Lincoln Financial Group

FTC/SEC Red Flags
Identity Theft Prevention Program

Program Summary
## Table of Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>The Red Flags Rule</td>
<td>3</td>
</tr>
<tr>
<td>Key Points of the Program</td>
<td>4</td>
</tr>
<tr>
<td>Covered Accounts</td>
<td>5</td>
</tr>
<tr>
<td>Identifying Red Flags</td>
<td>7</td>
</tr>
<tr>
<td>Red Flags Detection Methods and Response Procedures</td>
<td>7</td>
</tr>
<tr>
<td>Preventing and Mitigating Identity Theft</td>
<td>7</td>
</tr>
<tr>
<td>Updating the Identity Theft Prevention Program</td>
<td>8</td>
</tr>
<tr>
<td>Administering the Identity Theft Prevention Program</td>
<td>8</td>
</tr>
<tr>
<td>Complying with the Program</td>
<td>8</td>
</tr>
<tr>
<td>Program Controls</td>
<td>9</td>
</tr>
<tr>
<td>Summary</td>
<td>10</td>
</tr>
</tbody>
</table>
The Red Flags Rule

Lincoln Financial Group (“LFG”) has developed an Identity Theft Prevention Program, in response to the Red Flags Rules of the Federal Trade Commission (“FTC”) and the Securities and Exchange Commission (“SEC”), as outlined below. The program is designed to detect, prevent, and mitigate identity theft in connection with the opening of covered accounts or any existing covered account.

Introduction

The FTC has issued Identity Theft Red Flag Rules that are effective May 1, 2009, with an enforcement date of December 31, 2010. The FTC, along with the Federal Banking agencies, issued the Rules under the Fair and Accurate Credit Transactions Act of 2003 (the “FACT Act”). The FTC Rules require financial institutions and creditors to establish reasonable policies and procedures implementing the agencies’ identity theft guidelines and identifying possible risks to the covered accounts of customers. The regulations implement Section 114 and Section 315 of the FACT Act.

As of July 21, 2011, the Dodd-Frank Wall Street Reform and Consumer Protection Act transferred responsibility for joint rulemaking and enforcement of identity theft red flag guidelines and regulations from the FTC to the SEC for those subject to SEC jurisdiction. The new Regulation S-ID, at 17 C.F.R. part 248, became effective on May 20, 2013, and compliance with these regulations will be required as of November 20, 2013. The new regulations require broker-dealers, investment advisers, investment companies, and other entities subject to the SEC’s enforcement authority to establish programs to address identity theft risks.

References to “the Rules” or “Red Flags Rules” throughout this document will refer to both the FTC and SEC Rules.

Section 114 – Red Flag Regulations and Guidelines

Section 114 of the FACT Act issues guidelines for financial institutions and creditors regarding identity theft with respect to customers. It requires financial institutions and creditors to establish reasonable policies and procedures for implementing the guidelines and identifying possible risk to customers.

The “Red Flags Rule,” was adopted under these regulations and requires the development, implementation, and maintenance of an Identity Theft Prevention Program by covered companies that hold customer accounts.

“Red Flags” are patterns, practices, or specific activities that indicate the possible existence of identity theft in connection with a ‘covered’ account.

A “Covered Account” is an account maintained primarily for personal, family, or household purposes that involves or is designed to permit multiple payments or transactions; or, any other account, including a business account that poses a reasonably foreseeable risk to clients or the safety and soundness of the creditor from identity theft, including financial, operational, compliance, reputation or litigation risks.

Section 315 – Duties of Users Regarding Address Discrepancies

Section 315 of the FACT Act provides guidance regarding reasonable policies and procedures that a user of a consumer report should employ when the user receives a notice of address discrepancy.
The following business areas within LFG must have procedures to comply with Section 315:

- Producer Solutions (for consumer reports requested as part of the contracting and appointment process of a new producer of the LFG life insurance companies)
- Registration (for consumer reports requested as part of the registration process for new registered representatives of the LFG broker-dealers)
- Human Resources (for consumer reports during the hiring process of a new LFG employee)
- Underwriting (for consumer reports requested on higher risk prospective insureds under a LFG life insurance policy)

Each business area must document a reasonable policy and procedure for the handling of address discrepancies and communicate to the appropriate team members within their area. Sample language to be incorporated into these procedures include, but are not limited to, the following:

- Verifying the address with the person to whom the consumer report pertains;
- Reviewing records to ensure the correct address was provided;
- Verifying the address through third party sources; or
- Using other reasonable means.

If a business area has reasonably confirmed a consumer’s address is accurate, the business area must report the correct address to the consumer reporting agency from which it received the notice of address discrepancy when:

- It can form a reasonable belief that the consumer report relates to the consumer about whom the user requested the report;
- It has established a continuing relationship with the consumer; and
- It regularly and in the ordinary course of business furnishes information to the consumer reporting agency from which the notice of address discrepancy relating to the consumer was obtained.

These Section 114 and 315 requirements have a mandatory compliance date of May 1, 2009, with an enforcement date of December 31, 2010.

The four general elements that the program must contain are “reasonable policies and procedures” to:

- Identify and incorporate Red Flags for covered accounts.
- Detect Red Flags that are included in the Program.
- Respond to those Red Flags appropriately.
- Update the Program periodically to reflect the risk to the customer of identity theft or to the safety of the financial institution or creditor in handling and safeguarding customer information to prevent identity theft

**Key Points of the Program**

- The mandatory compliance effective date was May 1, 2009, with an enforcement date of December 31, 2010.
- The requirement of a written, board-approved (or a committee of the board) Identity Theft Prevention Program. Board Approval of the initial program occurred on June 3, 2009.
• Existing policies and practices were leveraged to satisfy requirements including those related to:
  o Customer Identification Programs (“CIP”)
  o Data protection
  o Fraud protection
  o Privacy
• Staff are to be trained, as necessary, to effectively implement the Program.
• The Program will be reviewed at least annually, or when significant changes occur within the company, and updated as appropriate.
• The Rules provide for review of reports prepared, when significant changes within the company occur, or at least annually, by staff regarding compliance with the regulations. The reports must be made to the Board of Directors, an appropriate committee of the Board, a designated employee at the level of senior management, or at the company’s discretion, to the individual who is responsible for the aspects of the Program.

**Affiliates**
This program covers certain accounts of certain affiliated companies of LFG. Each impacted affiliate and type of account is listed in the Covered Accounts section below. Each affiliate has created and implemented its own program specific to their business model.

**Designated Supervisor**
Kenneth J. Elder  
Assistant Vice President  
AML Officer  
AML, Fraud and Investigations  
Lincoln Financial Group  
Office: (336-691-3116)

Email: kenneth.elder@lfg.com

**Covered Accounts**
Identified covered accounts held by LFG are as follows:

• Lincoln Financial Advisors Corporation (“LFA”) & Lincoln Financial Securities Corporation (“LFS”):
  o Brokerage accounts with the following services:
    ▪ Margin accounts
    ▪ Debit cards
    ▪ Checkwriting
    ▪ Wire transfers to third parties
  o Investment advisory accounts
• Lincoln Financial Group Trust Company, Inc. (“LFGTC”):
  o Individual Retirement Accounts (“IRA”)
  o Retained asset accounts
  o Deferred fixed, indexed and variable annuities
• Lincoln Financial Investment Services Corporation (“LFISC”):
  o Deferred variable annuities
The following LFG affiliates are entities that are subject to the Rules but do not have any covered accounts as defined by the Rules because they do not have individual customers:

- Lincoln Investment Management Company: Investment advisor
- Lincoln Variable Insurance Products Trust: Investment company and advisor
- Lincoln Advisors Trust: Investment company and advisor
- Lincoln Financial Distributors, Inc.: Broker/Dealer
- Lincoln Investment Advisors Corporation: Investment advisor

Some examples of identity theft methods that could be used on brokerage accounts:

- Fraudulent applications for accounts
- Fraudulent withdrawals from accounts
- Fraudulent use of debit card numbers
- Fraudulent creation of debit cards
- Fraudulent change of address requests
- Fraudulent requests for new access after requesting change of address
- Counterfeit checks
- Other use of individuals’ identifying information by telephone, mail or web site
- Computer intrusion

Some examples of identity theft methods that could be used on LFGTC IRA accounts:

- Fraudulent applications for accounts
- Fraudulent withdrawals from accounts
- Fraudulent change of address requests
- Other use of individuals’ identifying information by telephone, mail or website
- Computer intrusion

Some examples of identity theft methods that could be used on retained asset accounts:

- Fraudulent death claims, partial surrenders or surrenders against the account
- Fraudulent withdrawals or partial withdrawals from accounts
- Fraudulent change of address requests
- Fraudulent requests for new access after requesting change of address
- Counterfeit checks
- Other use of individuals’ identifying information by telephone, mail or website
- Computer intrusion

Some examples of identity theft methods that could be used on deferred annuities:

- Fraudulent application for accounts
- Fraudulent death claims, partial surrenders or surrenders against the account
- Fraudulent withdrawals or partial withdrawals from accounts
- Fraudulent change of address requests
- Fraudulent requests for new access after requesting change of address
- Other use of individuals’ identifying information by telephone, mail or website
- Computer intrusion
Identifying Red Flags

Risk Factors
When identifying which red flags are relevant, LFG will consider the following, as appropriate:

- The types of covered account offered or maintained
- The process LFG uses to open covered accounts
- The process LFG uses to access covered accounts
- Previous experiences with identity theft

Sources of Red Flags
Relevant Red Flags will be incorporated from such sources as:

- Incidents of identity theft the company has experienced
- Methods of identity theft that LFG has identified that reflect changes in identity theft risks
- Applicable supervisory guidance

Categories of Red Flags
Federal guidelines state that the program must contain policies and procedures to detect red flags a company has identified as relevant to its covered accounts. The final regulations require that a financial institution’s program should include relevant red flags from five specific categories, as appropriate to the nature of the business. The five categories are:

- Alerts, notifications, or other warnings received from consumer reporting agencies or service providers, such as fraud detection services
- The presence of suspicious documents
- The receipt of suspicious personal identification information, such as a suspicious address change
- The unusual use of, or other suspicious activity related to, a covered account
- Notices from customers, victims of identity theft, law enforcement authorities, or other persons regarding possible identity theft in connection with covered accounts held by LFG

Red Flags Detection Methods and Response Procedures
LFG has identified Red Flags for each covered account type and implemented appropriate detection methods and response procedures.

LFG has reviewed applicable system features and functionality, as well as policies, procedures and business practices, to determine appropriate responses to the 26 red flags outlined in the FACT Act. Additional Red Flags were also developed by LFG.

See Red Flag Rules spreadsheets for each identified affiliate and covered account.

Preventing and Mitigating Identity Theft
LFG’s Identity Theft Prevention Program policies and procedures provide for appropriate responses to the Red Flags that the company has detected and are in line with the degree of risk posed.

In determining an appropriate response, LFG will consider factors that may heighten the risk of identity theft.
Updating the Identity Theft Prevention Program

The Rules recognizes that new red flags may emerge as technology changes or identity thieves change their tactics. As a result, the program requires periodic updates to ensure it is current with identity theft risks. We must factor in our experiences with identity theft, changes in how identity thieves operate, new methods to detect, prevent and mitigate identity theft, changes in the accounts we offer and changes in our business, such as mergers, acquisitions, alliances, joint ventures, arrangement with service providers, etc.

At a minimum, a calendar year-end review of the Identity Theft Prevention Program will be performed annually. Review of the program will also occur when significant changes occur within the company.

Administering the Identity Theft Prevention Program

Oversight
LFG’s Audit Committee of the Board of Directors is responsible for the initial approval of the program. LFG has designated the Corporate AML Officer to have overall responsibility and supervision for the Identity Theft Prevention Program. Supervision of the Program includes:

- Assigning specific responsibility to ensure the Program's implementation.
- Reviewing annual reports or reports created when significant changes occur within the company, regarding compliance by LFG to the program.
- Approving material changes to the program, as necessary, to address new identity theft risks.

Reporting
LFG’s Corporate AML Officer is responsible for the development, implementation, and administration of the Program. The Rule provides for review of reports prepared when significant changes within the company occur, or at least annually by staff regarding compliance with the regulations. The reports must be made to the Board of Directors, an appropriate committee of the Board, a designated employee at the level of senior management, or at the company’s discretion, to the individual who is responsible for the aspects of the Program. The reports will address material matters related to the Program and evaluate applicable issues.

Training
The Red Flag Regulation guidelines require that companies train staff “as necessary” to implement an effective Identity Theft Prevention Program. Relevant LFG staff is required to complete annual fraud prevention training, privacy training and AML training.

Complying with the Program

New Accounts
When verifying the identity of the person who is opening a new account, reasonable procedures include getting a name, address and identification number, and for in-person verification, checking a current government-issued identification card like a driver’s license or passport. Depending on the circumstances, we may want to compare the information with the information found from other sources such as a credit reporting company, SSN Death Master file or publicly available information.
**Existing Accounts**

To detect red flags on existing accounts, we need to include reasonable procedures to authenticate customers, monitor transactions, and verify the validity of change-of-address requests.

Using programs already in place to monitor transactions (such as ProSurv for LFA & LFS) will help to identify behavior that indicates the possibility of fraud and identity theft, or validate a change of address.

**Preventing and Mitigating Identity Theft**

When a red flag is identified, LFG must respond appropriately. The response will depend on the degree of risk posed.

Some examples of appropriate responses may include:

- Monitoring a covered account for evidence of identity theft
- Contacting the customer
- Changing passwords, security codes, or other ways to access a covered account
- Closing an existing account
- Reopening an account with a new account number
- Not opening a new account
- Not trying to collect on an account
- Notifying law enforcement
- Determining that no response is warranted under the identified circumstance

Depending on the incident, one or several responses (options above or another response altogether) may be appropriate. When determining the response, consider whether any aggravating factors might heighten the risk of identity theft.

**Program Controls**

LFG has a number of program controls in place to support the LFG Identity Theft Prevention Program. The program-level controls, in conjunction with specific business unit controls, provide a strong foundation for the protection of customer information and LFG’s Program. Examples of these current program controls are as follows:

**Anti-Money Laundering:** AML, Fraud & Investigations has a dedicated AML Unit for the LFG enterprise.

**Clearing Firms:** LFA & LFS have relationships with two Clearing Firms that have implemented Identity Theft Prevention programs. LFA & LFS will respond appropriately if notified by the Clearing Firm of an identified red flag.

**Compliance Manual:** Appropriate Compliance Manuals should be updated to reflect the adoption of the Program.

**Fraud Prevention:** AML, Fraud & Investigations has dedicated Fraud Prevention and Special Investigation Units.

**Information Handling Policy:** The protection of nonpublic personal information is imperative when conducting business with LFG. The Information Handling Policy is presented to all LFG new hires, and is available to all employees on company websites. The Information Handling Policy is also incorporated into our annual privacy training.
Information Security Policies and Procedures: LFG employees are required to follow the corporate Information Security Policy.

Information Security Program: LFG has a strong Information Security program with processes in place that help facilitate the security of LFG and customer data.

Investment Services - Processing: The Investment Services – Processing Units within LFA & LFS have controls and processes in place in response to their responsibilities with regards to account maintenance, management, and data integrity.

Privacy: The Corporate Privacy Office is a dedicated privacy unit for the LFG enterprise.

Broker Dealer Surveillance Tool: LFA & LFS use a computerized surveillance tool, which provides an additional layer of controls for online transactions.

Red Flags Policies and Procedures: All departments impacted by the Red Flag Rules have updated appropriate policies and procedures.

Red Flags Written Supervisory Procedures: All departments impacted by the Red Flag Rules have updated appropriate Written Supervisory Procedures.

Retained Asset Accounts: LFG’s Retained Asset Accounts are held at The Northern Trust Company, which has established an Identity Theft Prevention Program to detect, prevent and mitigate identity theft in connection with the opening of accounts or the processing of transactions through existing accounts.

Summary
LFG has created a detailed written Identity Theft Prevention Program, which was effective May 1, 2009, with an enforcement date of December 31, 2010.

In conclusion, LFG has undertaken the effort to both comply with the requirements of the law in a timely manner and develop a comprehensive Program. LFG will continually review and enhance the program to help ensure the protection of our customers’ information as new challenges and opportunities arise.
<table>
<thead>
<tr>
<th>Date</th>
<th>Version</th>
<th>Revision</th>
</tr>
</thead>
<tbody>
<tr>
<td>June 3, 2009</td>
<td>1.0</td>
<td>Initial program approved by board. Business owner Paula Mango and Carolyn White</td>
</tr>
<tr>
<td>December, 2011</td>
<td>2.0</td>
<td>Updated by Carolyn White</td>
</tr>
<tr>
<td>February, 2012</td>
<td>3.0</td>
<td>Updated to reflect Ken Elder as designated supervisor and ECE name change.</td>
</tr>
<tr>
<td>November, 2012</td>
<td>4.0</td>
<td>Updated typo’s and Kens email and phone#</td>
</tr>
<tr>
<td>April 4, 2013</td>
<td>5.0</td>
<td>Updated Business Unit name and replaced old docs in the intranet</td>
</tr>
<tr>
<td>July 18, 2013</td>
<td>6.0</td>
<td>Added LFGTC</td>
</tr>
<tr>
<td>September 9, 2013</td>
<td>7.0</td>
<td>Added updates to reflect new SEC rules, added further explanation of Section 315 requirements, added deferred annuities and investment advisory accounts as covered accounts, identified affiliates excluded from program, and merged “Complying with the Program” document into main program document.</td>
</tr>
<tr>
<td>November 6, 2013</td>
<td>8.0</td>
<td>Changed title of document to FTC SEC Red Flags Program</td>
</tr>
</tbody>
</table>