

ID Theft Responsibilities – FACTA Red Flag Guidance

October 8, 2008

FDIC Technology Supervision Branch

ID Theft Responsibilities

FACTA Red Flag Guidance

FDIC Dallas Regional Office
October 8, 2008



FDIC Technology Supervision Branch

Agenda

- Background
- Overview of regulation & guidelines
- Exam procedures
- What examiners will be looking for
- Misconceptions/Questions



FDIC Technology Supervision Branch

Background

Regulation & guidelines implement sections 114 & 315 of FACT Act of 2003

Enacted to help prevent ID theft, improve resolution of consumer disputes, and improve accuracy of consumer records.

- Joint final rule published on 11/9/07
- Effective 1/1/08
- Compliance by 11/1/08



ID Theft Responsibilities – FACTA Red Flag Guidance

October 8, 2008

 Technology Supervision Branch

Overview

Regulation requires 3 things:

- A written ID theft prevention program (334.90)
- Verification of consumer identity before use of a consumer report, when user receives notice of address discrepancy (334.82)
- Validation of change of address requests before issuing new cards (334.91)



 Technology Supervision Branch

Overview

Federal Register notice has 3 parts:

- Regulation (covers all 3 provisions)
- Guidelines (red flags only)
- Supplement to guidelines (red flags only)



 Technology Supervision Branch

Red Flags Overview

Program must be designed to detect, prevent, and mitigate identity theft in connection with **“covered accounts”**

Appropriate to size & complexity of the FI and nature & scope of business

Regulation does not require use of automated systems

Board of Directors must approve initial program



ID Theft Responsibilities – FACTA Red Flag Guidance

October 8, 2008

 Technology Supervision Branch

Identification of Covered Accounts

Identify covered accounts:

- All consumer transactional accounts covered
- Any other accounts that pose reasonably foreseeable risk of ID theft to customer or bank



 Technology Supervision Branch

Business Accounts?

FI must decide whether to cover business accounts, based on:

- Methods for opening accounts
- Methods for accessing accounts
- Previous experiences with ID theft



 Technology Supervision Branch

Detect, Prevent & Mitigate

Program must be able to **detect** red flags in connection with any covered account

FI must respond appropriately to detected red flags to **prevent** ID theft or **mitigate** damages to FI and customers

- Guidelines list 9 possible responses as examples



ID Theft Responsibilities – FACTA Red Flag Guidance

October 8, 2008

FDIC Technology Supervision Branch

Address Discrepancies

Bank that receive a notice of address discrepancy from a CRA, must form a reasonable belief that report relates to consumer about whom it has been requested

- If not, agencies expect that bank will not use the consumer report



FDIC Technology Supervision Branch

Address Discrepancies

Bank can verify identity by comparing information in consumer report with:

- Information bank uses to verify identity in accordance with CIP;
- Information in its own records; or
- Information obtained from 3rd party

- Bank can verify information with consumer directly



FDIC Technology Supervision Branch

Address Discrepancies

If bank regularly & in ordinary course of business furnishes information to CRA, then it must furnish confirmed address to CRA when:

- It forms reasonable belief that report relates to consumer, and
- It establishes a new relationship with that consumer



ID Theft Responsibilities – FACTA Red Flag Guidance

October 8, 2008

FDIC Technology Supervision Branch

Change of Address Requests

Bank that issues credit or debit cards must assess the validity of change of address requests if, within a short time thereafter, it receives request for new or replacement card

- Request can be from consumer or USPS
- Applies to credit, debit and payroll cards
- Does not apply to gift cards or other prepaid cards



FDIC Technology Supervision Branch

Change of Address Requests

Bank can choose to verify address change either:

- When it receives request for new card; or
- When it receives notice of address change

Many banks commented that it may be easier to simply verify all address changes when received



FDIC Technology Supervision Branch

Principles-based Regulation

Red flags is an excellent example of principles-based regulation

FIs get more flexibility, but must be more creative

Creates more uncertainty about whether FI is in compliance



ID Theft Responsibilities – FACTA Red Flag Guidance

October 8, 2008

FDIC Technology Supervision Branch

Importance of Collaboration

An interdisciplinary* approach to compliance is necessary and desirable

Examiners will be looking for this, evidence of an effective Program

* E.g., compliance, fraud prevention, IT security, business lines should be working together



FDIC Technology Supervision Branch

Examination Procedures

Expect to be published soon

Very high level, not a roadmap to compliance

Each agency may use different types of examiners to assess compliance

FDIC:

- Risk Management examiners will assess compliance with red flags
- Compliance examiners will assess compliance with address discrepancy and change of address



FDIC Technology Supervision Branch

What Examiners Will Be Looking For

During first exam, examiners will be looking for "basic blocking and tackling"

Regulation requires more than just documenting existing fraud prevention efforts, although they may form a significant part of your Program

Regulators don't expect perfect Programs



ID Theft Responsibilities – FACTA Red Flag Guidance October 8, 2008

 Technology Supervision Branch

What Examiners Will Be Looking For

A written, comprehensive Program
Thorough risk assessment, including:
– Accurate identification of covered accounts
Evidence that written procedures actually work, i.e., detected red flags are responded to appropriately
Program must span business silos
Board of Directors' approval



 Technology Supervision Branch

Enforcement

Compliance is expected by 11/1/08
Expect an approach similar to what was taken with the authentication guidance
Examiners will be looking for a good faith effort to comply, including:
– Timely commencement of efforts
– Involvement of appropriate/sufficient staff
– Cross discipline cooperation
– Realistic timeframes for completion



 Technology Supervision Branch

Correcting Misconceptions

Business/commercial accounts may be covered, if risk of ID theft is reasonably foreseeable (look to past experiences)
In most cases, CDs are not covered because they are not transaction accounts
FIs may choose to treat all accounts as covered, because it may be cheaper/easier than delineating



ID Theft Responsibilities – FACTA Red Flag Guidance
October 8, 2008

FDIC Technology Supervision Branch

Questions (Red Flags)

Q. After the Program is implemented, what type of follow-up is necessary?

A. Update the program on a regular basis and make annual reports to the Board, including:

- Effectiveness of program
- Incidents of identity theft experienced
- Changes to program to address deficiencies



FDIC Technology Supervision Branch

Questions

Q. Are service providers those entities that provide red flag identification services?

A. No, they are entities that provide any service directly to the FI that involves covered accounts, e.g., core banking system providers



FDIC Technology Supervision Branch

Questions

Q. Is there a template for the Program and/or the annual report to the Board

A. No. Generally, agencies are not fond of templates since they encourage FIs to just fill in the blanks and programs should differ among FIs



ID Theft Responsibilities – FACTA Red Flag Guidance
October 8, 2008

FDIC Technology Supervision Branch

Questions

Q. Does the entire staff of the FI have to be trained?

A. No, staff should be trained “as necessary” depending on their specific job responsibilities.



FDIC Technology Supervision Branch

Questions

Q. Does the person responsible for the Program have to be approved by the Board?

A. There is no such explicit requirement in the regulation.



FDIC Technology Supervision Branch

Questions (Address Discrepancy)

Q. Does user have to “confirm” verified address to CRA or just report back?

A. Agency staffs are of the opinion that regulation does not require confirmation, but we understand that reporting system is being updated to permit it & we encourage FIs to take advantage of this feature.



ID Theft Responsibilities – FACTA Red Flag Guidance
October 8, 2008

FDIC Technology Supervision Branch

Questions

Q. Are agencies planning to publish FAQs?

A. Agency staffs are discussing, but no final decision has been made.



FDIC Technology Supervision Branch

Questions?



FDIC Technology Supervision Branch

Contacts

For any questions related to the material presented in this Regulatory Conference Call, you may contact via email:

Risk Management Questions
James Brignac
JBrignac@fdic.gov

Compliance Questions
Luke Wong
LWong@fdic.gov


