Identity Theft Prevention Program
Lake Forest College
Revision 1.0

This document supersedes all previous identity theft prevention program documents.

Approved and Adopted by:
The Board of Directors

Date: __________________
# Table of Contents

1 Introduction ........................................................................................................................................ 3
2 Risk Assessment .................................................................................................................................. 5
  2.1 Risk Matrix ...................................................................................................................................... 7
3 Program Elements ................................................................................................................................. 9
  3.1 Identification of Relevant Red Flags .............................................................................................. 10
  3.2 Detection of Red Flags .................................................................................................................... 12
  3.3 Prevention and Mitigation of Identity Theft ...................................................................................... 13
  3.4 Update the Program ....................................................................................................................... 14
  3.5 Administration of the Program ....................................................................................................... 15
  3.6 Other Applicable Legal Requirements ............................................................................................ 16
4 Red Flag Policies and Procedures ........................................................................................................ 17
  4.1 Alerts, Notifications or Warnings .................................................................................................... 18
    4.1.1 Consumer Report Alert ....................................................................................................... 19
    4.1.2 Consumer Report Address Discrepancy .............................................................................. 20
    4.1.3 Protection of Faculty, Staff and Student Information .......................................................... 21
  4.2 Suspicious Documents .................................................................................................................... 22
    4.2.1 Documents Altered or Forged ............................................................................................. 23
    4.2.2 Photograph or Physical Description Inconsistency ............................................................... 24
    4.2.3 Information on ID Inconsistent with Information on File .................................................. 25
  4.3 Suspicious Personal Identifying Information .................................................................................... 26
    4.3.1 Personal ID or SSN is Associated with Known Fraudulent Activity .................................... 27
    4.3.2 The SSN has been Submitted by Other Persons ................................................................. 28
  4.4 Unusual Use or Suspicious Activity ................................................................................................ 29
    4.4.1 Mail is Returned on a Current Employee and/or Student Account ..................................... 30
    4.4.2 Service Providers to Lake Forest College .............................................................................. 31
  4.5 Notice Given ................................................................................................................................... 32
    4.5.1 Notice that a Fraudulent Account has been Opened ............................................................ 33
5 Appendices ......................................................................................................................................... 34
  5.1 Adoption/Revision Log .................................................................................................................... 35
  5.2 Report Template ............................................................................................................................. 36
  5.3 Regulations .................................................................................................................................... 38
    5.3.1 16 CFR Part 681 ................................................................................................................ 39
Statement of Need and Definition

Customers depend on Lake Forest College to properly protect personal, nonpublic information, which is gathered and stored in internal records. Regulatory agencies are charged with the responsibility to ensure financial institutions and creditors information security controls and procedures are in compliance with the intent of the regulations to protect a customer's identity. Therefore, it is important for management and staff to understand the basic security requirements and provide ongoing assistance in detection, prevention, and mitigation of identity theft to Lake Forest College's customers.

Compliance

This Identity Theft Prevention Program is designed to emphasize compliance with all information security requirements, including those detailed in the regulatory agency guidelines. Specifically, the intent of the Identity Theft Prevention Program is to meet the objectives of the FACT Act, as set forth in FTC Rules and Regulations 16 CFR Part 681 – Identity Theft Red Flags. Furthermore, the Identity Theft Prevention Program is aligned with FFIEC and FTC requirements.

Objective

Lake Forest College’s objective is to develop a written Identity Theft Prevention Program, designed to detect, prevent, and mitigate identity theft in connection with the opening of a covered account or any existing covered account.

- An officer and/or senior management employee of Lake Forest College will serve as the organization’s Identity Theft Prevention Coordinator.
- The program will be updated periodically to reflect changes in risks to customers and to the safety and soundness of the financial institution or creditor from identity theft.
Goals

The specific goals of this program are to:

- Identify relevant Red Flags for the covered accounts that Lake Forest College offers or maintains.
- Define reasonable policies and procedures to detect and respond to identified Red Flags.
- Update the program and Red Flags periodically to reflect changes in risks to customers and to the safety and soundness of Lake Forest College.
- Ensure Board of Directors involvement in the adoption of the organization’s written Identity Theft Prevention Program and ongoing oversight of the integral parts of the Identity Theft Prevention Program and related Red Flags.
- Establish responsibility for implementation and maintenance of the Identity Theft Prevention Program, including ongoing review of Red Flags.
- Design, implement, and maintain information security controls to address identified risks relative to the sensitivity level of customer information.
- Train management and staff, as necessary, to effectively implement the Identity Theft Prevention Program.
- Exercise appropriate and effective oversight of service providers and require these vendors to provide appropriate measures designed to meet the control objectives of the Identity Theft Prevention Program.
- Report to the Board of Directors at least annually. The report will address material matters related to the Program and evaluate issues such as: the effectiveness of policies and procedures in addressing the risk of identity theft in connection with the opening of covered accounts and with respect to existing covered accounts; service provider arrangements; significant incidents involving identity theft and management’s response; and recommendations for material changes to the Program.

Responsibility

The responsibility of maintaining an effective Identity Theft Prevention Program is assigned to the Budget & Audit.

The Budget & Audit will be responsible for the appointment of an Identity Theft Prevention Coordinator. The current Identity Theft Prevention Coordinator will be Doris Dumas. The Identity Theft Prevention Coordinator will report to the Budget & Audit.
Regulatory Requirement

16 CFR Part 681 (c) (Periodic Identification of Covered Accounts) states:

“Each financial institution or creditor must periodically determine whether it offers or maintains covered accounts. As part of this determination, a financial institution or creditor must conduct a risk assessment to determine whether it offers or maintains covered accounts described in paragraph (b)(3)(ii) of this section, taking into consideration:

(1) The methods it provides to open its accounts;
(2) The methods it provides to access its accounts; and
(3) Its previous experiences with identity theft.”

Purpose

The risk assessment required per 16 CFR Part 681 (c) determines if an institution has covered accounts and, consequently, must develop a formal Identity Theft Prevention Program. The risk assessment must be updated periodically based on changes in methods used to open accounts, methods available to access accounts and the institution’s experience with identity theft.

Risk Factors

Based on Lake Forest College’s Identity Theft Prevention Program Risk Assessment, the following risk factors have been identified:

Types of covered accounts offered:

- Cash Management
- Employee and Student Records
- Loan and Tuition Accounts

Methods to open a covered account:

- By Telephone
- In Person
- Over the Internet
- Through a Third Party
- Through the Mail

Methods to access a covered account:

- ACH
- ATM
- Automatic Transfers
- By Telephone
- Check
- Credit Card
- Debit Card
- In Person
- Merchant Capture
Threat and Risk Levels

The Identity Theft Risk Assessment follows a qualitative model. Risk levels are determined by considering the likelihood and potential damage of an event as defined below.

Likelihood definitions
- **Low**: Identity Theft is not expected, but there's a slight possibility it may occur at some time.
- **Medium**: Identity Theft might occur at some time based on a history of limited occurrence, type of covered account, and size and complexity of the organization.
- **High**: Identity Theft will probably occur based on a history of frequent occurrence, type of covered account, and size and complexity of the organization.

Damage Potential definitions
- **Minimal**: Identity Theft may result in the minor loss of some resources and reputation.
- **Moderate**: Identity Theft may result in loss of resources and reputation which could harm the organization’s ability to achieve its mission.
- **Major**: Identity Theft may result in the loss of major resources and reputation which would harm the organization's ability to achieve its mission.

Risk Level definitions
- **Low**: Impact is minimal and could even be considered a cost of doing business.
- **Medium**: Impact could be significant and possibly affect the stability of the organization.
- **High**: Impact is major and could threaten the stability of the organization.

Conclusion

Based on the Identity Theft Prevention Program Risk Assessment, Lake Forest College has confirmed it is required to develop and maintain an Identity Theft Prevention Program.
## 2.1 Risk Matrix

<table>
<thead>
<tr>
<th>Covered Account</th>
<th>Threat</th>
<th>Methods</th>
<th>Controls (Red Flags)</th>
<th>Likelihood</th>
<th>Potential Damage</th>
<th>Risk</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Cash Management</strong></td>
<td>Opened Fraudulently</td>
<td>In Person, Through a Third Party, Through the Mail</td>
<td>Documents Altered or Forged, Information on ID Inconsistent with Information on File, Mail is Returned on a Current Employee and/or Student Account, Personal ID or SSN is Associated with Known Fraudulent Activity, Photograph or Physical Description Inconsistency, The SSN has been Submitted by Other Persons</td>
<td>Medium</td>
<td>Minimal</td>
<td>Low</td>
</tr>
<tr>
<td></td>
<td>Unauthorized Access</td>
<td>ACH, ATM, Automatic Transfers, By Telephone, Check, Credit Card, Debit Card, In Person, Merchant Capture, Over the Internet, Through a Third Party, Through the Mail, Wire Transfers</td>
<td>Documents Altered or Forged, Information on ID Inconsistent with Information on File, Mail is Returned on a Current Employee and/or Student Account, Notice that a Fraudulent Account has been Opened, Personal ID or SSN is Associated with Known Fraudulent Activity, Photograph or Physical Description Inconsistency</td>
<td>Low</td>
<td>Major</td>
<td>High</td>
</tr>
<tr>
<td><strong>Employee and Student Records</strong></td>
<td>Opened Fraudulently</td>
<td>By Telephone, In Person, Through the Mail</td>
<td>Documents Altered or Forged, Information on ID Inconsistent with Information on File, Mail is Returned on a Current Employee and/or Student Account, Personal ID or SSN is Associated with Known Fraudulent Activity, Photograph or Physical Description Inconsistency, Protection of Faculty, Staff and Student Information</td>
<td>Low</td>
<td>Minimal</td>
<td>Low</td>
</tr>
<tr>
<td></td>
<td>Unauthorized Access</td>
<td>ACH, Automatic Transfers, Check, Credit Card, Over the Internet, Through a Third Party, Through the Mail, Wire Transfers</td>
<td>Consumer Report Address Discrepancy, Documents Altered or Forged, Notice that a Fraudulent Account has been Opened, Personal ID or SSN is Associated with Known Fraudulent Activity, Photograph or Physical Description Inconsistency, Protection of Faculty, Staff and Student Information, The SSN has been Submitted by Other Persons</td>
<td>Low</td>
<td>Minimal</td>
<td>Low</td>
</tr>
<tr>
<td><strong>Loan and Tuition Accounts</strong></td>
<td>Opened Fraudulently</td>
<td>In Person, Over the Internet, Through a Third Party, Through the Mail</td>
<td>Documents Altered or Forged, Information on ID Inconsistent with Information on File, Mail is Returned on a Current Employee and/or Student Account, Notice that a Fraudulent Account has been Opened, Personal ID or SSN is Associated with Known Fraudulent Activity, Photograph or Physical Description Inconsistency, The SSN has been Submitted by Other Persons</td>
<td>Medium</td>
<td>Major</td>
<td>High</td>
</tr>
<tr>
<td>Covered Account</td>
<td>Threat</td>
<td>Methods</td>
<td>Controls (Red Flags)</td>
<td>Likelihood</td>
<td>Potential Damage</td>
<td>Risk</td>
</tr>
<tr>
<td>-----------------</td>
<td>-------------------------</td>
<td>-------------------------------------------------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>------------</td>
<td>------------------</td>
<td>-------</td>
</tr>
<tr>
<td></td>
<td>Unauthorized Access</td>
<td>ACH, Automatic Transfers, By Telephone, Check, In Person, Over the Internet, Through a Third Party, Through the Mail, Wire Transfers</td>
<td>Documents Altered or Forged, Information on ID Inconsistent with Information on File, Mail is Returned on a Current Employee and/or Student Account, Notice that a Fraudulent Account has been Opened, Personal ID or SSN is Associated with Known Fraudulent Activity, Photograph or Physical Description Inconsistency, The SSN has been Submitted by Other Persons</td>
<td>Medium</td>
<td>Major</td>
<td>High</td>
</tr>
</tbody>
</table>
Statement

The Board of Directors of Lake Forest College requires the organization to develop and implement a comprehensive Identity Theft Prevention Program, which identifies relevant Red Flags for all covered accounts. The program will be reviewed and assessed on an annual basis, and the results will be reported to the Board of Directors.

The following other Programs relate to the Identity Theft Prevention Program:

- The Customer Identification Program per 31 U.S.C. 5318(l) (31 CFR 103.121)
- The Fraud Prevention Program
3.1 Identification of Relevant Red Flags

Risk Factors

To identify relevant Red Flags, Lake Forest College has evaluated the following factors (see Risk Assessment section above):

Types of covered accounts:

Lake Forest College offers the following types of covered accounts:

- Cash Management
- Employee and Student Records
- Loan and Tuition Accounts

Methods to open a covered account:

- By Telephone
- In Person
- Over the Internet
- Through a Third Party
- Through the Mail

Methods to access a covered account:

- ACH
- ATM
- Automatic Transfers
- By Telephone
- Check
- Credit Card
- Debit Card
- In Person
- Merchant Capture
- Over the Internet
- Through a Third Party
- Through the Mail
- Wire Transfers

Previous experiences with identity theft:

Lake Forest College will take into account previous experiences with identity theft when defining and updating Red Flags.

Sources of Red Flags

Lake Forest College will incorporate relevant Red Flags from sources such as:

- Incidents of identity theft Lake Forest College has experienced.
- Methods of identity theft that reflect changes in identity theft risks.
- Applicable supervisory guidance.

Categories of Red Flags

Lake Forest College will categorize relevant Red Flags into the following categories:
- Alerts, notifications, or other warnings received from consumer reporting agencies or service providers, such as fraud detection services.
- The presentation of suspicious documents.
- The presentation of suspicious personal identifying information, such as a suspicious address change.
- The unusual use of, or other suspicious activity related to, a covered account.
- Notice from customers, victims of identity theft, law enforcement authorities, or other persons regarding possible identity theft in connection with covered accounts held by the financial institution or creditor.

See Section 4 (Red Flag Policies and Procedures) for a list of identified, relevant Red Flags.
Detecting Red Flags

Lake Forest College will address detection of Red Flags in connection with opening of covered accounts and existing covered accounts by:

- Obtaining identifying information about, and verifying the identity of, a person opening a covered account. Lake Forest College will use the policies and procedures regarding identification and verification set forth in the Customer Information Program (CIP), as defined in 31 U.S.C. 5318(l) (31 CFR 103.121).
- Authenticating customers, monitoring transactions, and verifying the validity of change of address requests, in the case of existing covered accounts.
3.3 Prevention and Mitigation of Identity Theft

Preventing and Mitigating Red Flags

Lake Forest College has measures in place to appropriately respond to Red Flags detected that are commensurate with the degree of risk posed. Appropriate responses may include:

- Monitoring a covered account for evidence of identity theft;
- Contacting the customer;
- Changing any passwords, security codes, or other security devices that permit access to a covered account;
- Reopening a covered account with a new account number;
- Not opening a new covered account;
- Closing an existing covered account;
- Not attempting to collect on a covered account or not selling a covered account to a debt collector;
- Notifying law enforcement; or
- Determining that no response is warranted under the particular circumstances...

When determining the appropriate response, Lake Forest College will consider aggravating factors that may heighten the risk of identity theft, such as a data security incident that results in unauthorized access to a customer’s account records held by the Lake Forest College or a third party, or notice that a customer has provided information related to a covered account held by Lake Forest College to someone fraudulently claiming to represent Lake Forest College or to a fraudulent website.
3.4 Update the Program

Updating the Program

Lake Forest College will update the Program (including a review of relevant Red Flags) periodically, to reflect changes in risks to customers or to the safety and soundness of Lake Forest College from identity theft based on factors such as:

- The experiences of Lake Forest College with identity theft.
- Changes in methods of identity theft.
- Changes in methods to detect, prevent, and mitigate identity theft.
- Changes in the types of accounts that Lake Forest College offers or maintains.
- Changes in the business arrangements of Lake Forest College including mergers, acquisitions, alliances, joint ventures, and service provider arrangements.
3.5 Administration of the Program

Oversight of the Program

The responsibility of maintaining an effective Identity Theft Prevention Program is assigned to the Budget & Audit.

The Budget & Audit will be responsible for the appointment of an Identity Theft Prevention Coordinator. The current Identity Theft Prevention Coordinator will be Doris Dumas. The Identity Theft Prevention Coordinator will report to the Budget & Audit.

The Identity Theft Prevention Coordinator will:

- Work closely with the organization’s senior management and front line personnel to identify, detect, and respond to appropriate Red Flags,
- Assign specific responsibility for the Program’s implementation,
- Approve material changes to the Program as necessary to address changing identity theft risks, and
- Report to the Board of Directors at least annually on the compliance of the Program. The report should address material matters related to the Program and evaluate issues such as:
  - The effectiveness of the policies and procedures of Lake Forest College in addressing the risk of identity theft in connection with the opening of covered accounts and with respect to existing covered accounts,
  - Service provider arrangements,
  - Significant incidents involving identity theft and management’s response, and
  - Recommendations for material changes to the Program.

Oversight of Service Providers

Whenever Lake Forest College engages a service provider to perform an activity in connection with one or more covered accounts, Lake Forest College will 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, Lake Forest College might require the service provider by contract to have policies and procedures in place to detect relevant Red Flags that may arise in the performance of the service provider’s activities, and either report the Red Flags to Lake Forest College or take appropriate steps to prevent or mitigate identity theft.

Staff Training

Financial institutions or creditors need to educate employees to identify and respond to Red Flags. Training supports security awareness and strengthens compliance with the Identity Theft Prevention Program. Ultimately, the behavior and priorities of senior management heavily influence the level of employee awareness and policy compliance, so training and the commitment to security starts with senior management.

Staff will be trained as necessary to effectively implement the Program. Training materials for Lake Forest College will review the identification, detection and response to Red Flags.
3.6 Other Applicable Legal Requirements

Lake Forest College will be mindful of other related legal requirements that may be applicable, such as:

- Filing a Suspicious Activity Report under 31 U.S.C. 5318 (g);
- Implementing requirements under 15 U.S.C. 1681c-1(h) regarding the circumstances under which credit may be extended when the Lake Forest College detects a fraud or active duty alert;
- 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
- 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.
The following Red Flag Policies and Procedures are designed to identify, detect, and respond appropriately to identity theft in connection with the opening of a covered account or access to an existing covered account.
4.1 Alerts, Notifications or Warnings

Red Flags associated alerts, notifications, or other warnings received from consumer reporting agencies or service providers, such as fraud detection services.
4.1.1 Consumer Report Alert

Red Flag

A fraud or active duty alert is included on a consumer report.

Detection

Lake Forest College becomes aware of fraud on a consumer report.

Response

Lake Forest College becomes aware of fraud or notification on a consumer report, Lake Forest College will take the following steps:

- Determine from the consumer or customer the reason for the alert.
- Notify faculty, staff or student member that fraud has been attempted.
- Cancel or reverse any transactions that were done erroneously.
- Notify and cooperate with appropriate law enforcement.
- Determine if no response is warranted under the particular circumstances.

Verification

Ensure appropriate employees are trained to adequately review consumer reports and act on adverse information.

Responsibility

Identity Theft Prevention Coordinator
4.1.2 Consumer Report Address Discrepancy

Red Flag
Lake Forest College receives notice of an address discrepancy from a consumer reporting agency or third-party servicer.

Response
Lake Forest College will do the following:
- Determine from internal files whether address is different.
- Verify with faculty, staff or student the correct address.
- Verify the address with the consumer report or third party.

Verification
Ensure appropriate employees are trained to adequately review consumer reports and resolve discrepancies.

Responsibility
Identity Theft Prevention Coordinator
4.1.3 Protection of Faculty, Staff and Student Information

Red Flag

Personal faculty, staff or student data is compromised or misused by internal persons.

Detection

Lake Forest College will safeguard all sensitive information and will confirm that only specific personnel have access to data.

Response

Lake Forest College will take the following steps with respect to internal operating procedures to protect data:

- Use proper internal controls to ensure only authorized persons have access to data.
- Identify employees who need access to personnel data and restrict those who do not.
- Provide View only access for anyone who does not need to make changes to data.
- Request minimal information on forms, only what is necessary to identify faculty, staff or student member.
- Mitigate the times social security number is requested on forms.
- Immediately and properly discard any credit card data received.
- Completely and securely discard paper documents and computer files when no longer relevant.
- Required system passwords are changed frequently.
- Ensure the website is secure and provide notice when not secure.
- Ensure computer virus protection is kept up to date.
- Have new employees signed an agreement to properly protect sensitive data.

Verification

Ensure that proper personnel are adequately trained. Use system for various validity checks.

Responsibility

Identity Theft Prevention Coordinator
4.2 Suspicious Documents

Red Flags associated with the presentation of suspicious documents.
4.2.1 Documents Altered or Forged

Red Flag

Documents provided for identification appear to have been altered or forged. Documents could include passports, driver's licenses, and social security cards.

Detection

Faculty, staff or student's identity is verified prior to being hired, receiving cash, inquiring on a tuition or loan account or making changes to personal data (i.e. direct deposit or address changes). Documents used to verify a customer’s identity may include:

- Unexpired, government-issued identification evidencing nationality, residency or non-residency and bearing a photograph or similar safeguard, such as driver’s license or passport.
- For students, a current student Identification card is required. If non-students, a form of government identification bearing a photograph.

See Lake Forest College’s Customer Identification Program for more details.

Response

Lake Forest College will do the following:

- Determine from the faculty, staff or student the reason for the appearance of the documents.
- Obtain other evidence to verify identity.
- Consider reporting to law enforcement personnel.

Verification

Ensure appropriate employees are adequately trained to review documents provided for identification purposes.

Responsibility

Identity Theft Prevention Coordinator
4.2.2 Photograph or Physical Description Inconsistency

Red Flag

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

Detection

Employee's and Student's identity is verified prior to being hired, receiving cash, inquiring on an tuition or loan account or making changes to personal data (i.e. direct deposit or address changes). In the event photograph provided is not consistent with the appearance of the person's identity, documents used to verify person's identity may include:

- Unexpired, government-issued identification evidencing nationality, residency or non-residency and bearing a photograph or similar safeguard, such as driver's license or passport.
- For students, a current student Identification card is required. If non-students, any form of government identification bearing a photograph.

See Lake Forest College’s Customer Identification Program for more details.

Response

Lake Forest College will do the following:

- Determine from the faculty, staff or student the reason for the appearance of the documents.
- Obtain other evidence to verify identity.
- Consider reporting to law enforcement personnel.

Verification

Ensure appropriate employees are trained to adequately review documents provided for identification purposes.

Responsibility

Identity Theft Prevention Coordinator
4.2.3 Information on ID Inconsistent with Information on File

Red Flag

Other information on the identification is not consistent with readily accessible information that is on file with Lake Forest College, such as a signature card or a recent check.

Detection

Verify suspicious data with that on file with Lake Forest College. Match information timely with that on file to negate any loss.

Response

Lake Forest College will do the following:

Determine from the faculty, staff or student the reason for the appearance of the documents.

Investigate any differences.

Obtain other evidence to verify identity.

Obtain other evidence to validate information. If none is provided, notify appropriate college personnel and likely law enforcement.

Verification

Ensure appropriate employees are trained to adequately review documents provided for identification purposes.

Responsibility

Identity Theft Prevention Coordinator
4.3 Suspicious Personal Identifying Information

Red Flags associated with the presentation of suspicious personal identifying information, such as suspicious address change.
4.3.1 Personal ID or SSN is Associated with Known Fraudulent Activity

Red Flag

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:

- The address on an application is the same as the address provided on a fraudulent application;
- The phone number on an application is the same as the number provided on a fraudulent application.

Detection

Lake Forest College becomes aware of that faculty, staff or student's Identification or Social Security Number is associated with fraudulent activity.

Response

Once determined that ID or Social Security Number is associated with fraudulent activity, Lake Forest College will:

- Verify fraudulent activity exists from internal records or our third-party servicer. Verify information to that on file.
- Notify faculty, staff or student member.
- Place cash, loan, and tuition accounts on hold.
- Notify appropriate personnel and likely law enforcement.

Verification

Ensure appropriate employees are trained to adequately review documents provided for identification purposes.

Responsibility

Identity Theft Prevention Coordinator
4.3.2 The SSN has been Submitted by Other Persons

Red Flag

The Social Security Number (SSN) provided is the same as that submitted by other persons affiliated with Lake Forest College.

Detection

Lake Forest College will run reports to search for duplicate social security numbers in file. Once determined that a duplicate number exists, the college will then verify data in the Social Security Administration File.

See Lake Forest College’s Customer Identification Program for procedures for verifying the identity of a customer.

Response

Lake Forest College will verify, periodically, whether duplicate SSN's are in file. Once we determine that there are, we will then vouch information to that in the Social Security Administration File. Is discrepancy truly exists, the college will do the following:

Notify faculty, staff or student member of discrepancy.
If not immediately resolved, terminate from employment and request employee to leave premises.

Verification

Ensure appropriate employees are trained to adequately process reports and review documents provided for identification purposes. Ensure appropriate employees will properly conclude results in Social Security Administration File.

Responsibility

Identity Theft Prevention Coordinator
4.4 Unusual Use or Suspicious Activity

Red Flags associated with the unusual use of, or other suspicious activity related to, a covered account.
4.4.1 Mail is Returned on a Current Employee and/or Student

Red Flag
Mail sent to a current Lake Forest College faculty, staff or student is returned repeatedly as undeliverable although transactions continue to be conducted in connection with the their covered account.

Detection
Lake Forest College becomes aware that mail is repeatedly returned undeliverable when employee is active.

Response
Lake Forest College will do the following:
- Notify faculty, staff or student member.
- Ensure their identity.
- Determine from the faculty, staff or student the reason mail is being returned.
- Request proof of legal address.
- Place a stop mail note on file if address is not resolved.
- Put note in Notepad file so that once person contacts college, we can retrieve information.
- Flag transcripts for Hold until resolved.

Verification
Ensure appropriate employees are trained to address returned mail.

Responsibility
Identity Theft Prevention Coordinator
4.4.2 Service Providers to Lake Forest College

Red Flag
Ensure that third party service providers are not violating any sensitive information.

Detection
Lake Forest College will require third party service providers to have policies and procedures in place to detect relevant Red Flags that may arise, and safeguard personal information.

Response
Lake Forest College will require third party servicers to have policies and procedures in place to mitigate identity theft and fraud.
If servicer refuses to provide policy, Lake Forest College will consider withdrawing from the engagement.

Verification
Third Party Servicers that maintain our data are:

- Ceridian
- Educational Computer Systems
- General Revenue Corporation
- Jenzabar
- National Credit Management
- Northern Trust Bank
- Sallie Mae
- TIAA-CREF
- University Accounting Service

Responsibility
Identity Theft Prevention Coordinator
Red Flags associated with notice from customers, victims of identity theft, law enforcement authorities, or other persons regarding possible identity theft in connection with covered accounts held by Lake Forest College.
### 4.5.1 Notice that a Fraudulent Account has been Opened

<table>
<thead>
<tr>
<th><strong>Red Flag</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Lake Forest College is notified that a faculty, staff or student member is a victim of identity theft, and that an account was opened fraudulently.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Detection</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Lake Forest College is notified a fraudulent account has been opened for a person engaged in identity theft.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Response</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Lake Forest College will close the account and work with law enforcement.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Verification</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Ensure employees are trained to respond appropriately to a notification that an account has been opened for a person engaging in identity theft.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Responsibility</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Identity Theft Prevention Coordinator</td>
</tr>
</tbody>
</table>
## 5.1 Adoption/Revision Log

<table>
<thead>
<tr>
<th>Revision #</th>
<th>Revision Date</th>
<th>Approval Date</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Identity Theft Prevention Program Annual Report to the Board of Directors

Date of Report

The intent of this report is to provide the overall status of the Identity Theft Prevention Program, along with providing any updates to any of the program components.

Status

The Identity Theft Prevention Program was last updated on Date. The overall status of the Identity Theft Prevention Program is very good.

Effectiveness of Policies and Procedures

Lake Forest College has implemented appropriate policies and procedures to comply with 16 CFR Part 681 (Identity Theft Red Flags) to address the risk of identity theft in connection with the opening of covered accounts and with respect to existing covered account.

See Identity Theft Prevention Program provided separately.

Service Provider Arrangements

1. New service providers
   a.

2. Changes in vendor management processes, procedures, or requirements
   a.

Significant Incidents Involving Identity Theft and Management Response

1. Any significant incidents involving identity theft this year and action taken
   a.

2. Any service provider significant incidents involving identity theft this year and action taken
   a.

Recommendations for Changes in the Identity Theft Prevention Program

1. Additions to the Identity Theft Prevention Program
   a.

2. Deletions from the Identity Theft Prevention Program
   a.
5.3 Regulations
Federal Trade Commission
16 CFR Part 681

Authority and Issuance
For the reasons discussed in the joint preamble, the Commission is adding part 681 of title 16 of the Code of Federal Regulations as follows:

PART 681—IDENTITY THEFT RULES Sec. 681.1 Duties of users of consumer reports regarding address discrepancies.

681.2 Duties regarding the detection, prevention, and mitigation of identity theft.

681.3 Duties of card issuers regarding changes of address.

Appendix A to Part 681—Interagency Guidelines on Identity Theft Detection, Prevention, and Mitigation


§ 681.1 Duties of users regarding address discrepancies.

(a) Scope. This section applies to users of consumer reports that are subject to administrative enforcement of the FCRA by the Federal Trade Commission pursuant to 15 U.S.C. 1681a(a)(1) (users).

(b) Definition. For purposes of this section, a notice of address discrepancy means a notice sent to a user by a consumer reporting agency pursuant to 15 U.S.C. 1681c(h)(1), that informs the user of a substantial difference between the address for the consumer that the user provided to request the consumer report and the address(es) in the agency’s file for the consumer.

(c) Reasonable belief.

(1) Requirement to form a reasonable belief. A user must develop and implement reasonable policies and procedures designed to enable the user to form a reasonable belief that a consumer report relates to the consumer about whom it has requested the report, when the user receives a notice of address discrepancy.

(2) Examples of reasonable policies and procedures. (i) Comparing the information in the consumer report provided by the consumer reporting agency with information the user: (A) Obtains and uses to verify the address of the consumer; (B) Informs the consumer about whom it has reasonably confirmed is accurate to the consumer reporting agency from which the notice of address discrepancy relating to the consumer was obtained.

(3) Examples of confirmation methods. The user may reasonably confirm an address is accurate by:

(ii) Verifying the address with the consumer about whom it has requested the report;

(iii) Verifying the address through third-party sources;

(iv) Using other reasonable means.

(4) Timing. The policies and procedures developed in accordance with paragraph (d)(1) of this section must provide that the user will furnish the consumer’s address that the user has reasonably confirmed is accurate to the consumer reporting agency as part of the information it regularly furnishes for the reporting period in which it establishes a relationship with the consumer.

§ 681.2 Duties regarding the detection, prevention, and mitigation of identity theft.

(a) Scope. This section applies to financial institutions and creditors that are subject to administrative enforcement of the FCRA by the Federal Trade Commission pursuant to 15 U.S.C. 1681a(a)(1).

(b) Definitions. For purposes of this section, and Appendix A, the following definitions apply:

(1) Account means 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. Account includes:

(i) An extension of credit, such as the purchase of property or services involving a deferred payment; and

(ii) A deposit account.

(2) The term board of directors includes:

(i) In the case of a branch or agency of a foreign bank, the managing official in charge of the branch or agency; and

(ii) In the case of any other creditor that does not have a board of directors, a designated employee at the level of senior management.

(3) Covered account means:

(i) 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, such as a credit card account, mortgage loan, automobile loan, margin account, cell phone account, utility account, checking account, or savings account; and

(ii) 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.

(4) Credit has the same meaning as in 15 U.S.C. 1681a(r)(5).

(5) Creditor has the same meaning as in 15 U.S.C. 1681a(r)(5), and includes lenders such as banks, finance companies, automobile dealers, mortgage brokers, utility companies, and telecommunications companies.

(6) Customer means a person that has a covered account with a financial institution or creditor.

(7) Financial institution has the same meaning as in 15 U.S.C. 1681a(t).

(8) Identity theft has the same meaning as in 16 CFR 603.2(a).

(9) Red Flag means a pattern, practice, or specific activity that indicates the possible existence of identity theft.

(10) Service provider means a person that provides a service directly to the financial institution or creditor.

(c) Periodic Identification of Covered Accounts. Each financial institution or creditor must periodically determine whether it offers or maintains covered accounts. As a part of this determination, a financial institution or creditor must conduct a risk assessment to determine whether it offers or maintains covered accounts described in paragraph (b)(3)(ii) of this section, taking into consideration:

(1) The methods it provides to open its accounts;

(2) The methods it provides to access its accounts; and

(3) Its previous experiences with identity theft.

(d) Establishment of an Identity Theft Prevention Program. (1) Program requirement. Each financial institution or creditor that offers or maintains one or more covered accounts must develop
and implement a written Identity Theft Prevention Program (Program) that is
designed to detect, prevent, and mitigate identity theft in connection with the
opening of a covered account or any existing covered account. The Program
must be appropriate to the size and complexity of the financial institution or
creditor and the nature and scope of its activities.

(2) Elements of the Program. The
Program must include reasonable policies and procedures to:

(i) Identify relevant Red Flags for the
covered accounts that the financial institution or creditor offers or
maintains, and incorporate those Red Flags into its Program;
(ii) Detect Red Flags that have been
incorporated into the Program of the financial institution or creditor;
(iii) Respond appropriately to any Red
Flags that have been detected pursuant to paragraph (d)(2)(ii) of this section to
prevent and mitigate identity theft; and
(iv) Ensure the Program (including the
Red Flags determined to be relevant) is updated periodically, to reflect changes
in risks to customers and to the safety and soundness of the financial
institution or creditor from identity theft.

(e) Administration of the Program.
Each financial institution or creditor
that is required to implement a Program must provide for the continued
administration of the Program and must:

(1) Obtain approval of the initial
written Program from either its board of
directors or an appropriate committee of
the board of directors;
(2) Involve the board of directors, an
appropriate committee thereof, or a
designated employee at the level of
senior management in the oversight,
development, implementation and
administration of the Program;
(3) Train staff, as necessary, to
effectively implement the Program; and
(4) Exercise appropriate and effective
oversight of service provider
arrangements.

(f) Guidelines. Each financial
institution or creditor that is required to implement a Program must consider the
guidelines in Appendix A of this part and include in its Program those
guidelines that are appropriate.

§ 681.3 Duties of card issuers regarding
changes of address.

(a) Scope. This section applies to a
person described in § 681.2(a) that
issues a debit or credit card (card
issuer).

(b) Definitions. For purposes of this
section:

(1) Cardholder means a consumer
who has been issued a debit or debit
account.
(2) Clear and conspicuous means
reasonably understandable and
designed to call attention to the nature
and significance of the information
prented

(c) Address validation requirements. A
card issuer must establish and
implement reasonable policies and
procedures to assess the validity of a
change of address if it receives
notification of a change of address for a
consumer’s debit or credit card account
and, within a short period of time
afterwards (during at least the first 30
days after it receives such notification),
the card issuer receives a request for an
additional or replacement card for the
same account. Under these
circumstances, the card issuer may not
issue an additional or replacement card,
until, in accordance with its
reasonable policies and procedures and for
the purpose of assessing the validity of the
change of address, the card issuer:

(1)(i) Verifies the cardholder’s
address,
or

(1)(ii) Provides to the cardholder a
reasonable means of promptly reporting
an incorrect address change; or

(2) Otherwise assesses the validity of
the change of address in accordance
with the policies and procedures the
card issuer has established pursuant to
§ 681.2 of this part.

(d) Alternative timing of address
validation. A card issuer may satisfy
the requirements of paragraph (c) of this
section if it validates an address
pursuant to the methods in paragraph
(c)(1) or (c)(2) of this section when it
receives an address change notification,
before it receives a request for an
additional or replacement card.

(e) Form of notice. Any written or
electronic notice that the card issuer
provides under this paragraph must be
clear and conspicuous and provided
separately from its regular correspondence with
the cardholder.

Appendix A to Part 681—Interagency
Guidelines on Identity Theft Detection,
Prevention, and Mitigation

Section 681.2 of this part requires each
financial institution and creditor that offers or
maintains one or more covered accounts, as
defined in § 681.2(b)(3) of this part, 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.
These guidelines are intended to assist
financial institutions and creditors in the
formulation and maintenance of a Program
that satisfies the requirements of § 681.2 of
this part.

I. The Program

In designing its Program, a financial
institution or creditor may incorporate, as
appropriate, its existing policies, procedures,
and other arrangements that control
reasonably foreseeable risks to customers or
to the safety and soundness of the financial
institution or creditor from identity theft.

II. Identifying Relevant Red Flags

(a) Risk Factors. A financial institution or
creditor should consider the following factors
in identifying relevant Red Flags for covered
accounts, as appropriate:

(1) Types of covered accounts it offers
or maintains;

(2) The methods it provides to open its
covered accounts;

(3) The methods it provides to access its
covered accounts; and

(4) Its previous experiences with identity
theft.

(b) Sources of Red Flags. Financial
institutions and creditors should incorporate
relevant Red Flags from sources such as:

(1) Incidents of identity theft that the
financial institution or creditor has
experienced;

(2) Methods of identity theft that the
financial institution or creditor has identified
that reflect changes in identity theft risks;

(3) Applicable supervisory guidance;

(c) Categories of Red Flags. The Program
should include relevant Red Flags from the
following categories, as appropriate.

Examples of Red Flags from each of these
categories are appended as Supplement A to
this Appendix A.

(1) Alerts, notifications, or other warnings
received from consumer reporting agencies
or service providers, such as fraud detection
services;

(2) The presentation of suspicious
documents;

(3) The presentation of suspicious personal
identifying information, such as a suspicious
address change;

(4) The unusual use of, or other suspicious
activity related to, a covered account; and

(5) Notice from customers, victims of
identity theft, law enforcement authorities, or
other persons regarding possible identity
theft in connection with covered accounts
held by the financial institution or creditor.

III. Detecting Red Flags

The Program’s policies and procedures
should address the detection of Red Flags in
connection with the opening of covered
accounts and existing covered accounts, such as by:

(a) Obtaining identifying information
about, and verifying the identity of, a person
opening a covered account, for example,
using the policies and procedures regarding
identification and verification set forth in the
Customer Identification Program rules
implementing 31 U.S.C. 5318(l) (31 CFR
103.121); and

(b) Authenticating customers, monitoring
transactions, and verifying the validity of
change of address requests, in the case of
existing covered accounts.

IV. Preventing and Mitigating Identity Theft

The Program’s policies and procedures
should provide for appropriate responses to the
Red Flags the financial institution or
creditor has detected that are commensurate
with the degree of risk posed. In determining
an appropriate response, a financial
institution or creditor should consider
aggravating factors that may heighten the risk
of identity theft, such as a data security
incident that results in unauthorized access
to a customer’s account records held by the financial institution, creditor, or third party, or notice that a customer has provided information related to a covered account held by the financial institution or creditor to someone fraudulently claiming to represent the financial institution or creditor or to a fraudulent website. Appropriate responses may include the following:

(a) Monitoring a covered account for evidence of identity theft;
(b) Contacting the customer;
(c) Changing any passwords, security codes, or other security devices that permit access to a covered account;
(d) Reopening a covered account with a new account number;
(e) Not opening a new covered account;
(f) Closing an existing covered account;
(g) Not attempting to collect on a covered account or not selling a covered account to a debt collector;
(h) Notifying law enforcement; or
(i) Determining that no response is warranted under the particular policies and procedures of the financial institution or creditor 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 recommendations for material changes to the Program.

(c) Oversight of service provider arrangements. Whenever a financial institution or creditor engages a service provider to perform an activity in connection with one or more covered accounts the financial institution or creditor should 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, a financial institution or creditor could require the service provider by contract to have policies from the following illustrative examples in connection with covered accounts:

1. A fraud or active duty alert is included with a consumer report.
2. A consumer reporting agency provides a notice of credit freeze in response to a request for a consumer report.
3. A consumer reporting agency provides a notice of address discrepancy, as defined in § 681.1(b) of this part.
4. A consumer report indicates a pattern of activity that is inconsistent with the history and usual pattern of activity of an applicant or customer, such as:
   a. A recent and significant increase in the volume of inquiries;
   b. An unusual number of recently established credit relationships;
   c. A material change in the use of credit, especially with respect to recently established credit relationships; or
   d. An account that was closed for cause or identified for abuse of account privileges by a financial institution or creditor.

5. Documents provided for identification appear to have been altered or forged.
6. The photograph or physical description on the identification is not consistent with the appearance of the applicant or customer presenting the identification.
7. Other information on the identification is not consistent with information provided by the person opening a new covered account or customer presenting the identification.
8. 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.
9. An application appears to have been altered or forged, or gives the appearance of having been destroyed and reassembled.

Suspicious Personal Identifying Information
10. Personal identifying information provided is inconsistent when compared against external information sources used by the financial institution or creditor. For example:

   a. The address on an application is the same as the address provided on a fraudulent application; or
   b. The phone number on an application is the same as the number provided on a fraudulent application.

   a. The address on an application is fictitious, a mail drop, or a prison; or
   b. The phone number is invalid, or is
associated with a pager or answering service.
14. The SSN provided is the same as that submitted by other persons opening an account or other customers.
15. 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.
16. 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.
17. Personal identifying information provided is not consistent with personal identifying information that is on file with the financial institution or creditor.
18. 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.

**Unusual Use of, or Suspicious Activity Related to, the Covered Account**
19. Shortly following the notice of a change of address for a covered account, the institution or creditor receives a request for a new, additional, or replacement card or a cell phone, or for the addition of authorized users on the account.
20. 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., electronics equipment or jewelry); or
   b. The customer fails to make the first payment or makes an initial payment but no subsequent payments.
21. 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. Nonpayment 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.
22. 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).
23. Mail sent to the customer is returned repeatedly as undeliverable although transactions continue to be conducted in connection with the customer’s covered account.
24. The financial institution or creditor is notified that the customer is not receiving paper account statements.
25. 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 Held by the Financial Institution or Creditor**
26. 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.