Office of Inspector General

February 2006
Report No. 06-009

FDIC's Guidance to Institutions and Examiners for Implementing the Gramm-Leach-Bliley Act Title V and the Fair and Accurate Credit Transactions Act

Office of Audits

OIG

Office of Audits

Report No. 06-009
February 2006

FDIC's Guidance to Institutions and Examiners for Implementing the Gramm-Leach-Bliley Act Title V and the Fair and Accurate Credit Transactions Act

Background and Purpose of Audit

The privacy and security of consumer information in financial institutions is regulated by Title V of the Gramm-Leach-Bliley Act of 1999 (GLBA), the Fair and Accurate Credit Transactions Act of 2003 (FACT Act), and the Fair Credit Reporting Act of 1968 (FCRA). The FACT Act made many substantive amendments to the FCRA and covers, for example, identity theft, consumers' access to credit information, enhanced consumer report accuracy, and financial literacy. The statutes prescribe financial institutions' responsibilities for protecting consumer information and sharing it with other entities.

The audit objective was to determine whether the FDIC provided adequate guidance to FDIC-supervised institutions and examiners for implementing the data privacy and security provisions of the GLBA Title V and the FACT Act. The audit also determined whether the FDIC has implemented GLBA-related recommendations in Office of Inspector General Audit Report No. 03-044, *The Federal Deposit Insurance Corporation's Progress in Implementing the Gramm-Leach-Bliley Act, Title V - Privacy Provisions*, dated September 26, 2003.

To view the full report, go to www.fdicig.gov/2006reports.asp

Results of Audit

The FDIC has established rules and regulations and issued adequate guidance to institutions and examiners for implementing the GLBA Title V provisions related to the privacy and security of consumer information. These actions are sufficient to address our prior recommendations. In contrast, some FACT Act provisions are still lacking rules and regulations.

Ten FACT Act provisions require compliance by FDIC-supervised institutions and rulemaking by the federal banking agencies, National Credit Union Administration (NCUA), or Federal Trade Commission (FTC). The FDIC, jointly or in coordination with the other federal banking agencies and NCUA, has completed the rulemaking process for two of the seven FACT Act provisions that require FDIC rulemaking. The FTC has completed rules and regulations for the three provisions for which it has rulemaking responsibility. The Act did not designate a lead agency for the five provisions requiring rules and regulations. The FDIC must coordinate with other federal agencies to issue guidance for the five provisions, but meeting timeframes for publishing the regulations has proved to be difficult. Further, the FDIC had not issued final financial institution or examination guidance on those provisions where the FTC had issued final rules and regulations and for so-called "self-executing" provisions (require financial institution compliance but not rulemaking by the federal agencies).

The lack of final rules and regulations could limit the effectiveness of the FACT Act and reduce assurance that institutions are taking steps to prevent identity theft to the extent intended by the Act. However, to some degree, the FDIC has mitigated that risk by issuing interim financial institution and examination guidance addressing all of the provisions that require such guidance.

Recommendations and Management Response

We recommended that the FDIC finalize the interim examination guidance that addresses FACT Act provisions and develop, in coordination with the joint-agency rulemaking committee, a more aggressive project management plan to expedite the issuance of final rules and regulations for all FACT Act provisions. The FDIC concurred with the recommendations and stated that it is fully committed to, and is in the process of, developing and issuing financial institution and examination guidance. Also, as a member of the separate working groups responsible for drafting each set of rules or guidelines, the FDIC has consistently made efforts to move the process forward and will continue to promote expedited processes during 2006. Management's planned actions are responsive to the recommendations.

TABLE OF CONTENTS

Federal Deposit Insurance Corporation
801 17th Street NW, Washington, DC 20434

Office of Audits
Office of Inspector General

DATE: February 24, 2006

MEMORANDUM TO: Sandra L. Thompson, Acting Director
Division of Supervision and Consumer Protection

FROM: Russell A. Rau [Electronically produced version; original signed by Russell A. Rau]
Assistant Inspector General for Audits

SUBJECT: *FDIC's Guidance to Institutions and Examiners for Implementing the Gramm-Leach-Bliley Act Title V and the Fair and Accurate Credit Transactions Act* (Report No. 06-009)

This report presents the results of our audit of the FDIC's implementation of the Gramm-Leach-Bliley Act of 1999 (GLBA) Title V and the Fair and Accurate Credit Transactions Act of 2003 (FACT Act). The audit objective was to determine whether the FDIC's Division of Supervision and Consumer Protection (DSC):

- provided adequate guidance to FDIC-supervised institutions and examiners for implementing the data privacy and security provisions of the GLBA Title V and the FACT Act, and

- implemented the recommendations in Office of Inspector General (OIG) Audit Report No. 03-044, *The Federal Deposit Insurance Corporation's Progress in Implementing the Gramm-Leach-Bliley Act, Title V - Privacy Provisions*, dated September 26, 2003.

To address our objective, we assessed the FDIC's progress in implementing the GLBA provisions related to the privacy and security of bank consumer[1] data, and all of the FACT Act provisions. This audit is the second in a series of audits planned to review the FDIC's implementation of GLBA Title V and FACT Act provisions. Subsequent audit coverage of this area will include detailed reviews of examinations and supervisory efforts addressing the privacy and security of consumer information. Details on our objective, scope, and methodology are in Appendix I of this report.

[1] GLBA, Subtitle A, uses the terms "consumer" and "customer." GLBA, Section 509(9), defines "consumer" as an individual (or legal representative) who obtains, from a financial institution, financial products or services that are to be used primarily for personal, family, or household purposes. The FDIC's Rules and Regulations, Section 332.3, implements GLBA Section 509(11) by defining "customer relationship" as a continuing relationship between a consumer and the financial institution that provides one or more financial products or services to the consumer that are to be used primarily for personal, family, or household purposes. This report uses "consumer" unless, in the particular context, "customer" would be more appropriate.

BACKGROUND

Since the early 1970s, the FDIC has recognized the significant risk associated with the potential for data security weaknesses to disrupt bank operations, harm consumers, and undermine confidence in the nation's financial system. The failure or misuse of technology can impact the safety and soundness of an institution with sudden and severe losses or compromise the security of consumer financial information. Elements of risk in this area include a potential impact on the deposit insurance funds if continued breaches in data security are not controlled. This issue has received increased public and congressional attention.

The security and privacy of consumer information in financial institutions is regulated by the GLBA, Fair Credit Reporting Act of 1968 (FCRA), and FACT Act, which amended the FCRA. These statutes describe financial institutions' responsibilities for protecting consumer information and sharing it with other entities. The FDIC and other regulatory agencies establish regulations to implement the statutes and monitor compliance through routine supervisory programs, including on-site examinations of financial institutions. DSC reviews financial institutions' compliance with: (1) GLBA privacy notice requirements through compliance examinations and (2) GLBA and Fact Act provisions on safeguarding consumer information through information technology (IT) examinations. Supervisory actions for regulatory noncompliance range from informal agreements and enforcement actions to civil money penalties.

The GLBA was enacted on November 12, 1999. Title V of the GLBA contains data privacy and security provisions that prohibit financial institutions from sharing nonpublic, personally identifiable consumer information with nonaffiliated third parties[2] and require institutions to provide notice of their privacy policies to customers and to safeguard the security and confidentiality of consumer information. Finally, Title V delegates rulemaking and enforcement authority to the federal banking and securities regulators, the Federal Trade Commission (FTC), and state insurance regulators.[3]

The FCRA establishes standards for collecting and disseminating data by consumer reporting agencies (CRAs).[4] The primary purpose of the FCRA is to regulate the nationwide consumer reporting system to help ensure the accuracy and security of consumer reports.[5]

---

[2] The GLBA requires financial institutions to provide notices describing the type of information they intend to share with third parties and how customers may "opt out," or say "no," to information sharing under certain circumstances.

[3] According to section 3 of the Federal Deposit Insurance Act, "[t]he term 'Federal banking agency' means the Office of the Comptroller of the Currency, the Office of Thrift Supervision, the Board of Governors of the Federal Reserve System, or the Federal Deposit Insurance Corporation."

[4] FCRA, Section 603, defines "consumer" as "an individual." Also, FCRA Section 603 defines the term "consumer reporting agency" as "any person which, for monetary fees, dues, or on a cooperative nonprofit basis, regularly engages in whole or in part in the practice of assembling or evaluating consumer credit information or other information on consumers for the purpose of furnishing consumer reports to third parties, and which uses any means or facility of interstate commerce for the purpose of preparing or furnishing consumer reports."

[5] FCRA, Section 603, defines "consumer report" as any written, oral, or other communication of any information by a consumer reporting agency bearing on a consumer's creditworthiness, credit standing, credit capacity, character, general reputation, personal characteristics, or mode of living, which is used or expected to be used or collected in whole or in part for the purpose of serving as a factor in establishing the consumer's eligibility for: (1) credit or insurance to be used primarily for personal, family, or household purposes; (2) employment purposes; or (3) any other purpose authorized under section 604.

The FACT Act was signed into law on December 4, 2003. One of its primary purposes was to amend the FCRA to make several expiring federal preemptions permanent, in response to industry concern that state or local laws might interfere with the continuity of the credit reporting system. In addition to the federal preemption, the FACT Act also made many substantive amendments to the FCRA to address issues raised by industry and consumer advocates. In response to industry concerns, the FACT Act preserves and expands uniform national standards for the accuracy and integrity of consumer report information and access to such information. In response to concerns raised by consumer advocates, the FACT Act contains many new provisions to combat identity theft, protect privacy, and improve consumer access to, and the overall accuracy of, consumer reports. The FACT Act also restricts the use and disclosure of sensitive medical information. To bolster efforts to improve financial literacy among consumers, Title V of the Act (entitled, *Financial Literacy and Education Improvement Act*) creates a new Financial Literacy and Education Commission, of which the FDIC is a member, empowered to take appropriate actions to improve financial literacy and education programs, grants, and materials of the federal government.

Appendix II contains additional information on the requirements of the GLBA, FCRA, and FACT Act.

RESULTS OF AUDIT

The FDIC has established rules and regulations and issued adequate guidance to institutions and examiners for implementing the GLBA Title V provisions related to the privacy and security of consumer information. In doing so, the FDIC has taken sufficient corrective action to address prior OIG recommendations associated with the Corporation's implementation of these provisions. In contrast, the FDIC, jointly or in coordination with the other federal banking agencies, National Credit Union Administration (NCUA), and FTC, has not yet issued rules and regulations addressing some FACT Act provisions. The lack of final rules and regulations could limit the effectiveness of the FACT Act and reduce assurance that institutions are taking steps to prevent identity theft to the extent intended by the Act. The FDIC has mitigated that risk, to some degree, by issuing interim financial institution and examination guidance addressing all of the provisions that require such guidance.

FINDING AND RECOMMENDATIONS

FDIC'S PROGRESS IN IMPLEMENTING GLBA TITLE V DATA PRIVACY AND SECURITY PROVISIONS AND FACT ACT PROVISIONS

The FDIC has established rules and regulations that appropriately address the GLBA Title V provisions related to the privacy and security of consumer information. In addition, the FDIC has provided adequate guidance to FDIC-supervised institutions and established adequate examination guidance and procedures to ensure that these institutions meet GLBA requirements. Examination guidance issued in April 2004 includes procedures that adequately address prior OIG recommendations associated with the Corporation's implementation of GLBA privacy provisions.

Ten FACT Act provisions require compliance by FDIC-supervised institutions and rulemaking by the federal banking agencies and NCUA or FTC. The FDIC, jointly or in coordination with the other federal banking agencies and NCUA, has completed the rulemaking process for two of the seven FACT Act provisions that require rulemaking by the FDIC. The FTC has completed rules and regulations for the three provisions for which it has rulemaking responsibility. The Act did not designate a lead agency for the five provisions still lacking rules and regulations. Therefore, the FDIC must coordinate with other federal agencies to issue guidance for the five provisions, but meeting timeframes for publishing the regulations has proved to be difficult.[6] The lack of final rules and regulations that establish implementing requirements could limit the effectiveness of the FACT Act provisions, thus reducing assurance that institutions are limiting the potential for identity theft. However, the FDIC has acted to mitigate that risk by issuing interim financial institution and examination guidance to address all of the FACT Act sections that require such guidance.

FDIC Rules and Regulations That Address GLBA Title V Provisions

During our 2003 audit of the FDIC's progress in implementing GLBA Title V, we determined that the FDIC had made reasonable progress in implementing GLBA Title V Subtitle A's provisions.[7] However, federal regulators had not yet finalized the interagency-proposed regulations for GLBA Title V Subtitle A, Section 506, *Protection of the Fair Credit Reporting Act*. According to Subtitle A, Section 506(a), the authority of the federal banking agencies to conduct routine examinations for compliance with the FCRA was restored, and the federal banking agencies were to jointly prescribe regulations, as necessary, for financial institutions to carry out the purposes of FCRA. Based on the results of our current audit, we determined that the requirements of the provision have been fulfilled.

On October 26, 2000, the FDIC issued Financial Institution Letter (FIL) 71-2000, *Proposed Regulations Implementing the Fair Credit Reporting Act*. This FIL distributed the proposed rule, Part 334, published in the *Federal Register* (Vol. 65, No. 204). During fieldwork for our 2003 audit, we found that banking regulators anticipated issuing a new proposed rulemaking for public comments, addressing comments received on the October 2000 proposal. During our current audit, we discussed the status of the proposed regulation with FDIC's Legal Division and were informed that Section 506 of GLBA did not require the development of regulations but that regulations were to be prescribed "as necessary" to carry out the FCRA. According to DSC, the underlying purpose of the proposed regulation issued in FIL-71-2000 was to provide functional, specific requirements for the provision of an opt out notice as required by the FCRA. The requirement to provide an opt out notice in the FCRA had existed in the statute, without regulation, since 1996. The "as necessary" approach to Section 506 refers to whether the agencies believed a specific instruction regarding the opt out notice was necessary. Ultimately, DSC determined that a specific instruction was not necessary because banks would generally follow similar guidance in the privacy regulations (FDIC Rules and Regulations Part 332) that cover the FCRA opt out notice. According to DSC, although the GLBA and the FCRA opt out

[6] For these five provisions, the FACT Act states that the federal banking agencies, NCUA, and FTC shall either jointly or in coordination, establish and maintain guidelines, and prescribe regulations. For provisions requiring coordination, the FACT Act states that each agency required to prescribe regulations shall consult and coordinate with each other so that, to the extent possible, the regulations prescribed are consistent and comparable.

[7] On September 26, 2003, the OIG issued Audit Report No. 03-044. The objective of the audit was to determine whether the FDIC had made reasonable progress in implementing the GLBA Title V privacy provisions.

notice requirements are different and based in different statutory requirements, a bank's practices for delivering notices and honoring opt outs is almost always structured in the same way. Therefore, although GLBA Section 506 requirements are not addressed in a specific regulation, under the FCRA, FDIC-insured institutions are subject to the statutory requirement to provide an opt out notice.

FDIC Guidance That Addresses GLBA Title V Provisions

During our 2003 audit of the FDIC's progress in implementing GLBA Title V, we also conducted an analysis of the corresponding guidance issued to FDIC-supervised banks and FDIC examiners. At the time of our 2003 audit report, we determined that, on May 9, 2001, the FDIC issued FIL-39-2001, *Guidance on Identity Theft and Pretext Calling*, as a supplement to FDIC regulations on customer information security, issued February 1, 2001, pursuant to Section 501(b) of the GLBA.[8] In our 2003 audit report, we stated that the guidance provided steps that financial institutions should take to safeguard customer information and reduce the risk of loss from identity theft and pretext calling. However, we also noted that DSC's examination procedures did not include steps to specifically assess how banks protect customer information from unauthorized disclosure through identity theft and pretext calling.

On April 16, 2004, DSC's Technology Supervision Branch issued Regional Directors Memorandum (RDM) 2004-014, *Information Technology General Work Program Revision*. During our current audit, we reviewed the RDM and found that it provides examiners adequate guidance for assessing how banks protect customer information from unauthorized disclosure to reduce the risks of loss related to identity theft and pretext calling.

In 2005, DSC issued the following additional interpretations and guidance related to establishing standards for safeguarding customer information.

- FIL-27-2005, *Final Guidance on Response Programs - Guidance on Response Programs for Unauthorized Access to Consumer Information and Consumer Notice*, dated April 1, 2005, requires financial institutions to develop and implement a response program designed to address incidents of unauthorized access to sensitive consumer information maintained by the financial institution or its service provider.

- RDM 2005-012, *Examination Procedures to Evaluate Response Programs for Unauthorized Access to Consumer Information,* dated April 5, 2005, distributes examination procedures to determine compliance with the *Interagency Guidance on Response Programs for Unauthorized Access to Consumer Information and Consumer Notice*.

[8] Section 501(b), *Disclosure of Nonpublic Personal Information*, requires each agency to establish appropriate standards for the financial institutions under their jurisdiction relating to administrative, technical, and physical safeguards. Specifically, the standards are to (1) ensure the security and confidentiality of customer records and information; (2) protect against any anticipated threats or hazards to the security or integrity of such records; and (3) protect against unauthorized access to or use of such records or information that could result in substantial harm or inconvenience to any customer. On February 1, 2001, the federal banking regulators issued a final rule under FDIC Rules and Regulations Part 364, *Standards for Safety and Soundness*, Appendix B, *Interagency Guidelines Establishing Standards for Safeguarding Customer Information.* On August 28, 2001, the FDIC issued Regional Directors Memorandum (RDM) 2001-032, *Examination Procedures to Evaluate Customer Information Safeguards*, to distribute examination procedures to determine compliance with Appendix B to Part 364.

- FIL-64-2005, *Pharming Guidance on How Financial Institutions Can Protect Against Pharming Attacks*, dated July 18, 2005, describes the practice of "pharming," how it occurs, and potential preventive approaches. The guidance states that financial institutions offering Internet banking should assess potential threats posed by pharming attacks and protect Internet domain names, which – if compromised – can heighten risks to the institutions.

- FIL-66-2005, *Spyware Guidance on Mitigating Risks From Spyware*, dated July 22, 2005, recommends an effective spyware prevention and detection program based on an institution's risk profile. The guidance and the attached informational supplement discuss the risks associated with spyware from both a bank's and consumer's perspective and provide recommendations to mitigate these risks.

- FIL-69-2005, *Voice Over Internet Protocol Guidance on the Security Risks of VoIP,* dated July 27, 2005, addresses the security risks associated with voice over Internet protocol (VoIP).[9] VoIP is susceptible to the same security risks as data networks if security policies and configurations are inadequate. To address section 501(b) of GLBA, the guidance states that associated risks should be evaluated as part of a financial institution's periodic risk assessment and discussed in status reports submitted to the institution's board of directors. The guidance provides financial institutions with a detailed summary of the risks associated with VoIP and the available sources to develop VoIP security policies and procedures and recommends best practices. In addition, FIL-69-2005 states that bank management should perform a comprehensive risk assessment to ensure the confidentiality, integrity, and availability of voice communications using VoIP technology.

During our current audit, we reviewed DSC's guidance and found that it provided adequate procedures for both institutions and examiners in ensuring compliance with GLBA, Section 501. In addition, since September 26, 2003, the FDIC has issued several policy documents to banks and examiners that address data privacy or data security. Many of the documents are advisory in nature or for informational purposes and are not required by GLBA. Appendix III provides a list of the policy documents developed by DSC for both FDIC-supervised institutions and FDIC examiners.

FDIC Rules and Regulations That Address FACT Act Provisions

The FACT Act contains 10 provisions that require compliance by FDIC-supervised institutions and rulemaking by the federal banking agencies and the NCUA or FTC. The FDIC, jointly or in coordination with other federal banking agencies and the NCUA, has completed the rulemaking process for two of the seven FACT Act provisions that require FDIC rulemaking. The FTC has completed rules and regulations for the three provisions for which it has rulemaking responsibility. The Act did not designate a lead agency for the five provisions still lacking rules and regulations, and the FDIC must coordinate with other federal agencies to issue the guidance. The table on the next page summarizes the status of the regulations and guidance related to FACT Act provisions affecting FDIC-supervised institutions. Appendix IV describes each title and section of the FACT Act.

[9] VoIP refers to the delivery of traditional telephone voice communications over the Internet.

Status of Regulations and Guidance Issued for FACT Act Provisions Affecting FDIC-Supervised Institutions

FACT Act Section	Status of Rules and Regulations			Status of FDIC Financial Institution Guidance			Status of FDIC Examiner Guidance		
	Nothing Issued	Proposed	Final	Nothing Issued	Interim	Final	Nothing Issued	Interim	Final
Regulations Required To Be Issued Jointly by the FDIC and Five Other Federal Banking Agencies									
114(e)	√				√			√	
214(a)		√			√			√	
216			√ FDIC			√			√
312(a)	√ [a]				√			√	
312(c)	√ [a]				√			√	
315	√				√			√	
411			√ FDIC			√		√	
Regulations Required To Be Issued by the Federal Trade Commission									
151(a)			√ FTC		√			√	
153			√ FTC		√			√	
213			√ FTC		√			√	
Self-Executing Provisions Not Requiring Regulations [b]									
112					√			√	
152					√			√	
154(a)					√			√	
212					√			√	

Source: FDIC Legal Division's FACT Act Status Report and various FILs and RDMs.

[a] On February 10, 2006, the FDIC Board of Directors approved the *Interagency Advance Notice of Proposed Rulemaking Regarding the Accuracy and Integrity of Information Furnished to Consumer Reporting Agencies under the Fair and Accurate Credit Transactions Act of 2003.*

[b] Self-executing provisions are FACT Act provisions that do not require rulemaking by the federal banking agencies but require financial institution compliance.

As of the time of our audit fieldwork, the FDIC, in coordination with the other regulators, had issued final rules in reference to two FACT Act provisions:

- Section 216, *Disposal of Consumer Report Information and Records,* and
- Section 411, *Protection of Medical Information in the Financial System*.

In addition, the FTC has issued final rules in reference to three FACT Act provisions for which the FDIC does not have explicit authority to publish rules but which require FDIC-supervised institutions' compliance:

- Section 151(a), *Summary of Rights of Identity Theft Victims*;
- Section 153, *Coordination of Identity Theft Complaint Investigations*; and
- Section 213, *Enhanced Disclosure of the Means Available to Opt Out of Prescreened* Lists.

The rulemaking process either has not started or has not been completed for the remaining five provisions, which require that the federal banking agencies coordinate to issue regulations. According to sections 114(e), 312(c), and 315 of the FACT Act, the federal banking regulators, NCUA, and FTC *shall jointly* prescribe regulations with respect to the entities that are subject to

their respective enforcement authority. For other rulemaking sections (214(a) and 312(a)) the law states that the federal banking agencies, NCUA, and FTC, *in coordination,* shall prescribe regulations with respect to the entities that are subject to their respective enforcement authority. The FDIC's Legal Division informed us that the agencies had agreed on timelines to ensure the timely publication of final rules when the FACT Act was enacted but found it difficult to meet the timelines. DSC's efforts to issue regulations related to the FACT Act are, to a great degree, dependent upon other entities and DSC's participation in joint rulemaking committees.

Joint Guidance

As discussed earlier, the FDIC has issued final rules related to two FACT Act provisions. DSC has issued final guidance to institutions and examiners, addressing one of those provisions, Section 216, *Disposal of Consumer Report Information and Records*. We found that the guidance provides adequate procedures related to complying with requirements of the disposal of consumer information. For the other provision, we also found that DSC has issued final guidance (in the form of a FIL transmitting the regulation) to institutions, but not examiners, addressing Section 411, *Protection of Medical Information in the Financial System.* We found that the guidance provides FDIC-supervised institutions adequate procedures related to complying with requirements on the use of medical information in determining credit eligibility.

On December 28, 2004, the FDIC issued final rules to implement FACT Act Section 216, *Disposal of Consumer Report Information and Records*. To address the regulation, the FDIC issued FIL-07-2005 entitled, *Fair and Accurate Credit Transactions Act of 2003 Guidelines Requiring the Proper Disposal of Consumer Information,* dated February 2, 2005. According to the FIL, Section 216 is designed to protect consumers against the risks associated with identity theft and other types of fraud and requires a financial institution that maintains or otherwise possesses consumer information derived from consumer reports to properly dispose of it. Under the final rule, the agencies amended their *Guidelines Establishing Standards for Safeguarding Customer Information* (renamed *Interagency Guidelines Establishing Information Security Standard*s).

We reviewed the revised guidance and found it to be adequate to address FACT Act Section 216 in that the guidelines require each financial institution (1) to develop and maintain, as part of its information security program, appropriate controls designed to ensure that it properly disposes of "consumer information" derived from a consumer report in a manner consistent with the financial institution's existing obligation under the guidelines and (2) to assess the risks to the institution's *consumer* information as well as *customer* information by evaluating security measures to control the risks.

On November 22, 2005, the FDIC issued a final rule (12 Code of Federal Regulations (C.F.R.) Part 334) to address FACT Act Section 411, *Protection of Medical Information in the Financial System*. To address the regulation, the FDIC issued FIL-121-2005 entitled, *Fair Credit Reporting – Medical Information Final Rules*, dated December 8, 2005. We reviewed the guidance and found it to be adequate to address FACT Act Section 411 in that the guidelines prohibit institutions from obtaining and using medical information in determining credit eligibility, except as permitted by the financial institution regulatory agencies. In addition, the FIL identifies exceptions that will allow institutions to obtain and use medical information in appropriate circumstances. However, DSC has not yet issued final examination guidance related

to this provision of the FACT Act. The effective date for FDIC-supervised institutions to comply with the rule is April 1, 2006. According to DSC, this area will be addressed in an amendment to the FCRA examination procedures before the April 1, 2006, effective date.

FTC Regulations Required

During this audit, we identified three sections of the FACT Act for which the FTC was given authority to publish rules that require compliance by FDIC-supervised institutions. The federal banking agencies and the NCUA were consulted by the FTC in issuing these final rules.

- Section 151(a) of the FACT Act requires the development of a *Summary of Rights of Identity Theft Victims*. According to DSC, FDIC-supervised banks will use the model summary of rights notice when necessary. In this area, a CRA must provide the notice to consumers who have alerted the CRA that they may be a victim of identity theft. According to DSC, currently, none of the FDIC-supervised institutions are considered to be CRAs. Section 151 also addresses providing information about transactions or accounts that may be the result of identity theft to victims and/or law enforcement. There is no requirement for the FDIC to promulgate regulations for Section 151, and the FDIC was not given any explicit authority to do so. DSC provided guidance to examiners in the *Interim Compliance Examiner Job-Aid* attached to RDM 2004-055, *Fair and Accurate Credit Transactions Act of 2003 – Effective Dates*, dated November 29, 2004.

- Section 153 of the FACT Act requires nationwide CRAs to develop and maintain procedures to inform one another when an identity theft complaint is received. According to DSC, the FDIC currently does not supervise any financial institutions that are considered to be nationwide CRAs; therefore, there is no need for final guidance for this section.

- Section 213 of the FACT Act requires FDIC-supervised institutions to provide pre-screened consumer report notices and to use the FTC's form for this purpose. The specific requirements became effective for financial institutions on August 1, 2005. According to DSC, at that time, the FDIC was leading a working group under the Federal Financial Institutions Examination Council (FFIEC)[10] Consumer Compliance Task Force to re-write all of the FCRA examination procedures to include the FACT Act amendments. The FTC's rules to implement Section 213 were part of this project. The procedures were approved by the FFIEC in September 2005, and DSC plans to communicate them to all FDIC offices using an RDM.

Self-executing Provisions

During this audit, we noted that the FACT Act includes some provisions that do not require rulemaking by the federal banking agencies but do require financial institution compliance:

[10] The FFIEC, established in March 1979, is a formal interagency body empowered to prescribe uniform principles, standards, and report forms for the federal examination of financial institutions by the Board of Governors of the Federal Reserve System (FRB), the FDIC, NCUA, Office of the Comptroller of the Currency, and Office of Thrift Supervision and to make recommendations to promote uniformity in the supervision of financial institutions.

- Section 112, *Fraud and Active Duty Alerts*;
- Section 152, *Blocking of Information Resulting from Identity Theft*;
- Section 154(a)-(b), *Prevention of Repollution of Consumer Reports*; and
- Section 212(c), *Disclosure of Credit Scores*.

The FDIC informed its supervised institutions of the effective dates related to these self-executing provisions through FIL-130-2004*, Fair and Accurate Credit Transactions Act of 2003 - Effective Dates*, dated December 13, 2004. According to the FIL, these provisions were effective December 1, 2004. With regard to the provisions that do not require implementing regulations, the FDIC expects covered entities to begin to comply by the dates contained in the FACT Act or by the effective dates jointly set by the FTC and FRB. The FTC and FRB published these dates in a rulemaking in February 2004. In addition, DSC issued RDM 2005-055 *Fair and Accurate Credit Transactions Act of 2003 – Effective Dates*, dated November 29, 2004, to explain the effective dates for the FACT Act. RDM 2005-055 has an attached supplement, *Interim Job-Aid,* which contains guidance for examiners in reviewing institution compliance with the self-executing requirements. Also, as noted earlier, the FDIC led a working group to re-write all of the FCRA examination procedures to include the FACT Act amendments. The revised procedures were approved by the FFIEC in September 2005, and copies of the procedures were provided to examiners during training sessions in all regions; however, the official FIL and RDM are still pending.

CONCLUSION

Consumers have become increasingly concerned about the privacy of their personal information, and adequate protection of that information is an important element of public trust and confidence in depository financial institutions. With the rapid growth of electronic commerce, and the increased collection of diverse pieces of consumer personal information, the potential for use of the information in ways unwanted by consumers is a growing risk to financial institutions. To address this risk, the Congress passed both GLBA and the FACT Act to improve data security and expand safeguards over the confidentiality of consumer information. The effectiveness of those laws is dependent upon regulatory agencies, including the FDIC, to issue appropriate guidance. In that regard, the FDIC has been successful in addressing all of the GLBA Title V provisions related to the security and privacy of consumer information and implementing our prior recommendations in this area. However, the FDIC needs to finalize examiner guidance related to provisions of the FACT Act that were self-executing and for which FTC issued regulations. The Corporation also needs to work with the other federal banking agencies to issue final rules and regulations addressing FACT Act provisions that required they be issued jointly by the agencies. Until such time that these efforts are completed, there is less assurance that the increased protection of consumer information intended by the two laws is, in fact, occurring.

RECOMMENDATIONS

We recommend the Director, DSC:

(1) Finalize interim examination guidance that addresses FACT Act provisions for which final rules and regulations have been issued or that are self-executing.

(2) Develop, in coordination with the joint-agency rulemaking committee, a more aggressive project management plan that will expedite the issuance of final rules and regulations for all FACT Act provisions.

CORPORATION COMMENTS AND OIG EVALUATION

On February 15, 2006, the Acting Director, DSC, provided a written response to the draft report. The response is presented in its entirety in Appendix V of this report. DSC concurred with the intent of both recommendations.

Regarding recommendation 1, the written response states that DSC is in the process of developing and issuing examination guidance that addresses FACT Act provisions for which final rules and regulations have been issued or that are self-executing. For areas covered by compliance examinations, procedures that include the self-executing FACT Act provisions have been approved by the FFIEC Consumer Compliance Task Force and are being formally distributed to both examiners and the industry through an RDM and a FIL.

For recommendation 2, DSC stated that the FDIC is actively participating in and is committed to expediting the process to issue final rules and regulations for all FACT Act provisions. DSC is committed to expediting the interagency process and, as a member of the separate working groups responsible for drafting each set of rules or guidelines, the FDIC has consistently made efforts to move the process forward and will continue to promote expedited processes during 2006.

OIG Evaluation: Management's planned actions are responsive to the recommendations. The recommendations are resolved but will remain open until we have determined that the agreed-to corrective actions have been completed and are effective. Appendix VI contains a summary of management's response to the recommendations and the status of the recommendations as of the date of this report. Also, on February 21, 2006, the FDIC issued final financial institution and examiner guidance related to the self-executing provision of the FACT Act. We will review the guidance to assess whether it addresses our recommendation.

OBJECTIVE, SCOPE, AND METHODOLOGY

Objective

The objective of this audit was to determine whether DSC has:

- provided adequate institution and examination guidance for implementing the data privacy and security provisions of the GLBA Title V and the FACT Act; and
- implemented the recommendations contained in OIG Audit Report No. 03-044, *The Federal Deposit Insurance Corporation's Progress in Implementing the Gramm-Leach-Bliley Act, Title V - Privacy Provisions*, dated September 26, 2003.

We performed our audit from September 2005 through December 2005 in accordance with generally accepted government auditing standards.

Scope and Methodology

The scope of the audit included consumer privacy and data security requirements for FDIC-supervised institutions enacted under GLBA Title V, FCRA, and the FACT Act since we issued Audit Report No. 03-044 in September 2003. Details on that report are provided later in this appendix. The objective of the 2003 audit was to determine whether DSC had made reasonable progress in implementing Title V privacy provisions of the GLBA and had addressed both Subtitle A – *Disclosure of Nonpublic Personal Information* and Subtitle B – *Fraudulent Access to Financial Information*.

For the current audit, our assessment of the FDIC's progress was based on an analysis of the Corporation's and DSC's efforts to establish regulations, issue implementing guidelines to financial institutions, and develop and implement procedures to examine financial institution compliance with GLBA Title V, FCRA, and FACT Act provisions. In addition, we followed up on the status of the recommendations in Audit Report No. 03-044.

Specifically, we:

- reviewed applicable laws and statutes related to consumer data privacy and security at FDIC-supervised institutions;
- reviewed applicable FDIC rules and regulations, DSC procedure manuals, RDMs and FILs, and DSC Internal Review reports; and
- interviewed key Legal Division personnel, DSC personnel, and senior management to obtain general information on privacy-related requirements and examinations.

We conducted our audit work at the FDIC's Washington, D.C., Headquarters office.

Compliance With Pertinent Laws and Regulations

This audit addressed both GLBA Title V and FACT Act Titles I, II, III, and IV related to the protection and privacy of consumer information. The GLBA Title V provisions govern financial institution treatment of consumers' nonpublic personal information. The FACT Act amended the FCRA and governs the content of consumer reports and restrictions on access. The Results of Audit section of this report summarizes the FDIC's compliance with the applicable GLBA and FACT Act provisions, and details are provided in the findings.

Reliance on Computer-based Data, Government Performance and Results Act, Fraud and Illegal Acts, and Internal Control

Validity and Reliability of Data from Computer-based Systems

During this audit, we did not rely on data from computer-based systems. Our assessment of the FDIC's efforts to establish regulations, issue implementing guidelines to financial institutions, and develop and implement procedures to examine financial institutions' compliance was based on interviews with FDIC staff and reviews of applicable documents.

Performance Measures

In fulfilling its primary supervisory responsibilities, the FDIC pursues two strategic goals:

- FDIC-supervised institutions are safe and sound, and
- FDIC-supervised institutions invest in their communities,[11] and consumers' rights are protected.

Two strategic objectives support the consumer rights strategic goal. The first strategic objective is that consumers have access to easily understood information about their rights and the disclosures due them under consumer protection and fair lending laws.[12] The FDIC's annual performance goals related to this objective are:

- Provide effective outreach and technical assistance on topics related to the CRA, fair lending, and community development.
- Meet the statutory mandate to investigate and respond to consumer complaints about FDIC-supervised financial institutions.

The second strategic objective is that FDIC-supervised institutions comply with consumer protection, CRA, and fair lending laws. The FDIC's annual performance goals related to this objective follow.

[11] The goals are stated in the *FDIC 2005-2010 Strategic Plan* and the *FDIC 2005 Annual Performance Plan*.
[12] The FDIC periodically publishes *Consumer Alerts* on its Web site to provide consumers information on emerging and continuing issues, including fraudulent efforts to obtain consumer information and on new laws that provide consumers with new opportunities or protections. The most recent *Consumer Alerts* topics include phishing scams, identity theft, and the Check Clearing for the 21st Century Act, FACT Act, and GLBA.

- Conduct CRA and compliance examinations in accordance with the FDIC's examination frequency policy.

- Take prompt and effective supervisory action to monitor and address problems identified during compliance examinations of FDIC-supervised institutions that receive a 4 or 5 rating for compliance with consumer protection and fair lending laws.

We limited our scope to the issuance of regulations and guidance related to the GLBA and FACT Act and did not review DSC's examination assessment of compliance.

Fraud and Illegal Acts

The objective of this audit did not lend itself to specific steps for providing reasonable assurance of detecting fraud or illegal acts. Although we were alert to the potential for such activity, we did not identify any illegal acts or abuse or potential areas susceptible to illegal acts or abuse.

Internal Controls Reviewed

During the audit, we reviewed DSC's guidance related to compliance and IT examinations at FDIC-supervised institutions. For compliance examinations, we also identified the systems used for measuring and monitoring program performance and compliance with laws and regulations and policies and procedures. We reviewed this information to gain an understanding of the applicable control environment.

Summary of Prior Audit Coverage

On September 23, 2005, the OIG issued Audit Report No. 05-038, *Division of Supervision and Consumer Protection's Risk-focused Compliance Examination Process*. The overall objective of this audit was to determine whether DSC's risk-focused compliance examination process results in examinations that are adequately planned and effective in assessing financial institution compliance with consumer protection laws and regulations. Specifically, we determined whether DSC examiners were adequately risk-scoping compliance examinations and conducting appropriate levels of transaction testing and making sound risk-scoping decisions when relying on the work of the financial institutions' internal or external compliance review functions. We found that DSC examiners generally complied with the policies and procedures related to risk-scoping compliance examinations and that the Risk Profile and Scoping Memorandums prepared by examiners provided an adequate basis for planned examination coverage. However, we found that examination documentation did not always show the transaction testing or spot checks conducted during the on-site portion of the examinations, including testing to ensure the reliability of the institutions' compliance review functions. Examiners also did not always document whether the examination reviewed all the compliance areas in the planned scope of review. The report recommended that DSC clarify and reinforce requirements that examiners adequately document the scope of the work performed, including transaction testing and spot checks of the reliability of the institutions' compliance review functions, during the on-site portions of compliance examinations. DSC management agreed with the recommendation and has taken corrective action.

On June 15, 2004, the OIG issued Audit Report No. 04-022, *FDIC's Information Technology Examination Program*. The objective of this audit was to determine whether the FDIC's IT examinations provide reasonable assurance that IT risks are being addressed by the risk management programs in FDIC-supervised financial institutions. We concluded that the FDIC's IT examination program provides reasonable assurance that IT risks are being addressed by risk management programs in FDIC-supervised financial institutions. We did, however, identify opportunities for improving the quality of the IT examination process. Specifically, DSC did not have a review process in place to determine whether appropriate examination procedures are applied and that findings and conclusions are adequately supported. DSC has a quality review process in place for its safety and soundness examinations but generally had not conducted similar quality reviews for IT examinations. We recommended that DSC institute a standardized quality review of all phases of the IT examination process and supporting documentation prior to issuance of IT examination results. DSC's comments on the audit report were responsive, and DSC's proposed actions were sufficient to resolve each recommendation.

On September 26, 2003, the OIG issued Audit Report No. 03-044, *The Federal Deposit Insurance Corporation's Progress in Implementing the Gramm-Leach-Bliley Act, Title V - Privacy Provisions*. Overall, we found that the FDIC had made reasonable progress in implementing GLBA Title V provisions related to safeguarding consumer information and privacy notice requirements and modest progress in implementing provisions related to fraudulent access to financial information. As a result, we recommended that DSC (1) identify specific procedures in its examination work programs for examiners to assess the financial institutions' compliance with guidance on protecting consumer information against identity theft; (2) identify the specific procedures in the IT General Work Program that are designed to assess compliance with the safeguarding standards; and (3) standardize guidance related to reporting the results of evaluating a financial institution's compliance with the standards for safeguarding consumer information. DSC's comments on the report were responsive, and DSC's proposed actions were sufficient to resolve each recommendation.

To date, there have been no OIG audits conducted that relate specifically to the FCRA or the FACT Act.

SUMMARY OF LAWS AND REGULATIONS

Gramm-Leach-Bliley Act of 1999 (GLBA)

The GLBA requires federal regulators to issue rules to financial institutions, establishing standards for ensuring the security and privacy of consumer information. The GLBA Title V, *Privacy,* includes two subtitles – A and B. Subtitle A provides a mechanism to protect the confidentiality of a consumer's nonpublic personal information. Subtitle B prohibits "pretext calling," which is a deceptive practice used to obtain information on the financial assets of consumers. Criminal penalties and regulatory and administrative enforcement mechanisms were established to help prevent this practice. Title V of GLBA also requires agencies to strengthen prohibitions on identity theft and requires a federal study on information sharing among financial institutions and their affiliates.[13] Included are prohibitions on disclosing consumer account numbers to nonaffiliated third parties for use in telemarketing, direct mail marketing, or other marketing through electronic mail.

On June 1, 2000, the four federal bank and thrift regulators published substantively identical regulations that implemented provisions of the GLBA governing the privacy of consumer financial information. The FDIC established Part 332, *Privacy of Consumer Financial Information,*[14] which establishes the duties of a financial institution to provide particular notices and limitations on its disclosure of nonpublic personal information. Furthermore, each institution must provide notices of its privacy policies to its customers. Under this regulation, financial institutions are required to disclose, initially when a customer relationship is established and annually, thereafter, their privacy policies, including policies on sharing information with affiliates and nonaffiliated third parties. The privacy regulations became effective on November 13, 2000. Compliance was required as of July 1, 2001.

Fair Credit Reporting Act of 1968 (FCRA)

The FCRA establishes standards for the collection and permissible purposes for dissemination of data by CRAs. The primary purpose of the FCRA is to regulate the nationwide consumer reporting system to help ensure the accuracy and security of consumer reports. The FCRA contains substantive requirements for CRAs. The requirements can be applicable to banks that engage in information-sharing practices that constitute the communication of consumer reports. Specifically, the FCRA prescribes standards that address information collected by businesses that provide information used to determine consumer eligibility for credit, insurance, or employment. FCRA imposes requirements for accuracy, limits purposes for which such information may be disseminated, allows certain rights for consumer access, and includes civil and criminal penalties for its violations.

[13] Under Subtitle A, the term "affiliate" means any company that controls, is controlled by, or is under common control with another company.

[14] Part 332 applies to financial institutions for which the FDIC has primary supervisory authority, including state-charted institutions that are not members of the Federal Reserve System, insured state branches of foreign banks, and certain subsidiaries of such entities.

The FCRA was amended in 1996 to allow financial institutions to share information other than their own transactions and experiences, but only with their affiliates. The GLBA made additional changes, including provisions removing the prohibition against conducting routine FCRA examinations and permitting regulations to be adopted to implement FCRA requirements. The purposes of the FCRA, as amended, include the following:

- to regulate aspects of the consumer reporting industry,
- to place disclosure obligations on users of consumer reports,
- to establish requirements applicable to the furnishing of information to CRAs, and
- to require timely responses to consumer inquiries regarding information maintained by CRAs.

The FCRA was amended again in 2003 by the FACT Act, which created many new responsibilities designed to address the growing problem of identity theft.

Fair and Accurate Credit Transactions Act of 2003 (FACT Act)

The FACT Act preserves uniform national standards for the content of consumer report information and consumer access to such information and restricts the use and disclosure of sensitive medical information. The FACT Act provisions apply primarily to banks and CRAs. Some of the FACT Act provisions contain deadlines for establishing regulations, while others do not. In addition, the FACT Act contains a number of self-executing provisions that require bank compliance. The first three sections of the FACT Act address the title of the act, definitions, and effective dates. The remainder of the FACT Act contains the following titles:

- Title I: *Identity Theft Prevention and Credit History Restoration* – focuses on the responsibilities of institutions and CRAs to prevent identity theft and to help consumers remedy the effects when such a theft occurs.
- Title II: *Improvements in Use of and Consumer Access to Credit Information* – creates new rights for consumers with regard to accessing and limiting the use of their personal information.
- Title III: *Enhancing the Accuracy of Consumer Report Information* – addresses the issue of inaccurate credit reports, with main requirements addressing improvements in the reporting process as well as new disclosures designed to help consumers understand the role of their credit scores in underwriting and pricing decisions.
- Title IV: *Limiting the Use and Sharing of Medical Information in the Financial System* – prohibits banks from obtaining or using medical information about a consumer for determining eligibility for credit.
- Title V: *Financial Literacy and Education Improvement* – requires that several federal government agencies, including the federal banking agencies, form a financial literacy commission charged with developing and implementing strategies for improving financial literacy among the American public.
- Title VI: *Protecting Employee Misconduct Investigations* – requires that certain communications from employee investigations be excluded from the definition of consumer reports.

- Title VII: *Relation to State Laws* – addresses the FACT Act's impact on state laws.
- Title VIII: *Miscellaneous* – addresses clerical amendments to the FACT Act.

The FACT Act contains new responsibilities for CRAs, financial institutions, and other users of consumer reports and provides many new consumer rights and protections. The FDIC and other federal agencies are responsible for implementing rules and conducting studies in regard to these issues. These issues impact both the compliance and risk management aspects of a financial institution's operations.

Two new restrictions under the FACT Act deal directly with consumer information privacy and financial institutions. First, pursuant to Title IV, Section 411, creditors are prohibited in general from obtaining or using a consumer's medical information in connection with any determination of the consumer's eligibility or continued eligibility for credit. The effective date for Section 411 is June 3, 2004. On November 8, 2005, the FDIC's Board of Directors voted to adopt a final rule on this provision effective April 1, 2006.

The second new restriction addresses the use of information obtained from affiliates. Title II of the FACT Act prohibits an entity from using information obtained from an affiliate to market its products or services, unless the consumer is given the opportunity to opt out first. This prohibition does not impact a bank's ability to share information; rather, the restriction limits the affiliates' use of the information. Title II, Section 214, requires that regulations be issued in final form by September 4, 2004, with an effective date of March 4, 2005. The FDIC issued a proposed regulation on July 15, 2004.

VARIOUS FDIC ISSUANCES RELATED TO GLBA AND THE FACT ACT

GRAMM-LEACH–BLILEY ACT		
DOCUMENT NUMBER	**TITLE**	**DATE**
FIL-83-2003	FFEIC Information Technology Examination Handbook: *New Guidance for Examiners, Financial Institutions and Technology Service Providers on Electronic Banking, Information Technology (IT) Audits, and the FedLine Electronic Funds Transfer Application*	October 27, 2003
RDM-2004-002	*Report Treatment of Compliance with the Interagency Guidelines Establishing Standards for Safeguarding Consumer Information*	January 29, 2004
FIL-27-2004	*Guidance on Safeguarding Consumers Against E-Mail and Internet-Related Fraudulent Schemes*	March 12, 2004
FIL-84-2004	Guidance on Instant Messaging: *Guidance on the Risks Associated with Instant Messaging*	July 21, 2004
FIL-103-2004	Internet Banking Fraud: *Interagency Informational Brochure on Internet "Phishing" Scams*	September 13, 2004
FIL-132-2004	Identify Theft: *Study on "Account-Hijacking" Identity Theft and Suggestions for Reducing Online Fraud*	December 14, 2004
FIL-59-2005	*Identity Theft Study Supplement on "Account-Hijacking" Identity Theft*	July 5, 2005
FIL-64-2005	"Pharming": *Guidance on How Financial Institutions Can Protect Against Pharming Attacks*	July 18, 2005
FIL-66-2005	*Spyware Guidance on Mitigating Risks From Spyware*	July 22, 2005
FIL-103-2005	FFEIC Guidance: *Authentication in an Internet Banking Environment*	October 12, 2005
Press Release 127-2005	Federal Bank and Thrift Regulatory Agencies Publish *Guide to Help Financial Institutions Comply with Information Security Guidelines*	December 14, 2005
FAIR AND ACCURATE CREDIT TRANSACTIONS ACT		
DOCUMENT NUMBER	**TITLE**	**DATE**
FIL-47-2004	Medical Privacy Regulations Under the Fair and Accurate Credit Transactions Act of 2003: *Notice of Proposed Rulemaking Regarding Medical Privacy (Part 334 of the FDIC's Rules and Regulations)*	April 28, 2004
FIL-73-2004	Disposal of Consumer Information: *Notice of Proposed Rulemaking on Disposal of Consumer Information*	June 17, 2004
FIL-82-2004	Affiliate Marketing Opt Out Regulations: *Notice of Proposed Rulemaking Regarding Affiliate Marketing Opt Outs (Part 334 of the FDIC's Rules and Regulations)*	July 15, 2004
RDM-2004-055	*Fair and Accurate Credit Transactions Act of 2003 – Effective Dates*	November 29, 2004
FIL-130-2004	*Fair and Accurate Credit Transactions Act Effective Dates*	December 13, 2004

Source: FDIC Legal Division's FACT Act Status Report and various FILs and RDMs.

CROSSWALK OF FACT ACT PROVISIONS TO FDIC RULES AND REGULATIONS AND RELATED GUIDANCE

FACT Act Section Number and Heading	FDIC Rules and Regulations	Financial Institution Letters (FIL) and/or DSC Examination Procedures (OIG Comments Are in Bold)
Section 1: Short Title and Table of Contents		
Section 2: Definitions		
Section 3: Effective Dates		
TITLE I – IDENTITY THEFT PREVENTION AND CREDIT HISTORY RESTORATION		
Subtitle A – Identity Theft Prevention		
111. Amendment to Definitions		
Section 111	The FDIC is not required to issue regulations. The Federal Trade Commission (FTC) may issue regulations to define "identity theft."	**Amends Section 603 of FCRA (re: definitions) by adding definitions to include, but not limited to "fraud alert," "identity theft," "identity theft report," and "federal banking agency."**
112. Fraud Alerts and Active Duty Alerts		
Section 112	The FDIC is not required to issue regulations. FTC issued regulations on November 3, 2004.	RDM-2004-055, *Fair and Accurate Credit Transactions Act of 2003-Effective Dates*, dated November 29, 2004, reiterates the requirements of this provision and includes a procedure to be performed in compliance examinations beginning after December 1, 2004. FIL-130-2004, *Fair and Accurate Credit Transactions Act Effective Dates*, dated December 13, 2004, provides an effective date of December 1, 2004 for this self-executing provision.

FACT Act Section Number and Heading	FDIC Rules and Regulations	Financial Institution Letters (FIL) and/or DSC Examination Procedures (OIG Comments Are in Bold)
113. Truncation of Credit and Debit Card Account Numbers		
Section 113	The FDIC is not required to issue regulations.	**Amends FCRA Section 605 by adding Subsection (g), which includes effective-date provisions.** RDM-2004-055, *Fair and Accurate Credit Transactions Act of 2003-Effective Dates*, dated November 29, 2004, reiterates the requirements of this provision and includes procedures to be performed in compliance examinations beginning after December 1, 2004. The RDM also provides additional effective dates for Automated Teller Machines and Point of Sale terminals.
114. Procedures for Identification of Possible Instances of Identity Theft		
Section 114	The federal banking regulators, National Credit Union Administration (NCUA), and FTC are required to issue regulations jointly. There is no statutory due date for issuing regulations.	**Amends FCRA Section 615 by replacing Subsection (e). Regulations are to address financial institutions, creditors, and/or card issuers.** RDM-04-055, *Fair and Accurate Credit Transactions Act of 2003-Effective Dates,* dated November 29, 2004, reiterates the requirements of this provision and states that this provision will be reviewed during IT examinations once final regulations are issued. FIL-130-2004, *Fair and Accurate Credit Transactions Act Effective Dates,* dated December 13, 2004, states that the effective date for this provision will be set forth in the final rule.
115. Authority to Truncate Social Security Numbers		
Section 115	The FDIC is not required to issue regulations.	**Amends FCRA Section 609(a)(1) by adding additional language thereto.**

FACT Act Section Number and Heading	FDIC Rules and Regulations	Financial Institution Letters (FIL) and/or DSC Examination Procedures (OIG Comments Are in Bold)
Subtitle B – Protection and Restoration of Identity Theft Victim Credit History		
151. Summary of Rights of Identity Theft Victims		
Section 151	FTC, in consultation with the federal banking agencies, shall prepare a model summary of rights for fraud and identity theft victims. Final rule codified at 16 C.F.R. Part 698; 69 FR 69776 (November 30, 2004). Also contains a self-executing provision that requires, within 30 days after receiving a request from an identity theft victim, a business entity that has entered into a commercial transaction with a person, who has allegedly made unauthorized use of the means of identification of a victim, shall provide a copy of the application and transaction records to: the victim, federal/state/local authorities, or any law enforcement agency investigating the identity theft and authorized by the victim to take receipt of the records.	**Amends FCRA Section 609 by adding Subsections (d) and (e), which contain detailed provisions regarding victims of identity theft. Section 609(d) requires FTC, in consultation with the federal banking agencies, to prepare a model summary of rights for fraud and identity theft victims. Financial institutions are required to distribute a summary of rights to identity theft victims. Section 609(e) is a self-executing provision that requires, within 30 days after receiving a request from an identity theft victim, a business entity that has entered into a commercial transaction with a person, who has allegedly made unauthorized use of the means of identification of a victim, shall provide a copy of the application and transaction records to: the victim, federal/state/local authorities, or any law enforcement agency investigating the identity theft and authorized by the victim to take receipt of the records. FCRA Section 609(e) (9)(A) has reference to GLBA's privacy provisions Subtitle A of Title V; and Section 609(e)(9)(B) addresses law enforcement.** RDM-2004-055, *Fair and Accurate Credit Transactions Act of 2003-Effective Dates*, dated November 29, 2004, reiterates the requirements of this provision and includes procedures to be performed in compliance examinations beginning after December 1, 2004 for the portion of this provision that was effective June 4, 2004, which did not require the issuance of regulations (self-executing).

FACT Act Section Number and Heading	FDIC Rules and Regulations	Financial Institution Letters (FIL) and/or DSC Examination Procedures (OIG Comments Are in Bold)
152. Blocking of Information Resulting From Identity Theft		
Section 152	The FDIC is not required to issue regulations. The FTC issued regulations on November 3, 2004.	**Adds Section 605B entitled, *Block of Information Resulting from Identity Theft,* to FCRA. FACT Act Section 112(b) requires FTC to issue regulations on what constitutes "appropriate proof of identity" for purposes of FCRA Sections 605A, 605B, and 609(a)(1).** FIL-130-2004, *Fair and Accurate Credit Transactions Act Effective Dates*, dated December 13, 2004, provides an effective date of December 1, 2004 for this provision.
153. Coordination of Identity Theft Complaint Investigations		
Section 153	The FTC published a Notice of FTC Publication in 70 *Federal Register* 21792 (April 27, 2005). Notice is effective as of May 2, 2005. The FTC, in consultation with the federal banking agencies, shall develop a model form and procedures to be used by victims of identity theft to contact and inform creditors and consumer reporting agencies.	**Amends FCRA Section 621 by adding Subsection (f).** RDM-2004-055, *Fair and Accurate Credit Transactions Act of 2003-Effective Dates,* dated November 29, 2004, reiterates the requirements of this provision and states that it will be reviewed during IT examinations once final regulations are issued.
154. Prevention of Repollution of Consumer Reports		
Section 154	The FDIC is not required to issue regulations.	**FACT Act Section 154(a) amends FCRA Section 623(a) by adding paragraph (6), which applies to persons furnishing information to credit reporting agencies. FACT Act Section 154(b) amends FCRA Section 615 by adding Subsection (f), which pertains to persons who sell, transfer, or place for collection debts after being notified of identity theft.** RDM-2004-055, *Fair and Accurate Credit Transactions Act of 2003-Effective Dates,* dated November 29, 2004, reiterates the requirements of this provision and includes a procedure to be performed in compliance examinations beginning after December 1, 2004.

FACT Act Section Number and Heading	FDIC Rules and Regulations	Financial Institution Letters (FIL) and/or DSC Examination Procedures (OIG Comments Are in Bold)
		FIL-130-2004, *Fair and Accurate Credit Transactions Act Effective Dates*, dated December 13, 2004, provides an effective date of December 1, 2004, for this self-executing provision.
155. Notice by Debt Collectors With Respect to Fraudulent Information		
Section 155	The FDIC is not required to issue regulations.	**Amends FCRA Section 615 by adding Subsection (g). Applies to debt collectors acting on behalf of creditors or other users of a consumer report.** RDM-2004-055, *Fair and Accurate Credit Transactions Act of 2003-Effective Dates,* dated November 29, 2004, reiterates the requirements of this provision and includes a procedure to be performed in compliance examinations beginning after December 1, 2004.
156. Statute of Limitations		
Section 156	The FDIC is not required to issue regulations.	**Amends FCRA Section 618 by substituting revised language.**
157. Study on the Use of Technology to Combat Identity Theft		
Section 157	The FDIC is not required to issue regulations. The Secretary of the Treasury is to consult with the federal banking agencies on a study of technology used to combat identity theft 180 days after enactment of the FACT Act.	

FACT Act Section Number and Heading	FDIC Rules and Regulations	Financial Institution Letters (FIL) and/or DSC Examination Procedures (OIG Comments Are in Bold)
TITLE II – IMPROVEMENTS IN USE OF AND CONSUMER ACCESS TO CREDIT INFORMATION		
211. Free Consumer Reports		
Section 211	The FDIC is not required to issue regulations. The FTC is required to issue regulations and a model summary of consumer rights.	**Amends FCRA Sections 609(c) and 612(a) and adds Section 629 entitled, *Corporate and Technological Circumvention*.**
212. Disclosure of Credit Scores		
Section 212	The FDIC is not required to issue regulations.	**Amends FCRA Sections 605(d), 609(c), and 625(b) and adds Subsections 609(f) and (g). The latter provision applies to mortgage lenders who use consumer credit reports. These lenders are required to provide a notice to loan applicants regarding credit scores.** RDM-2004-055, *Fair and Accurate Credit Transactions Act of 2003-Effective Dates,* dated November 29, 2004, reiterates the requirements of this provision and includes a procedure to be performed in compliance examinations beginning after December 1, 2004. FIL-130-2004, *Fair and Accurate Credit Transactions Act Effective Dates*, dated December 13, 2004, provides an effective date of December 1, 2004 for this self-executing provision.
213. Enhanced Disclosure of the Means Available to Opt Out of Prescreened Lists		
Section 213	FTC to consult with federal banking agencies and NCUA to issue regulations on the format of notices for opting out of prescreened lists. Final rule at 70 *Federal Register* 5022 (January 31, 2005). Final rule sets an effective date of August 1, 2005.	**Amends FCRA Section 615(d)(2). Section 213(d) requires FTC to wage public awareness campaign on the issue of opting out.** RDM-2004-055, *Fair and Accurate Credit Transactions Act of 2003-Effective Dates*, dated November 29, 2004, reiterates the requirements of this provision and states that it will be reviewed during compliance examinations once final regulations are issued.

FACT Act Section Number and Heading	FDIC Rules and Regulations	Financial Institution Letters (FIL) and/or DSC Examination Procedures (OIG Comments Are in Bold)
214. Affiliate Marketing		
Section 214(a) *Special Rule for Solicitation for Purposes of Marketing*	The federal banking agencies, NCUA, and FTC (with respect to the entities that are subject to their respective enforcement) and the Securities and Exchange Commission (SEC) were required to issue final regulations no later than September 4, 2004, with an effective date no later than 6 months after issuance of the final regulations. Each agency was required to consult and coordinate with each other to the extent possible to ensure the regulations each agency issued are consistent and comparable. A proposed regulation was issued July 15, 2004.	**FACT Section 214(a) redesignates certain existing FCRA Sections and adds a new Section 624, to FCRA. Section 624 deals with a limitation on affiliates' marketing efforts based on credit-report-type information shared by another affiliate and includes notice requirements to the consumer.** FIL-82-2004, *Affiliate Marketing Opt Out Regulations*, dated July 15, 2004, includes proposed rules and solicits comments from financial institutions that were due by August 16, 2004. RDM-2004-055*, Fair and Accurate Credit Transactions Act of 2003-Effective Dates*, dated November 29, 2004, reiterates the requirements of this provision and states that it will be reviewed during compliance examinations once final regulations are issued. The RDM also states that this provision will be effective within 6 months after final regulations are issued.
Section 214(e) *Studies of Information Practices*	The federal banking agencies, NCUA, and FTC are required to jointly conduct studies and initially report the results and any recommendations for legislative or regulatory action to the Congress by December 4, 2006. Follow-up reports are required at least once every 3 years thereafter.	**FACT Act Section 214(e) sets forth requirements for the federal banking agencies, NCUA, and FTC to conduct regular joint studies of consumer information-sharing practices of financial institutions.**
215. Study of Effects of Credit Scores and Credit-Based Insurance Scores on Availability and Affordability of Financial Products		
Section 215	The FDIC is not required to issue regulations. The Federal Reserve Board and FTC are required to consult with the Office of Fair Housing and Equal Opportunity to conduct a study and shall include input from relevant federal regulators.	

FACT Act Section Number and Heading	FDIC Rules and Regulations	Financial Institution Letters (FIL) and/or DSC Examination Procedures (OIG Comments Are in Bold)
216. Disposal of Consumer Report Information and Records		
Section 216	Final rules codified at 12 C.F.R. Part 334.83 and 364.101. Final regulation was published December 28, 2004 and became effective on July 1, 2005.	**The FACT Act adds Section 628 entitled, *Disposal of Records,* to FCRA. This Section requires persons who maintain consumer information to dispose of that information properly.** FIL-73-2004, *Disposal of Consumer Information: Notice of Proposed Rulemaking on Disposal of Consumer Information,* dated June 17, 2004, includes the proposed requirements and solicits comments from financial institutions. RDM-2004-055, *Fair and Accurate Credit Transactions Act of 2003-Effective Dates*, dated November 29, 2004, reiterates the requirements of this provision and states that it will be reviewed during IT examinations after final regulations are issued. FIL-130-2004, *Fair and Accurate Credit Transactions Act Effective Dates*, dated December 13, 2004, states that the effective date for this provision will be set forth in the final rule. FIL-7-2005, *Fair and Accurate Credit Transactions Act of 2003 Guidelines Requiring the Proper Disposal of Consumer Information,* dated February 2, 2005, includes the requirements for financial institutions in ensuring compliance with the final rule.
217. Model Disclosure for Furnishing Negative Information		
Section 217	The Federal Reserve is to issue a model disclosure that a financial institution may use to notify a consumer that it has furnished negative information to credit reporting agencies. Final rule codified at 12 C.F.R. Part 222; 69 *Federal Register* 33281 (June 15, 2004).	**Amends FCRA Section 623(a) by adding new paragraph (7). Requires certain financial institutions that provide negative information about a consumer to a CRA to furnish a notice to the consumer.** RDM-2004-055, *Fair and Accurate Credit Transactions Act of 2003-Effective Dates*, dated November 29, 2004, reiterates the

FACT Act Section Number and Heading	FDIC Rules and Regulations	Financial Institution Letters (FIL) and/or DSC Examination Procedures (OIG Comments Are in Bold)
		requirements of this provision and includes procedures to be performed in compliance examinations beginning after December 1, 2004.
TITLE III – ENHANCING THE ACCURACY OF CONSUMER REPORT INFORMATION		
311. Risk Based Pricing Notice		
Section 311	The FDIC is not required to issue regulations.	**Amends FCRA Section 615 by adding Subsection (h) requiring any person that uses a consumer report in granting credit on "material terms that are materially less favorable than the most favorable terms available to a substantial portion of [certain] consumers" to provide an oral, written, or electronic notice to the consumer in the form required by the regulations.** RDM-2004-055, *Fair and Accurate Credit Transactions Act of 2003-Effective Dates,* dated November 29, 2004, reiterates the requirements of this provision and states that this provision will be reviewed during compliance examinations once final regulations are issued. FIL-130-2004, *Fair and Accurate Credit Transactions Act Effective Dates,* dated December 13, 2004, states that this provision becomes effective December 1, 2004, but the parameters for and date of compliance will be established in the final rule.
312. Procedures to Enhance the Accuracy and Integrity of Information Furnished to Consumer Reporting Agencies		
Section 312(a) *Accuracy Guidelines and Regulations*	There is no statutory due date for issuance of final regulations. The federal banking agencies, NCUA, and FTC, with respect to the entities that are subject to their respective enforcement, are required to issue guidelines and regulations regarding the accuracy and integrity of information provided to consumer reporting agencies.	RDM-2004-055, *Fair and Accurate Credit Transactions Act of 2003-Effective Dates*, dated November 29, 2004, reiterates the requirements of this provision and states that it will be reviewed during compliance examinations once final regulations are issued.

FACT Act Section Number and Heading	FDIC Rules and Regulations	Financial Institution Letters (FIL) and/or DSC Examination Procedures (OIG Comments Are in Bold)
	Each agency was required to consult and coordinate with each other to the extent possible to ensure the regulations issued by each are consistent and comparable.	FIL-130-2004, *Fair and Accurate Credit Transactions Act Effective Dates*, dated December 13, 2004, states that the effective date for this provision will be set forth in the final rule.
Section 312(c) *Ability of Consumer to Dispute Information Directly With Furnisher*	There is no statutory due date for issuance of final regulations. The federal banking agencies, NCUA, and FTC are required to jointly issue regulations regarding reinvestigations of disputes concerning the accuracy of consumer-report information.	RDM-2004-055, *Fair and Accurate Credit Transactions Act of 2003-Effective Dates*, dated November 29, 2004, reiterates the requirements of this provision and states that it will be reviewed during compliance examinations after final regulations are issued. FIL-130-2004, *Fair and Accurate Credit Transactions Act Effective Dates*, dated December 13, 2004, states that the effective date for this provision will be set forth in the final rule.
313. FTC and Consumer Reporting Agency Action Concerning Complaints		
Section 313	The FDIC is not required to issue regulations. The FTC and Federal Reserve Board are to jointly study how consumer agency and furnishers of information to credit reporting agencies are complying with requirements related to disputed information. The progress report was due 1 year after the FACT Act's enactment.	**FACT Act 313(a) amends FCRA 611 by adding Subsection (e), which requires the FTC to compile complaints related to inaccurate or incomplete information.**
314. Improved Disclosure of the Results of Reinvestigation		
Section 314	The FDIC is not required to issue regulations.	RDM-2004-055, *Fair and Accurate Credit Transactions Act of 2003-Effective Dates*, dated November 29, 2004, reiterates the requirements of this provision and includes procedures to be performed in compliance examinations beginning after December 1, 2004.

FACT Act Section Number and Heading	FDIC Rules and Regulations	Financial Institution Letters (FIL) and/or DSC Examination Procedures (OIG Comments Are in Bold)
315. Reconciling Addresses		
Section 315	The federal banking regulators, NCUA, and FTC are to jointly issue regulations providing guidance regarding policies and procedures that a user of a consumer report should employ when the user has received notice of a discrepancy in a consumer's address. The FACT Act does not provide a statutory due date for issuance of the regulations.	**Amends FCRA Section 605 by adding Subsection (h) regarding the need for a CRA to notify a consumer about a discrepancy in the consumer's address in the CRAs' files.** RDM-2004-055, *Fair and Accurate Credit Transactions Act of 2003-Effective Dates,* dated November 29, 2004, reiterates the requirements of this provision and states that this provision will be reviewed during compliance examinations after final regulations are issued. FIL-130-2004, *Fair and Accurate Credit Transactions Act Effective Dates*, dated December 13, 2004, states that the effective date for this provision will be set forth in the final rule.
316. Notice of Dispute Through Reseller		
Section 316	The FDIC is not required to issue regulations.	
317. Reasonable Reinvestigations Required		
Section 317	The FDIC is not required to issue regulations.	**Amends FCRA Section 611(a)(1)(A) regarding reinvestigations.**
318. FTC Study of Issues Relating to the Fair Credit Reporting Act		
Section 318	The FDIC is not required to issue regulations. FTC is to study ways to improve the operations of FCRA. The report was due 1 year after the FACT Act's enactment.	
319. FTC Study of Accuracy of Consumer Reports		
Section 319	The FDIC is not required to issue regulations. FTC is to study the accuracy and completeness of information in consumer reports prepared by CRAs. An interim report	

FACT Act Section Number and Heading	FDIC Rules and Regulations	Financial Institution Letters (FIL) and/or DSC Examination Procedures (OIG Comments Are in Bold)
	was due 1 year after the FACT Act's enactment and every 2 years thereafter for 8 years. The final report is due 2 years after the last interim report.	
TITLE IV – LIMITING THE USE AND SHARING OF MEDICAL INFORMATION IN THE FINANCIAL SYSTEM		
411. Protection of Medical Information in the Financial System		
Section 411	Final rules codified at 12 C.F.R. Part 334 and published in the *Federal Register* on November 22, 2005.	**FACT Act Section 411(a) amends FCRA Section 604(g) by placing limitations on CRAs and creditors with respect to the use of medical information about consumers and the redisclosure of that information by any person.** FIL-47-2004, *Medical Privacy Regulations Under the Fair and Accurate Credit Transactions Act of 2003*, dated April 28, 2004, includes proposed rules and solicits comments from financial institutions that were due by May 28, 2004. RDM-2004-055, *Fair and Accurate Credit Transactions Act of 2003-Effective Dates*, dated November 29, 2004, reiterates the requirements of this provision and includes procedures to be performed in compliance examinations beginning after December 1, 2004. The RDM also states that implementing rules defining exceptions will become effective after final regulations are issued. FIL-51-2005, *Fair Credit Reporting Medical Information Interim Final Rules*, dated June 16, 2005 includes interim final rules that will take effect on March 7, 2006, and solicits comments from financial institutions that were due by July 11, 2005.

FACT Act Section Number and Heading	FDIC Rules and Regulations	Financial Institution Letters (FIL) and/or DSC Examination Procedures (OIG Comments Are in Bold)
		FIL-121-2005, *Fair Credit Reporting – Medical Information Final Rules*, dated December 8, 2005, includes the final rules that will take effect on April 1, 2006.
412. Confidentiality of Medical Contact Information in Consumer Reports		
Section 412	The FDIC is not required to issue regulations.	
TITLE V – FINANCIAL LITERACY AND EDUCATION IMPROVEMENT		
511. Short Title		
Section 511	The FDIC is not required to issue regulations.	
512. Definitions		
Section 512	The FDIC is not required to issue regulations.	
513. Establishment of Financial Literacy and Education Commission		
Section 513	The FDIC is not required to issue regulations.	
514. Duties of the Commission		
Section 514	The FDIC is not required to issue regulations.	
515. Powers of the Commission		
Section 515	The FDIC is not required to issue regulations.	
516. Commission Personal Matters		
Section 516	The FDIC is not required to issue regulations.	
517. Studies by the Comptroller General		
Section 517	The FDIC is not required to issue regulations.	

FACT Act Section Number and Heading	FDIC Rules and Regulations	Financial Institution Letters (FIL) and/or DSC Examination Procedures (OIG Comments Are in Bold)
518. The National Public Service Multimedia Campaign to Enhance the State of Financial Literacy		
Section 518	The FDIC is not required to issue regulations.	
519. Authorization of Appropriations		
Section 519	The FDIC is not required to issue regulations.	
TITLE VI – PROTECTING EMPLOYEE MISCONDUCT INVESTIGATIONS		
611. Certain Employee Investigation Communications Excluded From Definition of Consumer Report		
Section 611	The FDIC is not required to issue regulations.	
TITLE VII – RELATION TO STATE LAWS		
711. Relation to State Laws		
Section 711	The FDIC is not required to issue regulations.	
TITLE VIII – MISCELLANEOUS		
811. Clerical Amendments		
Section 811	The FDIC is not required to issue regulations.	

CORPORATION COMMENTS

FDIC
Federal Deposit Insurance Corporation
550 17th St. NW Washington DC, 20429
Division of Supervision and Consumer Protection

February 15, 2006

TO: Stephen M. Beard, Deputy Inspector General
Office of Inspector General

FROM: Christopher J. Spoth, Acting Director [Electronically produced version; original signed by Christopher J. Spoth]

SUBJECT: DSC Response to OIG Draft Report Entitled *FDIC's Guidance to Institutions and Examiners for Implementing the Gramm-Leach-Bliley Act Title V and the Fair and Accurate Credit Transactions Act (Assignment No. 2005-054)*

The Division of Supervision and Consumer Protection (DSC) appreciates the opportunity to respond to the Office of Inspector General (OIG) draft report entitled *FDIC's Guidance to Institutions and Examiners for Implementing the Gramm-Leach-Bliley Act (GLBA) Title V and the Fair and Accurate Credit Transactions Act (FACT Act)*. We are gratified that you found that DSC "has established rules and regulations that appropriately address the GLBA Title V provisions related to the privacy and security of consumer information." Further, that DSC "provided adequate guidance to FDIC-supervised institutions and established adequate examination guidance and procedures to ensure that these institutions meet GLBA requirements." With respect to the FACT Act, FDIC continues to be fully engaged in the inter-agency processes to issue joint guidance on remaining items.

OIG RECOMMENDATIONS

We recommend the Director, DSC:

(1) Finalize interim examination guidance that addresses FACT Act data security provisions for which final rules and regulations have been issued or that are self-executing.

(2) Develop, in coordination with the joint-agency rulemaking committee, a more aggressive project management plan that will expedite the issuance of final rules and regulations for all FACT Act data security provisions.

DSC RESPONSE

DSC concurs, with the intent of your recommendations, and provides the following responses to your recommendations.

CORPORATION COMMENTS

(1) We are fully committed and are in process of developing and issuing examination guidance. Examination guidance that addresses FACT Act provisions for which final rules and regulations have been issued or that are self-executing will be issued as planned by year-end 2006. For areas to be covered by compliance examinations, procedures which include the self-executing FACT Act provisions have been approved by the FFIEC Consumer Compliance Task Force. These procedures have been provided to compliance examination staff at regional training conferences and other training venues subsequent to their approval. They are being formally distributed to both examination staff and the industry through a Regional Director memorandum and a Financial Institution Letter that are now under review by DSC senior management. These actions will also be completed by year-end 2006.

(2) The recommendation suggests that there is one multi-agency rulemaking committee. However, through the FACT Act, Congress directed different groups of agencies to issue rules and guidance in different areas. Where Congress required the FDIC to participate in these efforts, the FDIC is actively participating. Moreover, we are committed to expediting the process. As members of the separate working groups responsible for drafting each set of rules or guidelines, FDIC staff has consistently made efforts to move the process forward. We will continue to promote expedited processes during 2006.

Note: The OIG has characterized its recommendations as applicable to FACT Act "data security provisions." However, the OIG's draft report addresses all of the FACT Act provisions, not just those dealing with data security. Consequently, we suggest deleting the references to "data security" from the recommendations and have provided our answers assuming that deletion is made in the final report.

MANAGEMENT RESPONSE TO RECOMMENDATIONS

This table presents the management response on the recommendations in our report and the status of the recommendations as of the date of report issuance.

Rec. Number	Corrective Action: Taken or Planned/Status	Expected Completion Date	Monetary Benefits	Resolved:[a] Yes or No	Open or Closed[b]
1	DSC concurred with the intent of the recommendation. DSC will issue examination guidance that addresses FACT Act provisions for which final rules and regulations have been issued or that are self-executing by year-end 2006. For areas to be covered by compliance examinations, procedures that include the self-executing FACT Act provisions have been approved by the FFIEC Consumer Compliance Task Force. They are being formally distributed to both examiners and the industry through an RDM and a FIL.	December 31, 2006	None	Yes	Open
2	DSC concurred with the intent of the recommendation. According to DSC, the FDIC is actively participating in and is committed to expediting the interagency process to issue final rules and regulations for all FACT Act provisions. As a member of the separate working groups responsible for drafting each set of rules or guidelines, the FDIC has consistently made efforts to move the process forward and will continue to promote expedited processes.	December 31, 2006	None	Yes	Open

[a] Resolved – (1) Management concurs with the recommendation, and the planned corrective action is consistent with the recommendation.
(2) Management does not concur with the recommendation, but planned alternative action is acceptable to the OIG.
(3) Management agrees to the OIG monetary benefits, or a different amount, or no ($0) amount. Monetary benefits are considered resolved as long as management provides an amount.

[b] Once the OIG determines that the agreed-upon corrective actions have been completed and are effective, the recommendation can be closed.