OFFICE OF THRIFT SUPERVISION
1989

Identity Theft Rules and Guidelines

Presentation of Identity Theft Rule and Guidelines

August 11, 2008

Red Flags and Information Security Examiner Guidance

- Key points of 12 CFR Part 571.90, Identity Theft Red Flags Regulation, Appendix and Supplement
- Relationship to existing OTS Information Security examination guidance and procedures

Red Flags and Information Security Red Flags Regulation

- Effective January 1, 2008
- Compliance date November 1, 2008
- Thrift Industry concerns—more documentation, more training, more oversight, new framework?

Red Flags and Information Security Red Flags Regulation

- Not new framework but add-on to existing, effective programs that have been in place and operating for several years now
- Information Security Programs
  - □ Sections 501(b) GLB Act and 216 FACT Act
- Customer Identification Programs
  - □ USA PATRIOT Act

Red Flags and Information Security Red Flags Regulation

- For many thrifts, compliance with the Identity Theft Red Flags Regulation—12 CFR Part 571.90—is not as much about developing and implementing new controls but about applying more consistency around existing controls and formalizing these into a written program

Red Flags and Information Security Red Flags Regulation

- Thrifts in compliance with Interagency Security Guidelines likely will meet Red Flags Compliance November 1, 2008

Red Flags and Information Security Key Points Red Flags Regulation

- Applies to FDIC-insured thrifts and operating subsidiaries not functionally regulated
- Identity Theft definition,16 CFR 603.2(a), Federal Trade Commission
  - Identity theft means a fraud committed or attempted using the identifying information of another person without authority

Red Flags and Information Security Key Points Red Flags Regulation

- Covered Accounts
  - Not all accounts; personal, permits multiple transactions; maybe business
- Risk Assessments to identify covered accounts, how accessed or opened, where vulnerabilities exist and how to mitigate weaknesses

Red Flags and Information Security Key Points Reds Flag Regulation

- Prepare Written Identity Theft Prevention Program
- Involve Board of Directors or Committee
- Train staff
- Oversee Service Providers
- Must Consider Guidelines

Red Flags and Information Security Key Points Red Flags Guidelines

- Additional guidance on how to:
  - □ Identify and Detect Red Flags
  - □ Prevent and Mitigate Identity Theft
  - □ Update and Administer the Program
- Thrifts may incorporate existing policies and procedures that control risks to customers and thrift
  - □ Written Information Security Program that complies with 12 CRF Part 570 Appendix B

Red Flags and Information Security Key Points Red Flags Supplement

- 26 Examples of Red Flags thrifts may consider incorporating into Identity Theft Prevention Program
- Remember: Thrift-wide Teamwork
  - Deposits, loans, retail branches, call centers, online banking, information technology, information security, compliance, audit

Red Flags and Information Security Relationship to Security Guidelines

- Many similarities with Interagency Security Guidelines 12 CFR Part 570 Appendix B Supplement A
- Board approvals
  - Initial Program by November 1, 2008
- Board or Board Committee involvement in Program oversight
  - Review staff reports on compliance

Red Flags and Information Security Relationship to Security Guidelines

- Risk Assessments—for covered accounts or non-public customer information
- OTS Guidance
  - April 2006 Examination Handbook Section 341, IT Risks and Controls
  - July 2006 FFIEC IT Examination Handbook Information Security booklet, CEO Memo 241
  - December 2005 Compliance Guide CEO Memo 231

Red Flags and Information Security Relationship to Security Guidelines

- Must consider and include/adopt those controls appropriate
- Train Staff to implement the Identity Theft Prevention Program effectively
- Identify, Detect, Prevent and Mitigate
  - Response Program Guidance, CEO Memo 214
  - Authentication Guidance, CEO Memo 228

Red Flags and Information Security Relationship to Security Guidelines

- Update the Identity Theft Program
  - New service providers
- Administer the Identity Theft Program
  - Assign responsibility; review reports
- Oversee service providers—check processors, check and credit card vendors
  - Require contractual clauses

Red Flags and Information Security OTS Examination Approach

- Scope and examine responsive to thrift's approach
- Same examination procedures for all disciplines
- Update Examination Handbook, Revise Preliminary Examination Response Kit (PERK)

Red Flags and Information Security Conclusion and Summary

- Thrifts already have measures to detect and address Identity Theft required by the Red Flags Regulation
  - □ Usual and customary business practices to minimize losses due to fraud
  - □ Many already implemented some of the requirements by complying with other regulations and guidance

Red Flags and Information Security Conclusion and Summary

- 2008 Reviews likely to find much reliance on Information Security Programs and Customer Identification Programs
- May be stand-alone program or compilation of written documentation where to find elements in existing policies, processes, and programs

Red Flags and Examiner Resources Follow-up and Questions

- Follow-up and questions for Information Technology Policy
  - William.Henley@ots.treas.gov
  - 202-906-6540
  - Kathleen.McNulty@ots.treas.gov
  - 202-906-6322
- Follow-up and questions for Compliance Policy
  - ekita.mitchell@ots.treas.gov
  - 202-906-6451