

# LENDERS COMPLIANCE GROUP

*"Converting Risk to Opportunity"*

## ADVISORY BULLETIN

November 29, 2007

### Identity Theft Prevention Program: "Red Flags Rule"

**EFFECTIVE DATE:** January 1, 2008

**MANDATORY COMPLIANCE:** November 1, 2008

#### **BACKGROUND**

The Fair Credit Reporting Act ("FCRA"), as amended by the Fair and Accurate Credit Transactions Act of 2003 ("FACTA"), requires certain procedures to prevent identity theft. On November 9, 2007, the Interagency Final Regulation and Guidelines (hereinafter, "Guidelines") were issued by the Federal Trade Commission (FTC), Office of the Comptroller of the Currency (OCC), the Board of Governors of the Federal Reserve System (Board), the Federal Deposit Insurance Corporation (FDIC), the Office of Thrift Supervision (OTS), and the National Credit Union Administration (NCUA) (collectively, the "Agencies").<sup>1</sup> Consequently, the Guidelines must be implemented by both creditors and financial institutions, such as banks and their subsidiaries, bank holding companies and their non-blank subsidiaries, savings associations and their subsidiaries, savings and loan associations and their subsidiaries, and credit unions.

The regulation and guidelines are intended to assist creditors and financial institutions in implementing Sections 114 and 315 of FACTA,<sup>2</sup> requiring the implementation of a written Identity Theft Prevention Program (the "Program"), including the "Red Flags" determined to be relevant, and also the methods to verify address discrepancies indicated by a consumer reporting agency.<sup>3</sup> Red Flags are patterns, practices, or specific activities that indicate the possible existence of identity theft. The Program should be updated periodically to reflect changes in risks to customers and to the Safety and Soundness standards of the financial institution or creditor from identity theft.

#### **Action Plan: Identity Theft Prevention Program**

Ratify and enforce a written Program that contains the core determinants of the Guidelines, which set forth certain procedures that would satisfy the requirements of the regulations to detect, prevent, and mitigate identity theft. The Program requires on-going administrative responsibility and the approval by the Board of Directors. There are numerous aspects to a comprehensive policy and procedure matrix; however, the Program should consist of certain salient features. The following provides a brief outline of an Identity Theft Prevention Program.

- **Program Requirements.** The Program must consist of at least four (4) elements:
  1. Identify relevant Red Flags for covered accounts and incorporate those Red Flags into the Program.<sup>4</sup>
  2. Detect Red Flags that have been incorporated into the Program.
  3. Respond appropriately to any Red Flags that are detected to prevent and mitigate identity theft.
  4. Ensure the Program is updated periodically, to reflect changes in risks to customers or to the safety and soundness of the financial institution or creditor from identity theft.
  
- **Red Flags.** Appendix J of the Guidelines includes an outline of the Program, consisting of the risk factors, sources, and categories of relevant Red Flags, procedures for Red Flag detection and identity theft prevention, and the periodic updates to and administration of those procedures.<sup>5</sup> An institution's Program should provide procedures to respond to the following Red Flag instances:
  - Alerts, Notifications, or Warnings from a Consumer Reporting Agency
  - Suspicious Documents
  - Suspicious Personal Identifying Information
  - Unusual use of, or 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 the Financial Institution or Creditor
  
- **Risk Assessment.** A risk assessment should be undertaken to evaluate an institution's or creditor's exposure to identity theft. Any such analysis must contain the following review criteria:
  - The types of covered accounts it offers or maintains<sup>6</sup>
  - The methods it provides to open its covered accounts
  - The methods it provides to access its covered accounts
  - Its previous experience with identity theft
  
- **Customer Information Program (CIP).**<sup>7</sup> The Guidelines specify that procedures be implemented to assure that a consumer's identity is verified in accordance with CIP rules.
  
- **Address Discrepancies.** An institution or creditor that receives a notice of address discrepancy from a consumer reporting agency must implement Program procedures to enable it to form a "reasonable belief" that a consumer report relates to the consumer about whom it has requested the report.<sup>8</sup>
  
- **Consumer's Address.** Reasonable policies and procedures must be developed for furnishing to a consumer reporting agency an address for the consumer that is reasonably confirmed to be accurate.
  
- **Third Party Arrangements.** Service provider arrangements must be implemented by Service Level Agreements and proper oversight regimes that confirm and carry out the proper handling of third party risk management requirements of an institution's or creditor's Information Security program.

## Administration

The Identity Theft Prevention Program should be established and maintained by means of the following methodologies:<sup>9</sup>

- A. Obtain the approval of the initial written Program from either the Board of Directors or an appropriate committee of the Board of Directors.
- B. 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.
- C. Train staff, as necessary, to effectively implement the Program.
- D. Exercise appropriate and effective oversight of service provider arrangements.

### **Lenders Compliance Group, Inc.**

167 West Hudson Street – Suite 200  
Long Beach, NY 11561  
(516) 442-3456

### ***“Converting Risk to Opportunity”***

<sup>1</sup> FR: Vol. 72, No. 217, 63718 – November 9, 2007 (“Rules and Regulations”) Citations for each Agency, see OCC: 12 CFR Part 41; FRS: 12 CFR Part 222; FDIC: 12 CFR Parts 334 and 364; OTS: 12 CFR 571; NCUA: 12 CFR Part 717; and, FTC: 16 CFR Part 681.

<sup>2</sup> See FACTA, Section 1(b), Title I – “Identity Theft Prevention and Credit History Restoration”, Subtitle A, Sec 114: “Establishment of Procedures for the identification of possible instances of identity theft;” and, Title III – “Enhancing the Accuracy of Consumer Report Information,” Sec 315: “Reconciling Addresses.”

<sup>3</sup> FIL-100-2007 – November 15, 2007 (FDIC)

<sup>4</sup> The term “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, check 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 the safety and soundness of the financial institution or creditor from identity theft, including financial, operational, compliance, reputation, or litigation risks. [72 FR 217: 63757, Inter Alia]

<sup>5</sup> FR: Vol. 72, No. 217, 63754: “Appendix J to Part 41 – “Interagency Guidelines on Identity Theft Protection, Prevention, and Mitigation” [See: 12 CFR, Chapter I, Part 41 (“Fair Credit Reporting”), Inter Alia] All Agencies have adopted this two-part definition. Examples of Red Flags can be found in Supplement A of Appendix J. [Ibid. 63755-63756]

<sup>6</sup> The Guidelines have kept the term “account” from Section 114. The term “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.” [Ibid.] Therefore, the Program must include not only personal but also small business relationships.

<sup>7</sup> 31 U.S.C. 5318(l) [31 CFR 103.121]

<sup>8</sup> Pursuant to 15 U.S.C. 1681c(h)(1). Address Discrepancy is a Red Flag. [Supplement A/Appendix J]

<sup>9</sup> FR: Vol. 72, No. 217, 63758, Inter Alia

Published: November 29, 2007

© **Lenders Compliance Group, Inc.** 2007. All Rights Reserved. **Lenders Compliance Group** is a full service risk management firm, providing professional guidance to financial institutions in all areas of regulatory compliance related to the mortgage and lending industry. Information contained herein is not intended to be and is not a source of legal advice. [Website: [www.lenderscompliancegroup.com](http://www.lenderscompliancegroup.com)]