfield College offers “credit” through deferred payment plans, the College is covered by these pronouncements by virtue of offering payment plans. It also makes good business sense for the College to protect its constituents against the loss of confidential information.

3. DEFINITIONS

3.1. Board of Trustees and Officers
The collective body of Trustees and Officers charged with managing the operations of Bloomfield College.

3.2. Covered Account
Both new and existing accounts where a continuing relationship exists between the organization and the customer are considered “covered accounts.” There are two definitions.

3.2.1. An account that a financial institution or creditor offers or maintains, primarily for personal, family, or household purposes, that involve or is designated to permit multiple payments or transactions. Examples include a credit card account, mortgage loan, automobile loan, margin account, cell phone account, utility account, checking account, or savings account.

3.2.2. 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 mitigation risks.

3.3. Electronic or Soft Copy Format
Electronic or Soft Copy Format refers to any Confidential and Sensitive Information that exists electronically on CDs, DVDs, phones, computers, networks, portable devices, etc.

3.4. Hard Copy Format
Hard Copy Format refers to any Confidential and Sensitive Information that exists physically on paper.

3.5. Red Flags
Red Flags are patterns, practices, or specific activities involving covered accounts that indicate the possible risk of identity theft.

3.6. Service Provider
A service provider is any individual, group, or entity that directly provides a service to Bloomfield College or on behalf of Bloomfield College for its customers or clients.

3.7 Customer
A customer is a student, employee, alumnus, donor or other individual served by Bloomfield College.

4. SUMMARY OF RESPONSIBILITIES
Red flags procedures are authorized methods for detecting, preventing, and mitigating identity theft. These procedures apply to all personnel that open new or access existing covered accounts by customers. This includes all parties that may come into contact with covered accounts, such as, contractors, consultants, temporaries, and personnel of third party affiliates. Bloomfield College will implement and enforce these procedures, as well as, design more specific or new guidelines as needed.

Only authorized personnel may open new or access existing covered accounts. These accounts or records have been identified as covered accounts by Bloomfield College:

1. Admissions records
2. Student registration, grades and bio-demographic information
3. Student financial data including, financial aid, billing data, loans and collections.
4. Other academic information including records maintained by CITEL, STAR and McNair, Office of Disabilities, Office of Academic Affairs, Academic Divisions
5. Donor Information
6. Records from the Health Center, Residence Life, Student Affairs, Counseling Center, Athletics, Career Services, Security, EOF and Career Planning
7. Facilities – drivers licenses, workman’s comp claims, job applications, key request applications.
8. Human resources and payroll information( located in HR and Academic Affairs)
9. Accounting and accounts payable information
10. Information provided to third parties:
   a. ADP
   b. Hobson’s
   c. Cardsmith
   d. Allstate Data (data backup)
   e. Oxford, Delta Dental, Unum, VSP
   f. Collection agencies: ConServe, Summit Collections, Easter Revenue, AR resources
   g. Preferred student lenders: Citibank, Chase, NJ Class and Sallie Mae
   h. Aon
   i. T.L. Grosclose (athletic and student insurance)
   j. TIAA – CREF
   k. BMI Audit Services
   l. Crowe Horwath

The job classifications have been approved by various departments to work with covered accounts are included in the submissions from the following departments:

1. Admissions
2. Finance including Payroll, Bursar, Accounting and Accounts Payable
3. Human Resources
4. Athletics
5. Information Services
6. Student Life
7. Registrar
8. Advancement
9. ITPS
10. Facilities
11. Academic Affairs

5. SUMMARY OF PROCEDURES

Through the course of normal daily business operations authorized personnel may detect identity theft red flags when working with covered accounts. There are several procedures involved in making a reasonable effort to know our consumers, accurately open new accounts, and securely access existing accounts. The Identity Theft Red Flag Procedures are arranged according to the following outline:

5.1. Identification Verification Procedures. Steps that personnel take to make a reasonable effort to know individuals opening new accounts or requesting access to an existing account. This includes both document and non-document forms of verification.

5.2. Red Flags Response Procedures. Acceptable actions that each job classification may take when detecting an identity theft red flag.
5.3. **Address Discrepancy Procedures.** In the event the College or an agent of the College utilizes a Credit Reporting Agency (CRA), upon notification of an address discrepancy from a Consumer Reporting Agency (CRA), personnel are required to confirm the consumer’s address and furnish it to the CRA.

5.4. **Third Party Procedures.** The appropriate department in the College shall assure that each of the third party providers cited above must comply with our identity theft program. An affidavit for the maintenance of an identity theft prevention program shall be signed by each third party vendor. See attachment D.

6. **IDENTIFICATION VERIFICATION PROCEDURES**

Identification verification procedures are necessary for personnel to form a reasonable belief they know the identity of the individual opening a new covered account or accessing an existing covered account. The following procedures were derived from the CIP Rules in section 326 of the U.S. Patriot Act.

6.1. **Opening New Covered Accounts.** Personnel of Bloomfield College shall request identification, one primary or two secondary forms of identification when opening a new covered account for an individual. Examples of acceptable identification can be found in Appendix B. A red flag that occurs at any point in this procedure will stop the procedure and trigger a “Red Flags Response Procedure,” as indicated in section 7.

6.1.1. **Procedures for identification verification.** Bloomfield College has various procedures for identification verification for entering academic programs, obtaining employment at the College and establishment of an alumnus or donor record.

6.1.1.1. **Student Registrants.**
6.1.1.1.1. Obtain legal name, physical address, date of birth.
6.1.1.1.2. Request one form of primary identification to open the account; or two secondary forms. Verification will occur at the time a student obtains a College ID card.
6.1.1.1.3. Respond to red flags that may occur in the identification verification procedures as indicated in section 7, “Red Flags Response Procedures.”

6.1.1.2. **Employees**
6.1.1.2.1. Obtain legal name, physical address, date of birth.
6.1.1.2.2. Request one primary form of identification, birth certificate and social security card.

6.1.1.3. **Alumnus or Donor** Obtain legal name and physical address.
6.1.1.4. **Applicants** Obtain legal name, physical address and date of birth.
6.1.1.5. **Financial Aid** Obtain legal name, physical address, date of birth and social security number.

6.1.2. **Procedures for Opening Accounts By Mail (Registration for Course or Academic program) ITPS /admissions**
6.1.2.1. The applicant requesting to open an account by mail must include a copy of two forms of identification to open the account; one primary, and one secondary with the account application. Transcript may be counted as secondary form.
6.1.2.2. The account application must include legal name, physical address, date of birth, for all signatures on the account.
6.1.2.3. Non-Document Verification; Our method of non-document verification is Date of Birth and Home Address.
6.1.2.4. Respond to red flags that may occur in the identification verification procedures as indicated in section 7, “Red Flags Response Procedures.”

6.1.3. **Procedures for Verifying New Accounts On Line (Registration for Course or Academic Program) fin aid is already matching.**

6.1.3.1. Obtain legal name, physical address and date of birth.
6.1.3.2. Mail application to applicant for verification purposes.
6.1.3.3. Non-Document Verification: Our method of non-document verification is date of birth and home residence.
6.1.3.4. Respond to red flags that may occur in the identification verification procedures as indicated in section 7, “Red Flags Response Procedures.”

6.2. **Accessing Existing Covered Accounts.** Personnel of Bloomfield shall request the Bloomfield College ID card or in its absence a form of primary identification.

6.2.1. **Procedures for Accessing Accounts In Person**

6.2.1.1. Request Bloomfield College ID card or other primary identification.
6.2.1.2. Further verify if suspicious the identification with information on file for that individual including date of birth or home address.
6.2.1.3. Respond to red flags that may occur in the identification verification procedures as indicated in section 7, “Red Flags Response Procedures.”

6.2.2. **Procedures for Accessing Accounts on the Phone**

6.2.2.1 Request Name and Bloomfield College ID number.
6.2.2.2 Request date of birth, home address or home phone number.
6.2.2.3 Respond to red flags that may occur in the identification procedures as indicated in section 7, “Red Flags Response Procedures”.

6.2.3. **Procedures for Accessing Accounts By Mail**

6.2.3.1. The applicant requesting to transact on an account by mail must include a copy of two forms of identification; one primary, and one secondary with the transaction request.
6.2.3.2. Verify the identification with information on file for that individual.
6.2.3.3. Respond to red flags that may occur in the identification verification procedures as indicated in section 7, “Red Flags Response Procedures.”

6.2.4. **Procedures for Accessing Accounts On Line**

6.2.4.1. Request the user name and password.
6.2.4.2. Validate user name and password.
6.2.4.3. Respond to red flags that may occur in the identification verification procedures as indicated in section 7, “Red Flags Response Procedures.”

7. **RED FLAGS RESPONSE PROCEDURES**

Red Flags Response Procedures must be followed when any personnel detect a red flag while working with covered accounts. Each job classification at [department or organization] may have different functions with covered accounts. Therefore, each job classification’s responses to red flags may differ. This section addresses each job classification individually and the red flags categories that impact them specifically. A detailed list of relevant red flags is broken down by category in Appendix A.

7.1. **Front Line Staff (Job titles listed in Appendix B)**
Front line staff are authorized to take one or more of the following actions when a red flag is detected as described in each of the relevant categories in this section. A detailed list of relevant red flags is broken down by category in Appendix A. When all available actions have been exhausted, front line staff will escalate the response to supervisors.

7.1.1. Response to Alerts, Notifications or Warnings from a Consumer Reporting Agency
When presented with an alert, notification or warning from a consumer reporting agency, act quickly in an effort to prevent or mitigate loss for the customer and Bloomfield College. Appropriate responses are as follows:

- Take additional steps to verify identity.
- Flag relevant accounts.
- Monitor account activity.
- Decline account application.
- Validate address.
- Document with a Suspicious Activity Report (SAR) to supervisor.
- Notify existing customer on record.
- Other

When all available actions have been exhausted, escalate the response to supervisor.

7.1.2. Response to Suspicious Documents
While working with covered accounts, front line staff may be presented documents that appear suspicious or altered in some way. Appropriate responses are as follows:

- Verify using third party resources.
- Verify using existing account records.
- Decline application.
- Decline account access.
- Document with a Suspicious Activity Report (SAR) to supervisor.
- Notify existing customer on record

When all available actions have been exhausted, escalate the response to supervisor.

7.1.3. Response to Suspicious Identifying Personal Information
When a person provides suspicious or inconsistent identifying information while opening or accessing a covered account, the response is as follows:

- Escalate verification to a supervisor.
- Decline account application.
- Decline account access.
- Notify existing customer on record.
- Change account access information.
- Change account numbers.
- Document with a Suspicious Activity Report (SAR).
- Involve law enforcement.

When all available actions have been exhausted, escalate the response to supervisor.
7.1.4. **Response to Unusual Use of, Suspicious Activity Related to, the Covered Account**

Be vigilant in protecting customer accounts when transacting, servicing, or processing business. When suspicious activity or unusual patterns emerge in covered accounts, the appropriate responses are as follows:

- Use Personal Knowledge questions for verification.
- Validate address.
- Decline account access.
- Document with a Suspicious Activity Report (SAR).
- Notify existing customer on record.
- Change account access information.
- Change account numbers.

When all available actions have been exhausted, escalate the response to supervisor.

7.1.5. **Response to Notice From Customers, Victims of Identity Theft, Law Enforcement Authorities, or Other Persons Regarding Possible Identity Theft in Connection with Covered Accounts**

When notified of a security incident from customers, victims of identity theft, law enforcement authorities, or other persons regarding possible identity theft in connection with covered accounts must immediately inform senior management and the Identity Theft Prevention Officer. Appropriate responses are as follows:

- Decline account access.
- Close fraudulent account.
- Document with a Suspicious Activity Report (SAR).
- Notify existing customer on record.
- Open new account.
- Do Not Attempt to Collect on the Fraudulent Account from the True Identity.
- Cooperate with law enforcement.
- Notify supervisor.

7.2. **Supervisors**

Supervisors are authorized to take one or more of the following actions when a red flag is detected as described in each of the relevant categories in this section. A detailed list of relevant red flags is broken down by category in Appendix A. *When all available actions have been exhausted, supervisors will escalate to the appropriate Vice President.*

7.2.1. **Response to Alerts, Notifications or Warnings from a Consumer Reporting Agency**

When presented with an alert, notification or warning from a consumer reporting agency, act quickly in an effort to prevent or mitigate loss for the customer and Bloomfield College. Appropriate responses are as follows:

- Take additional steps to verify identity.
- Flag relevant accounts.
- Decline account application.
- Validate address.
- Document with a Suspicious Activity Report (SAR).
- Notify existing customer on record.
7.2.2. **Response to Suspicious Documents**

While working with covered accounts, [job classification 2] may be presented documents that appear suspicious or altered in some way. Appropriate responses are as follows:

- Verify using third party resources.
- Verify using existing account records.
- Decline application.
- Decline account access.
- Document with a Suspicious Activity Report (SAR).
- Notify law enforcement through Director of Public Safety (if necessary).
- Notify existing customer on record.

7.2.3. **Response to Suspicious Identifying Personal Information**

When a person provides suspicious or inconsistent identifying information while opening or accessing a covered account, the response is as follows:

- Escalate verification to a higher level.
- Decline account application.
- Decline account access.
- Notify existing customer on record.
- Change account access information.
- Change account numbers.
- Document with a Suspicious Activity Report (SAR).
- Involve law enforcement through Director of Public Safety.

7.2.4. **Response to Unusual Use of, Suspicious Activity Related to, the Covered Account**

Be vigilant in protecting customer accounts when transacting, servicing, or processing business. When suspicious activity or unusual patterns emerge in covered accounts, the appropriate responses are as follows:

- Use Personal Knowledge questions for verification.
- Validate address.
- Decline account access.
- Document with a Suspicious Activity Report (SAR).
- Notify existing customer on record.
- Change account access information.
- Change account numbers.
- Involve law enforcement through Director of Public Safety.

7.2.5. **Response to Notice From Customers, Victims of Identity Theft, Law Enforcement Authorities, or Other Persons Regarding Possible Identity Theft in Connection with Covered Accounts**

When notified of a security incident from customers, victims of identity theft, law enforcement authorities, or other persons regarding possible identity theft in connection with covered accounts must immediately inform senior management and the Identity Theft Prevention Officer. Appropriate responses are as follows:

- Decline account access.
- Close fraudulent account.
8. ADDRESS DISCREPANCY PROCEDURES

8.1. Change of Address Requirements

Section 114 of the FACT Act requires financial institutions assess the validity of a request for a change of address.

8.1.1. Request Bloomfield ID prior to processing an address change or primary or secondary ID or primary ID

8.1.2. Mail notification to the customer of the request at the customer's former address to provide the customer with a means to promptly report an incorrect address.
APPENDIX A

IDENTITY THEFT RED FLAGS

The following identity theft red flags have been identified as risks to the covered accounts in Bloomfield College

Suspicious Documents

1.1.1.1. Documents provided for identification appear to have been altered or forged.

1.1.1.2. The photograph or physical description on the identification is not consistent with the appearance of the applicant or customer presenting the identification.

1.1.1.3. Other information on the identification is not consistent with information provided by the person opening a new covered account or customer presenting the information.

1.1.1.4. Other information on the identification is not consistent with readily accessible information that is on file with the financial institution or creditor, such as a signature card or a recent check.

1.1.1.5. An application appears to be altered or forged, or gives the appearance of being reassembled.

Other

Suspicious Identifying Personal Information

1.1.1.6. Personal identifying information provided is inconsistent when compared to external identification sources used by the financial institution or creditor. For example: a) The address does not match any address on the consumer; or b) The Social Security Number (SSN) has not been issued, or is listed on the Social Security Administration’s Death Master File.

1.1.1.7. Personal identifying information provided by the consumer 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 the date of birth.

1.1.1.8. Personal identifying information provided is associated with known fraudulent activity as indicated by internal or third-party sources used by the financial institution or creditor. For example: a) the address on an application is fictitious, a mail drop, or prison; or b) the phone number on an application is the same as the number provided on a fraudulent application.

1.1.1.9. Personal identifying information provided is of a type commonly associated with fraudulent activity as indicated by internal or third-party sources used by the financial institution or creditor. For example: a) The address on an application is fictitious, a mail drop, or prison; or b) The phone number is invalid, or is associated with a pager or answering service.

1.1.1.10. The SSN provided is the same as that submitted by other persons.

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

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

1.1.1.13. Personal identifying information provided is not consistent with personal identifying information that is on file with the financial institution or creditor.

1.1.1.14. For financial institutions and creditors that use challenge questions, 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.
Other

Unusual Use of, Suspicious Activity Related to, the Covered Account

1.1.1.15. Shortly following the notice of a change of address for a covered account, the institution or creditor receives a request for new, additional, or replacement cards, or a cell phone, or for additional authorized users on the account.

1.1.1.16. A new revolving credit account is used in a manner commonly associated with known patterns of fraud patterns. For example: a) the majority of available credit is used for cash advances or merchandise that is easily convertible to cash (e.g. electronic equipment or jewelry); or b) the customer fails to make the first payment or makes an initial payment but no subsequent payments.

1.1.1.17. A covered account is used in a manner that is not consistent with established patterns of activity on the account. There is, for example: a) non-payment when there is no history of late or missed payments; b) a material increase in the use of available credit; c) a material change in purchasing or spending patterns; d) a material change in electronic fund transfer patterns in connection with a deposit account; or e) a material change in telephone call patterns in connection with a cellular phone account.

1.1.1.18. 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).

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

1.1.1.20. The financial institution or creditor is notified that the customer is not receiving paper account statements.

1.1.1.21. The financial institution or creditor is notified of unauthorized charges or transactions in connection with a customer’s covered account.

Notice From Customers, Victims of Identity Theft, Law Enforcement Authorities, or Other Persons Regarding Possible Identity Theft in Connection with Covered Accounts

1.1.1.22. The financial institution or creditor 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.

Appendix B – Forms of Acceptable ID

- Bloomfield College ID – Primary
- US Driver’s License - Primary
- Passport (any country) – Primary
- Alien registration card (green card) – Primary
- State ID – Primary
- Military ID – Primary
- Any photo ID (high school, credit card, employer) – primary
- Credit or ATM Card – Secondary
- Bank statement or record – Secondary
- Marriage Certificate – Secondary
- Bloomfield College Statement of Account Addressed to home
- Official transcript from another institution with raised seal - Secondary
- Health, Dental or Prescription Card - Secondary
- Social security card – required for employment - Secondary
Appendix C – List of Front Line and Supervisory Titles

Front Line

Registrar
Assistant Registrar
Assistant to the Registrar
Director of Advising/Coaching
Adviser/Coach
Secretary
Coordinator for Disabilities
Secretary for Office of Disabilities
Student Workers

Athletics

Secretary
Athletic Trainer
Sports Information
Baseball Coach
Men’s Soccer Coach
Women’s Soccer Coach
Tennis Coach
Women’s Basketball Coach
Men’s Basketball Coach
Softball Coach
Compliance Director

ITPS

Program Coordinator/Registration
Operations Coordinator
International Program Coordinator

Accounting

Accountant
Accounts Payable Manager

Payroll and Human Resources

Payroll Managers
Associate Director of Human Resources

Admissions

Enrollment Services Coordinator
International Student Coordinator
Admissions Counselor
Receptionist
Data Processor
Administrative Assistant to the VP

Advancement

Director of Donor Relations
Director of Grants
Director of Public Relations
Managing Director of WAC
Office Manager
Work Study Student
Identity Theft Red Flags Policies and Procedures

Office of Academic Affairs
Administrative Assistants to VPAA and AVPAA
Contract specialist
CITEL
Director
Secretaries
Master Tutors
Starr
McNair
Facilities
Secretary
Student Financial Services
Financial Aid Counselor

**Supervisor**
Registrar
Registrar
Associate Registrar

**Athletics**
Athletic Director

**ITPS**
Assistant Director of ALC
Assistant Director for Teacher Programs
Associate Director for Global Programs
Associate Director of Technology

**Facilities**
Supervisor

**Admissions**
VP Enrollment Management
Director of Admissions

**Advancement**
VP for Advancement

Office of Academic Affairs
VPAA
AVPAA

**Student Financial Services**
Director

**Finance**
Director of Business Services