Fair Credit Reporting Act

Examination Objectives

To determine the financial institution's compliance with the Fair Credit Reporting Act (FCRA).

To assess the quality of the financial institution's compliance risk management system to ensure compliance with the FCRA, as amended by the Fair and Accurate Credit Transaction Act of 2003 (FACT Act).

To determine the reliance you can place on the financial institution's internal controls and procedures for monitoring the institution's compliance with the FCRA.

To direct corrective action when you identify violations of law, or when the institution's policies or internal controls are deficient.

Background

A NOTE ABOUT THE STRUCTURE AND APPLICABILITY OF THE FCRA EXAMINATION PROCEDURES:

The applicability of the various sections of the FCRA and implementing regulations depend on an institution's unique operations. We present the functional examination requirements for these responsibilities topically in Modules 1 through 6 of these procedures. (We will issue Module 6 in a subsequent amendment to these procedures.)

The FCRA contains many different requirements that a financial institution must follow, even if it is not a consumer reporting agency. Subsequent to the passage of the FACT Act, individual compliance responsibilities are in the statute, joint interagency regulations, or agency-specific regulations.

In order to logically and systematically address FCRA compliance responsibilities and their applicability to particular operations of a financial institution, OTS organized the examination procedures by subject matter, versus strict regulatory or statutory construction. The Level I and II examination procedures are applicable to all areas of review, and you should use them when examining for compliance with any provision of the FCRA. We segregated and grouped the Level III examination procedures by function and they track the format of the modules contained in the handbook section. Only perform those groups of Level III procedures relevant to the functions you are reviewing. As you perform these examination procedures, please reference the handbook section for further examination guidance and insight.

Exam Date:	
Prepared By:	
Reviewed By:	
Docket #:	

EXAMINATION PROCEDURES

LEVEL I

WKP. REF.

Perform the following procedures for all applicable modules.

1. Review all written policies and procedures, management's self-assessments, and any compliance audit material including work papers and reports to determine whether:

   - The scope of the audit addresses all provisions as applicable.
   - Management has taken corrective actions to follow-up on previously identified deficiencies.
   - The testing includes samples covering all product types and decision centers.
   - The work performed is accurate.
   - Significant deficiencies and their causes are included in reports to management and/or to the Board of Directors.
   - The frequency of review is appropriate.

2. Where you conclude from this examination that the institution effectively administers and conducts a comprehensive, reliable, and self-correcting program that adequately ensures compliance with the statutory and regulatory requirements of FCRA, you should record the basis for this conclusion in the work papers and proceed to Program Conclusions.

   Alternatively, review Level II procedures and perform those necessary to test, support, and present conclusions from performance of Level I procedures.

Exam Date:	
Prepared By:	
Reviewed By:	
Docket #:	

WKP. REF.

LEVEL II

Perform the following procedures for all applicable modules.

1. Through discussions with management and review of available information, determine if the institution's internal controls are adequate to ensure compliance in the FCRA area under review. Consider the following:

   - Organization charts
   - Process flowcharts
   - Policies and procedures
   - Loan documentation
   - Checklists
   - Computer program documentation (for example, records illustrating the fields and types of data reported to consumer reporting agencies; automated records tracking customer opt-outs for FCRA affiliate information sharing; etc.).

2. Review the financial institution's training materials to determine whether:

   - The institution provides appropriate training to individuals responsible for FCRA compliance and operational procedures.
   - The training is comprehensive and covers the various aspects of the FCRA that apply to the individual financial institution's operations.

3. Where you conclude that the financial institution effectively manages its compliance responsibilities associated with the FCRA modules examined, you should record the basis for this conclusion in the work papers and proceed to Program Conclusions.

   Where you find procedural weaknesses or other risks requiring further investigation, perform applicable Level III examination procedures.

Exam Date:	
Prepared By:	
Reviewed By:	
Docket #:	

WKP. REF.

LEVEL III

Perform only those procedures within the modules relevant to your review.

MODULE 1: OBTAINING CONSUMER REPORTS

§604 Permissible Purposes of Consumer Reports and
§606 Investigative Consumer Reports

1. Determine if the financial institution obtains consumer reports.

2. Determine if the institution obtains prescreened consumer reports and/or reports for employment purposes. If so, complete the appropriate sections of Module 3.

3. Determine if the financial institution procures or causes an investigative consumer report to be prepared. If so, ensure that the appropriate disclosure is given to the consumer within the required time period. In addition, ensure that the financial institution certified compliance with the disclosure requirements to the consumer reporting agency.

4. Ensure that the institution obtains consumer reports only for permissible purposes. Confirm that the institution certifies to the consumer reporting agency the purposes for which it will obtain reports. (The certification is usually contained in a financial institution's contract with the consumer reporting agency.)

5. Review the consumer reports obtained from a consumer reporting agency for a period of time and determine if the financial institution had permissible purposes to obtain the reports.

Exam Date:	
Prepared By:	
Reviewed By:	
Docket #:	

WKP. REF.

MODULE 2: OBTAINING INFORMATION AND SHARING AMONG AFFILIATES

§603(d) Consumer Report and Information Sharing

1. Determine whether the financial institution shares consumer information with third parties, including both affiliated and nonaffiliated third parties. Determine the type of information shared and with whom the information is shared. (This portion of the examination process may overlap with a review of the institution's compliance with the Privacy of Consumer Financial Information Regulations that implement the Gramm-Leach-Bliley Act.)

2. Determine if the financial institution's information sharing practices fall within the exceptions to the definition of a consumer report. If they do not, complete Module 6 (Requirements for Consumer Reporting Agencies) of the examination procedures.

3. If the financial institution shares information other than transaction and experience information with affiliates subject to an opt-out, ensure that information regarding how to opt-out is in the institution's GLBA Privacy Notice, as required by the Privacy of Consumer Financial Information regulations.

4. Obtain a sample of opt-out rights exercised by consumers and determine if the financial institution honored the opt-out requests by not sharing "other information" about the consumers with the institution's affiliates subsequent to receiving a consumer's opt-out direction.

Exam Date:	
Prepared By:	
Reviewed By:	
Docket #:	

WKP. REF.

§604(g) Protection of Medical Information

5. Determine whether the financial institution collects and uses medical information pertaining to a consumer in connection with any determination of the consumer's eligibility, or continued eligibility for credit.

6. If the financial institution obtains and uses medical information pertaining to a consumer in the context of a credit transaction, assess whether there are adequate controls in place to ensure that the information is only used subject to the financial information exception in the rules, or under a specific exception within the rules.

7. If procedural weaknesses are noted or other risks requiring further investigation are noted, obtain samples of credit transactions to determine if the use of medical information pertaining to a consumer was done strictly under the financial information exception or the specific exceptions under the regulation.

8. Determine whether the financial institution limits the redisclosure of medical information about a consumer that was received from a consumer reporting agency.

9. Determine whether the financial institution shares medical information about a consumer with affiliates. If information is shared, determine whether it occurred under an exception in the rules that enables the financial institution to share the information without becoming a consumer reporting agency.

Exam Date:	
Prepared By:	
Reviewed By:	
Docket #:	

WKP. REF.

§624 Affiliate Marketing Opt Out

LEVEL I

1. Determine whether the financial institution receives consumer eligibility information from an affiliate. Stop here if it does not because Subpart C of 12 CFR 571 does not apply.

2. Determine whether the financial institution uses consumer eligibility information received from an affiliate to make a solicitation for marketing purposes that is subject to the notice and opt-out requirements. If it does not, stop here.

3. Evaluate the institution's policies, procedures, practices and internal controls to ensure that, where applicable, the consumer is provided with an appropriate notice, a reasonable opportunity, and a reasonable and simple method to opt out of the institution's using eligibility information to make solicitations for marketing purposes to the consumer, and that the institution is honoring the consumer's opt-outs.

LEVEL II

If compliance risk management weaknesses or other risks requiring further investigation are noted, obtain and review a sample of notices to ensure technical compliance and a sample of opt-out requests from consumers to determine if the institution is honoring the opt-out requests.

1. Determine whether the opt-out notices are clear, conspicuous, and concise and contain the required information, including the name of the affiliate(s) providing the notice, a general description of the types of eligibility information that may be used to make solicitations to the consumer, and the duration of the opt out (12 CFR 571.23(a)).

Exam Date:	
Prepared By:	
Reviewed By:	
Docket #:	

WKP. REF.

2. Review opt-out notices that are coordinated and consolidated with any other notice or disclosure that is required under other provisions of law for compliance with the affiliate marketing regulation (12 CFR 571.23(b)).

3. Determine whether the opt-out notices and renewal notices provide the consumer a reasonable opportunity to opt out and a reasonable and simple method to opt out (12 CFR 571.24 and .25).

4. Determine whether the opt-out notice and renewal notice are provided (by mail, delivery or electronically) so that a consumer can reasonably be expected to receive that actual notice (12 CFR 571.26).

5. Determine whether, after an opt-out period expires, a financial institution provides a consumer a renewal notice prior to making solicitations based on eligibility information received from an affiliate (12 CFR 571.27).

MODULE 3: DISCLOSURES TO CONSUMERS AND MISCELLANEOUS REQUIREMENTS

§604(b)(2) Use of Consumer Reports for Employment Purposes

1. Determine if the financial institution obtains consumer reports on current or prospective employees.

Exam Date:	
Prepared By:	
Reviewed By:	
Docket #:	

WKP. REF.

2. Ensure that the institution provides appropriate disclosures to current and prospective employees when a financial institution obtains consumer reports for employment purposes, including situations where the financial institution takes adverse actions based on consumer report information.

3. Review a sample of the disclosures to determine if they are accurate and in compliance with the technical FCRA requirements.

§604(c) and §615(d) of FCRA - Prescreened Consumer Reports and Opt-Out Notice (and Parts 642 and 698 of Federal Trade Commission Regulations)

4. Determine if the financial institution obtained and used prescreened consumer reports in connection with offers of credit and/or insurance.

   - If so, ensure that criteria used for prescreened offers, including all post-application criteria, are maintained in the institution's files and used consistently when consumers respond to the offers.

5. Determine if written solicitations contain the required disclosures of the consumers' right to opt-out of prescreened solicitations and comply with all requirements applicable at the time of the offer.

6. Obtain and review a sample of approved and denied responses to the offers to ensure that criteria were appropriately followed.

Exam Date:	
Prepared By:	
Reviewed By:	
Docket #:	

WKP. REF.

§605(g) Truncation of Credit and Debit Card Account Numbers

7. Ensure that electronically generated receipts from ATM and POS terminals or other machines do not contain more than the last five digits of the card number and do not contain the expiration dates.

8. For ATMs and POS terminals or other machines put into operation before January 1, 2005, determine if the institution brought the terminals into compliance or started a plan to ensure that these terminals comply by the mandatory compliance date of December 4, 2006.

9. Review samples of mock receipts to ensure compliance.

§609(g) Disclosure of Credit Scores by Certain Mortgage Lenders

10. Determine if the financial institution uses credit scores in connection with applications for closed-end or open-end loans secured by one- to four-family residential real property.

    - If so, determine if the institutions provides accurate disclosures to applicants as soon as is reasonably practicable after using credit scores.

11. Review a sample of disclosures given to home loan applicants to ensure technical compliance with the requirements.

Exam Date:	
Prepared By:	
Reviewed By:	
Docket #:	

WKP. REF.

§615(a) and (b) Adverse Action Disclosures

12. Ensure that the financial institution provides the appropriate disclosures when it takes adverse action against consumers based on information received from consumer reporting agencies, other third parties, and/or affiliates.

13. Review a sample of adverse action notices to determine if they are accurate and in technical compliance.

14. Review responses to consumer requests for information about these adverse action notices.

§615(g) Debt Collector Communications Concerning Identity Theft

15. Determine if the financial institution collects debts for third parties.

    - If so, ensure that the third parties are notified if the financial institution obtains any information that may indicate the debt in question is the result of fraud or identity theft.

16. Determine if the institution provides information to consumers to whom the fraudulent debts relate.

17. Review a sample of instances where consumers have alleged identity theft and requested information related to transactions to ensure that all of the appropriate information was provided to the consumer.

Exam Date:	
Prepared By:	
Reviewed By:	
Docket #:	

WKP. REF.

§615(h) Risk-Based Pricing Notice

Section 615(h) of the FCRA requires users of consumer reports who grant credit on material terms that are materially less favorable than the most favorable terms available to a substantial proportion of consumers who get credit from or through that person to provide a notice to those consumers who did not receive the most favorable terms. Implementing regulations for this section are under development jointly by the Federal Reserve Board and the Federal Trade Commission. Financial institutions do not have to provide this notice until final regulations are implemented and effective. We will issue this section of the examination procedures upon publication of the final regulations.

MODULE 4: DUTIES OF USERS OF CONSUMER REPORTS AND FURNISHERS OF CONSUMER REPORT INFORMATION

§ 605(h) Duties of Users of Credit Reports Regarding Address Discrepancies (12 CFR 571.82)

1. Determine whether a user of consumer reports has policies and procedures to recognize notices of address discrepancy that it receives from a nationwide consumer reporting agency (NCRA)[1] in connection with consumer reports.

2. Determine whether a user that receives notices of address discrepancy has policies and procedures to form a reasonable belief that the consumer report relates to the consumer whose report was requested (12 CFR 571.82(c)).

   See examples of reasonable policies and procedures "to form a reasonable belief" in 12 CFR 571.82(c)(2).

[1] A NCRA compiles and maintains files on consumers on a nationwide basis. As of the effective date of the rule (January 1, 2008) there were three such consumer reporting agencies: Experian, Equifax, and TransUnion. Section 603(p) of FCRA (15 USC 1681a).

Exam Date:	
Prepared By:	
Reviewed By:	
Docket #:	

WKP. REF.

3. Determine whether a user that receives notices of address discrepancy has policies and procedures to furnish to the NCRA an address for the consumer that the user has reasonably confirmed is accurate, if the user does the following:

   - Forms a reasonable belief that the report relates to the consumer;
   - Establishes a continuing relationship with the consumer; and
   - Regularly, and in the ordinary course of business, furnishes information to the NCRA. (12 CFR 571.82(d)(1))

   See examples of reasonable confirmation methods in 12 CFR 571.82(d)(2).

4. Determine whether the user's policies and procedures require it to furnish the confirmed address as part of the information it regularly furnishes to an NCRA during the reporting period when it establishes a relationship with the consumer (12 CFR 571.82(d)(3)).

5. If procedural weaknesses or other risks requiring further information are noted, obtain a sample of consumer reports requested by the user from an NCRA that included notices of address discrepancy and determine:

   - How the user established a reasonable belief that the consumer reports related to the consumers whose reports were requested; and
   - If a consumer relationship was established:
     — Whether the institution furnished a consumer's address that it reasonably confirmed to the NCRA from which it received the notice of address discrepancy; and

Exam Date:	
Prepared By:	
Reviewed By:	
Docket #:	

WKP. REF.

— Whether it furnished the address in the reporting period during which it established the relationship.

---

6. On the basis of examination procedures completed, form a conclusion about the ability of user's policies and procedures to meet regulatory requirements for the proper handling of address discrepancies reported by an NCRA.

---

§623 Furnishers of Information – General

1. Determine if the institution provides information to consumer reporting agencies.

   - If so, ensure compliance with the FCRA requirements for furnishing information to consumer reporting agencies.

---

2. If you note procedural weaknesses or ther risks requiring further investigation, such as a high number of consumer complaints regarding the accuracy of their consumer report information, select a sample of reported items and the corresponding loan or collection file to determine that the financial institution:

   - Did not report information that it knew, or had reasonable cause to believe, was inaccurate (Section 623(a)(1)(A) (15 USC § 1681s-2(a)(1)(A)).

   - Did not report information to a consumer reporting agency if it was notified by the consumer that the information was inaccurate and the information was, in fact, inaccurate (Section 623(a)(1)(B) (15 USC § 1681s-2(a)(1)(B)).

   - Did provide the consumer reporting agency with corrections or additional information to make the information complete and accurate, and thereafter did not send the consumer reporting agency the inaccurate or incomplete information in situations where the incomplete or inaccurate

Exam Date:	
Prepared By:	
Reviewed By:	
Docket #:	

WKP. REF.

information was provided (Section 623(a)(2) (15 USC § 1681s-2(a)(2)).

- Furnished a notice to a consumer reporting agency of a dispute in situations where a consumer disputed the completeness or accuracy of any information the institution furnished, and the institution continued furnishing the information to a consumer reporting agency (Section 623(a)(3) (15 USC § 1681s-2(a)(3)).

- Notified the consumer reporting agency of a voluntary account-closing by the consumer, and did so as part of the information regularly furnished for the period in which the account was closed (Section 623(a)(4) (15 USC § 1681s-2(a)(4)).

- Notified the consumer reporting agency of the month and year of commencement of a delinquency that immediately preceded the action. The financial institution must make notification to the consumer reporting agency within 90 days of furnishing information about a delinquent account that was being placed for collection, charged-off, or subjected to any similar action (Section 623(a)(5) (15 USC § 1681s-2(a)(5)).

3. Review a sample of notices of disputes received from a consumer reporting agency and determine whether the institution:

   - Conducted an investigation with respect to the disputed information (Section 623(b)(1)(A) (15 USC § 1681s-2(b)(1)(A)).

   - Reviewed all relevant information provided by the consumer reporting agency (Section 623(b)(1)(B) (15 USC § 1681s-2(b)(1)(B)).

   - Reported the results of the investigation to the consumer reporting agency (Section 623(b)(1)(C) (15 USC § 1681s-2(b)(1)(C).

   - Reported the results of the investigation to all other nationwide consumer reporting agencies to which the information was furnished if the investigation found that the reported information was inaccurate or incomplete (Section 623(b)(1)(D) (15 USC § 1681s-2)(b)(1)(D)).

Exam Date:	
Prepared By:	
Reviewed By:	
Docket #:	

WKP. REF.

- Modified, deleted, or blocked the reporting of information that could not be verified.

---

§623(a)(6) Prevention of Re-Pollution of Consumer Reports

4. If the financial institution provides information to a consumer reporting agency, ensure that items of information blocked due to an alleged identity theft are not re-reported to the consumer reporting agency.

---

5. Review a sample of notices from a consumer reporting agency of allegedly fraudulent information due to identity theft furnished by the financial institution to ensure that the institution does not re-report the item to a consumer reporting agency.

---

6. Verify that the financial institution has not sold or transferred a debt that was caused by an alleged identity theft.

---

§623(a)(7) Negative Information Notice

7. If the financial institution provides negative information to a nationwide consumer reporting agency, ensure that it provides the appropriate notices to customers.

---

8. Review a sample of notices provided to consumers to determine compliance with the technical content and timing requirements.

Exam Date:	
Prepared By:	
Reviewed By:	
Docket #:	

WKP. REF.

MODULE 5: CONSUMER ALERTS AND IDENTITY THEFT PROTECTIONS

605A(h) Fraud and Active Duty Alerts

1. Determine if the financial institution verifies the identity of consumers in situations where consumer reports include fraud and/or active duty military alerts.

2. Determine if the financial institution contacts consumers in situations where consumer reports include extended alerts.

3. Review a sample of transactions in which consumer reports including these types of alerts were obtained. Verify that the financial institution complied with the identity verification and/or consumer contact requirements.

§609(e) Information Available to Victims

4. Ensure that the institution verifies identities and claims of fraudulent transactions and that it properly discloses the information to victims of identity theft and/ or appropriately authorized law enforcement agents.

5. Review a sample of these types of requests to ensure that the institution properly verified the requestor's identity prior to disclosing the information.

Exam Date:	
Prepared By:	
Reviewed By:	
Docket #:	

WKP. REF.

§ 615(e) Duties Regarding the Detection, Prevention, and Mitigation of Identity Theft (12 CFR 571.90)

1. Verify that the financial institution periodically[2] identifies covered accounts it offers or maintains.[3] Verify that the financial institution:

   - Included accounts for personal, family, and household purposes that permit multiple payments or transactions.
   - Conducted a risk assessment to identify any other accounts that pose a reasonably foreseeable risk of identity theft, taking into consideration the methods used to open and access accounts, and the institution's previous experiences with identity theft (12 CFR 571.90(c)).

2. Review examination findings in other areas (e.g., Bank Secrecy Act, Customer Identification Program, and Customer Information Security Program) to determine whether there are deficiencies that adversely affect the financial institution's ability to comply with the Identity Theft Red Flags Rules (Red Flag Rules).

3. Review any reports, such as audit reports and annual reports prepared by staff for the board of directors[4] (or an appropriate committee thereof or a designated senior management employee) on compliance with the Red Flag Rules, including reports that address the following:

   - The effectiveness of the financial institution's Identity Theft Prevention Program (Program).
   - Significant incidents of identity theft and management's response.

[2] The risk assessment and identification of covered accounts is not required to be done on an annual basis. This should be done periodically, as needed.
[3] A "covered account" includes: (i) an account for personal, family, or household purposes, such as a credit card account, mortgage loan, auto loan, checking or savings account that permits multiple payments or transactions, and (ii) any other account that the institution offers or maintains for which there is a reasonable foreseeable risk to customers or the safety and soundness of the institution from identity theft (12 CFR 571.90(b)(3)).

Exam Date:	
Prepared By:	
Reviewed By:	
Docket #:	

WKP. REF.

- Oversight of service providers that perform activities related to covered accounts.
- Recommendations for material changes to the Program.

Determine whether management adequately addressed any deficiencies (12 CFR 571.90(f); Guidelines, Section VI).

4. Verify that the financial institution has developed and implemented a comprehensive written Program, designed to detect, prevent, and mitigate identity theft in connection with the opening of a covered account or an existing covered account. The Program must be appropriate to the size and complexity of the financial institution and the nature and scope of its activities (12 CFR 571.90(d)(1)).

   - Verify that the financial institution considered the Guidelines in Appendix J to the regulation (Interagency Guidelines on Identity Theft Detection, Prevention, and Mitigation) in the formulation of its Program and included those that are appropriate (12 CFR 571.90(f)).
   - Determine whether the Program has reasonable policies, procedures and controls to effectively identify and detect relevant Red Flags and to respond appropriately to prevent and mitigate identity theft (12 CFR 571.90(d)(2)(i)-(iii)). Financial institutions may, but are not required to use the illustrative examples of Red Flags in Supplement A to the Guidelines to identify relevant Red Flags (12 CFR 571.90(d)(2); Appendix J, Sections II, III and IV).
   - Determine whether the financial institution uses technology to detect Red Flags. If it does, discuss with management the methods by which the financial institution confirms the technology is working effectively.
   - Determine whether the Program (including the Red Flags determined to be relevant) is updated periodically to reflect changes in the risks to customers and the safety and soundness of the financial institution from identity theft (12 CFR 571.90(d)(2)(iv)).

[4] The term board of directors includes: (i) in the case of a branch or agency of a foreign bank, the managing official in charge of the branch or agency, and (ii) in the case of any other creditor that does not have a Board of Directors, a designated employee at the level of senior management.

Exam Date:	
Prepared By:	
Reviewed By:	
Docket #:	

WKP. REF.

- Verify that (i) the board of directors (or appropriate committee thereof) initially approved the Program; and (ii) the board (or an appropriate committee thereof, or a designated senior management employee) is involved in the oversight, development, implementation and administration of the Program (12 CFR 571.90(e)(1) and (2)).

4. Verify that the financial institution trains appropriate staff to effectively implement and administer the Program (12 CFR 571.90(e)(3)).

5. Determine whether the financial institution exercises appropriate and effective oversight of service providers that perform activities related to covered accounts (12 CFR 571.90(e)(4)).

6. On the basis of examination procedures completed, form a conclusion about whether the financial institution has developed and implemented an effective, comprehensive written Program designed to detect, prevent, and mitigate identity theft.

§ 615(e) Duties of Card Issuers Regarding Changes of Address (12 CFR 571.91)

1. Verify that the card issuer has policies and procedures to assess the validity of a change of address if:

   - It receives notification of a change of address for a consumer's debit or credit card account; and
   - Within a short period of time afterwards (during at least the first 30 days after it receives such notification), the card issuer receives a request for an additional or replacement card for the same account (12 CFR 571.91(c)).

Exam Date:	
Prepared By:	
Reviewed By:	
Docket #:	

WKP. REF.

2. Determine whether the policies and procedures prevent the card issuer from issuing additional or replacement cards until it:

   - Notifies the cardholder at the cardholder's former address or by any other means previously agreed to and provides the cardholder a reasonable means to promptly report an incorrect address (12 CFR 571.91(c)(1)(i)-(ii)); or
   - Uses other reasonable means of evaluating the validity of the address change; (12 CFR 571.91(c)(2)).

   In the alternative, a card issuer may validate a change of address request when it is received, using the above methods, prior to receiving any request for an additional or replacement card (12 CFR 571.91(d)).

3. Determine whether any written or electronic notice sent to cardholders for purposes of validating a change of address request is clear and conspicuous and is provided separately from any regular correspondence with the cardholder (12 CFR 571.91(e)).

4. If procedural weaknesses or other risks requiring further information are noted, obtain a sample of notifications from cardholders of changes of address and requests for additional or replacement cards to determine whether the card issuer complied with the regulatory requirement to evaluate the validity of the notice of address change before issuing additional or replacement cards.

5. On the basis of examination procedures completed, form a conclusion about whether a card issuer's policies and procedures effectively meet regulatory requirements for evaluating the validity of change of address requests received in connection with credit or debit card accounts.

Exam Date:	
Prepared By:	
Reviewed By:	
Docket #:	

WKP. REF.

PROGRAM CONCLUSIONS

1. Summarize the findings, supervisory concerns, and regulatory violations.

2. For the violations noted, determine the root cause by identifying weaknesses in internal controls, audit and compliance reviews, training, management oversight, or other factors. Determine whether the violation(s) are repetitive or systemic.

3. Identify action needed to correct violations and weaknesses in the institution's compliance system.

4. Discuss findings with the institution's management and, if necessary, obtain a commitment for corrective action.

EXAMINER'S SUMMARY, RECOMMENDATIONS, AND COMMENTS

Exam Date:	
Prepared By:	
Reviewed By:	
Docket #:	

CONTROLLING THE ASSAULT OF NON-SOLICITED PORNOGRAPHY AND MARKETING ACT OF 2003

EXAMINATION OBJECTIVES

Assess the quality of a financial institution's compliance program for implementing CAN-SPAM by reviewing the appropriate policies and procedures and other internal controls.

Determine the reliance that can be placed on a financial institution's audit or compliance review in monitoring the institution's compliance with CAN-SPAM.

Determine a financial institution's compliance with CAN-SPAM.

Initiate effective corrective actions when violations of law are identified, or when policies or internal controls are deficient.

EXAMINATION PROCEDURES

LEVEL I

WKP. REF.

1. Through discussions with appropriate management officials, determine whether or not management has considered the applicability of CAN-SPAM and what, if any, steps they have taken to ensure current and future compliance.

2. Through discussions with appropriate management officials, ascertain whether the financial institution is subject to CAN-SPAM by determining whether the financial institution initiates e-mail messages whose primary purpose is "commercial."

3. If you conclude from your examination that the financial institution does not initiate "commercial" electronic mail, the financial institution is not subject to CAN-SPAM. You may conclude this work program and record the basis for this conclusion in the work papers.

Exam Date:	
Prepared By:	
Reviewed By:	
Docket #:	

WKP. REF.

If the financial institution does initiate "commercial" electronic mail:

4. Review management's self-assessment, applicable audit and compliance review material, including work papers, checklists, and reports, to determine whether:

   - Procedures address CAN-SPAM provisions applicable to the institution.
   - Effective corrective action occurred in response to previously identified deficiencies.
   - Audits and reviews performed were reasonable and accurate.
   - Deficiencies, their causes, and the effective corrective actions are consistently reported to management or the members of the board of directors.
   - Frequency of the compliance review is satisfactory.

5. Determine, through a review of available information, whether the financial institution's internal controls are adequate to ensure compliance with CAN-SPAM. Consider the following:

   - Organization chart to determine who is responsible for the financial institution's compliance with CAN-SPAM.
   - Process flow charts to determine how the financial institution's CAN-SPAM compliance is planned for, evaluated, and achieved.
   - Policies and procedures.
   - Marketing plans that reflect electronic communication strategies.
   - Internal checklists, worksheets, and other relevant documents.

Exam Date:	
Prepared By:	
Reviewed By:	
Docket #:	

WKP. REF.

6. Where you conclude from your examination that the institution effectively administers and conducts a comprehensive, reliable, and self-correcting program that adequately ensures compliance with the regulatory requirements of CAN-SPAM, you should record the basis for this conclusion in the work papers and proceed to Program Conclusions.

LEVEL II

1. Review a sample of complaints to determine whether or not any potential violations of CAN-SPAM exist.

2. Obtain a list of products or services that the financial institution promoted with e-mail.

3. Obtain a sample of the e-mail messages to determine whether "commercial" promotion is their primary purpose.

4. Through review of e-mail messages whose primary purpose is "commercial," verify that the messages comply with the CAN-SPAM provisions:

   - Do not use false or misleading transmission information (Section 7704(a)(1)). such as:
     - — False or misleading header information.
     - — A "from" line that does not accurately identify any person who initiated the message.
     - — Inaccurate or misleading identification of a protected computer used to initiate the message.

Exam Date:	
Prepared By:	
Reviewed By:	
Docket #:	

WKP. REF.

- Do not use deceptive subject headings (Section 7704(a)(2)).
- Provide a functioning e-mail return address or other Internet-based response mechanism (Section 7704(a)(3)).
- Provide a clear and conspicuous identification that the message is an advertisement or solicitation; clear and conspicuous notice of the opportunity to decline to receive further commercial e-mail messages from the sender; and a valid physical postal address of the sender (Section 7704(a)(5)). Note: this provision does not apply to a commercial e-mail message if the recipient has given prior affirmative consent to receipt of the message.
- Do not reflect address harvesting, hijacking, or dictionary attacks (Section 7704(b)(1, 2)).
- Provide a warning label (in the subject and within the message body) on commercial e-mail messages containing sexually oriented material (Section 7704(d)).

5. Review any customer requests to opt out of receiving any additional e-mail messages from the institution (Section 7704(a)(4)). Confirm that there are controls in place to discontinue commercial e-mail messages within 10 days of receipt of opt-out notification.

6. Where you conclude that the institution effectively manages its compliance responsibilities associated with CAN-SPAM, you should record the basis for this conclusion in the work papers and proceed to Program Conclusions.

Exam Date:	
Prepared By:	
Reviewed By:	
Docket #:	

WKP. REF.

LEVEL III

If the Level II review reveals weaknesses in CAN-SPAM compliance, and you require additional in-depth testing of the institution's procedures, policies, and practices, expand the size and scope of the samples utilized in the above examination procedures. The sample size is at your discretion.

PROGRAM CONCLUSIONS

1. Summarize all findings, supervisory concerns, and regulatory violations.

2. For the violation(s), determine the root cause by identifying weaknesses in internal controls, audit and compliance reviews, training, management oversight, or other factors. Determine whether the violation(s) are isolated, repetitive, or systemic.

3. Identify action needed to correct violations and weaknesses in the institution's compliance program.

4. Discuss findings with the institution's management and obtain a commitment for corrective action.

5. Record violations according to agency policy in the EDS/ROE system to facilitate analysis and reporting.

EXAMINER'S SUMMARY, RECOMMENDATIONS, AND COMMENTS

Exam Date:	
Prepared By:	
Reviewed By:	
Docket #:	

TELEPHONE CONSUMER PROTECTION ACT AND JUNK FAX PROTECTION ACT

EXAMINATION OBJECTIVES

Assess the quality of a financial institution's compliance program for implementing TCPA by reviewing the appropriate policies, procedures, and other internal controls.

Determine the reliance that can be placed on a financial institution's audit or compliance review in monitoring the institution's compliance with TCPA.

Determine a financial institution's compliance with TCPA.

Initiate effective corrective actions when violations of law are identified, or when policies or internal controls are deficient.

EXAMINATION PROCEDURES

LEVEL I

WKP. REF.

1. Through discussions with appropriate management officials, determine whether or not management has considered the applicability of TCPA and what, if any, steps have been taken to ensure current and future compliance.

2. Through discussions with appropriate management officials, ascertain whether the financial institution is subject to TCPA by determining whether it or a third-party telemarketing firm engages in any form of telephone solicitation or sends unsolicited advertisements to telephone facsimile machines.

Exam Date:	
Prepared By:	
Reviewed By:	
Docket #:	

WKP. REF.

Stop here if the financial institution itself does not engage, directly or indirectly through a third party, in any form of telemarketing or sending unsolicited advertisements to facsimile machines. The financial institution is not subject to TCPA, and no further examination for TCPA is necessary.

3. Determine, through a review of the financial institution's policies and procedures, whether they meet the minimum standards required by 47 CFR 64.1200(d)(1)-(6). Specifically, they should provide for or include:

   - A written policy for maintaining a do-not-call list. Such policy must be available on demand (47 CFR 64.1200(d)(1)).
   - Training of personnel engaged in telemarketing about the existence and use of the do-not-call list (47 CFR 64.1200(d)(2)).
   - Recording and honoring of do-not-call requests within 30 days of the request. Disclosures of such requests may not be made to any other entity (except an affiliated entity) without the express permission of the residential telephone subscriber (47 CFR 64.1200(d)(3)).
   - Identification of sellers and telemarketers. The person or entity making the call must provide the called party with the name of the individual caller, the name of the person or entity on whose behalf the call is being made, and a telephone number or address at which the person or entity may be contacted. The telephone number provided may not be a 900 number or any other number for which charges exceed local or long distance transmission charges (47 CFR 64.1200(d)(4)).
   - Appropriate treatment of affiliated persons or entities. In the absence of a specific request by the subscriber to the contrary, a residential subscriber's do-not-call request shall apply to the particular business entity making the call (or on whose behalf a call is made), and will not apply to affiliated entities unless the consumer reasonably would expect them to be included given the identification of the caller and the product being advertised (47 CFR 64.1200(d)(5)).

Exam Date:	
Prepared By:	
Reviewed By:	
Docket #:	

WKP. REF.

- Maintenance of do-not-call lists. A person or entity making calls for telemarketing purposes must maintain a record of a consumer's request not to receive further telemarketing calls. A do-not-call request must be honored for five years from the time the request is made (47 CFR 64.1200(d)(6)).

4. Determine, through a review of available information, whether the financial institution's internal controls are adequate to ensure compliance with TCPA. Consider the following:

- Organization chart to determine who is responsible for the financial institution's compliance with TCPA;
- Process flow charts to determine how the financial institution's TCPA compliance is planned for, evaluated, and achieved;
- Established and implemented written procedures addressing:
  - Compliance with the national do-not-call rules if the institution makes telemarketing calls to consumers other than existing customers (47 CFR 64.1200(c)(2)(i)(A)).
  - Maintenance of an internal do-not-call-list (47 CFR 64.1200(d)(1),(3),(6)).
  - Use of a telephone facsimile machine, computer, or other device to send an unsolicited advertisement to a telephone facsimile machine.
- Training of the financial institution's personnel engaged in telemarketing as to the existence and use of the financial institution's do-not-call list and the national do-not-call rules (47 CFR 64.1200(d)(2));
- Process for recording a telephone subscriber's request not to receive calls and to place the subscriber's name, if provided, and telephone number on a do-not-call list (47 CFR 64.1200(d)(3));
- Process used to access the national do-not-call database if the institution makes telemarketing calls to consumers other than existing customers (47 CFR 64.1200(c)(2)(i)(D));
- Process used to maintain an internal do-not-call list or database (47 CFR 64.1200(d)(6));

Exam Date:	
Prepared By:	
Reviewed By:	
Docket #:	

WKP. REF.

- Process to ensure that the financial institution (and any third party engaged in making telemarketing calls on behalf of the financial institution) does not sell, rent, lease, purchase or use the national do-not-call database for any purpose except for compliance with the TCPA (47 CFR 64.1200(c)(2)(i)(E));
- Process to ensure that telemarketers making telemarketing calls are providing the called party with the name of the individual caller, the name of the financial institution on whose behalf the call is being made, and a telephone number (that is not a 900 number or number for which charges exceed local or long distance charges) or address at which the financial institution can be contacted (47 CFR 64.1200(d)(4));
- Process to ensure that unsolicited advertisements sent to a telephone facsimile machine by the institution or its facsimile broadcaster went only to entities with an existing business relationship with the institution and that have voluntarily provided their fax number (47 CFR 64.1200(a)(3)(i),(ii));
- Process for ensuring that unsolicited advertisements sent via a telephone facsimile machine, contain the required notice informing the recipient of the ability and means to avoid future unsolicited advertisements (47 CFR 64.1200(a)(3)(iii));
- Process for honoring opt-out requests from businesses or persons receiving unsolicited advertisements via a telephone facsimile machine, within the shortest reasonable time, not to exceed 30 days (47 CFR 64.1200(a)(3)(vi)); and
- Internal checklists, worksheets, and other relevant documents.

5. Review applicable audit and compliance review material, including work papers, checklists, and reports, to determine whether:

- The procedures address the TCPA provisions applicable to the institution;
- Effective corrective action occurred in response to previously identified deficiencies;
- The audits and reviews performed were reasonable and accurate;
- Deficiencies, their causes, and the effective corrective actions are consistently reported to management or the members of the board of directors; and

Exam Date:	
Prepared By:	
Reviewed By:	
Docket #:	

WKP. REF.

- The frequency of the compliance review is satisfactory.

LEVEL II

1. Review a sample of complaints to determine whether or not any potential violations of TCPA exist.

2. Based on the review of complaints that pertain to aspects of TCPA, revise the scope of examination focusing on the areas of particular risk. The verification procedures to be employed depend upon the adequacy of the institution's compliance program and level of risk identified.

Verification Procedures

1. Obtain a list of marketing or promotional programs for products and services that the financial institution promoted with telemarketing or facsimile machines either directly or through a third-party vendor or facsimile broadcaster.

2. Obtain a sample of data or, through testing or management's demonstration, for at least one program, determine whether:

Do-Not-Call List

- The institution or its third-party vendor verified whether the subscriber's telephone number was listed on the national do-not-call registry (47 CFR 64.1200(c)(2)).
- If the telephone subscriber is on the national do-not-call registry and a telemarketing call is made, the existence of an established business relationship between the subscriber and the financial institution can be confirmed (47 CFR 64.1200(f)(4)) or the safe harbor conditions have been met (47 CFR 64.1200(c)(2)).

Exam Date:	
Prepared By:	
Reviewed By:	
Docket #:	

WKP. REF.

- Through testing or management's demonstration, verify that the financial institution has a process to determine whether it has an established business relationship with a telephone subscriber (47 CFR 64.1200(f)(4)).
- A telephone subscriber's desire to be placed on a company-specific do-not-call list was honored for five years (47 CFR 64.1200(d)(6)).
- The institution or its third-party vendor employs a version of the national do-not-call registry or portions of the database for areas called that is obtained no more than 31 days prior to the call date (31 day process) (47 CFR 64.1200(c)(2)(i)(D)).
- The institution or its third-party vendor maintains records to support the 31-day process (47 CFR 64.1200(c)(2)(i)(D)).
- The telephone call was made between the hours of 8 a.m. and 9 p.m. local time for the called party's location (47 CFR 64.1200(c)(1)).

Automated Dialing and Abandoned Calls

- Any calls that were made using artificial or prerecorded voice messages to a residential telephone number met the limits on abandoned calls detailed in the regulation (47 CFR 64.1200(a)(6)(i)).
- The name, telephone number, and purpose of the call were provided to the subscriber, if the call was abandoned (47 CFR 64.1200(a)(6)).
- The institution or its third-party vendor maintains appropriate documentation of abandoned calls, sufficient to determine whether they exceed the 3-percent limit in the 30-day period reviewed (47 CFR 64.1200(a)(6)).
- The institution or its third-party vendor transmits caller identification information (47 CFR 64.1601(e)).

Facsimile Advertising

- Any unsolicited advertisements sent by the institution or its facsimile broadcaster went only to entities with an existing business relationship with the institution and that have voluntarily provided their fax number (47 CFR 64.1200(a)(3)(i),(ii)).

Exam Date:	
Prepared By:	
Reviewed By:	
Docket #:	

WKP. REF.

- Any unsolicited advertisements sent to telephone facsimile machines contain the required opt-out notice (47 CFR 64.1200(a)(3)(iii)).
- The telephone and facsimile numbers identified in the notice must permit an individual or business to make an opt-out request 24 hours a day, seven days a week (47 CFR 64.1200(a)(3)(iii)(E)).

3. Ensure that the financial institution does not participate in any purchase-sharing arrangement for access to the national do-not-call registry (47 CFR 64.1200(c)(2)(i)(E)).

4. Observe call center operations, if appropriate, to verify abandoned call practices regarding ring duration and two-second-transfer rule (47 CFR 64.1200(a)(5),(6)).

5. Ensure that the financial institution has not sent unsolicited advertisements to entities who have requested to opt-out of receiving future unsolicited advertisements via a telephone facsimile machine and that its procedures ensure timely honoring of such requests (47 CFR 64.1200(a)(3)(v),(vi)).

LEVEL III

If the Level II review reveals weaknesses in TCPA compliance, and you require additional in-depth testing of the institution's procedures, policies, and practices, expand the size and scope of the samples utilized in the above examination procedures. The sample size is at your discretion.

(This is in the current OTS procedures, but not in the FFIEC procedures.)

Exam Date:	
Prepared By:	
Reviewed By:	
Docket #:	

WKP. REF.

PROGRAM CONCLUSIONS

1. Summarize all findings, supervisory concerns, and regulatory violations.

2. For the violation(s), determine the root cause by identifying weaknesses in internal controls, audit and compliance reviews, training, management oversight, or other factors; also, determine whether the violation(s) are repetitive or systemic.

3. Identify action needed to correct violations and weaknesses in the institution's compliance program.

4. Discuss findings with the institution's management and obtain a commitment for corrective action.

5. Record violations according to agency policy in the EDS/ROE system to facilitate analysis and reporting.

EXAMINER'S SUMMARY, RECOMMENDATIONS, AND COMMENTS

Exam Date:	
Prepared By:	
Reviewed By:	
Docket #:	