

# Office of Inspector General



September 26, 2003  
Audit Report No. 03-044

---

The Federal Deposit Insurance  
Corporation's Progress in Implementing  
the Gramm-Leach-Bliley Act, Title V --  
Privacy Provisions



## TABLE OF CONTENTS

<b>BACKGROUND.....</b>	<b>2</b>
<b>Subtitle A of GLBA Title V.....</b>	<b>2</b>
<b>Subtitle B of GLBA Title V.....</b>	<b>3</b>
<b>Other Sections of GLBA Title V.....</b>	<b>4</b>
<b>FDIC Rules and Regulations.....</b>	<b>4</b>
<b>DSC's Approach for Examining Standards for Safeguarding     Customer Information.....</b>	<b>5</b>
<b>DSC's Approach for Examining Privacy Notice Requirements.....</b>	<b>7</b>
<b>RESULTS OF EVALUATION.....</b>	<b>8</b>
<b>FINDINGS AND RECOMMENDATIONS.....</b>	<b>10</b>
<b>FINDING A: FDIC'S PROGRESS IN IMPLEMENTING GLBA TITLE V -- PRIVACY PROVISIONS.....</b>	<b>10</b>
<b>FDIC Rules and Regulations and FDIC Procedures that Address     GLBA Title V Provisions.....</b>	<b>10</b>
<b>Internal Quality Assurance Review of the Privacy     Examination Process.....</b>	<b>12</b>
<b>DSC Views on Financial Institutions' Compliance with GLBA.....</b>	<b>13</b>
<b>FINDING B: DSC'S EXAMINATION PROCEDURES FOR GLBA TITLE V -- PRIVACY.....</b>	<b>15</b>
<b>Subtitle B - Fraudulent Access to Financial Information.....</b>	<b>15</b>
<b>Procedures for Examining Standards for Safeguarding     Customer Information.....</b>	<b>17</b>
<b>CONCLUSIONS AND RECOMMENDATIONS.....</b>	<b>22</b>
<b>CORPORATION COMMENTS AND OIG EVALUATION.....</b>	<b>22</b>
<b>APPENDIX I: OBJECTIVE, SCOPE, AND METHODOLOGY.....</b>	<b>24</b>
<b>APPENDIX II: ACRONYMS USED IN REPORT.....</b>	<b>27</b>
<b>APPENDIX III: SUMMARY CROSSWALK OF GLBA TITLE V PROVISIONS TO FDIC RULES AND REGULATIONS AND FDIC PROCEDURES.....</b>	<b>28</b>
<b>APPENDIX IV: CORPORATION COMMENTS.....</b>	<b>38</b>

**APPENDIX V: MANAGEMENT RESPONSES TO RECOMMENDATIONS.....41**

**TABLES:**

**Table 1: Technology Types and IT Examination Procedures.....7**

**Table 2: FDIC Rules, Guidance, and Implementing Procedures for Major  
GLBA Title V -- Privacy Provisions .....11**

**Table 3: DSC Action Plan Items.....12**

**Table 4: Interagency Procedures - Categories and Key Questions.....18**

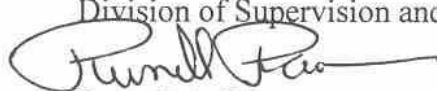
**Table 5: References to the Standards for Safeguarding Customer Information  
in the IT General Work Program "Help" Section.....19**

**Table 6: Example of GLBA-Related Examination Procedures  
that Do Not Reference GLBA.....20**

**Table 7: DSC's Guidelines on GLBA Reporting.....21**

**DATE:** September 26, 2003

**MEMORANDUM TO:** Michael J. Zamorski, Director  
Division of Supervision and Consumer Protection



**FROM:** Russell A. Rau  
Assistant Inspector General for Audits

**SUBJECT:** *The Federal Deposit Insurance Corporation's Progress in Implementing the Gramm-Leach-Bliley Act, Title V -- Privacy Provisions (Report No. 03-044)*

This report presents the results of our evaluation of the Federal Deposit Insurance Corporation's (FDIC) implementation of the Gramm-Leach-Bliley Act of 1999<sup>1</sup> (GLBA), Title V -- Privacy provisions. Congress enacted several privacy provisions in the GLBA in response to concerns about the growing inability of consumers to control access to their personal financial information, namely, GLBA, Title V -- Privacy, Subtitle A and B. These privacy provisions created new requirements for various federal and state regulatory agencies and financial institutions. Congress continues to emphasize the importance of consumer privacy as demonstrated by recent hearings covering the topics of identity theft and obligations regarding disclosures of personal information.<sup>2</sup>

The objective of our evaluation was to determine whether the FDIC has made reasonable progress in implementing the GLBA, Title V privacy provisions. Specifically, we reviewed actions that the FDIC's Division of Supervision and Consumer Protection (DSC)<sup>3</sup> has taken to implement the Title V provisions of GLBA. This evaluation addresses both Subtitle A – Disclosure of Nonpublic Personal Information,<sup>4</sup> and Subtitle B – Fraudulent Access to Financial

---

<sup>1</sup> Pub. L. No. 106-102, codified to titles 12 and 15, United States Code (U.S.C.). The privacy provisions of the Act are codified at 15 U.S.C., §§ 6801 – 6827 and 1681s.

<sup>2</sup> U.S. Senate Committee on Banking, Housing, and Urban Affairs conducted hearings in June 2003: (1) "The Growing Problem of Identity Theft and Its Relationship to the Fair Credit Reporting Act" (June 19, 2003); and (2) "Affiliate Sharing Practices and Their Relationship to the Fair Credit Reporting Act" (June 26, 2003).

<sup>3</sup> The FDIC's DSC, in conjunction with other federal and state regulators, examines financial institutions to ensure they are conducting business in compliance with consumer protection rules and in a way that minimizes risk to their customers and to the deposit insurance funds. There are five categories of examinations: Safety and Soundness, Community Reinvestment Act, Compliance, Information Technology, and Trust.

<sup>4</sup> Subtitle A defines nonpublic personal information as personally identifiable financial information that an institution obtains under any of the following three sets of circumstances: (1) the consumer (see definition in footnote 5) provides the information to the institution to obtain a financial product or service; (2) the information is about the consumer and results from any transaction involving a financial product or service between the institution and the consumer; or (3) the information is about the consumer and is otherwise obtained in connection with providing a financial product or service to that consumer.

Information. For purposes of this report, we generally refer to topics of “safeguarding customer<sup>5</sup> information” and “privacy notice requirements” rather than the specific section numbers within the GLBA. The DSC reviews financial institutions’ compliance with: (1) GLBA provisions on safeguarding customer information as part of DSC’s information technology (IT) examinations and (2) GLBA privacy notice requirements through compliance examinations.

Details of our objective, scope, and methodology are included as Appendix I of this report. Appendix II lists acronyms used in this report.

## **BACKGROUND**

In addition to reforming the financial services industry, the GLBA addressed concerns relating to consumer financial privacy. Title V of the GLBA established major privacy provisions under 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 are established to help prevent this practice. Appendix III of this report provides a summary “crosswalk” of GLBA Title V provisions to FDIC rules and regulations and DSC examination procedures.

### **Subtitle A of GLBA Title V**

In Subtitle A of GLBA Title V, Congress established requirements for financial institutions and regulatory agencies to protect the privacy of nonpublic personal information obtained by financial institutions.

**Financial Institution Responsibilities:** Section 501(a) of Subtitle A, states: “It is the policy of the Congress that each financial institution has an affirmative and continuing obligation to respect the privacy of its customers and to protect the security and confidentiality of those customers’ nonpublic personal information.” Section 502 applies this policy by generally prohibiting financial institutions from disclosing consumers’ nonpublic personal information to any entity that is not an affiliate<sup>6</sup> of, or related by common ownership or control to, the financial institution (nonaffiliated third party),

---

<sup>5</sup> Subtitle A uses the terms “customer” and “consumer” in different sections. “Customer” is not statutorily defined, although “customer relationship” is described in a definition which, in part, refers to regulations which the financial banking regulators were to draft. In those regulations, the federal banking regulators defined “customer” to mean a “consumer” who has established a “customer relationship” with the financial institution. “Consumer” is defined in GLBA Section 509 as an individual (or legal representative) who obtains, from a financial institution, financial products or services which are to be used primarily for personal, family, or household purposes. “Customer relationship” is defined in the regulations as a continuing relationship between a consumer and the financial institution which provided such financial products or services. As a general rule, in this report, we will use “consumer” unless, in the particular context, “customer” would be more appropriate.

<sup>6</sup> Under Subtitle A, the term “affiliate” means any company that controls, is controlled by, or is under common control with another company.

unless the consumer is given an opportunity to opt out<sup>7</sup> of such disclosure. Such an opportunity is provided under Section 503, which states that financial institutions must provide consumers with privacy notices that include an explanation of the institution's policies and practices for disclosing and protecting the privacy of nonpublic personal information.

**Regulatory Agency Responsibilities:** Subtitle A requires various federal<sup>8</sup> and state regulators to establish standards for financial institutions relating to the safeguarding of customer information (Section 501(b)) and to implement those standards, in the same manner, to the extent practicable, "as standards prescribed pursuant to section 39(a) of the Federal Deposit Insurance Act are implemented pursuant to such sections" (Sections 505(a)<sup>9</sup> and 505(b)).<sup>10</sup> In addition, the federal regulators are required to prescribe regulations (Section 504) governing the disclosure of customer information to nonaffiliated third parties.

### **Subtitle B of GLBA Title V**

Subtitle B of GLBA Title V makes it a federal crime to obtain customer information through fraudulent means (Section 521). It is also a violation of Section 521 "for any person to obtain or attempt to obtain, or cause to be disclosed or attempt to cause to be disclosed to any person," customer information through fraudulent means or to solicit someone to obtain such information through fraudulent means. Subtitle B provides for both criminal penalties and civil administrative remedies through the Federal Trade Commission (FTC) and enforcement by federal banking regulators.<sup>11</sup> Subtitle B places the primary responsibility for enforcing the subtitle's provisions with the FTC. However, with respect to financial institutions, the federal banking regulators are required to enforce Subtitle B provisions in accordance with Section 8 of the Federal Deposit Insurance (FDI) Act and may rely on other statutory enforcement authorities the federal banking regulators possess.

Section 525 of Subtitle B requires each federal banking regulator to "review regulations and guidelines applicable to financial institutions under their respective jurisdictions" and to "prescribe such revisions to such regulations and guidelines as may be necessary to ensure that such financial institutions have policies, procedures, and controls in place to prevent the

---

<sup>7</sup> A consumer's direction to a financial institution that it not disclose his or her nonpublic personal information to a nonaffiliated third-party.

<sup>8</sup> The federal regulators responsible for issuing Subtitle A regulations are the Board of Governors of the Federal Reserve System, the FDIC, Federal Trade Commission, National Credit Union Administration, Office of the Comptroller of the Currency, Office of Thrift Supervision, Secretary of the Department of the Treasury, Commodity Futures Trading Commission, and the Securities and Exchange Commission.

<sup>9</sup> Under Section 505(a), federal banking regulators are to enforce the provisions of Subtitle A and related regulations in accordance with Section 8 of the Federal Deposit Insurance Act (FDI Act) (12 U.S.C. § 1818), which contains such enforcement mechanisms as a cease and desist order and civil money penalties. Other statutory enforcement provisions apply in the case of the other federal and state regulators.

<sup>10</sup> Under Section 505(b), federal banking regulators are to implement Section 501(b) standards in the same manner, to the extent practicable, as standards prescribed pursuant to Section 39(a) of the FDI Act (12 U.S.C. §1831 p-1(a)).

<sup>11</sup> For this report, federal banking regulators are the Board of Governors of the Federal Reserve System, FDIC, Office of the Comptroller of the Currency, and the Office of Thrift Supervision.

unauthorized disclosure of customer financial information and to deter and detect” the unauthorized disclosure of customer financial information by false pretenses. Pretext calling is one common method used to fraudulently obtain a customer’s financial information from a financial institution. Pretext calling can lead to “identity theft” -- the fraudulent use of an individual’s personal identifying information to commit a financial crime.

## **Other Sections of GLBA Title V**

GLBA Title V, Section 506, Protection of Fair Credit Reporting Act (FCRA), requires the federal banking regulators to jointly prescribe FCRA regulations related to affiliate information-sharing provisions, as necessary, with respect to financial institutions. The affiliate information-sharing provisions have not yet been fully implemented, but are being addressed through interagency proposed regulations still in process.

GLBA Title V requires that (1) the Secretary of the Treasury, in conjunction with federal banking regulators and the FTC, prepare a report<sup>12</sup> to the Congress by January 1, 2002, regarding information-sharing practices among financial institutions and their affiliates; and (2) the General Accounting Office (GAO) consult with the federal banking regulators in preparing a report<sup>13</sup> on the efficacy of GLBA’s remedies for pretext calling.

## **FDIC Rules and Regulations**

FDIC Rules and Regulations, Parts 364, 332, and 308,<sup>14</sup> implement the requirements of the applicable sections of GLBA Title V, as follows:

**Part 364 – Standards for Safety and Soundness:** Appendix B to Part 364, *Interagency Guidelines Establishing Standards for Safeguarding Customer Information*, sets forth standards pursuant to Section 39 of the FDI Act and GLBA Subtitle A’s customer information safeguarding and enforcement provisions. These guidelines address standards for developing and implementing administrative, technical, and physical safeguards to protect the security, confidentiality, and integrity of customer information.

**Part 332 – Privacy of Consumer Financial Information:** Part 332 governs financial institutions’<sup>15</sup> treatment of nonpublic personal information about consumers and (1) requires a financial institution to provide notice to customers about its privacy policies and practices; (2) describes the conditions under which a financial institution may disclose nonpublic personal information about consumers to nonaffiliated third parties; and (3) provides a method for consumers to prevent a financial institution from

---

<sup>12</sup> As of August 29, 2003, this report had not been finalized.

<sup>13</sup> GAO report on Financial Privacy entitled, *Too Soon to Assess the Privacy Provisions in the Gramm-Leach-Bliley Act of 1999*, dated May 2001 (GAO-01-617).

<sup>14</sup> Codified to title 12 of the Code of Federal Regulations.

<sup>15</sup> Part 332 applies to financial institutions insured by the FDIC (other than members of the Federal Reserve System) for which the FDIC has primary supervisory authority, insured state branches of foreign banks, and certain subsidiaries of such entities.

disclosing that information to most nonaffiliated third parties by “opting out” of that disclosure, subject to exceptions.

**Part 308, Subpart R – Submission and Review of Safety and Soundness Compliance Plans and Issuance of Orders to Correct Safety and Soundness Deficiencies:** The FDIC may, based upon an examination, inspection, or any other information that becomes available to the FDIC, determine that a financial institution has failed to satisfy the safety and soundness standards set out in Part 364 and in Appendix B to Part 364. If the FDIC determines that a financial institution has failed to satisfy any such standard, the FDIC may request the submission of a compliance plan and may take appropriate enforcement actions if the financial institution fails to submit an acceptable plan or fails, in any material respect, to implement a plan accepted by the FDIC.

### **DSC’s Approach for Examining Standards for Safeguarding Customer Information**

The DSC includes the standards for safeguarding customer information in its examination procedures. Since 2001, the DSC has applied the following procedures:

- The federal banking regulators developed examination procedures in 2001 to assist examiners in evaluating a financial institution’s compliance with customer information safeguards established by the federal banking regulators and to ensure that the established standards are applied consistently. The FDIC advised its financial institutions of these procedures through Financial Institution Letter FIL-68-2001, *Examination Procedures to Evaluate Customer Information Safeguards*, dated August 24, 2001. The DSC distributed the examination procedures to its examiners through a Regional Directors Memorandum (RDM) entitled, *Examination Procedures to Evaluate Customer Information Safeguards*, dated August 28, 2001, Transmittal Number 2001-032 (RDM 2001-032). The DSC instructed examiners to assess compliance with customer information safeguards during examinations started after July 1, 2001.
- Examiners could also use the procedures contained in an Examination Documentation (ED) Module, “GLBA 501(b) – Safeguarding Customer Information.” The most recent version of this ED Module is dated April 2002. The FDIC and the Federal Reserve Board developed the ED Module to provide examiners with a tool to focus on risk management and to establish an appropriate examination scope. RDM 2001-039, entitled, *Guidelines for Examination Workpapers and Discretionary Use of Examination Documentation Modules* and dated September 25, 2001, provided for discretionary use of the ED Module.
- On October 9, 2002, the FDIC issued FIL-118-2002, *New Examination Procedures for Assessing Information Technology Risk*, to advise financial institutions of DSC’s new program for IT risk at FDIC-supervised financial institutions. The FDIC’s program incorporated a new philosophy for categorizing financial institutions’ use of technology and consequential exposure to technology risk, along with updated and more risk-focused IT examination procedures. In FIL-118-2002, the FDIC identified and included two new work programs, IT-MERIT (Maximum Efficiency, Risk-Focused, Institution-Targeted) Procedures and an IT General Work Program, and provided the following descriptions.



- IT-MERIT examination procedures will be used by examiners conducting technology risk reviews at FDIC-supervised financial institutions with the least technology risk. These simplified procedures will greatly streamline the review process for financial institutions in this group.
- The IT General Work Program was developed to improve efficiencies by consolidating several existing technology-related work programs into a single work program and eliminating redundant review areas. This work program will be used by examiners conducting IT risk reviews at FDIC-supervised financial institutions with low to moderate technology risk. The work program replaces several previously issued work programs, such as the Electronic Banking Work program, Examination Procedures to Evaluate Customer Information Safeguards, the Community Bank Work Program, and others.

The DSC issued RDM 2002-043, entitled, *Information Technology Maximum Efficiency, Risk-Focused, Institution Targeted (IT-MERIT); and IT General Work Program Guidelines*, dated September 30, 2002, to implement the new examination guidelines and procedures.

RDM 2002-043 states that to address the different levels of risk posed by financial institutions through their use of IT, four new categories were developed to describe an institution's technology risk profile: Type I, Type II, Type III, and Type IV financial institutions. Table 1 shows the examination procedures to be used for each type.

**Table 1: Technology Types and IT Examination Procedures**

Category	Description	IT Examination Procedures
Type I	Limited networking and E-Banking activities; No in-house programming or core processing; Minimal external threats; Primary risks are centered on the core banking system or vendor management; and No history of less than satisfactory examination ratings.	IT-MERIT Procedures
Type II	Limited networking and E-Banking activities; Usually do not conduct in-house programming or servicing of other financial institutions; Minimal external threats; Primary risks are centered on the core banking system or vendor management; and a History of less than satisfactory examination ratings.	IT General Work Program
Type III	Fully integrated networking within operations; Increased external threats from E-Banking activities and Internet connections; and Increased operational from limited programming activities or servicing responsibilities.	IT General Work Program, supplemented with Federal Financial Institutions Examination Council* (FFIEC) Work Programs as needed.
Type IV	Relies upon networks and other communication systems as a critical element of operations; Networking among business client and partners is common; Internet connectivity may be relied upon as a critical communications medium; Risk of compromise or access to critical systems from external sources is present; and Complexity of technology increases system administration and security risks.	FFIEC Work Programs

Source: RDM 2002-043 dated September 30, 2002.

\* The FFIEC, established in March 1979, pursuant to Title X of the Financial Institutions Regulatory and Interest Rate Control Act of 1978 (FIRICA – Pub. L. No. 95-630, codified to title 12, U.S.C. 3301 et seq.), 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, the FDIC, the National Credit Union Administration, the Office of the Comptroller of the Currency, and the Office of Thrift Supervision and to make recommendations to promote uniformity in the supervision of financial institutions.

### **DSC’s Approach for Examining Privacy Notice Requirements**

The FDIC and other federal banking regulators developed and approved examination procedures to review supervised financial institutions for compliance with the joint regulation on *Privacy of Consumer Financial Information*. On May 17, 2001, the FDIC issued to financial institutions FIL-46-2001, *FFIEC Compliance Examination Procedures for Part 332 – “Privacy of Consumer Financial Information,”* which provided the examination procedures to be used after July 1, 2001. FDIC’s Division of Compliance and Consumer Affairs (DCA)<sup>16</sup> distributed the interagency examination procedures to all DCA staff through a memorandum entitled, *Interagency Examination Procedures for Reviewing Compliance with Part 332 – Privacy of Consumer Financial Information* (Transmittal No. DCA 01-002), dated May 18, 2001.

---

<sup>16</sup> The FDIC merged the Division of Supervision and DCA into DSC effective July 1, 2002.

In June 2003, the DSC advised financial institutions of its revised compliance examination process through FIL-52-2003, *Compliance Examination Procedures*. Under the new approach, FDIC compliance examinations combine the risk-based examination process with an in-depth evaluation of a financial institution's compliance management system.

## RESULTS OF EVALUATION

Overall, the FDIC has made reasonable progress in implementing GLBA Title V provisions related to safeguarding customer information and privacy notice requirements and modest progress in implementing provisions related to fraudulent access to financial information. Our assessment of FDIC's progress is 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 institutions' compliance with GLBA Title V provisions.

Specifically, the FDIC established rules and regulations that appropriately address the applicable provisions related to safeguarding customer information and privacy notice requirements and established adequate guidance and examination procedures to help ensure that financial institutions under its jurisdiction meet the safeguarding and privacy notice requirements. The DSC assesses a financial institution's compliance (1) with standards for safeguarding customer information through IT examinations and (2) with privacy notice requirements through compliance examinations. The GLBA Title V provisions related to FCRA-affiliate information sharing have not yet been fully implemented, but are being addressed through proposed interagency regulations still in process.

Regarding GLBA Title V provisions related to fraudulent access to financial information, the FDIC issued guidance on identity theft and pretext calling to financial institutions, but DSC has not established specific examination procedures to determine financial institutions' compliance with the guidance. (See **Finding A: FDIC's Progress in Implementing GLBA Title V -- Privacy Provisions**.)

The FDIC has taken actions to implement the GLBA Title V provisions related to safeguarding customer information and privacy notice requirements. However, we noted that several management actions are needed related to DSC's IT examination process.

- Establish examination procedures for ensuring that financial institutions have controls in place to prevent unauthorized disclosure of customer financial information (Subtitle B). Although the FDIC has issued guidance on identity theft and pretext calling to inform financial institutions about developments in these two areas of consumer bank fraud, DSC's IT examination procedures do not include steps to specifically assess how banks protect customer information from unauthorized disclosure.
- Ensure consistency in assessing and reporting a financial institution's level of compliance with standards for safeguarding customer information (Subtitle A). DSC's IT General Work Program does not always specifically identify those procedures that are appropriate

and necessary for assessing a financial institution's compliance with these standards. If examination procedures do not specifically reference the safeguarding standards under review, the FDIC is at risk that key requirements may not be considered in assessing a financial institution's compliance with the standards.

Further, DSC has multiple guidelines at the headquarters and regional level that provide differing instructions to examiners for reporting a financial institution's compliance with standards for safeguarding customer information. These guidelines vary from an examiner's use of exception reporting to combined reporting of noncompliance or level of compliance. National DSC guidance on reporting compliance with the standards is needed to promote consistency among DSC's regional offices. (See **Finding B: DSC's Examination Procedures for GLBA Title V -- Privacy.**)

## **FINDINGS AND RECOMMENDATIONS**

### **FINDING A: FDIC'S PROGRESS IN IMPLEMENTING GLBA TITLE V -- PRIVACY PROVISIONS**

The FDIC made reasonable progress in implementing GLBA Title V Subtitle A's provisions, as demonstrated in the regulations, FILs, and other guidance the Corporation has issued to financial institutions it supervises. In addition, the FDIC participated in interagency efforts and jointly issued standards for safeguarding customer information, examination procedures to assess compliance with those standards, and examination procedures to review compliance with privacy notice requirements. However, the FDIC's progress in implementing Subtitle B's provisions is modest. The Corporation issued guidance to its supervised financial institutions on identity theft and pretext calling which referenced published guidelines on the safeguards financial institutions can put into place to help prevent problems caused by pretext calling. However, as discussed in **Finding B**, DSC has not established specific examination procedures to review a financial institution's compliance with the guidelines on pretext calling.

#### **FDIC Rules and Regulations and FDIC Procedures that Address GLBA Title V Provisions**

The FDIC has issued rules and regulations, guidance, and procedures that address most of the GLBA Title V provisions. Table 2 illustrates FDIC's activities for major GLBA Title V provisions and shows that, as discussed in **Finding B**, DSC has not specifically identified examination procedures related to Subtitle B. Appendix III lists all GLBA Title V privacy provisions.

**Table 2: FDIC Rules, Guidance, and Implementing Procedures for Major GLBA Title V Privacy Provisions**

Title V	Federal Register	FDIC Rules and Regulations	Financial Institution Letters	DSC Examination Procedures
<b>Subtitle A. – Disclosure of Nonpublic Personal Information</b>				
§501(b). <i>Financial Institutions Safeguards</i> and §505(b). <i>Enforcement of Section 501</i> – Requires each “agency” to establish and implement standards relating to administrative, technical, and physical safeguards to protect nonpublic personal information.	Vol. 66, 8616 - 8641 (February 1, 2001) Final Rule – <i>Interagency Guidelines Establishing Standards for Safeguarding Customer Information and Rescission of Year 2000 Standards for Safety and Soundness.</i>	Part 364, <i>Standards for Safety and Soundness</i> , Appendix B. Part 308, Subpart R, <i>Submission and Review of Safety and Soundness Compliance Plans and Issuance of Orders to Correct Safety and Soundness Deficiencies.</i>	a) FIL-22-2001, March 14, 2001. b) FIL-68-2001, August 24, 2001. c) FIL-118-2002, October 9, 2002. d) FIL-11-2003, February 12, 2003.	a) Examination Procedures to Evaluate Compliance with the Guidelines to Safeguard Customer Information. b) IT Examination Procedures: <ul style="list-style-type: none"> <li>• IT Merit.</li> <li>• General Work Program</li> <li>• FFIEC.</li> </ul>
§502 – 504. The “agencies” shall consult and coordinate in developing regulations necessary to carry out purpose of Subtitle A.	Vol. 65, 35162 - 35236 (June 1, 2000) Final Rule - <i>Privacy of Consumer Financial Information.</i>	Part 332, <i>Privacy of Consumer Financial Information.</i>	a) FIL-34-2000, July 5, 2000. b) FIL-3-2001, January 22, 2001. c) FIL-46-2001, May 17, 2001. d) FIL-73-2001, August 29, 2001. e) FIL-106-2001, December 20, 2001.	Interagency Examination Procedures for Reviewing Compliance with Part 332.
§506(a). <i>Amendment</i> – Section 621 of the Fair Credit Reporting Act is amended.	Vol. 65, 63120 - 63141 (October 20, 2000) Proposed Rule, <i>Fair Credit Reporting Regulations.</i>	Part 334 – <i>Fair Credit Reporting.</i> <sup>a</sup>	a) FIL-71-2000, October 26, 2000. b) FIL-26-2001, March 27, 2001.	DCA Memorandum Transmittal Number DCA-00-009, <i>Revised Interagency Examination Procedures for the Fair Credit Reporting Act</i> , directs the resumption of routine examinations for compliance with the FCRA.
<b>Subtitle B – Fraudulent Access to Financial Information</b>				
§525. Agencies to issue guidelines to ensure consistency with Subtitle B.	Not Applicable <sup>b</sup>	Not Applicable	FIL-39-2001, May 9, 2001.	Discussed in <b>Finding B.</b>

Source: OIG Analysis.

<sup>a</sup>The federal banking regulators anticipate issuing a new proposed rulemaking for public comments in response to comments received on the October 20, 2000 proposal.

<sup>b</sup>This section of GLBA Title V did not require the creation of an FDIC rule and regulation or standard.

To verify DSC’s implementation, we selected and reviewed examination workpapers for a judgmental sample of 11 IT examinations. In all cases, we confirmed that the examination team used the appropriate examination procedures -- IT MERIT, IT General Work Program, or alternative procedures<sup>17</sup> -- based on the complexity and risk of the financial institution’s technology functions.

**Internal Quality Assurance Review of the Privacy Examination Process**

DSC’s Internal Control Review Section (ICRS) issued a *Report on the Quality Assurance Review of the Privacy Examination Process*, dated December 2002, which addressed compliance examinations of privacy notice requirements conducted at FDIC-supervised financial institutions during the first 3 months of 2002. The report identified the following findings: (1) workpaper documentation did not consistently demonstrate that a thorough privacy examination was completed; (2) examination procedures were not consistently employed to conduct privacy examinations; and (3) time associated with conducting the privacy examination was not consistently reported in the Scheduling Hours and Reporting Package, a DSC system used to monitor examination resources.

DSC developed an Action Plan to address the report findings and sent the Action Plan to Regional Directors and Deputy Regional Directors (Compliance) on May 16, 2003. The Action Plan conveyed clarifying information regarding GLBA Title V and identified responsibilities and actions to be taken by management and examination staff to ensure improvements to the privacy examination process. Table 3 presents a summary of the actions planned by DSC to address the ICRS’s findings.

**Table 3: DSC Action Plan Items**

Action Planned
1. Using approved interagency procedures to conduct privacy examinations.
2. Interviewing institution management to determine whether written policies and procedures reflect actual practices.
3. Requesting and reviewing joint marketing agreements between the bank and third parties.
4. Preparing a scope memorandum for the entire compliance examination.
5. Preparing and filing examiner summaries with the workpapers.
6. Establishing a baseline measurement that documents the degree to which each region has complied with actions 1-5 mentioned above.
7. Ensuring that privacy issues are discussed in routine regional meetings and conference calls, as applicable.
8. Identifying a privacy subject matter expert in each region and privacy points-of-contact in each of the field offices.
9. Emphasizing privacy during Commissioned Compliance Examiner Workshops.
10. Preparing a “Job Aid” to be used by examiners for interviewing bank staff.
11. Conduct a follow-up review of the privacy examination process in October 2003.

Source: DSC’s May 16, 2003 Memorandum to Regional Directors and Deputy Regional Directors (Compliance) from Deputy Director for Compliance and Consumer Protection.

<sup>17</sup> Of the 11 IT examinations we reviewed, 6 were Type I, Type II, or Type III financial institutions, and examiners used the appropriate MERIT or IT General Work Program procedures; 2 were Type IV financial institutions, and examiners used the FFIEC Work Programs, as supplemented by other procedures; 2 were data processing servicers; and 1 was a visitation.

For this evaluation, we did not review examination workpapers for privacy notice requirements examinations because DSC was in the process of developing its Action Plan when we started our review.

### **DSC Views on Financial Institutions' Compliance with GLBA**

DSC officials responsible for IT examinations in FDIC's San Francisco Regional Office and Chicago Regional Office told us that the majority of FDIC-supervised financial institutions have adopted some type of information security program as required under GLBA and the implementing regulations. The examiners in the San Francisco Regional Office have encountered a few isolated instances where financial institutions were in substantial noncompliance with the standards for safeguarding customer information. For example, the examiners found either an inadequate assessment or no comprehensive risk assessment, lack of testing and monitoring of key controls, weak vendor/service provider oversight programs, and failure to provide for adequate reporting to the Board of Directors. Chicago Regional Office officials said that financial institutions' information security programs usually fall short of fully complying with the GLBA requirements. The Chicago Regional Office's examination findings often indicate that the information security program does not include all necessary elements; risk assessments are incomplete and/or informal; audits do not fully test key controls, systems, and procedures; and employee training and awareness initiatives are limited and infrequent.

Currently, DSC does not maintain formal statistics on instances of apparent noncompliance with standards for safeguarding customer information identified during IT examinations. Although we are not making formal recommendations in this regard, such statistics could be helpful in identifying emerging issues and trends and in assessing whether the IT examination program is achieving its desired outcomes. We encourage DSC to begin maintaining basic statistics.

The DSC does generate and maintain statistical information on noncompliance with privacy notice requirements identified during compliance examinations. We obtained summary information on the number and description of privacy notice deficiencies identified during compliance examinations conducted within the first year of the GLBA Title V enactment. Approximately 5 percent of the institutions that underwent a compliance examination were cited for a violation of FDIC Rules and Regulations, Part 332. Generally, the smaller the institution, the more often examiners found violations of Part 332. Some of the violations identified were related to the following sections of Part 332:

- Section 332.6 – Information to be Included in Privacy Notices.
- Section 332.4 – Initial Privacy Notice to Consumers.
- Section 332.7 – Form of Opt Out Notice to Consumers and Opt Out Methods.
- Section 332.12 – Limits on Sharing Account Number Information for Marketing Purposes.



The DSC's statistics for compliance examinations conducted in 2002 and early 2003 show the most common deficiencies tend to deal with the omission of information from banks' privacy notices and incorrect disclosures of information wherein information in a privacy notice does not always accurately reflect a financial institution's information-sharing practices.

## **FINDING B: DSC'S EXAMINATION PROCEDURES FOR GLBA TITLE V -- PRIVACY**

The FDIC has made progress in implementing the GLBA's Title V provisions related to safeguarding customer information and privacy notice requirements, yet enhancements are needed in the examination process to ensure financial institutions have controls in place to prevent unauthorized disclosure of customer financial information and to provide consistency in assessing and reporting a financial institution's compliance with standards for safeguarding customer information. DSC's IT examination procedures do not include steps designed to explicitly assess financial institutions' compliance with the guidance issued for Subtitle B. Without specific procedures, examinations may not be adequately assessing financial institutions' compliance with GLBA privacy provisions to prevent and detect fraudulent access to financial information. Moreover, DSC's IT General Work Program does not always specifically designate those procedures relevant to determining a financial institution's compliance with safeguarding standards (Subtitle A). Without specific procedures designated as addressing GLBA, the DSC cannot be assured that examiners will consider all relevant examination procedures in assessing a financial institution's compliance with the standards. Finally, to promote consistency in reporting financial institutions' compliance with these standards, DSC national guidance is needed to standardize differing instructions provided to examiners by regional and headquarters officials.

### **Subtitle B – Fraudulent Access to Financial Information**

According to Section 525 in Subtitle B, the FDIC and other federal banking regulators are to review their regulations and guidelines to ensure that financial institutions have policies, procedures, and controls in place to prevent the unauthorized disclosure of customer financial information and to deter and detect fraudulent access to such information. In response to these requirements, the FDIC and the other federal banking regulators issued guidance on how banking organizations should protect customer information against identity theft and pretext calling. The FDIC advised the financial institutions of *Guidance on Identity Theft and Pretext Calling* through FIL-39-2001 on May 9, 2001, and identified the guidance as a supplement to FDIC guidelines on customer information security, issued February 1, 2001, pursuant to Section 501(b) of the GLBA.

The *Guidance on Identity Theft and Pretext Calling* provides steps that financial institutions should take to safeguard customer information and reduce the risk of loss from identity theft and pretext calling, including the following:

- Establishing procedures to verify the identity of individuals applying for financial products.
- Establishing procedures to prevent fraudulent activities related to customer information.
- Maintaining a customer information security program.
- Reporting suspected identity theft and pretext calling through Suspicious Activity Reports (SAR).
- Making available to customers information about how to prevent identity theft.

However, DSC's examination procedures do not identify steps specifically designed to review a financial institution's compliance with the guidance on pretext calling. For example, the work program could include procedures to review:

- the measures taken by the financial institution to reduce the incidence of pretext calling, including limiting the circumstances under which customer information may be disclosed by telephone;
- the financial institution's training activities to determine whether employees are made aware of ways to recognize and report possible indicators of attempted pretext calling; or
- a financial institution's level of activity in identifying and tracking known or suspected criminal violations related to pretext calling and reporting such violations in a SAR.

Until the DSC establishes specific procedures for protecting customer financial information from unauthorized disclosure, examinations may not adequately assess financial institutions' compliance with guidance to prevent and detect fraudulent access to financial information. The statutory requirements of Subtitle B do not explicitly require agencies to examine financial institutions' compliance with guidance on identity theft and pretext calling. However, the legislative history of the GLBA Title V indicates a congressional expectation that federal banking regulators should examine financial institutions' compliance with regulators' guidance and the adequacy of those financial institutions' controls relative to preventing and detecting pretext calling. According to the House Commerce Committee Report (H.R. Report No. 106-74, pt. 3, (1999)), Subtitle B provides additional protections against pretext calling by increasing the then-existing penalties for fraudulent information gathering and gives the FTC specific directions to prosecute violations.<sup>18</sup> The report states that, "Subtitle B recognizes the importance of financial institutions implementing strong internal controls to prevent unauthorized disclosure of their customers' private financial information." Regarding Section 525 of Subtitle B, the congressional report indicates:

This section requires each Federal banking agency and the SEC [Securities and Exchange Commission] or self-regulatory organizations to review its regulations and guidelines governing the protection of confidential consumer financial information and to revise such provisions as necessary to ensure appropriate confidentiality safeguards. Those safeguards will include those policies, procedures, and controls as would reasonably be expected to prevent and detect activities proscribed by the legislation. *The Committee expects the appropriate examining authorities to include compliance with such guidelines and the adequacy of such internal controls in their examinations of these institutions* [emphasis added].

DSC officials told us that Bank Secrecy Act (BSA) examination procedures include steps for verification of controls and issuance of SARs; these areas relate to protecting customer information. Further, DSC's IT examination work programs include procedures related to reviewing a financial institution's information security program -- one of the safeguards

---

<sup>18</sup> The enacted version of Subtitle B includes the National Credit Union Administration in Section 525 and provides the federal banking regulators with administrative enforcement powers with respect to financial institutions under their respective jurisdictions.

identified in the guidance on pretext calling. However, DSC's IT examination work programs do not specifically or clearly identify the information security program steps or other procedures that would assist examiners in determining compliance with the guidance on identity theft and pretext calling.

DSC officials acknowledge that IT examination work programs do not specifically include procedures for determining a financial institution's compliance with guidance on pretext calling. However, DSC officials were not certain which examination (i.e., IT examination, safety and soundness, or compliance) should include these procedures. Accordingly, our recommendation to include steps for assessing financial institutions' compliance with the guidance on pretext calling references DSC's examination procedures in general rather than a specific type of examination.

### **Procedures for Examining Standards for Safeguarding Customer Information**

The FDIC initially advised financial institutions of its examination procedures to evaluate compliance with the standards for safeguarding customer information through FIL-68-2001, dated August 24, 2001. These examination procedures were developed on an interagency basis to promote consistency among the federal banking regulators. The DSC distributed the interagency procedures to its examiners through RDM 2001-032 on August 28, 2001.

The interagency procedures included the following examination objective: "Determine whether the financial institution has established an adequate written Information Security Program and whether the program complies with the Guidelines Establishing Standards for Safeguarding Customer Information mandated by section 501(b) of the Gramm-Leach-Bliley Act of 1999." The interagency procedures contained key questions and considerations that examiners should take into account when assessing the adequacy of a financial institution's information security program and grouped the work steps into five categories addressing the major provisions of the standards for safeguarding customer information. Table 4 shows the five categories and examples of a key question for each category.

**Table 4: Interagency Procedures – Categories and Key Questions**

<b>Category</b>	<b>Key Question</b>
Determine the involvement of the Board of Directors in the Information Security Program.	Has the Board or its designated committee approved a written Corporate Information Security Program that meets the requirements of the Information Security Guidelines?
Evaluate the risk assessment process.	How does the institution assess risk to its customer information systems and nonpublic customer information?
Evaluate the adequacy of the program to manage and control risk.	Review internal controls and policies. Are the controls adequate to support risk mitigation judgments?
Assess the measures taken to oversee service providers.	Do contracts require service providers to implement appropriate measures to meet the objectives of the standards for safeguarding customer information?
Determine whether an effective process exists to adjust the information security program.	Does the institution have an effective process to adjust the information security program as needed? Is the appropriate person assigned responsibility for adjusting the program?

Source: RDM 2001-032.

The interagency procedures clearly indicated that the work steps were intended to be in support of assessing the financial institutions' compliance with the standards for safeguarding customer information. The interagency procedures also included steps to summarize the procedures performed and to communicate findings related to assessing compliance with the standards for safeguarding customer information.

In September 2002, the DSC issued new examination guidelines and related streamlined procedures for IT examinations, including two new work programs, IT-MERIT and IT General Work Program. The IT General Work Program replaced various work programs, including the interagency procedures for evaluating the standards for safeguarding customer information. The IT General Work Program consists of work program questions (procedures) that are linked to a "Help" section for examiners to use, when needed. The "Help" section provides a description of the purpose of each work step question and the risk to the financial institution if the question is not addressed or implemented in an acceptable manner.

Unlike the interagency procedures, DSC's IT General Work Program is not structured to include key questions or considerations that an examiner would take into account in assessing the financial institution's compliance with the standards for safeguarding customer information. Further, DSC's new IT examination procedures do not include steps or references to specific procedures in the work program to assess compliance with the standards for safeguarding customer information. In addition, DSC's examination procedures do not include steps to summarize and communicate the results of the examiner's work related to evaluating compliance with the standards for safeguarding customer information.

We determined that 42 of the 67 procedures in the IT General Work Program relate to the standards for safeguarding customer information, but we identified only 1 procedure that

explicitly references GLBA and 1 procedure that cites a GLBA requirement, namely “Information Security Guidelines.” As shown in Table 5, we identified six references to the topic of safeguarding customer information in the “Help” section of the IT General Work Program.

**Table 5: References to the Standards for Safeguarding Customer Information in the IT General Work Program “Help” Section**

<b>IT General Work Program Examination Procedure</b>	<b>“Help” Section References to GLBA Customer Information Safeguarding</b>
<p><b>Audit</b> 1d. Does the internal and/or external auditor or designated officer or employee review the following... “Compliance with Section 501(b) of the Gramm-Leach-Bliley Act?”</p>	<p>Help Section Q1d – Does the internal and/or external auditor or designated officer review the following... “Compliance with Section 501(b) of the Gramm-Leach-Bliley Act?”</p>
<p><b>IT Policies</b> 2.1a. Has the board or its designated committee approved a written Corporate Information Security Program that meets the requirements of the Information Security Guidelines?</p>	<p>Help Section Q2.1a –</p> <ul style="list-style-type: none"> <li>➤ Section 501(b) of the Gramm-Leach-Bliley Act (GLBA) of 1999 requires each institution to implement a comprehensive written information security program.</li> <li>➤ For additional information see: FDIC Rules and Regulations – Part 364, Appendix B.</li> </ul>
<p><b>IT Policies</b> 2.1c. Consider the following when evaluating the Risk Assessment process...</p>	<p>Help Section Q2.1c (paraphrased) –</p> <ul style="list-style-type: none"> <li>➤ Accordingly, the GLBA guidelines indicate that institutions should consider the sensitivity of customer information.</li> <li>➤ Under the GLBA guidelines, a financial institution should identify the threats that could result in alteration of customer information systems.</li> </ul>
<p><b>IT Policies</b> 2.1e. Is staff adequately trained to implement the security program?</p>	<p>Help Section Q2.1e – Staff should be trained on information security and privacy guidelines promulgated by GLBA.</p>
<p><b>IT Policies</b> 2.1h. Determine the usefulness of risk assessment reports from management to the board (or its designated committee).</p>	<p>Help Section Q2.1h – Each bank should report to its Board on the status of its information security program and the bank’s compliance with the GLBA guidelines.</p>
<p><b>Support and Delivery</b> 4d. Is computer output (printouts, microfiche, optical disks, etc.) adequately controlled and disposed of?</p>	<p>Help Section Q4d – Controls over computer output must meet the requirements of Section 501(b) of the Gramm-Leach-Bliley Act.</p>

Source: OIG Analysis and DSC IT General Work Program

Table 6 illustrates IT General Work Program procedures that relate to the standards for safeguarding customer information but are not specifically identified in the procedures as related to GLBA.

**Table 6: Example of GLBA-Related Examination Procedures that Do Not Reference GLBA**

<b>IT General Work Program and Examination Procedure</b>	<b>Relates to GLBA Standards (Part 364) for Safeguarding Customer Information</b>
<p><b>IT Policies</b> 2.1d. Review written policies and procedures and determine whether the following controls have been considered.</p>	<p>Each bank shall: (1) identify internal and external threats that could result in unauthorized disclosure, misuse, alteration, or destruction of customer data or customer information systems; (2) assess the likelihood and potential damage of these threats, taking into consideration the sensitivity of customer information; and (3) assess the sufficiency of policies, procedures, customer information systems, and other arrangements in place to control risks.</p>
<p><b>Vendor Management</b> 2.2a. Does the bank have a vendor oversight program that includes analyzing financial statements and other reports on its significant vendor(s) and/or servicer(s)?</p>	<p>Each bank shall oversee service provider arrangements.</p>
<p><b>Support and Delivery</b> 4a. Is separation of duties and responsibilities adequate in the following areas...</p>	<p>Each bank shall design its information security program with security measures to include dual control procedures, segregation of duties, and employee background checks for employees with responsibilities for or access to customer information.</p>
<p><b>Data and Physical Security</b> 4.1i. Are adequate safeguards in effect to ensure that only authorized personnel are permitted in the computer area?</p>	<p>Each bank shall design its information security program with security measures to include access restrictions at physical locations containing customer information to permit access only to authorized individuals.</p>

Source: OIG Analysis, DSC IT General Work Program, and FDIC Rules and Regulations Part 364, Appendix B.

Without specific procedures designated as addressing GLBA, the DSC cannot be assured that examiners will consider all relevant examination procedures in assessing a financial institution’s compliance with standards for safeguarding customer information.

In regard to reporting a financial institution’s compliance with standards for safeguarding customer information, we noted disparities in DSC’s examination reporting guidance. DSC’s guidance for its new risk-focused IT examination procedures (RDM 2002-043) does not identify the standards for safeguarding customer information reporting requirements. However, DSC guidance (RDM 2001-032), which is still in effect, instructs examiners to note material instances of noncompliance in the report of examination. We also noted that regional DSC guidance varied from instructing examiners to report levels of compliance to instructing examiners to report on instances of noncompliance. Table 7 illustrates the different reporting guidelines.

**Table 7: DSC's Guidelines on GLBA Reporting**

<b>Guidelines</b>	<b>Reporting Instructions</b>
RDM 2001-032: <i>Examination Procedures to Evaluate Customer Information Safeguards.</i>	Material instances of non-compliance should be noted in the report of examination and discussed with bank management. Serious weaknesses and management's response should be documented where appropriate in the report of examination (i.e., the risk management pages, the Examination Conclusions and Comments page, and the Apparent Violations page).
Region 1. Memorandum from Regional Director to Examiners and Assistant Examiners.	In addition to including an introductory paragraph related to a review of safeguarding customer information, each report must address the bank's compliance with the provisions of section 501(b) of GLBA and Appendix B. The length of the report comment is expected to vary based on the size and complexity of the institution being examined and the number of section 501(b) of GLBA and Appendix B exceptions. In institutions where management is well aware of the GLBA requirements, and is in full compliance, the comment need only state that compliance with GLBA was reviewed and that the bank is in compliance with all requirements.
Region 2. Memorandum from Regional Director to DSC Risk Management Examiners, Assistant Examiners and Professional Staff.	When a bank has an acceptable program for the safeguarding of customer information and no material findings are noted, such cases include a brief overview of the program in the confidential section of the Report. If the program has minor deficiencies, a comment 'recommending that the bank review the Interagency Guidelines Establishing Standards for Safeguarding Customer Information (Appendix B to Part 364 of the FDIC Rules and Regulations)' may be appropriate. When findings are sufficiently deficient, they should be placed on the examination conclusions and supporting pages of the IT Report of Examination.
Region 3. Memorandum from Regional Director to Field Examiners and Regional Office Professional Staff.	Examiners should continue to assess compliance with the Guidelines at all Safety and Soundness and/or Information Technology examinations. Weaknesses should generally be documented in the Information Technology Assessment pages; however, material instances of non-compliance may be detailed on the Violations page as a Contravention of Part 364, Appendix B. Material instances of non-compliance should also be brought forward to the Risk Management and Examination Conclusions and Comments pages, where appropriate.

Source: RDM 2001-032 and Regional Guidance.

DSC issued RDM 2001-045, *Revised Report of Examination*, on October 11, 2001, as guidance for examiners to use in preparing reports of examination. DSC has taken the position that the report of examination in and of itself constitutes adequate documentation of the work performed and provides the basis for conclusions reached. Further, DSC officials stated that the report of examination has been the primary basis and support for legal proceedings. Additionally, the DOS [Division of Supervision] *Manual of Examination Policies* recognizes that the report of examination generally serves as the FDIC's primary evidentiary exhibit in formal administrative actions. For these reasons, consistency in reporting on compliance with GLBA Title V privacy provisions is important.



## **CONCLUSIONS AND RECOMMENDATIONS**

Although the FDIC has made progress in implementing the GLBA's Title V provisions related to safeguarding customer information and privacy notice requirements, the FDIC could take additional steps to help ensure full implementation of the GLBA Title V privacy provisions. To ensure that financial institutions have policies, procedures, and controls in place to prevent the unauthorized disclosure of customer financial information and to deter and detect fraudulent access to such information (Subtitle B), DSC needs to identify specific procedures in its examination work programs for examiners to assess the financial institutions' compliance with guidance on protecting customer information against identity theft. To promote consistency in assessing and reporting on a financial institution's compliance with standards for safeguarding customer information (Subtitle A), DSC should identify the specific procedures in the IT General Work Program that are designed to assess compliance with the safeguarding standards. Further, DSC should standardize its guidance related to reporting the results of evaluating a financial institution's compliance with the standards for safeguarding customer information.

We recommend the Director, DSC:

- (1) Modify examination procedures to identify steps for assessing financial institutions' compliance with GLBA Title V, Subtitle B, provisions intended to prevent the unauthorized disclosure of customer financial information and to deter and detect fraudulent access to such information.
- (2) Include in the IT General Work Program (a) procedures for summarizing the work performed in the area of GLBA Title V, Subtitle A, provisions for safeguarding customer information and (b) references to the specific procedures that examiners should consider when assessing compliance with those provisions.
- (3) Issue guidance to be used by all regions regarding the manner in which a financial institution's compliance with standards for safeguarding customer information is addressed in a report of examination.

## **CORPORATION COMMENTS AND OIG EVALUATION**

The Director, DSC, provided a written response, dated September 24, 2003, to a draft of this report. DSC's response is presented in its entirety in Appendix IV to this report. We also had subsequent discussions with DSC staff to clarify aspects of the written response.

DSC concurred with recommendations 1 and 3. DSC partially concurred with recommendation 2, but presented an alternative corrective action that addresses the intent of this recommendation. Specifically, DSC agreed with the intent of recommendation 2 but stated that the IT General Work Program was purposely written in general terms to serve as an all-inclusive document that replaced several existing IT work programs, including examination procedures to evaluate customer information safeguards. To address this recommendation, DSC agreed to issue guidance to examiners in the form of an RDM that will identify specific procedures that

examiners should consider when assessing compliance with GLBA Title V, Subtitle A, provisions and procedures for summarizing the work performed in this area. DSC stated that the RDM will be issued by December 31, 2003.

DSC's comments were responsive, and DSC's proposed actions are sufficient to resolve the recommendations. The recommendations will remain undispositioned and open for reporting purposes until we have determined that agreed-to corrective actions have been completed and are effective. Appendix V presents a summary table showing DSC's responses to our three recommendations.

## OBJECTIVE, SCOPE, AND METHODOLOGY

The objective of our evaluation was to determine whether DSC has made reasonable progress in implementing Title V privacy provisions of the GLBA. This evaluation addressed both Subtitle A – Disclosure of Nonpublic Personal Information and Subtitle B – Fraudulent Access to Financial Information.

To accomplish our objective, we performed the following work:

- Identified and reviewed laws, regulations, guidance, and procedures related to the FDIC’s responsibilities in the area of consumer financial privacy in order to gain an understanding of FDIC’s responsibilities in implementing GLBA Title V provisions and DSC’s approach to conducting examinations of financial institutions’ compliance with consumer privacy requirements.
  1. Gramm-Leach-Bliley Act of 1999, Title V -- Privacy.
  2. Federal Deposit Insurance Act, Section 8.
  3. FDIC Rules and Regulations, Part 334 Proposed Rule, *Fair Credit Reporting Regulations*.
  4. FDIC Rules and Regulations, Part 332, *Privacy of Consumer Financial Information*.
  5. FDIC Rules and Regulations, Part 364, *Standards for Safety and Soundness*, Appendix B, *Interagency Guidelines Establishing Standards for Safeguarding Customer Information*.
  6. FDIC Rules and Regulations, Part 308, Subpart R, *Submission and Review of Safety and Soundness Compliance Plans and Issuance of Orders to Correct Safety and Soundness Deficiencies*.
  7. DSC Regional Directors Memorandum (RDM) 2001-032, dated August 28, 2001, entitled *Examination Procedures to Evaluate Customer Information Safeguards*.
  8. RDM 2002-043, dated September 30, 2002, entitled *Information Technology Maximum Efficiency, Risk-Focused, Institution Targeted (IT-MERIT); and IT General Work Program Guidelines*.
  9. RDM 2001-045, dated October 11, 2001, entitled *Revised Report of Examination*.
  10. Division of Compliance and Consumer Affairs (DCA) Director’s Memorandum DCA 01-002, dated May 18, 2001, entitled *Interagency Examination Procedures for Reviewing Compliance with Part 332 – Privacy of Consumer Financial Information*.
  11. DSC Examination Procedures to Evaluate Compliance with the Guidelines to Safeguard Customer Information Safeguards, as of August 28, 2001.
  12. DSC IT Examination Procedures as of September 30, 2002, including: (a) Integrated Examination Guidelines, (b) Technology Profile Script, (c) IT Examination Questionnaire, (d) Request List, (e) IT-MERIT Examination Procedures, and (f) IT General Work Program.
  13. Interagency Examination Procedures for Reviewing Compliance with Part 332 – Privacy of Consumer Financial Information.

- Coordinated with FDIC OIG Counsel’s office to obtain a legal review or interpretation regarding: (1) evaluation approach; (2) our Summary Crosswalk of GLBA Title V Provisions to FDIC Rules and Regulations and FDIC Examination Procedures and related crosswalks; and (3) Subtitle B requirements.
- Reviewed Financial Institution Letters related to GLBA consumer privacy matters to gain an understanding of GLBA Title V requirements for federal banking regulators and financial institutions.
- Interviewed DSC officials in Washington, D.C., who are responsible for implementing DSC’s IT and compliance examination approaches for consumer privacy. We interviewed DSC officials in three FDIC regional offices in San Francisco, Chicago, and Dallas/Memphis who are responsible for implementing DSC’s IT examination procedures related to consumer privacy.
- To verify implementation of DSC’s examination procedures to assess financial institutions’ compliance with the standards for safeguarding customer information, we reviewed examination workpapers for 11 sampled IT examinations. The sample of IT examinations was selected by another OIG Corporate Evaluations team performing the evaluation of *Business Continuity at FDIC Supervised Institutions* (Assignment Number 2003-006). Due to the common focus of both evaluations, i.e., the IT examination process and the timing of both assignments, we used the sample of IT examinations selected by the team conducting the business continuity evaluation.
- The sample focused on IT examinations that started after January 1, 2003 and ended before May 22, 2003 in order to capture IT examinations that were conducted after issuance of the revised IT examination guidelines in September 2002. Two exceptions to this scope were: (1) an IT examination that was conducted in 2002, but had a related “visitation” in 2003; and (2) a Multi-Regional Data Processing Servicer (MDPS) examination that was performed in May 2002. This May 2002 MDPS examination was selected because it was the most recent MDPS examination for which the FDIC was the lead agency. To gain an understanding of the relative differences in DSC’s approach, the team conducting the business continuity evaluation judgmentally selected IT examinations for institutions that were located in large metropolitan areas with various asset sizes and complexities.

Our sample was composed of the following:

TYPE	NUMBER OF SAMPLED INSTITUTIONS
I	1
II	1
III	4
IV	2
Data Processing Servicers	2
Visitation	1

- For the sampled examinations, we reviewed, when available, the following documents in the examination workpapers:
  - Report of Examination.
  - Technology Profile Script.
  - IT Examination Questionnaire.
  - Request Lists and Entry Letter.
  - Pre-examination planning memorandum.
  - On-site examination procedures and work programs used and examiner's documentation of work performed.
  
- We interviewed the Examiner-in-Charge (EIC) for each of the sampled examinations to obtain an understanding of procedures performed to assess the financial institutions' compliance with standards for safeguarding customer information.
  
- We performed a cursory review of the workpapers related to the examination that was performed in 2002, but had a related "visitation" in 2003. We reviewed the workpapers related to GLBA to determine which procedures were performed in 2002 and at the visitation. In addition, we contacted the EIC for this visitation and asked the standard questions we asked of the other EICs.
  
- We gained an understanding of the management control activities associated with the implementation of GLBA Title V by reviewing DSC's examination procedures and through interviews with DSC management and EICs. Our testing of FDIC's compliance with laws and regulations was limited to those sections of GLBA Title V applicable to the FDIC. We developed a crosswalk between GLBA Title V and FDIC Rules and Regulations, and DSC's examination policies and procedures. We did not test for fraud or illegal acts or determine the reliability of computer-processed data obtained from the FDIC's computerized systems.
  
- Our work to address the Government Performance and Results Act<sup>19</sup> included reviewing the FDIC 2001-2006 Strategic Plan to identify any goals related to GLBA Title V -- Privacy. We also reviewed the FDIC's 2003 Annual Performance Plan, in particular, the plan for the Supervision Program, to identify strategic goals, objectives, or annual performance goals that relate directly to GLBA privacy. The 2001-2006 Strategic Plan and the 2003 Annual Performance Plan included the strategic goal: "Consumers' rights are protected and FDIC supervised institutions invest in their communities." However, we did not identify specific goals or objectives that mentioned GLBA Title V -- Privacy provisions.

We performed field work in the DSC headquarters in Washington, D.C.; San Francisco Regional Office; Chicago Regional Office; and Memphis Regional Office. We conducted our evaluation from April 2003 through August 2003, in accordance with generally accepted government auditing standards.

---

<sup>19</sup> Pub. L. No. 103-62, codified in titles 5, 31, and 39, U.S.C.

**ACRONYMS USED IN REPORT**

<b>BSA</b>	Bank Secrecy Act
<b>DCA</b>	Division of Compliance and Consumer Affairs
<b>DSC</b>	Division of Supervision and Consumer Protection
<b>ED</b>	Examination Documentation
<b>EIC</b>	Examiner-In-Charge
<b>FCRA</b>	Fair Credit Reporting Act
<b>FDI Act</b>	Federal Deposit Insurance Act
<b>FDIC</b>	Federal Deposit Insurance Corporation
<b>FFIEC</b>	Federal Financial Institutions Examination Council
<b>FIL</b>	Financial Institution Letter
<b>FTC</b>	Federal Trade Commission
<b>GAO</b>	General Accounting Office
<b>GLBA</b>	Gramm-Leach-Bliley Act of 1999
<b>H.R.</b>	U.S. House of Representatives
<b>ICRS</b>	Internal Control and Review Section
<b>IT</b>	Information Technology
<b>MDPS</b>	Multi-Regional Data Processing Servicer
<b>OIG</b>	Office of Inspector General
<b>RDM</b>	Regional Directors Memorandum
<b>SAR</b>	Suspicious Activity Report

**SUMMARY CROSSWALK OF GLBA TITLE V PROVISIONS TO  
FDIC RULES AND REGULATIONS AND FDIC PROCEDURES**

<b>GLBA Title V Section Number and Heading</b>	<b>FDIC Rules and Regulations</b>	<b>Financial Institution Letters (FIL) and/or DSC Examination Procedures (OIG Comments are in Bold)</b>
<b>Subtitle A – Disclosure of Nonpublic Personal Information</b>		
<b>501. Protection of Nonpublic Personal Information.</b>		
501(a) Privacy Policy.	[Financial Institution Responsibility]	[Financial Institution Responsibility]
501(b) Financial Institutions Safeguards.	Part 364, <i>Standards for Safety and Soundness</i> , Appendix B – <i>Interagency Guidelines Establishing Standards for Safeguarding Customer Information</i> .	<p>FIL-22-2001, <i>Guidelines Establishing Standards for Safeguarding Customer Information</i>, dated March 14, 2001, describes the agencies’ expectations for a financial institution to create, implement, and maintain an information security program that includes administrative, technical, and physical safeguards appropriate to the size and complexity of the financial institution and the nature and scope of its activities.</p> <p>FIL-68-2001, <i>Examination Procedures to Evaluate Customer Information Safeguards</i>, dated August 24, 2001, provided financial institutions the examination procedures to assist them in their compliance efforts.</p> <p>RDM 2001-032, <i>Examination Procedures to Evaluate Customer Information Safeguards</i>, issued by the FDIC on August 28, 2001, to distribute examination procedures to determine compliance with Appendix B to Part 364.</p> <p>FIL-118-2002, <i>New Examination Procedures for Assessing Information Technology Risk</i>, dated October 9, 2002, announced new examination procedures for assessing information technology (IT) risk.</p>

GLBA Title V Section Number and Heading	FDIC Rules and Regulations	Financial Institution Letters (FIL) and/or DSC Examination Procedures (OIG Comments are in Bold)
		<p>RDM 2002-043, <i>Information Technology Maximum Efficiency, Risk-Focused, Institution Targeted (IT-MERIT)</i>; and <i>IT General Work Program Guidelines</i>, issued by the FDIC on September 30, 2002:</p> <ul style="list-style-type: none"> <li>• IT-MERIT procedures used for banks with the least technology risk.</li> <li>• IT General Work Program used for banks with low to moderate technology risk.</li> <li>• IT General Work Program supplemented with FFIEC Work Programs used for banks having fully integrated networking into their operations.</li> <li>• FFIEC Work Programs used for banks relying upon networks and other communication systems as a critical element of their operations.</li> </ul> <p>FIL-11-2003, <i>New Information Security Guidance for Examiners and Financial Institutions</i>, dated February 12, 2003, describes the new FFIEC booklet with revised guidance for identifying institutions' information security risks and evaluating their risk-management practices.</p>
<b>502. Obligations with Respect to Disclosures of Personal Information.</b>		
502(a) Notice Requirements.	<p>Part 332, <i>Privacy of Consumer Financial Information</i>.</p> <p>Section 332.1(a) Purpose and scope</p> <ul style="list-style-type: none"> <li>• Requires a financial institution to provide notice to customers about its privacy policies and practices.</li> </ul>	<p>FIL-34-2000, <i>Final Rule on the Privacy of Consumers' Financial Information</i>, dated June 5, 2000, notified financial institutions of the issuance of the final rule on the privacy of consumers' financial information.</p> <p>FIL-3-2001, <i>FDIC Creates Privacy Rule Handbook to Assist Banks With Compliance</i>, dated January 22, 2001, provided a <i>Privacy Rule Handbook</i>, produced by the FDIC, to help financial institutions comply with the final rule governing the privacy of consumer financial information and implement effective consumer privacy policies.</p> <p>FIL-46-2001, <i>FFIEC Compliance Examination Procedures for Part 332 – "Privacy of Consumer Financial Information,"</i> dated May 17, 2001, announced FFIEC-developed examination procedures to be used to review</p>



GLBA Title V Section Number and Heading	FDIC Rules and Regulations	Financial Institution Letters (FIL) and/or DSC Examination Procedures (OIG Comments are in Bold)
	<ul style="list-style-type: none"> <li>• Describes the conditions under which a financial institution may disclose nonpublic personal information about consumers to nonaffiliated third parties.</li> <li>• Provides a method for consumers to prevent a financial institution from disclosing that information to most nonaffiliated third parties by “opting out” of that disclosure, subject to exceptions.</li> </ul>	<p>supervised financial institutions for compliance with the agencies’ regulation on Privacy of Consumer Information.</p> <p>FDIC’s Division of Compliance and Consumer Affairs (DCA) issued a memorandum (Transmittal No. DCA 01-002) on May 18, 2001, to all DCA staff distributing the approved examination procedures developed by the FFIEC. FFIEC procedures were effective for compliance examinations beginning after July 1, 2001.</p> <ul style="list-style-type: none"> <li>• FFIEC’s examination procedures include steps to: identify the financial institution’s information sharing practices with affiliates and nonaffiliated third parties; determine how the institution treats nonpublic personal information; and determine the manner in which the institution administers its opt-out rules. Depending on the institution’s information-sharing practices, examiners are directed to complete various modules within the procedures. There are six modules. The procedures include an examination checklist containing 50 questions designated for “Yes/No” responses.</li> </ul> <p>FIL-73-2001, <i>Federal Financial Institutions Examination Council CD-ROM on Financial Privacy and Information Security</i>, dated August 29, 2001, distributed a CD-ROM that contained 12 multimedia presentations with audio accompaniment addressing consumer financial privacy, including all aspects of the new privacy rule and the 501(b) security guidelines.</p> <p>FIL-106-2001, <i>Frequently Asked Questions for the Privacy Regulation</i>, dated December 20, 2001, developed with the other federal financial institution regulatory agencies, was issued as answers to "frequently asked questions" that represent clarifications and interpretations of the final rule governing the privacy of consumer financial information.</p>

<p><b>GLBA Title V Section Number and Heading</b></p>	<p><b>FDIC Rules and Regulations</b></p>	<p><b>Financial Institution Letters (FIL) and/or DSC Examination Procedures (OIG Comments are in Bold)</b></p>
<p>502(b) Opt Out.</p>	<p>Section 332.7 Form of opt out notice to consumers; opt out methods.</p> <p>Section 332.9 Delivering privacy and opt out notices.</p> <p>Section 332.13 Exception to opt out requirements for service providers and joint marketing.</p> <p>Section 332.15 Other exceptions to notice and opt out requirements.</p>	<p>FFIEC Procedures, Part A and Module 1.</p>
<p>502(c) Limits on Reuse of Information.</p>	<p>Section 332.11 Limits on redisclosure and reuse of information.</p>	<p>FFIEC Procedures, Part A and Modules 4 and 5.</p>
<p>502(d) Limitations on the Sharing of Account Number Information for Marketing Purposes.</p>	<p>Section 332.12 Limits on Sharing account number information for marketing purposes.</p>	<p>FFIEC Procedures, Part A and Module 6.</p>
<p>502(e) General Exceptions.</p>	<p>Section 332.14 Exceptions to notice and opt out requirements for processing and servicing transactions.</p> <p>Section 332.15 Other exceptions to notice and opt out requirements.</p>	<p>FFIEC Procedures, Part A and Module 1.</p>

GLBA Title V Section Number and Heading	FDIC Rules and Regulations	Financial Institution Letters (FIL) and/or DSC Examination Procedures (OIG Comments are in Bold)
<b>503. Disclosure of Institution Privacy Policy.</b>		
503(a) Disclosure Required.	Section 332.4 Initial privacy notice to consumers required.  Section 332.5 Annual privacy notice to customers required.  Section 332.8 Revised Privacy Notices.  Section 332.9 Delivering privacy and opt out notices.	FFIEC Procedures, Part A and Module 1.
503(b) Information To Be Included.	Section 332.6 Information to be included in privacy notices.	FFIEC Procedures, Part A and Module 1.
<b>504. Rulemaking.</b>		
504(a) Regulatory Authority.	Part 364, Appendix B, <i>Interagency Guidelines Establishing Standards for Safeguarding Customer Information</i> .  Part 332 <i>Privacy of Consumer Financial Information</i> .  Part 334 <i>Fair Credit Reporting</i> (proposed).	
504(b) Authority To Grant Exceptions.	Not Applicable	<b>The regulations do not prescribe any “additional exceptions” to subsection (a) through (d) of section 502.</b>

GLBA Title V Section Number and Heading	FDIC Rules and Regulations	Financial Institution Letters (FIL) and/or DSC Examination Procedures (OIG Comments are in Bold)
<b>505. Enforcement</b>		
505(a) In General.	Not Applicable – Covered under Section 8 of the FDI Act.	
505(b) Enforcement of Section 501.	Section 364.101(b); Part 364, Appendix B. <i>Interagency Guidelines Establishing Standards for Safeguarding Customer Information.</i>  Part 308, Subpart R, <i>Submission and Review of Safety and Soundness Compliance Plans and Issuance of Orders to Correct Safety and Soundness Deficiencies.</i>	
505(c) Absence of State Action.	Not Applicable	
505(d) Definitions.	Not Applicable	
<b>506. Protection of Fair Credit Reporting Act.</b>		
506(a) Amendment.--Section 621 of the Fair Credit Reporting Act (15 U.S.C. 1681s) is amended.	Part 334 – <i>Fair Credit Reporting.</i> The banking regulators anticipate issuing a new proposed rulemaking for public comments, due to comments being received on the October 20, 2000 proposal.	<b>The authority of the federal financial institution regulatory agencies to conduct routine examinations for compliance with the Fair Credit Reporting Act (FCRA) is restored.</b>  Division of Compliance and Consumer Affairs Memorandum Transmittal Number DCA-00-009, <i>Revised Interagency Examination Procedures for the Fair Credit Reporting Act</i> , directs the resumption of routine examinations for compliance with the FCRA.

GLBA Title V Section Number and Heading	FDIC Rules and Regulations	Financial Institution Letters (FIL) and/or DSC Examination Procedures (OIG Comments are in Bold)
		<p><b>Federal banking agencies shall jointly prescribe regulations as necessary to carry out the purposes of FCRA with respect to financial institutions.</b></p> <p>FIL-71-2000, <i>Proposed Regulations Implementing the Fair Credit Reporting Act</i>, dated October 26, 2000. This FIL distributes the proposed rule, Part 334, published in the Federal Register (Vol. 65, No. 204, dated October 20, 2000).</p> <p>FIL-26-2001, <i>Guidance on the Timing and Preparation of Privacy Notices to Conform to Fair Credit Reporting Act Requirements</i>, dated March 27, 2001. This FIL provides guidance on a technical and timing aspect of the proposed rule, Part 334.</p>
506(b) Conforming Amendment.	Not Applicable	
506(c) Relation to Other Provisions.	Section 332.16 Protection of Fair Credit Report Act.	
<b>507. Relation to State Laws.</b>		
507(a) In General.	Section 332.17 Relation to State Laws.	
507(b) Greater Protection Under State Law.	Section 332.17 Relation to State Laws.	
<b>508. Study of Information Sharing Among Financial Affiliates.</b>		
508(a) In General.	Not Applicable	
508(b) Consultation.	Not Applicable	
508(c) Report.	Not Applicable	
<b>509. Definitions .</b>		
	Part 364, Appendix B, Section I.C. Definitions Section 332.3 Definitions	

GLBA Title V Section Number and Heading	FDIC Rules and Regulations	Financial Institution Letters (FIL) and/or DSC Examination Procedures (OIG Comments are in Bold)
<b>510. Effective Date.</b>		
	Part 364, Appendix B, Section III.G. Implement the Standards  Section 332.18 Effective date; transition rule.	FIL-68-2001, <i>Examination Procedures to Evaluate Customer Information Safeguards</i> , dated August 24, 2001, stated that the effective date of the Section 501(b) provisions was July 1, 2001.  FIL-34-2000, <i>Final Rule on the Privacy of Consumers' Financial Information</i> , dated June 5, 2000, stated that the rule took effect on November 13, 2000, but financial institutions had until July 1, 2001, to be in mandatory compliance with the regulation.
<b>Subtitle B – Fraudulent Access to Financial Information</b>		
<b>521. Privacy Protection for Customer Information of Financial Institutions.</b>		
521(a) Prohibition on Obtaining Customer Information by False Pretenses.	Not Applicable	FIL-39-2001, <i>Guidance on Identity Theft and Pretext Calling</i> , dated May 9, 2001.
521(b) Prohibition on Solicitation of a Person to Obtain Customer Information from Financial Institution under False Pretenses.	Not Applicable	FIL-39-2001, <i>Guidance on Identity Theft and Pretext Calling</i> , dated May 9, 2001.
521(c) Nonapplicability to Law Enforcement Agencies.	Not Applicable	
521(d) Nonapplicability to Financial Institutions in Certain Cases.	Not Applicable	
521(e) Nonapplicability to Insurance Institutions for Investigation of Insurance Fraud.	Not Applicable	

<b>GLBA Title V Section Number and Heading</b>	<b>FDIC Rules and Regulations</b>	<b>Financial Institution Letters (FIL) and/or DSC Examination Procedures (OIG Comments are in Bold)</b>
521(f) Nonapplicability to Certain Types of Customer Information of Financial Institutions.	Not Applicable	
521(g) Nonapplicability to Collection of Child Support Judgments.	Not Applicable	
<b>522. Administrative Enforcement.</b>		
522(a) Enforcement by Federal Trade Commission.	Not Applicable	
522(b) Enforcement by Other Agencies in Certain Cases.	Not Applicable - Covered under Section 8 of the FDI Act.	
<b>523. Criminal Penalty.</b>		
523(a) In General.	Not Applicable	FIL-39-2001, <i>Guidance on Identity Theft and Pretext Calling</i> , dated May 9, 2001.
523(b) Enhanced Penalty for Aggravated Cases.	Not Applicable	FIL-39-2001, <i>Guidance on Identity Theft and Pretext Calling</i> , dated May 9, 2001.
<b>524. Relation to State Laws.</b>		
524(a) In General.	Not Applicable	
524(b) Greater Protection Under State Law.	Not Applicable	

GLBA Title V Section Number and Heading	FDIC Rules and Regulations	Financial Institution Letters (FIL) and/or DSC Examination Procedures (OIG Comments are in Bold)
<b>525. Agency Guidance.</b>		
	Not Applicable	<p>FIL-39-2001, <i>Guidance on Identity Theft and Pretext Calling</i>, dated May 9, 2001, summarized federal laws regarding identity theft and pretext calling; discusses measures that banks can take to protect customer information; informs banks on how suspected criminal activity should be reported; highlights the importance of consumer education; and provides references for additional assistance.</p> <p><b>The FDIC has not issued specific examination procedures that address this provision. (Refer to Finding B.)</b></p>
<b>526. Reports.</b>		
526(a) Report to the Congress.	Not Applicable	
526(b) Annual Report by Administering Agencies.	Not Applicable	
<b>527. Definitions.</b>		
	Not Applicable	



## CORPORATION COMMENTS



**Federal Deposit Insurance Corporation**  
550 17th St., NW, Washington, DC 20429

Division of Supervision and Consumer Protection

September 24, 2003

**TO:** Stephen M. Beard  
Deputy Assistant Inspector General for Audits

**FROM:** Michael J. Zamorski *Michael J. Zamorski*  
Director

**SUBJECT:** DSC Response to OIG Draft Report Entitled *The Federal Deposit Insurance Corporation's Progress in Implementing the Gramm-Leach-Bliley Act Title V-- Privacy Provisions* (Assignment No. 2003-033)

The subject draft report from the Office of Inspector General (OIG) includes three recommendations to improve the Division of Supervision and Consumer Protection's (DSC) approach to implementing the Gramm-Leach-Bliley Act Title V -- Privacy Provisions. Each recommendation is listed below followed by DSC's response.

- (1) *Modify examination procedures to identify steps for assessing financial institutions' compliance with GLBA Title V, Subtitle B, provisions intended to prevent the unauthorized disclosure of customer financial information and to deter and detect fraudulent access to such information.*

DSC concurs with this recommendation. We will incorporate specific examination procedures into the IT General work program for evaluating a bank's compliance with the pretext calling guidelines as described in Financial Institution Letter 39-2001, dated May 9, 2001. However, DSC would like to defer any revision of current procedures dealing with this area in order to also incorporate elements of the interagency guidance for financial institution identity theft response programs, which is currently out for comment to the general public (see Financial Institution Letter 63-2003, dated August 12, 2003).

DSC Action:

The DSC E-Banking Branch is in the process of performing a periodic review of the IT General Work Program and IT-MERIT procedures. Revisions will be made to accommodate the OIG's recommendation. This review and edit process will be completed by March 31, 2004.

- (2) Include in the IT General Work Program (a) procedures for summarizing the work performed in the area of GLBA Title V, Subtitle A, provisions for safeguarding customer information and (b) references to the specific procedures that examiners should consider when assessing compliance with those provisions.*

DSC partially concurs with this recommendation. The IT General Work Program was purposely written in general terms to serve as an all inclusive document, which replaced several existing IT work programs, including examination procedures to evaluate customer information safeguards. The IT General Work Program eliminated redundancies that existed in the numerous work programs and was written to ensure examiners evaluate all critical risk areas involving IT, including customer information safeguards.

Other resource tools available to examiners when conducting assessments of customer information safeguards include the Interagency Examination Procedures to Evaluate Customer Information Safeguards (FIL-68-2001, dated August 24, 2001) and Section 501(b) training materials provided to each risk management examiner in 2001. The interagency examination procedures include a concluding section on summarizing and communicating findings.

To address this recommendation, DSC will issue guidance to examiners in the form of a Regional Director memorandum on the subject of summarizing conclusions reached in the area of GLBA Title V, Subtitle A. This guidance will include procedures for summarizing the work performed and communicating an overall assessment of compliance with the provisions.

DSC Action:

A Regional Director memorandum will be issued to examiners regarding conclusions reached in the area of GLBA Title V, Subtitle A, and the manner in which a compliance with standards should be addressed in the report of examination. The Regional Director memorandum will be issued by December 31, 2003.

- (3) Issue guidance to be used by all regions regarding the manner in which a financial institution's compliance with standards for safeguarding customer information is addressed in a report of examination.*

DSC believes this recommendation has merit. Consistent application and presentation of examination procedures is a goal we endorse. Existing guidance in Transmittal 2001-032, Examination Procedures to Evaluate Customer Information Safeguards, allows some flexibility on when and how comments should appear in the ROE. However, we believe consistency can be improved by issuing guidance to examiners as part of the proposed Regional Director memorandum mentioned in our response to recommendation 2 above. The memorandum will address the manner in which a financial institution's compliance with customer information safeguard standards is addressed in a report of examination.

DSC Action:

A Regional Director memorandum will be issued to examiners regarding conclusions reached in the area of GLBA Title V, Subtitle A, and the manner in which a compliance with standards should be addressed in the report of examination. The Regional Director memorandum will be issued by December 31, 2003.

### MANAGEMENT RESPONSES TO RECOMMENDATIONS

This table presents the management responses that have been made on recommendations in our report and the status of recommendations as of the date of report issuance. The information in this table is based on management's written response to our report (and subsequent communication with management representatives.)

Rec. Number	Corrective Action: Taken or Planned/Status	Expected Completion Date	Monetary Benefits	Resolved: <sup>a</sup> Yes or No	Dispositioned: <sup>b</sup> Yes or No	Open or Closed <sup>c</sup>
1	Incorporate specific examination procedures into the IT General Work Program for evaluating a bank's compliance with the pretext calling guidelines.	March 31, 2004	none	Yes	No	Open
2	Issue guidance to examiners in the form of a Regional Directors Memorandum that will identify specific procedures relative to GLBA Title V, Subtitle A, that examiners should consider and provide guidance for summarizing the work performed.	December 31, 2003	none	Yes	No	Open
3	Issue guidance to examiners as part of the proposed Regional Directors Memorandum to be issued in response to recommendation 2. The memorandum will provide guidance regarding the manner in which a financial institution's compliance with customer information safeguard standards is addressed in a report of examination.	December 31, 2003	none	Yes	No	Open

<sup>a</sup> 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.

<sup>b</sup> Dispositioned – The agreed-upon corrective action must be implemented, determined to be effective, and the actual amounts of monetary benefits achieved through implementation identified. The OIG is responsible for determining whether the documentation provided by management is adequate to disposition the recommendation.

<sup>c</sup> Once the OIG disposes the recommendation, it can then be closed.