



American  
Bankers  
Association®

ABAWorks  
on Fraud

# Identity Theft Red Flag Regulation

An ABA Members-Only Publication



Identity Theft  
ALERT

A 3D-rendered red flag on a black pole, positioned over a blurred background of a document with a grid pattern. The flag is slightly curved and has a white border. The text 'Identity Theft' is in a smaller font above the larger, bold word 'ALERT'.

## ABAWorks on Fraud: Identity Theft Red Flag Regulation

On December 4, 2003, the President signed the Fair and Accurate Credit Transaction Act (“FACT Act”) to amend the Fair Credit Reporting Act (“FCRA”). FCRA generally addresses consumer reports and the FACT Act addressed various issues related to consumer reports, but Congress also saw the need and opportunity to address the growing problem of identity theft. Accordingly, the FACT Act contains a number of provisions directed at identity theft. Among them is a requirement that federal agencies develop identity theft prevention guidelines and regulations, the so-called “red flag” provision.

The federal banking agencies and the Federal Trade Commission (FTC) published final regulations interpreting the identity theft red flag provisions of the FACT Act on November 9, 2007. They were effective January 1, 2008, and compliance is mandatory November 1, 2008. The core of the regulation is the requirement to develop, implement, and update an “Identity Theft Prevention Program.” Specifically, the Identity Theft Program must be designed to “detect, prevent, and mitigate identity theft in connection with the opening of a covered account or any existing covered account, “taking into account the size and complexity of the depository institution and the nature and scope of its activities.”

This ABAWorks reviews the legal and regulatory issues and presents a sample process to help institutions devise their own red flags program required by the regulation: It was reviewed in April 2013, but no changes were made.

## Who Should Read This ABAWorks?

ABAWorks on Identity Theft Red Flag Regulation is designed to help senior bank executives and compliance officers understand the scope of the red flag identity theft regulation and assist them in leading their compliance efforts. The ABAWorks will also help boards of directors who, under the Regulation, are responsible for approving the initial written Identity Theft Prevention Program. Tools provided in this ABAWorks, such as a slide presentation explaining key requirements, will advise directors about regulator expectations of them.

## How is This ABAWorks Organized?

There are three sections to this ABAWorks. The first presents a legal analysis of the Regulation and background information on the underlying statute, the Fair and Accurate Credit Transactions Act of 2003. The second section provides detailed guidance on how to comply with the requirements. The third section contains a model worksheet that follows the process outlined in the previous section. This worksheet may be customized to meet each individual institution’s situation and be used to document compliance with the Regulation. In addition, the appendices provide: (1) Supplement A to the Guidelines of the Regulation that lists 26 “illustrative examples” of red flags; (2) a legal memorandum discussing coverage of the rule; and (3) a PowerPoint presentation that depository institutions may customize and use for presentations to their board of directors and appropriate staff.

### About American Bankers Association

The American Bankers Association brings together banks of all sizes and charters into one association. ABA works to enhance the competitiveness of the nation’s banking industry and strengthen America’s economy and communities. Its members—the majority of which are banks with less than \$125 million in assets—represent over 95 percent of the industry’s \$12.7 trillion in assets and employ over 2 million men and women.

© 2008 American Bankers Association, Washington, D.C.

This publication was paid for in part with the dues of ABA member financial institutions and is intended solely for their use. Please call 1-800-BANKERS if you have any questions about this resource, ABA membership or would like to copy or license any part of this publication.

This publication is designed to provide accurate information on the subject addressed. It is provided with the understanding that neither the authors, contributors nor the publisher is engaged in rendering legal, accounting, or other expert or professional services. If legal or other expert assistance is required, the services of a competent professional should be sought. This guide in no way intends or effectuates a restraint of trade or other illegal concerted action.

---

## SPECIAL THANKS

---

It would have been impossible to produce this ABAWorks on the Identity Theft Fraud Prevention Regulation without the guidance of two bankers, Alina Grabala and Keith Monson, who volunteered their time to share their knowledge and expertise to help create this ABAWorks. ABA thanks them for their thoughtfulness, creativity, attention to detail, and patience in endless conference calls and document reviews, right through several holiday periods.

---

## BANKER ADVISORS

---

**Alina M. Grabala, CRCM**  
Vice President  
and Compliance Manager  
Webster Bank, N.A.  
New Britain, Connecticut

**Keith E. Monson, CRCM**  
Senior Vice President  
Audit and Compliance Manager  
Premier Bank  
Jefferson City, Missouri

---

## REVIEW COMMITTEE

---

**Leonard J. Bolton, CRCM**  
Senior Vice President  
Rockland Trust Company  
Rockland, Massachusetts

**Michael A. Olson**  
Community Bank President  
US Bank NA  
Pella, Iowa

**Doris Waldman, CRCM**  
Senior Vice President  
Salem Five Cents Savings Bank  
Salem, Massachusetts

**John Bonora**  
Vice President,  
Compliance Officer  
Fairfield County Bank  
Ridgefield, Connecticut

**Dan Soto**  
Chief Compliance Officer  
RBC Centura Bank  
Raleigh, North Carolina

---

## ABA CONTRIBUTING AUTHORS

---

**Nessa Feddis**  
Vice President  
and Senior Counsel  
Center for Regulatory Compliance

**Steve Kenneally**  
Vice President  
and Senior Counsel  
Center for Regulatory Compliance

**Richard Riese**  
Senior Vice President  
Center for Regulatory Compliance

---

## ABA STAFF CONTRIBUTORS

---

**Jim Chessen**  
Chief Economist

**Mako Parker**  
Senior Program Manager

**Deanne Mariño**  
Writer/Policy Analyst

**Susan Einfalt**  
Senior Designer

**Ellen Collier**  
Manager



# Identity Theft Red Flag Regulation

## SECTION ONE

---

Background and Legal Analysis	1
Key Provisions of Regulation Related to Identity Theft Prevention Program	3
Other Requirements of the Regulation Related to Address Changes and Discrepancies	14

## SECTION TWO

---

Risk Assessment and Administration of Identity Theft Prevention Program	19
---	----

## SECTION THREE

---

Identity Theft Red Flag Analysis Model Worksheets	37
---	----

## APPENDICES

---

Appendix A: Supplement A to the Guidelines of the Regulation: List of 26 Examples of Red Flags	43
Appendix B: Legal Memorandum on Coverage of the Regulation	49
Appendix C: PowerPoint Summary of the Regulation	53

## **Key Points for Developing, Implementing, and Updating Identity Theft Prevention Program**

- **Mandatory compliance date: November 1, 2008.**
- **Written, board-approved Identity Theft Prevention Program is required.**
- **Existing policies and practices can and should be leveraged to satisfy requirements including those related to:**
  - Customer Identification Procedures (“CIP”)
  - Data protection
  - Fraud protection
  - Privacy
- **Most consumer accounts and some business accounts are covered.**
- **Staff must be trained.**
- **Program must be updated periodically.**
- **Annual reports on compliance are required.**
- **Depository institutions will be examined for compliance.**

## SECTION ONE

# Background and Legal Analysis

On December 4, 2003, the President signed the Fair and Accurate Credit Transaction Act (“FACT Act”) to amend the Fair Credit Reporting Act of 2003 (“FCRA”). FCRA generally addresses consumer reports and the FACT Act addressed various issues related to consumer reports, but Congress also saw the need and opportunity to address the growing problem of identity theft. Accordingly, the FACT Act contains a number of provisions directed at identity theft. Among them is a requirement that federal agencies develop identity theft prevention guidelines and regulations, the so-called “red flag” provision.

The press, politicians, consumer activists, and financial institutions had been increasingly concerned about the deleterious effects of identity theft, specifically its effect on victims. Identity theft victims described in the news and Congressional hearings how identity theft had ruined their lives. Victims who had credit cards and bank accounts, but also mortgages, car loans, and other accounts, opened or taken over by imposters found their credit histories in tatters. In some cases, it took years to untangle the financial mess identity theft had caused.

While in most cases victims were not responsible for fraudulent debts and transactions, they suffered inconvenience, frustration, and lost opportunities. They had to spend time and resources restoring order to their financial lives and lost confidence in financial institutions. While it was recognized that financial institutions have a vested interest in preventing identity theft as they usually suffer any loss, there was a sense among some that financial institutions simply viewed such

losses as a cost of doing business. For these reasons, Congress felt compelled to create new laws to help prevent identity theft and assist victims of identity theft.

Among the provisions of the FACT Act addressing identity theft is the identity theft “red flag” provision. This provision requires the banking agencies and Federal Trade Commission jointly to create identity theft prevention guidelines and prescribe regulations to establish reasonable policies and procedures for implementing the guidelines. In developing the guidelines, the federal agencies are instructed to “identify patterns, practices, and specific forms of activity that indicate the possible existence of identity theft.”

The federal agencies published a final Regulation interpreting the identity theft red flag provisions of the FACT Act on November 9, 2007. ([Go to edocket.access.gpo.gov/2007/pdf/07-5453.pdf.](http://edocket.access.gpo.gov/2007/pdf/07-5453.pdf)) They were effective January 1, 2008 and **compliance is mandatory November 1, 2008**. The core of the regulation is the requirement to develop, implement, and update an “Identity Theft Prevention Program.” Specifically, the Identity Theft Program must be designed to “detect, prevent, and mitigate identity theft in connection with the opening of a covered account or any existing covered account,” taking into account the size and complexity of the depository institution and the nature and scope of its activities.

Keep in mind that the Regulation defines “identity theft” broadly. In effect, much of what historically had been classified as traditional



**Compliance is mandatory  
November 1, 2008.**

**The Identity Theft  
Program must be  
designed to “detect,  
prevent, and mitigate  
identity theft in  
connection with the  
opening of a covered  
account or any existing  
covered account.”**



The federal agencies have indicated that they expect that most depository institutions will already have in place fraud prevention programs and controls that they will be able to incorporate into their Identity Theft Prevention Program, and it will be a matter of formalizing, documenting, and perhaps enhancing those practices and policies where appropriate.

fraud, such as unauthorized credit and debit card transactions, now falls under the catchall term, identity theft.

The federal agencies have indicated that they expect that most depository institutions will already have in place fraud prevention programs and controls that they will be able to incorporate into their Identity Theft Prevention Program, and compliance will be a matter of formalizing, documenting, and perhaps enhancing those practices and policies where appropriate. Accordingly, depository institutions should leverage existing policies and procedures where appropriate. Indeed, the federal agencies estimate that the annual burden for “information collection” related to compliance with the entire Regulation, including the Identity Theft Prevention Program, to be 41 hours in total, with 25 hours designated to the development of an Identity Theft Prevention Program.<sup>1</sup>

Depository institutions should keep in mind, however, that creation of the Identity Theft Prevention Program is not a single event, but a continuing and dynamic project that requires periodic review and modifications. Just as criminals are constantly changing and evolving

tactics, so must the solutions to detect and prevent fraud. In addition, staff training is a critical component. Creating the Identity Theft Prevention Program is of course, not only a legal requirement, but a prudent practice. A well-designed and administered program will help the institution to avoid fraud losses and protect the institution’s customers and protect the institution’s financial soundness and reputation.

In addition to adopting the Identity Theft Prevention Program requirements, the regulators implemented two other, separate statutory requirements. One relates to identity theft and addresses customer address change requests. Another relates to the accuracy of consumer reports and imposes requirements when there is a discrepancy between the address on a consumer report and the address on the request for the consumer report.

The following offers a summary and analysis of the Regulation and its related Guidelines that will help depository institutions to understand better the Regulation and how to comply. Also included are explanations of the other provisions adopted by the federal agencies.

1. 72 FR 63741 (Nov. 3, 2007).

### Leverage Existing Policies and Procedures

Depository institutions should leverage existing policies and procedures where appropriate. Indeed, the federal agencies estimate that the annual burden for “information collection” related to compliance with the entire Regulation, including the Identity Theft Prevention Program, to be 41 hours in total, with 25 hours designated to the development of an Identity Theft Prevention Program.



# Key Provisions of Regulation Related to Identity Theft Prevention Program

## Basic Provision

Depository institutions must “develop and implement a written Identity Theft Prevention 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 Identity Theft Prevention Program must be “appropriate to the size and complexity” of the depository institution and the “nature and scope of its activities.”

## Coverage

The Regulation generally covers most consumer accounts and potentially other accounts, including business accounts, for which there is a “reasonably foreseeable risk” of identity theft. The Supplementary Information suggests that the Regulation’s focus is accounts held by small businesses, such as sole proprietorship businesses. However, coverage will be determined on a case-by-case basis.

## Federal Preemption of State Laws

The federal red flag Regulation also preempts state law. This means that state laws related to conduct required by the Identity Theft Prevention Regulation (as the term identity theft is broadly defined under the Regulation) are preempted.

## Effective Date and Mandatory Compliance Date

The final Regulation went into effect January 1, 2008. **Compliance is mandatory by November 1, 2008.** The complete Regulation is available at: [edocket.access.gpo.gov/2007/pdf/07-5453.pdf](http://edocket.access.gpo.gov/2007/pdf/07-5453.pdf).

This means that the board of directors or board committee must have approved the Identity Theft Prevention Program by this date.

## Enforcement

The new rule is enforced administratively, which for depository institutions means that they will be examined for compliance and potentially subject to cease and desist orders and monetary penalties. Institutions not regulated by banking agencies, such as insurance companies and investment companies, are generally subject to the jurisdiction of the Federal Trade Commission.<sup>2</sup> FCRA does not provide a private right of action for violations of the identity theft prevention Regulation. State attorneys general may have enforcement authority.

## Regulatory Structure

Each of the federal agencies has amended its own existing Regulation that implements various provisions of FCRA. The Identity Theft Prevention Program rules of each agency are virtually identical in substance, but depending on the jurisdiction of the particular agency, their scope will vary. Depository institutions and their affiliates will usually be covered by one of the banking agency Regulations. However, some subsidiaries of depository institutions may be covered by the Federal Trade Commission’s Regulation rather than a banking agency Regulation. This would include, for example, insurance company subsidiaries and subsidiaries regulated by the SEC that offer brokerage and investment advisory accounts if those subsidiaries offer “covered accounts.”<sup>3</sup>

2. See Section 681.2 (a) of Federal Trade Commission Identity Theft Rules at 72 FR 63772 (Nov. 3, 2007) and Section 621 (a) of Fair Credit Reporting Act.
3. See Oliver Ireland memorandum, Appendix B.



The Identity Theft Prevention Program must be “appropriate to the size and complexity” of the depository institution and the “nature and scope of its activities.”

## Regulation (Subpart J)

The banking agencies have added a new Subpart J entitled “Identity Theft Red Flags” to their regulations implementing the Fair Credit Reporting Act. Section \_\_90 under Subpart J contains a new provision labeled, “Duties regarding the detection, prevention, and mitigation of identity theft.” This document will use the section numbers of the banking agencies’ Regulations when referencing particular provisions. The Federal Trade Commission’s “Duties regarding the detection, prevention, and mitigation of identity theft” has been inserted as new Section 681.2 in Part 681, Identity Theft Rules. The final Regulation and Supplementary Information explaining the provisions and the federal agencies’ reasoning begins on page 63718 of the *Federal Register* notice found at [edocket.access.gpo.gov/2007/pdf/07-5453.pdf](https://www.edocket.access.gpo.gov/2007/pdf/07-5453.pdf). Subpart J, as adopted by each of the implementing agencies, is found in the *Federal Register* as follows:

### **Comptroller of the Currency**

12 CFR Part 41 (Subpart J begins on p. 63753 of the *Federal Register* notice.)

### **Federal Reserve System**

12 CFR Part 222 (Regulation V) (Subpart J begins on p. 63757 the of *Federal Register* notice.)

### **FDIC**

12 CFR Parts 334 and 364 (Subpart J begins on p. 63761 of the *Federal Register* notice.)

### **Office of Thrift Supervision**

12 CFR Part 571 (Subpart J begins on p. 63765 of the *Federal Register* notice.)

### **Federal Trade Commission**

16 CFR Part 681 (Section 681.2 begins on p. 63772 of the *Federal Register* notice.)

The regulatory provision related to the Identity Theft Prevention Program is divided into three parts:

1. **Regulation (Subpart J)** which contains the specific requirements;
2. **Guidelines** (Appendix J to the Regulation) which depository institutions must consider in implementing the Identity Theft Prevention Program and which offer direction on how to comply with the Regulation; and
3. **Supplement A to the Guidelines** which lists 26 examples of red flags that depository institutions “may consider.”

## Board Involvement and General Administration of Identity Theft Prevention Program

The Regulation requires that either the board of directors or an appropriate committee of the board of directors approve the initial written Identity Theft Prevention Program. However, an employee at the level of senior management rather than the board or committee of the board may be the designated person involved

in the oversight, development, implementation, and administration of the Identity Theft Prevention Program. That person (or the board or board committee) should:

- Assign specific responsibility for implementation;
- Review annual reports prepared by staff; and
- Approve material changes to the Identity Theft Prevention Program as necessary to address changing identity theft risk.

Thus, depository institutions have flexibility in determining who is in charge of the project generally. However, the board should be mindful that, ultimately, it is responsible for compliance.

In addition, a party other than the board, appropriate board committee, or someone at a senior management level may be in charge of actual implementation and administration (the administrator). The administrator is accountable to the board, an appropriate board committee, or a person at the level of senior management, and is responsible for submitting annual reports.

Board or board committee	Approve initial Program
Board, board committee, or “designated employee at the level of senior management”	Be “involved” in oversight, development, and implementation
	Assign specific responsibility for Program’s implementation
	Review annual reports from staff
	Approve material changes to Program
Administrator or staff responsible for Program	Be responsible for development, implementation, and administration of Program
	Report annually to board, board committee, or designated employee at level of senior management on compliance



The board should be mindful that, ultimately, it is responsible for compliance.



After approval of the initial Identity Theft Prevention Program, board involvement may be a matter of sound governance judgement.

## Key Definitions of “Identity Theft” and “Covered Accounts”

### Identity Theft. (15 C.F.R. 90(b)(8))<sup>4</sup>

“A fraud committed or attempted using the identifying information of another person without authority.” “Identifying information” means “any name or number that may be used, alone, or in conjunction with any other information, to identify a specific person including any—

- Name, social security number, date of birth, official State or government issued driver’s license or identification number, alien registration number, government passport number, employer or taxpayer identification number;
- Unique biometric data such as fingerprint, voice print, retina or iris image, or other unique physical representation;
- Unique electronic identification number, address, or routing code; or
- Telecommunication identifying information or access device (as defined in 18 U.S.C. 1029(e))

Under 18 U.S.C.1029(e) “Access Device” means:

Any card, plate, code, account number, electronic serial number, mobile identification number, personal identification number, or other telecommunications service, equipment or instrument, alone or in conjunction with another access device, to obtain money, goods, services, or any other thing of value, or that can be used to initiate a transfer of funds (other than a transfer originated solely by paper instrument).

Thus, identity theft includes not only a thief opening an account in someone else’s name, it also includes unauthorized use of account or access device numbers (such as credit card and debit card numbers), access devices, passwords for online access, or other means to access an account.

4. The Regulation cross-references the Federal Trade Commission’s rule that defines identity theft for purposes of FCRA.



Identity theft is broadly defined. It includes not only new account fraud and account take-over, but unauthorized transactions of existing accounts.



### Covered accounts:

- Most consumer deposit and credit accounts
- Potentially:
  - Small business and other accounts
  - Brokerage, investment advisory accounts, custodial accounts if they are offered by a “financial institution” or creditor and if there is a “foreseeable risk” to customers or bank from identity theft

### Account. ( \_\_.90(b)(1))<sup>5</sup>

“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.” It includes:

- An extension of credit;
- A deposit account.

The definition of “account” applies to fiduciary, agency, or custodial, brokerage, and investment advisory activities.<sup>6</sup>

### Covered Account. ( \_\_ 90(b)(2))

**Certain consumer accounts.** An account a financial institution or creditor offers or maintains:

- Primarily for personal, family, or household purposes, and
- Involves or is designed to permit multiple payments or transactions.

**Other covered accounts.** Any other account a 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 operational, compliance, regulation, or litigation risks.

Because the term “account” only covers products involving a “continuing relationship,” single transactions, such as purchase of a money order are not covered. Prepaid cards fall into a gray area. A gift card may not involve a “continuing” relationship, and therefore is probably not covered. However, a reloadable general purpose spending card that functions similarly to a deposit account probably would be.

5. See Oliver Ireland memorandum, Appendix B for additional analysis.  
 6. 72 FR 63721 (Nov. 3, 2007), Footnote 12 of the Supplementary Information to the Regulation.

### Automatically Covered Accounts

In addition to an analysis of whether a product is an “account,” the Regulation provides a two-prong approach in determining “covered accounts.” Under the first prong, certain consumer accounts are automatically covered. Under the second, other accounts that present an identity theft risk are covered.

Most consumer accounts, but not necessarily all, are covered under the first prong. These include:

- **Credit accounts**
  - Credit card accounts
  - Mortgage loans
  - Student loans
  - Consumer leases
  - Unsecured loans (closed- and open-end)
  - Automobile loans
  - Margin accounts
- **Deposit accounts**
  - Checking accounts
  - Savings accounts
  - Health savings accounts
  - Electronic transfer accounts
  - Payroll card accounts
  - 401(k) account
  - IRAs

### Accounts That May be Covered

**Other consumer accounts.** Other accounts that are not automatically covered under the first test may be covered under the second one if there is a “reasonably foreseeable risk” from identity theft. This second prong of the definition presents an institution’s first level of risk assessment. Depository institutions will need to evaluate these accounts to determine whether there is a “reasonably foreseeable risk” from identity theft, taking into consideration the fraud prevention controls already in place.

For example, certificates of deposit may not be automatically included under the first test if transactions are limited to renewals and redemption because they would not be



Because the term “account” only covers products involving a “continuing relationship,” single transactions, such as purchase of a money order by anon-customer, are not covered.

A gift card may not involve a “continuing” relationship, and therefore is probably not covered.

“designed to permit multiple payments or transactions.” However, a depository institution may conclude that they are covered under this second test, because the depository institution permits funds from mature certificates of deposit to be transferred online to an account at another depository institution, and it has experienced identity theft, indicating a higher risk of identity theft. In contrast, another institution may determine that its controls on such transfers are effective and that the account is, therefore, not covered.

In some cases, only a quick, perfunctory analysis may be necessary. For example, while safe deposit boxes might be considered an “account,” the depository institution might quickly conclude that the risk of identity theft is very low given the controls used to verify those accessing safe deposit boxes and accordingly, safe deposit boxes should not be covered.

#### **Possible coverage of some business accounts.**

The Regulation is not confined to consumer accounts. Some business accounts may be covered under the second test. Again, the test is whether for business accounts there is a “reasonably foreseeable risk” from identity theft, taking into consideration the controls already in place.

The federal agencies suggest that their concern lies with small businesses such as sole proprietorships. The agencies note in the Supplementary Information that they are:

[A]ware that small businesses also have been targets of identity theft. Over time, identity theft could expand to affect other types of accounts. Thus, the definition of “account” ... continues to cover any relationship to obtain a product or service that an account holder or customer may have with a financial institution or creditor.<sup>7</sup>

The federal agencies further explain that the second part of the definition “reflects the Agencies’ belief that other types of accounts, such as small business accounts or sole proprietorship accounts, may be vulnerable to identity theft ...”<sup>8</sup> In addition, the Supplementary Information indicates, “the risk-based nature of the final rules allows each financial institution or creditor flexibility to determine which business accounts will be covered by its Program through a risk evaluation process.”<sup>9</sup>

In evaluating the risk of identity theft, depository institutions may consider controls used by the business itself. Accordingly, while it will vary on a case-by-case basis, the Supplementary Information suggests that accounts of large businesses will usually not be covered, given their sophistication and resources. If for example, however, there has been a past incident of identity theft on such accounts, they may be covered.

#### **Periodic Review of Covered Accounts**

The Regulation also specifically requires that a depository institution “periodically determine whether it offers or maintains covered accounts.” Thus, as part of section \_\_.90.(d)(iv)’s requirement to update periodically the Identity Theft Prevention Program, depository institutions must review which accounts are covered.

7. *Ibid.* p. 63721.

8. *Ibid.*

9. *Ibid.*

## Four Key Elements of the Identity Theft Prevention Program

### General Rule of the Regulation. (1.90(d))

Under the Regulation, the Identity Theft Prevention Program must be in writing and include reasonable policies and procedures designed to:

1. **Identify relevant red flags** for the covered accounts that the financial institution or creditor offers or maintains, and incorporate those red flags into its Identity Theft Prevention Program;
2. **Detect red flags** that have been incorporated into the Identity Theft Prevention Program of the financial institution or creditor;
3. **Respond appropriately** to any red flags that are detected;
4. **Update** the Identity Theft Prevention Program periodically to reflect changes in risks to customers and to the safety and soundness of the financial institution or creditor from identity theft.<sup>10</sup>

### Guidelines to the General Rule of the Regulation.

In addition to the Regulation are the “Interagency Guidelines on Identity Theft Detection, Prevention, and Mitigation” (“Guidelines”) found in Appendix J of the Regulation. These provide direction on how to incorporate into the Identity Theft Prevention Program each of the elements of the Regulation. The Regulation specifically requires depository institutions to “consider” the Guidelines and include in their Identity Theft Prevention Program “those guidelines that are appropriate.”

The Guidelines provide that an institution may “incorporate, as appropriate, its existing policies, procedures, and other arrangements that control reasonably foreseeable risk to customers or to the safety and soundness of the financial institution or creditor from identity theft.” The Agencies emphasize in the Supplementary Information that

depository institutions already will have in place much of what is required by the Regulation and, indeed, the Agencies estimate that the institutions will spend 25 hours for “information collection” to develop their Identity Theft Prevention Program:<sup>11</sup>

The Agencies continue to believe that most covered entities already employ a variety of measures to detect and address identity theft that are required by section 114 [of the FACT Act and implemented by the regulation] of the final rulemaking because these are usual and customary business practices that they employ to minimize losses due to fraud. In addition, the Agencies believe that many financial institutions and creditors already have implemented some of the requirements of the final rules implementing section 114 as a result of having to comply with other existing regulations and guidance, such as the CIP regulations implementing section 326 of the USA PATRIOT Act ... that require verification of the identify of persons opening new accounts, the Information Security Standards that implement section 501(b) of the Gramm-Leach-Bliley Act (GLBA) 15 U.S.C. 6801, and section 216 of the FACT Act 15 U.S.C. 1681 and guidance issued by the Agencies or the Federal Financial Institutions Examination Council regarding information security, authentication, identity theft, and response programs. The final rulemaking underscores the ability of a financial institution or creditor to incorporate into its program its existing processes that control reasonably foreseeable risks to customers or to its own safety and soundness from identity theft, such as those already developed in connection with the covered entity’s fraud prevention program.<sup>12</sup>

10. It is not necessary for depository institutions to lay out their analysis in the precise order as provided in the Regulation. For example, some institutions may find that it is more efficient or rational to first identify their existing fraud controls and then list the red flags that those controls detect to determine whether any gaps should be filled.

11. Ibid. p.63741.

12. Ibid. p. 63740.

Thus, depository institutions should be able to rely heavily on existing rules and practices, including those related to Customer Identification Procedures (CIP), Gramm-Leach-Bliley information security rules, privacy policies, multi-factor authentication, identity theft provisions of the FACT Act, and others.

## Customer Identification Program

The Customer Identification Program required under the USA PATRIOT ACT requires depository institutions to obtain certain information about a person before opening a new account and to verify the identity of individuals within a reasonable time thereafter.

Under the interagency Customer Identification Program rules, before opening an account, a bank must obtain, at a minimum, an individual's:

1. Name
2. Address
3. Date of birth
4. Taxpayer identification number, which for most individuals is a social security number. [Individuals who are not U.S. persons may provide a taxpayer identification number or a number from any other government-issued document evidencing nationality or residence and bearing a photograph or similar safeguard.]

## Element 1: Identify Relevant Red Flags. (Guidelines §II)

To assist depository institutions in identifying the relevant red flags, the Guidelines:

1. List risk factors that should be considered as appropriate;
2. Offer examples of sources of red flags; and
3. List categories of red flags that should be considered “as appropriate.”

Some types of red flags will typically only be relevant for detecting identity theft at account

opening. For example, many red flags that CIP programs are designed to detect are useful at account opening (e.g., inconsistencies in an application and external information sources), but typically will not be useful in detecting identity theft for existing accounts. Equally, some red flags will only be relevant for existing accounts, for example, systems to detect unusual activity. Red flags may be different for business accounts than they are for consumer accounts. Red flags for dormant accounts may be unique. Also, some events or situations, such as a data breach, alone might not be a red flag, but an aggravating factor that might “heighten the risk of identity theft.”

### Risk Factors in Identifying Red Flags. (Guidelines §II (a))

The Guidelines list various risk factors depository institutions should consider “as appropriate” in identifying relevant red flags:

**Types of accounts:** The types of covered accounts it offers or maintains for customers;

**Methods to open accounts:** The methods it provides to customers to open its covered accounts;

**Methods of access:** The methods it provides to customers to access its covered accounts; and

**The institution’s identity theft experience:** Past incidents of identity theft.

The Agencies recognized that a finite list of risk factors for institutions to consider would limit financial institutions’ ability or incentive to respond to new or different types of identity theft. Accordingly, the Guidelines list factors institutions “should consider ... as appropriate.”

In addition, the Regulation recognizes that different red flags might apply to different types of accounts. For example, red flags that apply to deposit accounts might not be relevant for credit accounts. Similarly, red flags for accounts that may be opened online may not apply to those that may only be opened face-to-face. Equally, accounts that may have limited access, such as



Depository institutions should be able to rely heavily on existing rules and practices, including those related to CIP, Gramm-Leach-Bliley information security rules, privacy policies, multi-factor authentication, identity theft provisions of the FACT Act, and others.



The Identity theft prevention program regulation and guidelines provide information and examples related to:

- Risk factors to determine relevant red flags
- Sources and categories of possible red flags
- Controls to detect relevant red flags
- Responses when red flags are detected

passbook savings accounts or some certificates of deposit, are less vulnerable to identity theft than a checking account that may be accessed online and by debit card and check.

A depository institution's own experience with identity theft will also help to measure the risk of identity theft. Depository institutions can gather information about their identity theft experience from a variety of sources such as: SARs; information from fraud prevention units; information security units; lines of business; and complaints from customers and identity theft victims.

#### Sources of Red Flags. (Guidelines §II (b))

The Guidelines offer examples of *sources* of red flags that institutions should incorporate into their list of relevant red flags:

1. Incidents of identity theft that the depository institution has experienced;
2. Methods of identity theft that the depository institution has identified that reflect changes in identity theft risks; and
3. Applicable supervisory guidance.

Supplement A of the Guidelines<sup>13</sup> includes 26 “illustrative examples” of red flags. The Guidelines reference items in this list as examples of the “categories” of red flags institutions should include in their program. However, the federal agencies deliberately did not reference this list as one of the “sources of red flags” in the final Guidelines themselves. Thus, while the list of red flags contained in Supplement A may be useful for depository institutions to consider, depository institutions are not obligated to justify to examiners why they failed to include a specific red flag on this list.

The Agencies also have decided not to single out any specific red flags as mandatory for all financial institutions and creditors. Rather, the final rule continues to follow the risk-based, non-prescriptive approach regarding the identification of red flags that was set forth in the proposal. The Agencies recognize that the final rules and guidelines cover a wide variety of financial institutions and creditors that offer and maintain many different products and

services, and require the flexibility to be able to adapt to rapidly changing risk of identity theft.<sup>14</sup>

*Internal sources* of red flags depository institutions might want to consider include:

- SARs;
- Information from fraud prevention units and information security units;
- Complaints related to identity theft;
- Regulations E and Z claims of unauthorized card use; and
- Consumer notifications about identity theft.

*External sources* might include fraud prevention vendors, such as those offering systems to detect inconsistent or false application information or unusual account activity that suggests fraud. Depository institutions might also learn about predictive red flags based on industry experiences from industry benchmarking, conferences, and other fraud prevention resources.

#### Categories of Red Flags. (Guidelines §II (c))

To provide additional assistance in identifying relevant red flags, the Guidelines set forth five “categories of red flags.” These categories are also used to classify the list of 26 examples of red flags contained in Supplement A to the Guidelines. The Identity Theft Prevention Program should include “relevant” red flags from these five categories “as appropriate.”

- 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; and
- Notice from customers, victims

13. See Appendix A.

14. *Ibid.* p. 63727.



While the list of red flags contained in Supplement A may be useful for depository institutions to consider, depository institutions are not obligated to justify to examiners why they failed to include a specific red flag on this list.



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.

## Element 2: Detect Red Flags. (Guidelines §III)

The Identity Theft Prevention Program must also address how the depository institution will detect the identity theft red flags it has determined are relevant. The Guidelines offer as one example of a control to detect identity theft related to account opening, the policies and procedures regarding identification verification in place pursuant to CIP rules. The Agencies in the Supplementary Information suggest that depository institutions may “wish to integrate the policies and procedures already developed for purpose of complying” with CIP, but note, “Such policies and procedures may need to be supplemented.”<sup>15</sup> They explain that the CIP rules are intended to target money laundering and financing of terrorism. Accordingly, under the CIP rules, certain types of customers and accounts are exempt or receive special treatment because they pose a lower risk for these activities. These exemptions and special treatment may not be appropriate for the detection and prevention of identity theft. Accordingly, the Agencies expect depository institutions to review CIP policies and practices to ensure that CIP policies adequately detect relevant identity theft red flags.

For existing accounts, the Guidelines offer as examples:

- Authenticating customers;
- Monitoring transactions; and
- Verifying the validity of change of address requests, in the case of existing covered accounts.

The means for detecting red flags might also be different for business accounts than it is for consumer accounts.

15. *Ibid.* p. 63728.

## Element 3: Prevent and Mitigate Identity Theft. (Guidelines §IV)

Under the Guidelines, the Identity Theft Prevention Program must include “appropriate responses” when a red flag is detected “*commensurate with the degree of risk posed.*” An institution’s response may differ based on the size and complexity of the depository institution and the nature and scope of its activities.

In determining its response, the depository institution should “consider aggravating factors that may heighten the risk of identity theft.” The Guidelines give the following examples of aggravating factors:

- A data security incident that results in unauthorized access to a customer’s account records;
- Notice that a customer has provided information related to a covered account to someone fraudulently claiming to represent the depository institution or to a fraudulent website (e.g., phishing).

Thus, a data security breach alone might not warrant a response. However, if the institution learns that the breach has resulted in account numbers or card numbers being compromised, it might have to take steps to prevent identity theft such as monitoring accounts or reissuing cards.

Examples listed in the Guidelines of potential responses when a red flag is detected are:

- 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.

Other responses include crediting the customer's account for unauthorized card transactions pursuant to requirements under Regulation Z (Truth in Lending Act) and Regulation E (Electronic Fund Transfer Act).

#### Element 4: Update the Program. (Section \_\_.90(d)(2)(iv) of the Regulation and Guidelines §V)

Both the Regulation and the Guidelines require depository institutions to update the Identity Theft Prevention Program periodically to reflect changes in risks to customers and to the safety and soundness of the institution from identity theft. The Guidelines elaborate that the updates should be based on a number of factors such as:

- The experiences of the depository institution 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 the depository institution offers or maintains; and
- Changes in the business arrangements, including mergers, acquisitions, alliances, joint ventures, and service provider arrangements.

The Supplementary Information makes clear that depository institutions are not required to update their programs immediately or continuously.<sup>16</sup> Depository Institutions might consider incorporating, as necessary, major changes that enhance the overall effectiveness of the Identity Theft Prevention Program. Certainly, changes to the program should be reflected in the required annual report.

#### Administration of the Program. (\_\_.90(e) and Guidelines §VI)

The Regulation requires depository institutions to provide for the continued administration of the Identity Theft Prevention Program.

##### Board Approval of Initial Identity Theft Prevention Program.

Depository institutions must obtain approval of the initial written Identity Theft Prevention Program from either their board of directors or an appropriate committee of the board of directors. The Board or appropriate board committee need only approve the initial written Identity Theft Program. After initial board approval, the board, a committee of the board, or a *designated employee at the level of senior management* should approve material changes to the program.

##### Involvement of Board or Senior Management in Identity Theft Prevention Program.

Depository institutions must “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 Identity Theft Prevention Program. Under the Guidelines, one of these three should:

1. Assign specific responsibility for the program's implementation;
2. Review annual reports as required; and
3. Approve material changes to the Identity Theft Prevention Program as necessary to address changing identity theft risks.

**Staff Training.** Depository institutions must train staff, “as necessary,” to implement effectively the Identity Theft Prevention Program. Thus, only relevant staff need be trained. In addition, staff already trained as part of anti-fraud prevention efforts or under other policies and programs such as CIP, or for other reasons, need not be retrained except “as necessary.” The federal agencies estimate that four hours of training will be necessary.<sup>17</sup>

16. *Ibid.* p. 63730.

17. *Ibid.* pp. 63740, 63741.



The Board or appropriate board committee need only approve the initial written Identity Theft Program. After initial board approval, the board, a committee of the board, or a designated employee at the level of senior management should approve material changes to the program.



The Supplementary Information makes clear that depository institutions are not required to update their programs immediately or continuously.

**Oversight of Service Providers.** Depository institutions must exercise appropriate and effective oversight of service provider arrangements. The Guidelines elaborate that depository institutions which rely on service providers should ensure that service providers have in place “reasonable policies and procedures designed to detect, prevent, and mitigate the risk of identity theft” with regard to the services they provide. They offer as an example including in contracts a provision that the service provider agrees to have such policies and procedures in place and either report the detection of red flags to the depository institution or take appropriate steps to prevent or mitigate identity theft.

**Annual Reports.** Under the Guidelines, at least annually, the staff assigned responsibility for implementation of the Identity Theft

Prevention Program must report on compliance with the Regulation to the board of directors, an appropriate committee of the board, or a designated employee at the level of senior management. The report should address material matters related to the Identity Theft Prevention Program and evaluate issues such as:

- Effectiveness of the policies and procedures in addressing the risk of identity theft;
- Service provider arrangements;
- Significant incidents involving identity theft and management’s response; and
- Recommendations for material changes to the Identity Theft Prevention Program.



**Staff must be trained “as necessary” to implement effectively the Program.**

**Training related to existing policies and procedures need not be repeated.**

### **Other Applicable Legal Requirements. (Guidelines VII)**

The Guidelines also remind depository institutions of related legal requirements. Specifically:

- SAR responsibilities (31 U.S.C. 5318(g));
- FCRA requirements for users of consumer reports related to fraud and active duty alerts (15 U.S.C. 1681c-1(h));
- FCRA requirements to correct and update inaccurate or incomplete information and not report information the furnisher has reasonable cause to believe is inaccurate (15 U.S.C. 1681s-2)); and
- FCRA provision related to prohibitions on the sale, transfer, and placement for collection of certain debts resulting from identity theft. (15 U.S.C. 1681m(f)).



**Banks must ensure that service providers have in place “reasonable policies and procedures designed to detect, prevent, and mitigate the risk of identity theft” with regard to the services they provide.**

## Other Requirements of the Regulation Related to Address Changes and Discrepancies

In addition to the Identity Theft Prevention Program requirement, the Regulation also includes other specific legal requirements, one relating to identity theft and the other to the accuracy of consumer reports:

- Duties of card issuers regarding changes of address requests; and
- Duties of users regarding address discrepancies.

The provisions amend each of the agencies' Regulations that implements various provisions of FCRA. For the banking agencies' Regulations, the requirements related to changes of address are found in Subpart J, (Identity Theft Red Flags), Section \_\_.91. Those related to address discrepancies are found in Subpart I, (Duties of users of consumer reports regarding address discrepancies), Section \_\_.82. This document will use the section numbers of the banking agencies' Regulations when referencing particular provisions. The Federal Trade Commission provisions are found in Sections 681.3 and 681.1, respectively, of Part 681 (Identity Theft Rules).

### Duties of Debit and Credit Card Issuers Regarding Changes of Address. (\_\_ .91)

The provisions relating to the duty of card issuers regarding changes of address are found at:

**Comptroller of the Currency**

p. 63754 of the *Federal Register* notice.

**Federal Reserve System**

p. 63758 of the of *Federal Register* notice.

**FDIC**

p. 63761 of the *Federal Register* notice.

**Office of Thrift Supervision**

p. 63765 of the *Federal Register* notice.

**Federal Trade Commission**

p. 63772 of the *Federal Register* notice.

### Duties of Debit and Credit Card Issuers Regarding Changes of Address. (\_\_ .91)

**Basic Rule: Response if Card Issuer Receives Address Change Notification.** The FACT Act includes a provision intended to prevent criminals from obtaining access to someone's deposit or credit account through a credit or debit card by first asking the card issuer to change the address of the accountholder and then requesting an additional or replacement credit or debit card. It prohibits card issuers from issuing an additional or replacement card if they receive a notice of address change and shortly afterwards (during at least the first 30 days), receive a request for a card, unless they notify the cardholder or otherwise verify the validity of the change of address.

The Regulation implementing this provision provides flexibility and gives depository institutions options. Depository institutions will comply with this provision if they validate *all* addresses when they receive an address change notification, whether or not a replacement or additional card is requested.

In the alternative, the depository institution's policies and procedures may provide that no card will be issued if it receives a request for a card received within 30 days of an address change notice unless it does *one* of the following:

1. Notifies the cardholder of the address change request:
  - At the cardholder's former address; or
  - By any other means as agreed to by the cardholder and card issuer and
- Provides the cardholder a reasonable means of promptly reporting incorrect address changes, 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 the requirements of the Regulation related



Depository institutions will comply with this provision if they validate all addresses when they receive an address change notification, whether or not a replacement or additional card is requested.

to duties regarding the detection, prevention, and mitigation of identity theft (i.e., the depository institution's Identity Theft Prevention Program).

**Types of Cards Covered.** The provision applies to debit and credit cards. Both credit and debit card are defined in FCRA. Credit card is defined by a cross-reference to the Truth in Lending Act. Debit card is “any card issued by a financial institution to a consumer for use in initiating an electronic fund transfer from the account of the consumer at such financial institution for the purposes of transferring money between accounts or obtaining money, property, labor, or services.” Neither the Electronic Fund Transfer Act (“EFTA”) nor its implementing Regulation E contains a definition of debit card. However, FCRA provides that “account” and “electronic fund transfer” have the same meanings as those terms have in EFTA. Accordingly, the definitions of “account” and “electronic funds transfer” under EFTA and Regulation E will determine the meaning of debit card.

Thus, the provision covers credit cards and debit cards as those terms are generally understood. Also subject to the rule are cards issued to access home equity lines of credit and payroll account cards. Gift cards are excluded.

The provision only applies to cards issued to cardholders, which under the Regulation means, a consumer. FCRA defines consumer as an individual. However, business purpose cards are covered if issued to an individual. The Agencies concluded that identity theft may occur with a card a consumer uses for business purposes, and if it does, may affect the cardholder's personal credit standing.

#### **Notice Requirements to Cardholders.**

Notices sent to cardholders must be clear and conspicuous. This means “reasonably understandable and designed to call attention to the nature and significance of the information presented.” In addition, given the importance of the notice, it must be provided separately from the card issuer's

regular correspondence with the cardholder. This means, for example, that the card issuer's notice of the address change may not be included with the periodic statement.

#### **Address Discrepancies: Handling Notices of Address Discrepancy.**

**Basic Rule.** The Regulation imposes certain responsibilities on users of consumer reports when they receive a notice of address discrepancy from a nationwide consumer reporting agency.<sup>18</sup> The general purpose of this provision is to ensure that consumer reports are accurate. However, the provision may be useful in detecting potential identity theft.

Many depository institutions today already have policies and procedures to resolve address discrepancies and report confirmed addresses to consumer reporting agencies in the normal course of business. Accordingly, for compliance purposes, it will be a question of reviewing, verifying, and documenting those practices.

Specifically, the Regulation requires users to develop and implement reasonable policies and procedures for handling notices of an address discrepancy received from a consumer reporting agency. The policies and procedures must be 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; and
- To furnish an address that the user has reasonably confirmed as accurate to the consumer reporting agency if it establishes a continuing relationship and regularly reports to the consumer reporting agency.

18. Under this provision, depository institutions are only required to respond when they receive a notice of an address discrepancy from one of the three nationwide credit reporting agencies, specifically, Experian, TransUnion, and Equifax. The requirement does not apply to notices from other consumer reporting agencies.



Also subject to the rule are cards issued to access home equity lines of credit and payroll account cards. Gift cards are excluded.



Notices sent to cardholders must be clear and conspicuous. This means “reasonably understandable and designed to call attention to the nature and significance of the information presented.”

The first obligation, that is, to form a reasonable belief that a consumer report relates to the consumer about whom it has requested the report, applies not only when a new account is involved, but also when a depository institution obtains a consumer report for an existing account and receives a notice about an address discrepancy. The second requirement, to report the confirmed address to the consumer reporting agencies, however, does not apply unless the institution (1) “establishes a continuing relationship with the consumer;” *and* (2) regularly reports information to the consumer reporting agency.

### Forming a Reasonable Belief that the Consumer Report Relates to the Person About Whom the Report was Requested.

Examples:

- Comparing the information in the consumer report with the information the depository institution:
  - Uses to verify the consumer’s identity pursuant to CIP requirements;
  - Maintains in its own records (applications, change of address notifications, other customer account records, or retained CIP documentation); or
  - Obtains from third-party sources.
- Verifying the information in the consumer report with the consumer.

Depository institutions may rely upon their existing CIP policies and procedures, so long as they apply to all situations where the depository institution receives a notice of address discrepancy. This requirement to form a reasonable belief that the report relates to the person subject to the report request applies whether or not an account is opened. However, if the depository institution receives a notice of the discrepancy about an existing account, (e.g., application for additional credit) *after* earlier having identified and verified the consumer pursuant to CIP rules, the regulators “would not expect a user to employ the CIP procedures again.”<sup>19</sup> The examples listed above offer other options in this case.

### Response if Unable to Resolve the Discrepancy.

The Regulation itself does not mandate any particular response if the depository institution is unable to resolve the discrepancy, but the expectation is that the report will not be used in such a case. In addition, other rules may apply, such as CIP requirements. For example, CIP procedures may require that in such instances an existing account be closed or a new account not opened. Moreover, the address discrepancy might be a red flag under Subpart J of the Regulation, “Identity Theft Red Flags,” and require a response to prevent or mitigate identity theft.

19. *Ibid.* p. 63737.

### Address Discrepancy Regulation

The provisions for each agencies’ Regulation related to address discrepancies may be found at:

**Comptroller of the Currency**  
p. 63753 of the *Federal Register* notice.

**Federal Reserve System**  
p. 63756 of the of *Federal Register* notice.

**FDIC**  
p. 63760 of the *Federal Register* notice.

**Office of Thrift Supervision**  
p. 63764 of the *Federal Register* notice.

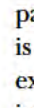
**Federal Trade Commission**  
p. 63771 of the *Federal Register* notice.

### Meaning of Notice of Address Discrepancy.

The Regulation defines a “notice of address discrepancy.” In effect, it means a notice sent by a nationwide consumer reporting agency that informs the user of a substantial difference between the consumer’s address that the depository institution provided in its request for the consumer report and the address in the consumer report. It is the consumer reporting agency, not the depository institution, that determines whether there is an “address discrepancy.” The depository institution’s responsibility is to respond appropriately when it receives such a notice from one of the nationwide consumer reporting agencies.



If the depository institution receives a notice of the discrepancy about an existing account, (e.g., application for additional credit) after earlier having identified and verified the consumer pursuant to CIP rules, the regulators “would not expect a user to employ the CIP procedures again.” The Regulation lists other options in this case.



It is the consumer reporting agency that determines whether there is an “address discrepancy.”

## Requirement to Furnish Confirmed Address to Consumer Reporting Agency.

**Reporting address to consumer reporting agency.** The depository institution must furnish to the consumer reporting agency an address that it has reasonably confirmed is accurate if it receives a notice of address discrepancy under the following circumstances:

- It has formed a reasonable belief that the consumer report belongs to the consumer about whom it requested the report;
- It established a continuing relationship with the consumer; and
- It regularly, and in the ordinary course of business, furnishes information to the consumer reporting agency that provided the notice of address discrepancy.

Depository institutions must have reasonable policies and procedures to accomplish this task.

**Confirming the address.** The federal agencies recognize that there may be various valid reasons for the address discrepancy, e.g., the consumer has moved or has a second home. Thus, the emphasis here is on verifying the consumer address rather than reviewing the depository institution's records. Accordingly, the Regulation offers four examples of how the depository institution may confirm an address if there is a discrepancy:

- Verify the address with the consumer;
- Review its own records;
- Verify the address through third-party sources; or
- Use other reasonable means.

### **Timing of reporting confirmed address.**

Depository institutions may report the confirmed address at the time they usually furnish information when they establish a new relationship.

## Carefully Review Policies and Procedures for Preventing Identity Theft

Depository institutions should review carefully their current policies and procedures for preventing identity theft. Depository institutions will find that they already have in place much of what the Regulation requires and that compliance with this Regulation is a question of reviewing, documenting, and perhaps enhancing existing policies and procedures.

Additional information and direction on how to comply with the Regulation follows. Section Two will offer a step-by-step guidance on how to develop an Identity Theft Prevention Program.





## SECTION TWO

# Risk Assessment and Administration of Identity Theft Prevention Program

In 2007, the banking agencies and the Federal Trade Commission adopted final rules related to the identity theft red flag provision of the Fair and Accurate Credit Reporting Act of 2003 (“FACT Act”). The core of the final Regulation is the requirement that depository institutions develop, implement, and periodically update a written Identity Theft Prevention 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 Identity Theft Prevention Program must contain reasonable policies and procedures to achieve four elements:

1. Identify red flags associated with covered accounts;
2. Detect red flags that were incorporated into the Program;
3. Respond to red flags that have been detected; and,
4. Update the Program to reflect changing risk conditions.

“Identify red flags” means identifying what situations or facts may indicate the possibility of identity theft. For example, unusual activity in an account might be a red flag that someone other than the authorized accountholder is using the account. “Detect red flags” means ensure that there are controls or systems in place to detect the red flag. In this example, this might be an automated system that detects unusual account activity. “Respond to red

flags” means evaluate the red flag detected, investigate, and possibly take additional steps. In the example, this might mean contacting the customer to determine whether the customer has authorized the transactions. In some cases, a single fact or event alone may not be a red flag for identity theft, but when combined with others may indicate the possibility of identity theft.

The process of developing and implementing the Identity Theft Prevention Program begins with determining who will be responsible for the project and for the ongoing administration of the Identity Theft Prevention Program. Once that is established, there are various possible and appropriate approaches in the initial stages of developing an Identity Theft Prevention Program. One option is to begin by creating an inventory of all the types of products the depository institution offers to determine which accounts are covered under the rule. The inventory could include a description of identity theft risks for each account based on, for example, how accounts are opened and accessed and the history of identity theft of each account. For each inventory item, the red flags currently detected, the controls to detect those red flags, and the institution’s response when a red flag is detected could be noted. This facilitates an evaluation of existing red flags to determine (i) whether those red flags reflect their own experience and those suggested in supervisory guidance and (ii) whether other relevant red flags should be added to the institution’s program of controls to further lower the risk of, or loss from, identity theft. The Identity

### Key Elements of the Identity Theft Prevention Program

1. Identify red flags associated with covered accounts;
2. Detect red flags that were incorporated into the Program;
3. Respond to red flags that have been detected; and,
4. Update the Program to reflect changing risk conditions.

Theft Prevention Program must incorporate oversight of service providers and staff training. Finally, depository institutions must ensure administration of the Identity Theft Prevention Program and prepare annual reports about compliance with the Regulation.

While there are different ways to create an Identity Theft Prevention Program, this section offers one option, which may be modified as depository institutions determine appropriate and useful. A model worksheet is provided to help in the analysis and documentation (Section Three) and may serve as a “base inventory.” Depository institutions may choose to use the model worksheet as presented or modify as they find appropriate. Institutions may also choose a different approach. Depository institutions may find the worksheet to be a useful tool when drafting their Identity Theft Prevention Program. Section Three also contains the model worksheet with examples of information it might contain.

This risk assessment and administration section is divided into the following parts:

1. Determining responsibilities and administration
2. Putting together a base inventory
3. Identifying covered accounts
4. Identifying relevant red flags for covered accounts: red flag gap analysis
5. Incorporating controls to detect red flags
6. Responding when red flags are detected
7. Overseeing service providers
8. Training staff
9. Administering the program
10. Documenting and updating the Identity Theft Prevention Program
11. Submitting annual reports

# Determining Responsibilities and Administration

## Step 1: Board Involvement

The Regulation requires that the board of directors or an appropriate committee of the board of directors approve the initial written Identity Theft Prevention Program. Thus, the depository institution has to decide whether either the board or a committee of the board will approve the initial Identity Theft Prevention Program. The board or board committee will also be receiving annual reports regarding compliance with the Regulation. However, a designated employee at the level of senior management rather than the board or board committee may be the one involved in the oversight, development, implementation, and administration of the Identity Theft Prevention Program. Depository institutions should keep in mind that the board or board committee must have approved the Identity Theft Prevention Program by November 1, 2008, and should thus coordinate the board's or board committee's schedule to ensure approval by the compliance due date.

## Step 2: Determine Responsibilities

The board, an appropriate committee of the board, or a designated employee at the level of senior management must be "involved" in the oversight, development, implementation, and administration of the Identity Theft Prevention Program. In addition, one person in this group must:

- Assign specific responsibility for implementation;
- Review annual reports prepared by staff; and
- Approve material changes to the Identity Theft Prevention Program as necessary to address changing identity theft risk.

Thus, depository institutions have flexibility in determining who is in charge of general oversight. Clearly, the board, committee, and

senior management may entrust administrative staff with implementation. However, the board, a board committee, or senior management should receive progress reports as appropriate and ensure that staff is accountable for compliance.

In addition, someone other than the board, appropriate board committee, or someone at a senior management level may be in charge of actual implementation and administration (the administrator). The administrator should understand the fundamentals of the regulatory requirements, the nature of the institution's lines of business, and the institution's identity theft challenges and fraud prevention policies. The administrator could, for example, be someone in the compliance or the fraud/risk management area. It is also critical that the administrator have the necessary authority to ensure implementation is complete and controls and responses to red flags are reasonable across lines of businesses and other departments. The administrator is also responsible for submitting annual reports to the board, an appropriate board committee, or a person at the senior management level.

The PowerPoint presentation found in Appendix C provides a general overview of the Regulation that might be useful for presentations to the board or board committee and various staff of the depository institution. This overview may be customized to include information specific to the depository institution's own efforts to reduce identity theft.

## Step 3: Getting a Team Together

Development, implementation, and administration of the Identity Theft Prevention Program will require the participation of various disciplines and departments within the depository institution. Potential partners include departments and units in charge of: compliance; fraud/risk management; lines of business; information security; vendor management; and privacy.



**Depository institution should coordinate the board's or board committee's schedule to ensure approval by the compliance due date of November 1, 2008.**

## Putting Together a Base Inventory

### Step 1: Create a Worksheet that Includes an Inventory of all Existing Accounts, Identity Theft Experience, and Controls Related to all Accounts. (See model worksheet in Section Three)

To begin the process of developing its Identity Theft Prevention Program, depository institutions might find it helpful to create a worksheet that shows an inventory of all the accounts they offer and maintain and their current controls and responses if problems are detected. This includes legacy accounts which may no longer be offered, but are maintained. The inventory process should confirm what the regulators recognized in creating the rule—that depository institutions already have identity theft controls in place. Institutions are not starting from scratch.

In addition, such a worksheet may serve as a base document to build on and used as a reference as the depository institution moves through the analysis and development process. It will first be used to determine which accounts are covered, the first level of the risk assessment. It will later be used to evaluate the institutions' current controls, use of red flags, and responses when red flags are detected and to determine whether additional red flags should be detected. This worksheet can serve as a tool to draft an Identity Theft Prevention Program and also as documentation of compliance.

A model worksheet is found in Section Three along with a worksheet that includes examples of information it might contain. Depository institutions may choose to use as is, or modify this model, or use a different approach. One option, shown in the worksheet, is to distinguish within each of the columns whether the information or description relates to account opening or account access.

The worksheet might initially contain for each account offered or maintained by the depository institution columns for:

- Column A: Lines of Business
- Column B: Type of Account Product
- Column C: Risk Factors
- Column D: Past Identity Theft Experience
- Column E: Existing Controls to Detect Red Flags
- Column F: Existing Red Flags
- Column G: Response to Red Flags
- Column H: Residual Risk Rate
- Column I: Account Covered?
- Column J: Gap Analysis
- Column K: Action Plan
- Column L: Comments

### Step 2: Complete Columns A-G

Each line of business could complete its own worksheet independently for its accounts and submit them to the Identity Theft Prevention Program team for consolidation. A smaller depository institution may choose to create the inventory from one central location. The inventory might group types of products, for example, by credit and deposit type. Another means of differentiation is the product's delivery channel, e.g., in-person, by telephone, or on-line.

**Column B records the accounts offered by the depository institution.** Because the definition of "covered accounts" mandates the inclusion of consumer accounts that permit multiple transactions, listing such automatically covered accounts together will facilitate the analysis.

For brevity's sake, depository institutions may wish to avoid multiple entries of the same or similar information by referencing entries made elsewhere with regard to other accounts. For many depository institutions, accounts will often have similar features, be accessible through identical delivery channels, and be subject to the same controls. In such cases, consolidating like accounts into an aggregated



The inventory process should confirm what the regulators recognized in creating the rule—that depository institutions already have identity theft controls in place. Institutions are not starting from scratch.



The Regulation defines "identity theft" as a "fraud committed or attempted using the identifying information of another person without authority."

row of the worksheet will streamline the inventory process and minimize redundant entries.

**Column C covers risk factors.** Because the red flags, controls, and responses may vary depending on whether they relate to opening accounts (new accounts) or accessing accounts (existing accounts including dormant accounts), the institution could capture these distinctions within a “risk factor” column, along with risks associated with volume and frequency. “Past experience” could then be in its own column, Column D. (See Figure 1.)

The worksheet demonstrates one way to capture this fundamental risk dichotomy between account opening and account access through use of shading, font, or format. Figure 1 illustrates this by recording account opening risks in a shaded row and account access risks in an unshaded row. Adopting this approach in Column C will establish a convention that enables tracing the risk and its related controls, red flags, and responses through the entire worksheet. The opening and accessing risk factors column can capture risk variation based on volume of transactions and/or delivery channels among other types of differentiation.

**In Column D, describe briefly past identity theft experience with the account, based on information from:**

- Suspicious Activity Reports (SARs);
- Fraud prevention unit;
- Information security unit;
- Lines of business;
- Complaints from customers, identity theft victims; and
- Comments from employees.

This experience description should include both unsuccessful identity theft attempts as well as incidents resulting in a loss or control evasion. This column offers depository institutions the opportunity to demonstrate that their history validates the success of their current controls.

**FIGURE 1**

Type of Account Product	Risk Factors	Past ID Theft Experience*
Consumer Checking	<p><b><u>Account Opening</u></b></p> <p><u>Means</u></p> <ul style="list-style-type: none"> <li>• In person only</li> </ul> <p><u>Frequency/Volume</u></p> <ul style="list-style-type: none"> <li>• Number of accounts opened per month/year</li> </ul>	<p>Number of accounts opened fraudulently in someone else's name is low.</p> <p>Attempts to open accounts using false identification documents or personal information have been detected, but accounts not opened</p>
	<p><b><u>Account Access</u></b></p> <p><u>Means</u></p> <ul style="list-style-type: none"> <li>• Checks</li> <li>• Debit card (signature and PIN authorization)</li> <li>• Online access</li> </ul> <p><u>Frequency/Volume</u></p> <ul style="list-style-type: none"> <li>• Volume of transactions is X</li> </ul>	<p>Databreach or card skimming caused substantial losses in 200X</p> <p>Series of successful account hijackings by insider resulted in substantial losses to depository institutions</p> <p>Multiple unsuccessful attempts to log-in with wrong password triggered contacts to customer</p> <p>Losses from checks with forged signatures and stolen and counterfeit checks drawn on customer accounts is low</p> <p>* Institution may consider noting or referencing its fraud statistics when describing identity theft experience</p>

**For Columns E, F, and G, for each account type, the depository institution should review the internal controls and policies it already has in place.** For example, before issuing a credit card or approving a mortgage, the depository institution may review a credit report on the applicant. The credit report may contain a fraud alert because of past identity theft activity. The depository institution may have procedures in these instances to take additional steps to verify the identity of the applicant. In this example, the fraud alert is the red flag detected through the internal control, (i.e., “check for fraud alerts”) that permits the institution to detect the alert when pulling a credit report. The “response” is requiring a higher level of verification to ensure applicants are who they say they are.

Another example is the case of repeated attempts to access an account online. After multiple, unsuccessful attempts to access an account via the Internet with an invalid password, a depository institution may halt attempts for a set time period, ask challenge questions to ensure that the person attempting to access the account is the account holder, or freeze online access until the customer verifies the online access attempts. The multiple log-on failures would be the red flag, the system that counts and limits the successive failures would be the control, and the depository institution’s attempts to verify the user’s identity would be the response.

Examples of *controls* (Column E) are found in the Part III of the Guidelines to the Regulation (See Section One, page 11):

- Authenticating customers;
- Monitoring transactions; and
- Verifying the validity of change of address requests, in the case of existing covered accounts.

Examples of *responses* (Column G) when red flags are found in Part IV of the Guidelines to the Regulation (See Section One, page 11.):

- Monitoring the account for evidence of identity theft;
- Contacting the customer;
- Changing passwords, PINs, etc., that allow access to the account;
- Changing the account number;
- Not opening a new covered account;
- Closing an existing covered account;
- Not attempting to collect on a covered account or not attempting to sell a covered account to a debt collector;
- Notifying law enforcement; and
- Determining that no response is needed.

Other responses include crediting the customer’s account for unauthorized card transactions pursuant to requirements under Regulation Z (Truth in Lending Act) and Regulation E (Electronic Fund Transfer Act).

When completing Columns E, F, and G, the depository institution should take full advantage of existing controls and refer to policies and procedures that may be housed elsewhere in the institution, without necessarily going into great detail in the chart or written program. Those policies could be reviewed separately for evaluation and should be readily available for examiners. For example, all account address changes might be handled in a single unit or department, or Customer Identification Procedures (“CIP”) might apply to all covered accounts. A simple reference to that unit or policy would be adequate for these purposes. In the alternative, the depository institution could specify each control, red flag, and response. The sample worksheet below provides examples of controls, red flags, and responses when red flags are detected.

**FIGURE 2**

Sample of existing controls, red flags, and responses when red flags are detected (selected columns from the worksheet in Section 3.)

<b>C</b> <b>Risk Factors</b>	<b>E</b> <b>Existing Controls to Detect Red Flags</b>	<b>F</b> <b>Existing Red Flags</b>	<b>G</b> <b>Response to Red Flags</b>
Account Opening	CIP procedures* or Check identification information with other sources  * Depository institution may choose to reference policy or describe specifically each control.	See CIP procedures* or Identification information not consistent with other sources  Application, personal information, or identification information inconsistent, suspicious, or invalid	See CIP procedures* or Do further analysis to verify identity of applicant  Do not open the account
Account opening (or increase in existing line of credit)	Consumer reporting agency alert/freeze detection	Receipt of alert or freeze from consumer reporting agency	Contact customer to verify application
Account access	Unusual account activity detectors	Detection of unusual activity in deposit or credit card account	Notify customer to confirm activity
Account access	Third party vendor systems that provide alerts about compromised card numbers	Receipt of notice that customers' cards or card numbers have been compromised	Monitor affected accounts; re-issue cards; or limit transactions on affected accounts
Account access	<ul style="list-style-type: none"> <li>• Fraud prevention policies</li> <li>• Address change policies</li> <li>• Signature reviews (with signature cards or internal sources);</li> <li>• Use of challenge questions (internal or external)</li> </ul>	<ul style="list-style-type: none"> <li>• Customer responds that he or she did not request address change request bank received</li> <li>• Signatures do not match</li> <li>• Challenge question answered incorrectly</li> </ul>	<ul style="list-style-type: none"> <li>• Do not make address change</li> <li>• Do not proceed with the transaction</li> <li>• Do not proceed with the transaction</li> </ul>
Account access	Procedures for identifying and handling complaints of identity theft	Customer calls reporting unauthorized transactions on credit or checking account	Investigate and remove unauthorized transactions from account
Account access	Programs that detect that dormant accounts are accessed or transactions made	<p>Employee accesses a dormant account (internal fraud)</p> <p>Unauthorized transactions are detected (may be internal or external fraud)</p>	Investigate reasons for access. If unauthorized transaction made, reverse them

### Step 3: Determine the Residual Risk for Each Account and add to Column H of Worksheet.

The next step is to measure the residual risk of identity theft for all accounts. The residual risk is the risk that remains, taking into account current controls. A depository institution could rate the risk low, medium, or high or use a scale of 1 to 5, for example. How to rate or score the risk is subjective and will vary by depository institution. This residual rate will be used to determine: (1) which accounts should be covered that are not automatically covered; (2) whether additional relevant red flags and controls are appropriate for covered accounts; and (3) where the depository institution should focus its attention and resources. In determining the residual risk, the depository institution should consider risk factors and existing controls.

Risk factors to determine the risk depository institutions might consider include, but are not limited to:

- The type of account;
- How the accounts are opened;
- How the accounts are accessed;
- The volume of account openings and account activity; and
- The institution's past history of identity theft.

The size and complexity of the depository institution may also be a factor.

For example, an account that may be opened via the Internet may present a higher inherent

risk than an account that must be opened in person at a branch. Similarly, in measuring risk, depository institutions should consider how accounts are accessed. Deposit accounts that are accessible online, by debit card, by check, and by telephone are inherently riskier than those only accessible by check. The greater the number of channels to open or access the account, the greater the inherent risk of identity theft.

Other possible factors to consider are the size and geographic location of the institution. Smaller institutions serving smaller populations may have lower risks in some situations because of a particular security feature—familiarity with their customers. A teller at a one-branch bank in a small town is likely to detect potential fraud if an outsider is attempting to impersonate a town citizen. This may be more effective for an institution in a small city than for a large institution in a metropolitan area.

As the Guidelines suggest, depository institutions should also use their past experience with identity theft to assess risk. (See Section One, page 9.) A type of account that has no history of identity theft will present a lower risk than one that has more frequently been a target.

Having reviewed the inherent risk and identity theft history, depository institutions should then determine the residual risk, based on the controls already in place. For example, a depository institution may conclude that for checking accounts there is a high inherent risk of identity theft, but conclude that the residual risk is low after taking into account the institutions' current controls, e.g. CIP, monitoring for unusual activity, as well as the history of identity theft on checking accounts.



# Identifying Covered Accounts

## Step 1: Review Definition of “Covered Account” and Explanation in Section One, Page 6

In addition to an analysis of whether a product is an “account,” the Regulation provides a two-prong approach in determining “covered accounts.” Under the first prong, certain consumer accounts are automatically covered. Under the second, other accounts that present an identity theft risk are covered.

Accounts that are not automatically covered under the first test may be covered under the second one if there is a “reasonably foreseeable risk” from identity theft. This second prong of the definition presents an institution’s first level of risk assessment. Depository institutions will need to evaluate these accounts to determine whether there is a “reasonably foreseeable risk” from identity theft, taking into consideration the fraud prevention controls already in place.

## Step 2: Identify Accounts that are Automatically Covered Under First Test of the Definition of Covered Account

This will include most consumer accounts, such as:

Credit Accounts:

- Credit Card Accounts;
- Mortgage Loans;
- Student Loans;
- Automobile Loans;
- Consumer Leases;
- Overdraft Lines of Credit;
- Unsecured Loans (closed and open-end); and
- Margin Accounts.

Deposit Accounts:

- Checking Accounts;
- Savings Accounts;
- IRAs;
- 401(k) Accounts; and
- Payroll Card Accounts.

Accounts that are automatically covered should have a “yes” entry in Column I. If done on a spreadsheet, this will allow the sorting of the list by covered or non-covered accounts.

Other consumer accounts, such as some certificates of deposit, may not automatically be included, for example, if they are not designed to permit multiple payments. Accounts not covered should have a “no” entry in Column I.

## Step 3: Analyze the Accounts that are Not Automatically Covered

Review the residual risk rate for each account in the worksheet that is not automatically covered to determine if the residual level of risk associated with that account justifies inclusion as a covered account.

Identify as covered accounts those accounts “for which there is a reasonably foreseeable risk” to customers or to the safety and soundness of the depository institution from identity theft, including operational, compliance, regulation, or litigation risks, ***taking into consideration current fraud prevention controls***. For example, a depository institution may determine that, because of the transaction limits on some certificates of deposit, they are not covered under the first test in the definition of covered account.<sup>20</sup> However, they

20. Under the first test, only those accounts that involve or are designed to permit multiple payments or transactions are covered.

may be covered under the second test because the depository institution permits funds from matured certificates of deposit to be transferred online to an account at a different institution, and it has experienced unauthorized transfers. Nevertheless, if there are sufficient controls so that the risk of identity theft is low, it might not be covered. For example, another depository institution may determine that such certificates of deposit are not covered because the institution only allows certificates of deposit to be redeemed in person or there are sufficient controls with online transfers. Depository institutions may conclude that some business and checking and credit accounts are covered under the second test because the risks posed are similar to those present for consumer accounts. This may be especially true for small

businesses that do not have the sophistication of anti-fraud measures in place that large corporations may have.

Accounts that are covered under this analysis should be noted by a “yes” entry in Column I and grouped with accounts automatically covered. Account products marked with a “yes” are considered covered accounts and will require further analysis. This completed part of the worksheet can be used to document and demonstrate compliance with the Regulation and to draft the Identity Theft Prevention Program.

Staff from lines of business that have no covered accounts may be excused from further team participation in the project or program administration.



# Identifying Relevant Red Flags

An Identity Theft Prevention Program is expected to identify relevant red flags. This part of the analysis will take the depository institution through a step-by-step process so that it covers the “categories” of red flags that examiners will look for in examinations.

## Step 1: Categorize Red Flags Currently Used

Depository institutions may start this step by dividing the inventory of red flags they currently use, as listed in Column F of the worksheet, into the five categories listed in the Guidelines (See Section One, page 10):

- Alerts from consumer reporting agencies
- Presentation of suspicious documents
- Presentation of suspicious personal identifying information
- Unusual or suspicious activity involving a covered account
- Notice regarding possible identity theft

This will demonstrate that the depository institution’s program draws from the appropriate categories. Because the depository institution’s inventory derives from existing controls that have been built around the institution’s operations, the red flags already in use will have come from a variety of sources, including sources not listed in the Guidelines.

A table such as illustrated in Figure 3 may be used to aggregate similarly featured products/accounts that share common controls (and therefore cover common red flags), thereby streamlining the categorization of relevant red flags.

### Red Flag Categories

Dividing red flags currently in use into the red flag categories listed in the Guidelines may be an effective way to demonstrate that the depository institution’s red flags are derived from the appropriate categories.

### Key Elements of the Identity Theft Prevention Program

1. Identify red flags associated with covered accounts;
2. Detect red flags that were incorporated into the Program;
3. Respond to red flags that have been detected; and,
4. Update the Program to reflect changing risk conditions.

FIGURE 3

Account Type	Alerts	Suspicious Documents	Suspicious Personal Identifying Information	Unusual or Suspicious Activity on Account	Notice of Possible Identity Theft
Checking Account		Forged or altered identification documents presented  When presenting check for cashing: (1) Forged or altered documents presented (2) Identification photo or description inconsistent with customer	SSN is the same as other customer's or applicant's  Personal identifying information inconsistent with external database or application information	Customer notification of unauthorized charges  Unusual activity on account  New activity on dormant account	Customer notification that bank has opened account for identity thief

## Step 2: Confirm Sufficiency of Existing Red Flags

For each covered account or group of similarly featured covered accounts, the depository institution should consider whether the residual risk from existing controls meets the institution's risk tolerance or expectation for identity theft prevention and mitigation.

Depository institutions may determine that current controls and relevant red flags are adequate for covered accounts with low residual risk rates and that no additional measures are necessary. For example, an institution's current CIP practices may be a sufficient control to prevent identity theft at account opening for a consumer checking account or credit card account and conclude that additional measures are unnecessary.<sup>21</sup> Similarly, a depository institution may also conclude that its automated systems for detecting unusual account activity are highly effective and further measures are not needed. An institution might conclude that its address change policies are sufficient to detect identity thieves' attempts to reroute account information and access devices to the thieves' address. The analysis showing the existing controls and low residual risk rate may be useful for documentation purposes and can be referenced in Column J as "No Gap" and in Column K as, "No Action required."

## Step 3: Supplement Red Flags Where Appropriate

For each covered account or group of similarly featured covered accounts whose residual risk is higher than the depository institution's risk tolerance or expectation for identity theft prevention and mitigation, the institution should consider whether it should use additional "relevant" red flags in any of the *categories* listed in the Guidelines and to establish controls to detect them.

21. The Supplementary Information notes that CIP policies may have to be supplemented because CIP rules are intended to target money laundering and financing of terrorism. Accordingly, certain customers are exempt because they pose a lower risk of those activities. The exemptions may not be appropriate for detection and prevention of identity theft. 72 FR 63728 (Nov. 3, 2007).

## Examples of Sources of Red Flags

The Guidelines offer three examples of sources of red flags to consider when identifying relevant red flags:

- Incidents of identity theft that the depository institution has experienced.
- Methods of identity theft that the depository institution has identified that reflect changes in identity theft risk; and
- Applicable supervisory guidance.

In addition, Supplement A of the Guidelines includes 26 "illustrative examples" of red flags that depository institutions may find useful. (See Appendix A.) However, the federal agencies have not specifically listed Supplement A, the list of red flag examples, as a "source" of red flags in the Regulation or Guidelines.<sup>22</sup> Rather, the Guidelines note that "examples" of individual red flags are provided in Supplement A to the Guidelines.

In addition, a depository institution may use the inventory of red flags it has described in the table that it currently uses for one product to consider whether they may be relevant for other products.

In analyzing whether additional red flags should be identified, the depository institution should consider the effectiveness and cost of their detection. For example, it might consider whether the control is manual or automatic,

22. The original proposal required institutions to incorporate relevant red flags listed in proposed Appendix J, the Guidelines, which included the list of red flag examples. However, the federal agencies amended the proposal by removing the list of examples from Appendix J and instead incorporating it into new Supplement A. In the Supplementary Information, the federal agencies note, "The Agencies did not intend for these examples to be a comprehensive list of all types of identity that a financial institution or creditor may experience ... The Agencies also have decided not to single out any specific Red Flags as mandatory for all financial institutions and creditors. Rather, the final rule continues to follow the risk-based, non-prescriptive approach regarding the identification of Red Flags that was set forth in the proposal." 72 FR 63727 (Nov. 3, 2007).



The analysis showing the existing controls and low residual risk rate may be useful for documentation purposes and can be referenced in Column J as "No Gap" and in Column K as, "No Action required."



Depository institutions are not obligated to explain why they did not use a particular red flag contained in Supplement A, the list of illustrative red flag examples.

and whether, given the volume of transactions and risk of identity theft, it is appropriate and cost-effective.

As a practical matter, an additional red flag may be “appropriate” if it (combined with its associated response) materially improves prevention or mitigation of identity theft experience *and* the control that detects it can be feasibly implemented at a cost that is noticeably less than the identity theft avoidance benefits to be achieved.

Improved performance of an institution’s Identity Theft Prevention Program may be facilitated by considering those red flags associated with “preventive” controls as opposed to “detective” (or “mitigating”) controls. When the identity theft experience is characterized by successful incursions that have to be mitigated after some level of identity theft damage has become manifest, then it may be worth considering adopting preventive controls when available and cost effective to stop identity theft at the attempt—not after the damage has already occurred and the institution is left trying to stem further losses.

Results will vary by product and by depository institution. Relevant red flags should be “appropriate to the size and complexity” of the institution and the “nature and scope of its activities.” For example, use of automated systems to detect unusual checking account or debit card activity might be appropriate for large depository institutions, but not appropriate for small institutions where it would probably not be cost effective.

#### Step 4: Document Additional Action Required

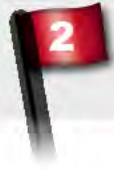
If additional red flag applications are indicated by a “yes” in Column J for gap analysis, then an explanation of those additional red flags should follow in Column K, “Action Plan.” Column K should also include the depository institution’s description of how it will detect the additional red flags and respond when they are detected. The information in these columns will be used in drafting the Identity Theft Prevention Program.

The depository institution may use Column L for additional clarifying notes on actions it did or did not take.

### Preventative Controls Stop Fraud Before It Occurs

*Detective* (or mitigating) controls identify fraud after it occurs and prompt responses that will minimize damages from the intrusion. *Preventative* controls stop fraud before it occurs. In general, automated, preventative controls are most effective. For example, a control that detects multiple failed PIN entries on a debit card and one that detects multiple, unsuccessful online access attempts and then freezes the account in real time are strong automated preventative controls. An example of a strong detective control is sending out welcome letters automatically after account opening and then closing the account when recipients report that they did not open the account. A manual detective control might be reviewing monthly reports showing multiple applications from the same address or reviewing reports of unusual account activity.

A manual control that detects identity theft that has already happened, such as, for example, a review of a customer complaint of unauthorized transactions on a periodic statement, is not as effective in preventing identity theft from happening, but is important in investigating the violation and in identifying potential new identity theft trends and weaknesses in current controls.



## Incorporating Controls to Detect Red Flags

### Key Elements of the Identity Theft Prevention Program

1. Identify red flags associated with covered accounts;
2. Detect red flags that were incorporated into the Program;
3. Respond to red flags that have been detected; and,
4. Update the Program to reflect changing risk conditions.

The second of the four key elements of an Identity Theft Fraud Prevention Program required by Section \_\_90(d) of the Regulation is to have reasonable policies and procedures designed to *detect the relevant red flags*. (See Section One, pages 8 and 11.) This requirement applies to both the opening of covered accounts and to access of existing covered accounts.

In order to draft this part of the Identity Theft Prevention Program, the depository institution should be able to rely on Column E of the worksheet which contains references or explanations of the controls currently used to detect relevant red flags. The institution may also rely on the analysis it used earlier to determine the residual risk. Similarly, with regard to the detection of new red flags the

depository institution has determined are relevant, the depository institution should be able to rely on its earlier analysis in completing Columns J or/and K that concluded which new red flags are relevant to the institution and its action plan, which includes controls to detect red flags.

In other words, the red flags identified as relevant will have with them associated controls that will detect their presence. Between the current controls accounted for in the inventory (Column E of the worksheet) and the controls necessary to detect any additional red flags added as a result of the gap analysis and recorded in the institution's action plan, the depository institution will have the information necessary to describe its coverage of this element of its Identity Theft Prevention Program.



## Responding When Red Flags are Detected

The third of the four key elements of an Identity Theft Fraud Prevention Program required by Section \_\_90(d) of the Regulation is to have reasonable policies and procedures to “*respond appropriately to any red flags that are detected.*” (See Section One, pages 8 and 11.) The response should match the type of red flag detected.

In order to draft this part of the Identity Theft Prevention Program, the depository institution should be able to rely on Column G of the worksheet which contains descriptions of the responses the depository institution currently uses when red flags are detected. It may also rely on analysis it used earlier to determine the residual risk. Similarly, with regard to appropriate responses to new red flags that the depository institution has determined are relevant, the depository institution should be able to rely on Column K, which outlines its action plan and which should include responses when red flags are detected.

Section IV of the Guidelines to the Regulation provides a range of possible responses that depository institutions may pursue as appropriate responses when red flags are identified. The list of possible responses provided in the Guidelines when red flags are detected includes:

- Monitoring the account for evidence of identity theft;
- Contacting the customer;
- Changing passwords, PINs, etc., that allow access to the account;

- Changing the account number;
- Not opening a new covered account;
- Closing an existing covered account;
- Not attempting to collect on a covered account or not attempting to sell a covered account to a debt collector;
- Notifying law enforcement; and
- Determining that no response is needed.

Other responses include crediting the customer’s account for unauthorized card transactions pursuant to requirements under Regulation Z (Truth in Lending Act) and Regulation E (Electronic Fund Transfer Act).

Depository institutions should review their written program to determine if the responses to the red flags match the risk exposure. For example, merely monitoring the account is not adequate in cases where customers report that they did not open an account. The account should be closed. Conversely, if a red flag alert is triggered because of sudden, high dollar volume transactions on a credit card account, it would be more appropriate to contact the customer to determine if the purchases were authorized than to close the account.

Once again, the depository institution should leverage existing policies and procedures. In addition, it should be able to rely on its earlier analysis, as reflected in Column G of the worksheet, to document existing responses. Responses to additional red flags identified as relevant should be reflected in Column K’s Action Plan.

### Key Elements of the Identity Theft Prevention Program

1. Identify red flags associated with covered accounts;
2. Detect red flags that were incorporated into the Program;
3. Respond to red flags that have been detected; and,
4. Update the Program to reflect changing risk conditions.

## Overseeing Service Providers

Depository institutions are required to oversee service provider arrangements to ensure that they have in place “reasonable policies and procedures designed to detect, prevent, and mitigate the risk of identity theft.” Examples of service providers include, but are not limited to, check vendors, credit card vendors, and third party data processors and check processors. Depository institutions should, for example, ensure that contracts provide that

the service provider agrees to have policies and procedures in place and either report the detection of red flags to the depository institution or take appropriate steps to prevent or mitigate identity theft. Audits could also verify compliance. For example, depository institutions might review their contracts with check vendors and the vendors’ responsibilities when checks are ordered with an address different from the address on record.

## Training Staff

The Regulation/Guidelines require that depository institutions train staff “as necessary” to implement effectively the Identity Theft Prevention Program. Thus, only relevant staff need be trained. In addition, staff already trained as part of anti-fraud prevention efforts, CIP, Bank Secrecy Act, data protection policies, privacy policies, and other reasons, need not be retrained except “as necessary.”

The depository institution could begin with an inventory of its current training programs and policies for fraud and identity theft prevention, CIP, BSA, data protection,

and privacy. The appropriate structure and channels for education will vary depending on the institution and its resources. One option, online training, is efficient. Another option, in-person meetings, is more interactive. Conference calls and e-mails to appropriate staff are also possibilities. Materials and programs may be general for enterprise-wide dispersion or customized, as appropriate, based on the target employees’ position and responsibilities. For example, a depository institution may consider a matrix which would be customized for each line of business.

## Administering the Program

Once the Identity Theft Prevention Program is complete, the depository institution must ensure its administration. It should be clear who is in charge and the source and extent of that person’s authority. Depository institutions should ensure that the Identity Theft Prevention Program is incorporated into their audit process and their general compliance risk assessment updates. Institutions should also ensure that staff training policies and programs are

up-to-date. Plans should be in place to ensure that, as appropriate, changes are made to identity theft prevention policies and procedures and incorporated into the Identity Theft Prevention Program. Finally, procedures should ensure that annual reports regarding compliance with the Regulation are drafted and delivered to the board, board committee, or designated person at the level of senior management.





## Documenting and Updating the Identity Theft Prevention Program

The formal Identity Theft Prevention Program should document the depository institution's existing policies and procedures to demonstrate compliance with the Regulation. In some cases, it may be a matter of referencing existing policies and practices. For example, if the depository institution is relying on its CIP policies and procedures as the basis for meeting portions of the requirements for the Identity Theft Prevention Program, it could simply reference those policies. This will be especially helpful for those existing procedures that cut across many product types and will save the institution the time and expense of re-documenting existing policies. However, depository institutions should have copies of their actual policies and procedures readily available to examiners. The worksheets and spreadsheets and other analysis should also be helpful for documenting compliance.

The Identity Theft Prevention Program must be updated as necessary to reflect changing risks to customers and the depository institution. In addition, the depository institution must "periodically determine whether it offers or maintains any covered accounts."

Section V of the Guidelines provides five examples of factors that may suggest the need to update a depository institution's Identity Theft Prevention Program:

- The experiences of the depository institution;
- Changes in identity theft methods;
- Changes in methods to detect, prevent, or mitigate identity theft;
- Changes in accounts offered by the bank; and
- Changes to the business arrangements of the bank including mergers, acquisitions, alliances, etc.

The Identity Theft Prevention Program should outline when the document will be updated and under what circumstances the institution will review controls and policies based on changing or new identify theft risks. A depository institution would typically adjust policies and procedures in response to new identity threats as quickly as possible and incorporate appropriate controls when it develops or offers new products or services. For example, if a new super computer virus is created that preys on depository institution customers, the depository institution should have a mechanism to allow it to respond quickly.

It is not necessary, however, to update the Identity Theft Program each time a new fraud surfaces or new control is implemented. The Supplementary Information to the Regulation makes clear that depository institutions are not required to immediately or continuously update their programs. The federal agencies concluded that requiring depository institutions "to immediately and continuously update their Programs would be overly burdensome." In addition, it would potentially slow a depository institution's ability to respond nimbly and quickly when a new type of fraud pops up. Changes to the program should certainly be reflected in the required annual report. For example, after new red flags are fully implemented, they would be reflected in the Identity Theft Prevention Program during its next update.

### No Requirement to Immediately or Continuously Update Programs

The Supplementary Information to the Regulation makes clear that depository institutions are not required to immediately or continuously update their programs. It would potentially slow a depository institution's ability to respond nimbly and quickly when a new type of fraud pops up.

### Key Elements of the Identity Theft Prevention Program

1. Identify red flags associated with covered accounts;
2. Detect red flags that were incorporated into the Program;
3. Respond to red flags that have been detected; and,
4. Update the Program to reflect changing risk conditions.



For documentation purposes, it may be a matter of referencing existing policies and practices. For example, if the depository institution is relying on its CIP policies and procedures as the basis for meeting portions of the requirements for the Identity Theft Prevention Program, it could simply reference those policies.

## Submitting Annual Reports

Under the Guidelines, at least annually, the staff person assigned responsibility for implementation of the Identity Theft Prevention Program (the administrator) must report on compliance with the Regulation to the board of directors, an appropriate committee of the board, or a designated employee at the level of senior management. The report should address material matters related to the Identity Theft Prevention Program and evaluate issues such as:

- Effectiveness of the policies and procedures in addressing the risk of identity theft;
- Service provider arrangements;
- Significant incidents involving identity theft and management's response; and
- Recommendations for material changes to the Identity Theft Prevention Program.

## Conclusion

This section offers just one approach to creating an Identity Theft Prevention Program. Depository institutions may modify it as appropriate and useful or determine that a different approach is more suitable. The model worksheet provided may be a useful tool to assist depository institutions in drafting their Identity Theft Prevention Program. Institutions should take advantage of their existing systems and policies and incorporate them into the Identity Theft Prevention Program. It is also

important not to overlook aspects of the Regulation, such as staff training, revisions to the Identity Theft Prevention Program as appropriate, annual reports about compliance, and board or board committee awareness of the Identity Theft Prevention Program. Depository institutions should also keep in mind that the Identity Theft Prevention Program is not a single event, but a continuous and evolving project that benefits and protects the depository institution and its customers.

## SECTION THREE

# Identity Theft Red Flag Analysis Model Worksheets

The following worksheets are available  
as Excel spreadsheets on ABA's Web site:



[Example 1: Red Flag Analysis Worksheet](#)

[Example 2: Sample Consumer Checking Account Worksheet](#)

**EXAMPLE 1: Red Flag Analysis Worksheet**

A Lines of Business	B Type of Account Product	C Risk Factors	D Past ID Theft Experience	E Existing Controls to Detect Red Flags	F Existing Red Flags	
<i>Deposits</i>	<i>E.g. Consumer Checking</i>	<u>Account Opening</u> Means				
		Frequency/Volume				
		<u>Account Access</u> Means				
		Frequency/Volume				
	<i>E.g. Consumer Savings</i>	<u>Account Opening</u> Means				
		Frequency/Volume				
<u>Account Access</u> Means						
Frequency/Volume						
<i>Credit</i>	<i>E.g. Consumer Credit Cards</i>	<u>Account Opening</u> Means				
		Frequency/Volume				
		<u>Account Access</u> Means				
		Frequency/Volume				

G Response to Red Flags	H Residual Risk Rate	I Account Covered? Yes - (Automatically) Yes - (Risk-based) No - (Risk-based)	J Gap Analysis	K Action Plan	L Comments

**EXAMPLE 2: Sample Consumer Checking Account Worksheet**

A Lines of Business	B Type of Account Product	C Risk Factors	D Past ID Theft Experience*	E Existing Controls to Detect Red Flags	F Existing Red Flags
<i>Deposits</i>	<i>E.g. Consumer Checking</i>	<p><b><u>Account Opening</u></b></p> <p><u>Means</u></p> <ul style="list-style-type: none"> <li>• In person only</li> </ul> <p><u>Frequency/Volume</u></p> <ul style="list-style-type: none"> <li>• Number of accounts opened per month/year</li> </ul>	<p>Number of accounts opened fraudulently low.</p> <p>Attempts to open accounts using false identification documents or personal information have been detected, but accounts not opened.</p>	CIP	Identifying information is inconsistent with other sources.
		<p><b><u>Account Access</u></b></p> <p><u>Means</u></p> <ul style="list-style-type: none"> <li>• Checks</li> <li>• Debit card</li> <li>• Online access</li> </ul> <p><u>Frequency/Volume</u></p> <ul style="list-style-type: none"> <li>• Volume of transactions is X</li> </ul>	<p>Data breach or card skimming caused substantial losses in 200X</p> <p>Series of successful account hijackings by insider resulted in substantial losses to depository institutions</p> <p>Multiple unsuccessful attempts to log-in with wrong password triggered contacts to customer</p> <p>Losses from checks with forged signatures and stolen and counterfeit checks drawn on customer accounts is low</p> <p>* Institution may consider noting or referencing its fraud statistics when describing identity theft experience</p>	<p>Multifactor authentication for Internet transactions.</p> <p>Monitor for unusual account activity etc.</p>	<p>Failed multiple attempts to access accounts</p> <p>Unusual account activity detected</p>

G  Response to Red Flags	H  Residual Risk Rate	I  Account Covered? Yes - (Automatically) Yes - (Risk-based) No - (Risk-based)	J  Gap Analysis	K  Action Plan	L  Comments
Request additional information. If inadequate, account not opened.	Low	Yes (automatically)	No		No additional measures necessary for account opening.
Account frozen after 5 unsuccessful log on attempts until challenge questions answered.  Customer contacted to verify transactions.	Medium	Yes (automatically)	Yes	Upon learning of databreach of critical debit card information by merchant or that customer cards have been skimmed, monitor compromised accounts or reissue cards, as appropriate  Monitor for unusual debit card activity	





# APPENDIX A

## **Supplement A to the Guidelines of the Regulation:**

### **List of 26 Examples of Red Flags**

## **Supplement A to Appendix J of the Identity Theft Red Flag Regulation**

In addition to incorporating Red Flags from the sources recommended in Section II.b of the Guidelines in Appendix J of this part, each financial institution or creditor may consider incorporating into its Program Red Flags, whether singly or in combination, from the following illustrative examples in connection with covered accounts:

### ***Alerts, Notifications or Warnings from a Consumer Reporting Agency***

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 § 334.82(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.

### ***Suspicious Documents***

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 does not match any address in the consumer report; or
- b. The Social Security Number (SSN) has not been issued, or is listed on the Social Security Administration's Death Master File.

11. Personal identifying information provided by the customer 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 date of birth.

12. 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 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.

13. 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.

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 new, additional, or replacement cards 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.



# APPENDIX B

## **Legal Memorandum on Coverage of the Regulation**

MEMORANDUM

---

TO: American Bankers Association

FROM: Oliver I. Ireland  
Morrison & Foerster LLP

DATE: February 22, 2008

RE: Coverage of the Identity Theft Red Flag Rules

---

You have asked for an analysis of the institutions and accounts covered under the Identity Theft Red Flag provisions (“Red Flag Rules”) of the rules that have been adopted by a number of federal regulatory agencies to implement the Fair and Accurate Credit Transactions Act of 2003 (“FACT Act”).<sup>1</sup> The Red Flag Rules are based on Section 615(e) of the Fair Credit Reporting Act (“FCRA”)<sup>2</sup> as added by section 114 of the FACT Act.

There are two ways that an organization may be covered by the Red Flag Rules. They are covered either if they are a financial institution or they are a creditor. The FCRA defines a financial institution as a state or national bank, state or federal savings association, mutual savings bank, or a state or federal credit union or any other person, that directly or indirectly, holds a transaction account (as defined in section 19(b) of the Federal Reserve Act) belonging to a consumer.<sup>3</sup> A creditor is defined by cross-reference to the Equal Credit Opportunity Act (“ECOA”) definition of creditor.<sup>4</sup> The ECOA definition of creditor is broad and includes “any person who regularly extends, renews, or continues credit; any person who regularly arranges for the extension, renewal or continuation of credit; or any assignee of an original creditor who participates in the decision to extend, renew, or continue credit.”<sup>5</sup> The definition of credit in the ECOA is also broad and means any “right granted by a creditor to a debtor to defer payment of debt or to incur debt and defer its payment or to purchase property or services and defer payment therefor.”<sup>6</sup> The definition of credit in the ECOA includes both consumer and business credit. The substance of these definitions is not changed by the Red Flag Rules, although the definition of creditor includes a number of illustrations of that definition.

---

<sup>1</sup> See 12 C.F.R. § 41.90. Citations in this memorandum are to the rules of the Comptroller of the Currency. The Board of Governors of the Federal Reserve System, the Office of the Federal Deposit Insurance Corporation, the Office of Thrift Supervision and the Federal Trade Commission have adopted virtually identical rules.

<sup>2</sup> 15 U.S.C. § 1681m(e).

<sup>3</sup> 15 U.S.C. § 1681a(f).

<sup>4</sup> See, 15 U.S.C. § 1681a(r)(5).

<sup>5</sup> 15 U.S.C. § 1691a(e).

<sup>6</sup> 15 U.S.C. § 1691a(d).



The definition of financial institution includes any bank or savings association. The definition of financial institution also includes any other person who offers insured consumer deposit accounts with unlimited check writing or transaction capabilities, such as consumer NOW accounts. The definition of financial institution probably does not include the vast majority of nonbank subsidiaries or affiliates of these institutions, even if the subsidiaries or affiliates offer checking services to their customers. For example, a broker-dealer that offers its customers the ability to draw checks on their brokerage accounts is probably not offering its customers transaction accounts, at least as defined by the Board of Governors of the Federal Reserve System in Regulation D.<sup>7</sup> However, a broker-dealer may be covered by this definition if it is offering checking against a deposit account at a bank that it holds for its customers as agent.

On the other hand, the broad definition of creditor would include many bank subsidiaries and affiliates. For example, while in most cases a broker-dealer is not a “financial institution” for purposes of the Red Flag Rules, most broker-dealers offer a form of credit (e.g. margin accounts) and thus would be a creditor under the rule and required to have an Identity Theft Prevention Program for any “covered accounts” they offer. The same would be true for a mortgage lending or finance company subsidiary or affiliate.<sup>8</sup> Further, the ECOA definition covers incidental credit, as well as more formal extensions of credit, such as those covered by the Truth in Lending Act. For example, the ECOA definition of credit would include circumstances where a service is provided or an asset purchased, but payment was deferred beyond the time of the delivery of the service or the asset, such as a cell phone or utility account.

Under the Red Flag Rules, once an institution is covered by the Red Flag Rules as a financial institution or a creditor, the Rules apply to any “covered accounts” it offers. An “account” is a continuing relationship between a person and a financial institution or creditor to obtain a product or service for personal, family, household, or business purposes. Accounts include extensions of credit and deposit accounts.<sup>9</sup> A “covered account” is (1) an account “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” or (2) any other account for which there is a reasonably foreseeable risk to customers or the financial institution or creditor “from identity theft, including financial, operational, compliance, reputation, or litigation risks.”<sup>10</sup>

It is important to recognize that covered accounts are not limited to transactions that would cause an entity to become a creditor or a financial institution. For example, the

<sup>7</sup> Accounts at broker-dealers have different legal characteristics than bank deposit accounts and the Board of Governors of the Federal Reserve System has never addressed how these accounts might be treated under Section 19(b).

<sup>8</sup> Although the rules implementing the ECOA provide an exemption for securities margin credit (12 C.F.R. § 202.3(b)), this exemption is not expressly incorporated into the Red Flag Rules, which refer to the statutory definition but not the regulation.

<sup>9</sup> 12 C.F.R. § 41.90(b)(1).

<sup>10</sup> 12 C.F.R. § 41.90(b)(3).

definition of “covered account” could include saving deposits that are not “transaction accounts.” It also would include custody relationships that would not be either a “transaction account” under the Federal Reserve Act or involve credit. In this regard, a broker-dealer that qualifies as a creditor because it provides for arranged margin credit would be covered with respect to accounts that did not provide for margin credit, such as a cash account. Similarly, an investment advisor that neither provided nor arranged credit nor had custody of its customers’ assets would probably not be covered as a financial institution or a creditor. However, if the investment advisor was a creditor because it arranged credit for some of its customers, all of its accounts would likely be covered.<sup>11</sup> Finally, the Red Flag Rules include business accounts as covered accounts that may pose a reasonably foreseeable risk.<sup>12</sup>

---

<sup>11</sup> In a number of cases identity theft has been a problem in securities transactions and therefore securities accounts probably pose reasonably foreseeable risk.

<sup>12</sup> See 72 Fed. Reg. 63,718, 63,721 (Nov. 9, 2007).

# APPENDIX C

## **PowerPoint Summary of the Regulation**

1

ABA American Bankers Association

## Summary of Identity Theft Prevention Program Regulation

Identity Theft Red Flags

aba.com | 1 800 BANKERS

2

## Identity Theft Prevention Program

- Basics
  - Written program
  - Mandatory compliance date: November 1, 2008
  - "Designed to detect, prevent, and mitigate identity theft" in connection with account opening or existing accounts
- "Appropriate to the size and complexity" of the bank and the "nature and scope of its activities"

aba.com | 1 800 BANKERS

ABA American Bankers Association

See pages 1, 8, 19.

3

## Identity Theft Prevention Program

- Board Involvement:
  - Approval of initial written program
  - Receipt of annual reports
- Board, Board Committee or senior management may assign actual implementation

aba.com | 1 800 BANKERS

ABA American Bankers Association

See pages 4, 12, 21.

4

## Responsibilities

Board or Board Committee	Approve: Initial Program
Board, Board Committee or "designated employee at level of senior management"	<ul style="list-style-type: none"> <li>Involved in oversight</li> <li>Assign responsibility</li> <li>Review annual reports</li> <li>Approve material changes</li> </ul>
Administrator	<ul style="list-style-type: none"> <li>Responsible for development, etc.</li> <li>Report annually to Board, Board Committee or designated employee</li> </ul>

aba.com | 1 800 BANKERS

ABA American Bankers Association

See pages 4, 12, 21.

5

## Identity Theft Prevention Program

- Banks will be able to incorporate existing policies and programs into Program: e.g.,
  - Customer Identification Procedures ("CIP")
  - Data protection
  - Fraud prevention
  - Privacy
- Banks should leverage existing policies

aba.com | 1 800 BANKERS

ABA American Bankers Association

See pages 8, 24, 26.

6

## Definition of Identity Theft

- Broadly defined
- Includes not only new account fraud and account take-over, but unauthorized transactions of existing accounts

aba.com | 1 800 BANKERS

ABA American Bankers Association

See page 5.

## Covered Accounts

- Most consumer deposit and credit accounts
- Potentially:
  - Small business and other accounts
  - Brokerage, investment advisory accounts, custodial accounts if there is a “foreseeable risk” to customers or bank from identity theft

7

aba.com | 1 800 BANKERS



See pages 6, 27.

## Covered Accounts

- Includes only “continuing relationships”
- Single transactions with noncustomers are excluded, for example

8

aba.com | 1 800 BANKERS



See pages 6, 27.

## Elements of Program

1. Identify and incorporate relevant red flags that indicate possible identity theft
2. Set up controls to detect relevant red flags
3. Respond appropriately when red flags are detected
4. Update program

9

aba.com | 1 800 BANKERS



See pages 8, 29.

## Identity Theft Prevention Program

- Regulation and Guidelines provide information and examples related to:
  1. Risk factors to determine relevant red flags
  2. Sources to create lists of possible red flags
  3. Controls to detect relevant red flags
  4. Responses when red flags are detected

10

aba.com | 1 800 BANKERS



See pages 9, 10, 11, 23, 24.

## Sources of Red Flags

- Incidents of identity theft
- Methods bank has identified that reflect changes to identity theft risk
- Applicable supervisory guidance

11

aba.com | 1 800 BANKERS



See pages 10, 30.

## Detect Red Flags

- Requirement is related to controls
- Integrate existing policies:
  - CIP
  - Data protection
  - Fraud protection policies and procedures
  - Privacy policies and procedures

12

aba.com | 1 800 BANKERS



See pages 11, 24, 32.

**13** **Prevent and Mitigate Identity Theft**


- Program must have “appropriate responses” “commensurate with the degree of risk posed”
- Response may vary based on size and complexity of the institution
- Aggravating factors might heighten risk of identity theft

aba.com | 1 800 BANKERS 

See pages 11, 25, 33.

**14** **Updating Program**


- Program must be updated “periodically” but not immediately or continuously
- Factors to consider in update:
  - Bank’s identity theft experience
  - Changes in methods of identity theft
  - Changes in methods to detect and respond
  - Changes in types of accounts and services offered
  - Changes in business, including mergers, acquisitions, etc.

aba.com | 1 800 BANKERS 

See pages 12, 35.

**15** **Staff Training**

- Staff must be trained “as necessary” to implement effectively the Program
- Training related to existing policies and procedures need not be retrained

aba.com | 1 800 BANKERS 

See pages 12, 34.

**16** **Oversight Service Providers**


- Banks must ensure that service providers have in place “reasonable policies and procedures designed to detect, prevent, and mitigate the risk of identity theft” with regard to the services they provide

aba.com | 1 800 BANKERS 

See pages 13, 34.

**17** **Annual Reports**

- Employee assigned responsibility for Program implementation must provide annual report to Board, Board Committee or designated employee at level of senior management

aba.com | 1 800 BANKERS 

See pages 12, 36.



