Comptroller of the Currency
Administrator of National Banks

Executive Summary

OCC Web and Telephone Seminar
June 17, 2008

The FACT Act: An Overview of the Final Rulemaking on Identity Theft Red Flags and Address Discrepancies

Speakers:

John C. Dugan
Ann F. Jaedicke
Deborah Katz
Andra Shuster
Paul E. Utterback

Following is an executive summary of this OCC Web/Telephone seminar covering:

Identity theft red flag rules.

Identity theft red flag guidelines.

Special rule for credit and debit card issuers.

Rule on address discrepancies.

Red flags implementation issues.

The FACT Act: An Overview of the Final Rulemaking on Identity Theft Red Flags and Address Discrepancies

Speakers: **John C. Dugan**, Comptroller of the Currency
Ann F. Jaedicke, Deputy Comptroller for Compliance
Deborah Katz, Senior Counsel, Legislative and Regulatory Activities Division
Andra Shuster, Special Counsel, Legislative and Regulatory Activities Division
Paul E. Utterback, National Bank Examiner & Senior Compliance Specialist, Compliance Policy Division

Overview

The recent rulemaking—implementing Sections 114 and 315 of the Fair and Accurate Credit Transactions Act of 2003 (the "FACT Act")—requires financial institutions and creditors to identify, detect, and respond appropriately to "red flags" suggesting possible identity theft. The rulemaking also contains certain requirements for users of consumer reports that receive notices of address discrepancy from a nationwide consumer reporting agency.

The red flag rules are more than a set of guidelines. They include specific regulations with which all institutions and creditors that offer "covered" accounts (consumer transaction accounts and any other accounts for which there is a reasonably foreseeable risk of identity theft) must comply by November 1, 2008. The regulations require these institutions and creditors to develop written identity theft prevention programs that effectively detect, prevent, and mitigate the risk of identity theft, employing measures appropriate to the size and scope of the institution or creditor's operations. Unlike the Patriot Act's customer identification rules, which apply only to account openings, these new rules also apply to existing covered accounts.

Accordingly, every financial institution and creditor with covered accounts must devote the time and resources to ensure organization-wide understanding of the new regulations, to develop and implement identity theft prevention programs, and to become fully compliant before November. An implementation checklist can help financial institutions and creditors ensure that the programs they develop are both effective and compliant.

Context

OCC staff involved in writing the final rulemaking that implements Sections 114 and 315 of the FACT Act explained what financial institutions and creditors need to know and do to comply with these new regulations. Specifically, they discussed the new red flag rules and guidelines implementing section 114—including special rules for card issuers—and provided implementation tips and examples of red flags. In addition, they discussed the address discrepancy rules implementing section 315. A Q&A session addressed numerous situation-specific questions from participants.

Background

On December 4, 2003, President Bush signed into law the Fair and Accurate Credit Transactions (FACT) Act, which amended the Fair Credit Reporting Act (FCRA). On November 9, 2007, a final rulemaking was published that implements two sections of the FACT Act:

- *Section 114,* directing the federal banking agencies jointly with the Federal Trade Commission to prescribe identity theft regulations and guidelines for financial institutions and creditors and a special rule for card issuers.
- *Section 315,* requiring these agencies to issue regulations for users of consumer reports that receive notices of address discrepancy from a nationwide consumer reporting agency.

Financial institutions and creditors with covered accounts must be in full compliance by November 1, 2008. After that date, any compliance examination may include a review of compliance with the red flag rulemaking.

The six agencies that collaborated on the regulations are: Comptroller of the Currency (OCC), Federal Deposit Insurance Corporation (FDIC), Federal Reserve Board (FRB), Office of Thrift Supervision (OTS), National Credit Union (NCU), and Federal Trade Commission (FTC). The agencies expect to issue FAQs on the Section 114 and 315 regulations to address some of the questions they have received.

Key Learnings

- **Important definitions govern how the identity theft red flag rules operate.**

  The rules implementing section 114 of the FACT Act apply to "financial institutions" and "creditors" as defined in the FCRA. Specifically, the new rules apply to:

  - *"Financial institutions"* including a bank, savings association, creditor, union or any other entity that directly or indirectly holds a transaction account (as defined in Section 19B of the Federal Reserve Act) belonging to a consumer; and
  - *"Creditors"* including any person who extends, renews, or continues credit, such as a telecommunication company, utility, automobile dealership, broker that permits the purchase of stock on margin, and insurer.

  Banks, savings associations, federal credit unions, branches and agencies of foreign banks, and subsidiaries of these entities (except for subsidiaries that are functionally regulated, such as broker-dealers) are subject to the rules issued by the bank regulatory agencies. The FTC's rules apply to state-chartered credit unions, and all other creditors.

  But importantly, the rules apply only to financial institutions and creditors with *"covered accounts,"* meaning consumer-owned accounts designed to permit multiple payments or transactions, such as checking accounts, mortgage loans, and credit cards,

and any other account for which there is a reasonably foreseeable risk of identity theft to customers or the safety and soundness of the financial institution or creditor. (For simplicity's sake, "financial institutions" and "creditors" with "covered accounts" are referred to henceforth as *"banks."*)

> *"Only financial institutions and creditors that have covered accounts need to have (an identity theft) program. Because all national banks have covered accounts, they need to have a program."*
> —Deborah Katz

Moreover, the programs, procedures, and processes that banks develop to comply with the new regulations need apply only to covered accounts. Each bank must determine which of its accounts qualify as "covered."

Other definitions for the purposes of the red flag rules:

"Identity theft" refers to fraud committed or attempted using the identifying information of another person without authority, including name, social security number, driver's license number, and unique biometric data such as a fingerprint. Identity theft includes:

- Creation of a fictitious identity using any single piece of information belonging to a real person (a growing problem, sometimes called "synthetic identity theft").
- Use of someone else's identifying information to open new covered accounts or take over existing accounts.

"Red flags" are patterns, practices, and specific forms of activity that indicate the possible existence of identity theft.

- **Banks must have a formal identity theft prevention program to identify, detect, and respond to identity theft red flags.**

The new regulations require banks to implement a written identity theft prevention program to detect, prevent, and mitigate the risk of identity theft in connection with an existing covered account or the opening of a covered account. The program must include policies and procedures to:

- Identify relevant red flags.
- Detect red flags that are a part of the program.
- Respond appropriately to any red flags detected.
- Ensure that the program is updated periodically to address changing risks.

> *"A bank has got to have policies and procedures to identify red flags relevant to its covered accounts . . . in other words, a method to choose the red flags it will look for."*
> —Deborah Katz

The regulations also stipulate certain program administrative requirements. Specifically, banks must:

- Obtain approval of the initial program by the board of directors or a board committee.
- Ensure oversight of the program.
- Train appropriate staff.
- Oversee service provider arrangements—a requirement that pertains whenever a bank engages a service provider to perform an activity in connection with covered accounts.

- **Banks must determine the appropriate red flag guidelines to incorporate into their identity theft programs.**

Besides regulations, Congress mandated that the rulemaking include identity theft guidelines to assist banks in developing and implementing their programs.

If a bank determines that a particular guideline is inappropriate for its circumstances, it does not need to include that guideline in its program—provided that the bank can ensure its program effectively detects, prevents, and mitigates the risk of identity theft and fulfills all red flag rule requirements.

> *"Each bank will have to account for the effectiveness of a program appropriate to its size and complexity and the nature and scope of its activities."*
> —Andra Shuster

The guidelines have seven sections that can be summarized as follows:

1. *Incorporating existing policies / procedures.* A bank's existing policies and procedures to control identity theft risks are fine to incorporate into its new program.
2. *Identifying red flags.* To identify red flags representing identity theft risk, banks should consider: 1) the types of covered accounts it offers or maintains; 2) the methods it provides for opening and accessing covered accounts; and 3) its own previous experiences with identity theft. Sources of red flags can be derived from prior incidents, methods of theft, or supervisory guidance. Categories of red flags include alerts or warnings from consumer reporting agencies; presentation of suspicious documents or personal identifying information; unusual use related to a covered account; or notice from customers.

> *"A bank will need to ensure that its red flags are sufficient to address the potential risks of identity theft."*
> —Paul E. Utterback

3. *Instituting red flag detection procedures.* To detect red flags, banks should have procedures to verify the identity of people opening accounts, authenticate customer identification, monitor transactions, and verify the validity of address changes.
4. *Responding appropriately to red flags.* Appropriate responses to red flags are situation-dependent and should take into account aggravating circumstances (such as a data security breach). Possible responses include account monitoring, contacting the customer, changing account access passwords, closing and reopening accounts, refusing to open an account, not collecting on or selling an account, notifying law enforcement, or no response if the bank concludes that no fraud was intended or occurred.
5. *Periodic program updating.* Banks must periodically update their programs on timetables they deem to be appropriate in light of past experiences with identity theft, changes in either theft methods or detect-prevent-mitigate

methods, changes in types of accounts offered, and changes in business arrangements.

6. *Administering the program.* The bank's board, a board committee, or a senior employee should be involved in program oversight, development, implementation, and administration. Such involvement includes assigning specific responsibilities, reviewing staff-prepared compliance reports, and approving program changes in response to shifting risks. Staff responsible for implementation and administration should report all material matters to overseers at least annually. Program evaluations should cover such issues as service provider compliance with bank policies and procedures, program effectiveness in addressing risks, significant identity theft incidents/responses, and recommendations for change.
7. *Complying with* other *identity theft laws.* Banks should be mindful of the full spectrum of other legal requirements they must fulfill regarding identity theft (such as the possible need to file a Suspicious Activity Report).

- **An implementation checklist can help banks ensure effective and compliant identity theft prevention programs.**

  Banks need to be sure their new identity theft prevention programs both comply with the new regulations and are designed to best meet the intended objectives—detecting, preventing, and mitigating identity theft—given the institution's particular circumstances. Several implementation-related steps can help banks ensure that these goals are met:

  — Involve the board of directors and senior management.

  — Consider all business lines when assessing covered accounts.

  — Perform a comprehensive risk assessment for covered accounts and red flags.

  — Document policies, procedures, and controls in the written program.

  — Ensure that planned red flag responses are commensurate with the risk.

  — Explore technology applications to facilitate program policies and procedures.

  — Review arrangements with service providers to identify those that handle covered accounts and ensure they have implemented reasonable policies and procedures designed to detect, prevent, and mitigate the risk of identity theft.

  — Validate the written program and obtain board approval prior to the November 1, 2008, implementation deadline.

  — Complete reporting requirements annually.

  — Update the program periodically.

> *"Banks must conduct a risk assessment to identify accounts that pose a reasonably foreseeable risk of identity theft."*
> —Paul E. Utterback

- **The final rulemaking includes a special rule for debit and credit card issuers.**

  The FACT Act also required the agencies to prescribe a rule for a red flag that occurs in connection with debit and credit card accounts. The rule titled, "Duty of Card Issuers Regarding Changes of Address," provides that a card issuer must have reasonable policies and procedures to assess the validity of a change-of-address notice followed closely (within 30 days) by a request for an additional or replacement card on the same account.

  The rule generally provides that the card issuer cannot issue an additional or replacement card during the first thirty days following a notification of change of address until (1) the cardholder has been notified of the request and provided a reasonable means to report an incorrect address change, or (2) the card issuer assesses the validity of the address change through other means.

  The rule gives the card issuer the option of validating the address when it receives the notice of change of address before it receives a request for an additional or replacement card. The rule also provides that any written notice to the cardholder must be clear and conspicuous and provided separately from regular correspondence with the cardholder.

- **The Section 315 rulemaking implements a new regulation for responding to address discrepancies.**

  The FACT Act's Section 315 rulemaking concerns the duties of any entity that uses consumer reports, upon receiving a notice of address discrepancy from a nationwide consumer reporting agency (NCRA)—which currently include only Equifax, Experian, and TransUnion. In this situation, regulations require the report user to have reasonable policies and procedures to:

  — Establish a reasonable belief that the consumer report relates to the consumer about whom the report was requested, e.g., by comparing the consumer report information to other sources (such as an address on record with the user) or verifying the information with the consumer.

  — Furnish the NCRA with a reasonably confirmed address for the consumer when the report user: 1) forms a reasonable belief that the report relates to the consumer; 2) establishes a continuing relationship with the consumer; and 3) regularly furnishes information to the NCRA.

  — Provide the NCRA with the reasonably confirmed address to the NCRA as part of the information the user regularly furnishes for the reporting period in which it establishes a relationship with the consumer

Other Important Points

- **Read all about it.** Download the new regulations at http:/l.occ.treas.dov/fr/fedredister/723718.pdf.
- **Red flag rule enforcement.** The bank regulatory agencies may use the enforcement tools in 12 USC 1818 to enforce compliance with the red flag rules. State Attorneys General may act in response to rule violations only if there is no federal action pending. The FCRA does not provide a private right of

action for violations of Section 114 so consumers cannot sue banks for rule violations. Also, there are no criminal penalties for violations of the red flag rules.

- **Red Flag Example— A Non-Inclusive List.** As mandated by Congress, the rulemaking also includes illustrative examples of red flags. The 26-item list is not all-inclusive. Rather, these examples are intended to assist banks in their identification of red flags that are relevant to their own operations. The examples fall into the following five categories:

  1. Alerts / notifications / warnings from consumer reporting agencies or service providers.
  2. Presentation of suspicious documents, such as those appearing to have been altered.
  3. Presentation of suspicious personal identifying information, such as information inconsistent with other sources.
  4. Unusual use of, or activity in, a covered account, such as usage inconsistent with historical patterns.
  5. Notice from customers, victims of identity theft, or law enforcement agencies.

Speaker Biographies

John C. Dugan
Comptroller of the Currency

John C. Dugan was sworn in as the 29th Comptroller of the Currency on August 4, 2005.

The Comptroller of the Currency is the administrator of national banks and chief officer of the Office of the Comptroller of the Currency (OCC). The OCC supervises 1,900 federally chartered commercial banks and about 50 federal branches and agencies of foreign banks in the United States, comprising more than half the assets of the commercial banking system. The Comptroller also serves as a director of the Federal Deposit Insurance Corporation, the Federal Financial Institutions Examination Council, and the Neighborhood Reinvestment Corporation.

Prior to his appointment as Comptroller, Mr. Dugan was a partner at the law firm of Covington & Burling, where he chaired the firm's Financial Institutions Group. He specialized in banking and financial institution regulation. He also served as outside counsel to the ABA Securities Association.

He served at the Department of Treasury from 1989 to 1993 and was appointed assistant secretary for domestic finance in 1992. While at Treasury, Mr. Dugan had extensive responsibility for policy initiatives involving banks and financial institutions, including the savings and loan cleanup, Glass-Steagall and banking reform, and regulation of government-sponsored enterprises. In 1991, he oversaw a comprehensive study of the banking industry that formed the basis for the financial modernization legislation proposed by the administration of the first President Bush.

From 1985 to 1989, Mr. Dugan was minority counsel and minority general counsel for the U.S. Senate Committee on Banking, Housing, and Urban Affairs. There he advised the committee as it debated the Competitive Equality Banking Act of 1987, the Proxmire Financial Modernization Act of 1988, and the Financial Institutions Reform, Recovery, and Enforcement Act of 1989.

Among his professional and volunteer activities before becoming Comptroller, he served as a director of Minbanc, a charitable organization whose mission is to enhance professional and educational opportunities for minorities in the banking industry. He was also a member of the American Bar Association's committee on banking law, the Federal Bar Association's section of financial institutions and the economy, and the District of Columbia Bar Association's section of corporations, finance, and securities laws.

A graduate of the University of Michigan in 1977 with an AB in English literature, Mr. Dugan also earned his JD from Harvard Law School in 1981. Born in Washington, DC in 1955, Mr. Dugan lives in Chevy Chase, Maryland, with his wife, Beth, and his two children, Claire and Jack.

Ann F. Jaedicke
Deputy Comptroller for Compliance, Office of the Comptroller of the Currency

Ann F. Jaedicke has served as deputy comptroller of Compliance since December 2003. She is responsible for policy and examination procedures relating to consumer issues, money laundering, and bank secrecy. She also sits on FFIEC's (Federal Financial Institution Examination Council) task force on consumer compliance and FFIEC's Bank Secrecy Act task force. These task forces of US regulators promote policy coordination and the uniform enforcement of laws and regulations.

Ms. Jaedicke has been employed by the Office of the Comptroller of the Currency (OCC) as a bank examiner for 28 years. She began her career in 1977 as a bank examiner in Texas. From 1984-1986, Ms. Jaedicke worked in OCC's London office where she examined branches of US banks. Later she served as the director for OCC's Large Bank Division. At the time, OCC's Large Bank Division supervised 12 of the largest national banks in the US. In 1997, Ms. Jaedicke was promoted to deputy comptroller for Supervision Operations where she managed, among other things, OCC's Problem Bank Division and sat on OCC's Enforcement Committee. In 2001 and 2002, Ms. Jaedicke led projects to restructure OCC's six districts and OCC's Washington, DC headquarters.

Ms. Jaedicke is a native Texan and a graduate of Texas A&M University.

Deborah Katz
Senior Counsel, Legislative and Regulatory Activities Division, Office of the Comptroller of the Currency

Deborah Katz is a Senior Counsel in the Legislative and Regulatory Activities Division of the Office of the Comptroller of the Currency (OCC). She has drafted interagency regulations relating to identity theft and information security. She also drafted the interagency Customer Identification Program rule implementing Section 326 of the USA PATRIOT Act. Ms. Katz joined the OCC in 1986. She has been Special Assistant to the Deputy Chief Counsel and has worked in the Enforcement and Compliance, Bank Organization and Structure, and Legal Advisory Services divisions of the OCC's law department.

Ms. Katz received a BS from the Edmund E. Walsh School of Foreign Service, Georgetown University, in 1979, and a JD from the Benjamin M. Cardozo School of Law, Yeshiva University, in 1986. She is a member of the New York Bar.

Andra Shuster
Special Counsel, Legislative and Regulatory Activities Division, Office of the Comptroller of the Currency

Andra Shuster is a Special Counsel in the Legislative and Regulatory Activities Division of the Office of the Comptroller of the Currency (OCC). Ms. Shuster joined the OCC in 1999 as a Senior Attorney in the Community and Consumer Law Division, where she worked through 2000. Her areas of expertise are preemption and visitorial powers, information security, and international banking. Ms. Shuster participated in drafting the interagency Identity Theft Red Flags and Address Discrepancies rulemaking. Prior to joining the OCC, Ms. Shuster was in private practice, representing clients in bank regulatory and transactional matters.

Ms. Shuster received a BA in economics and business in 1987 from Lafayette College and a JD and MBA in 1991 from Georgetown University. She is a member of the New York and District of Columbia Bars.

Paul E. Utterback
National Bank Examiner and Senior Compliance Specialist, Compliance Policy Division, Office of the Comptroller of the Currency

Paul Utterback joined the Office of the Comptroller of the Currency (OCC) in 1974. Mr. Utterback was commissioned as a National Bank Examiner in 1980 and served as an examiner-in-charge of safety and soundness and compliance examinations in the OCC's Central District. In 1984, Mr. Utterback transferred to the OCC's Western District where he continued his examination work and served as a field office and district office analyst. In 1991, he transferred to the OCC's headquarters in Washington, DC, where he has been responsible for developing consumer compliance policies and procedures. Mr. Utterback has served on many interagency working groups to develop compliance guidance and examination procedures.

Mr. Utterback received a BS degree in accounting from Miami University, Oxford, Ohio, where he was a member of Beta Alpha Psi, a national honorary accounting fraternity. He also is a graduate of the University of Colorado, Graduate School of Banking.