Office of Thrift Supervision **October 24, 2008**

Department of the Treasury

Regulatory Bulletin

RB 37-27

Handbook: **Examination**
Subjects: **Management,**
Fair Credit Reporting Act **Sections: 341, 1300**

Information Technology Risks and Controls and Fair Credit Reporting Act

Summary: This Regulatory Bulletin transmits revised Examination Handbook Section 341, Information Technology Risks and Controls, and revised Examination Handbook Section 1300, Fair Credit Reporting Act (FCRA). The revised Handbook Sections contain new guidance and examination procedures for the final rules on Identity Theft Red Flags and Address Discrepancies, which implement Sections 114 and 315 of the Fair and Accurate Credit Transactions Act (FACT Act) of 2003. This bulletin rescinds RB 37-15 dated April 20, 2006.

For Further Information Contact: Your OTS Regional Office, Kathleen M. McNulty, Technology Program Manager, in the Information Technology Examinations Division of the OTS, Washington, DC, at (202) 906-6322 for Examination Handbook Section 341, or Ekita Mitchell, Consumer Regulations Analyst, in the Consumer Protection Division of the OTS, Washington, DC, at (202) 906-6451 for Examination Handbook Section 1300. You may access this bulletin and the Examination Handbook at our website: www.ots.treas.gov.

Regulatory Bulletin 37-27

SUMMARY OF CHANGES

The Task Force on Consumer Compliance of the Federal Financial Institution Examination Council (FFIEC) recently approved new examination procedures developed by an FFIEC working group for Identity Theft Red Flags and Address Discrepancies. OTS is issuing revised Examination Handbook Sections 341, Information Technology Risks and Controls, and 1300, Fair Credit Reporting Act, to reflect the new guidance and examination procedures.

The FACT Act created new responsibilities for financial institutions that obtain or use consumer information, for example, to grant credit or open deposit accounts, provide consumer information to consumer reporting agencies, third parties, or affiliates, or to market credit or insurance products. OTS, along with the federal financial institution regulatory agencies, is revising the interagency FCRA examination procedures into the following modules that group similar requirements together:

- Module 1 Obtaining Consumer Reports.

- Module 2 Obtaining Information and Sharing Among Affiliates.
- Module 3 Disclosures to Consumers and Miscellaneous Requirements.
- Module 4 Financial Institutions as Furnishers of Information.
- Module 5 Consumer Alerts and Identity Theft Protections

This revision to Section 1300 of the Examination Handbook will be followed by revisions to other modules as the FACT Act regulations and interagency examination procedures are finalized.

Change bars in the margins of the handbook sections indicate revisions. We provide a summary of substantive changes below.

341 Information Technology Risks and Controls

OTS revised Examination Handbook Section 341, Information Technology Risks and Controls, to include guidance on the Identity Theft Red Flags as part of the information security guidance. The Regulatory Guidance and References in Examination Handbook Section 341 includes Information Technology guidance issued subsequent to April 2006 when Section 341 was most recently revised.

OTS revised the Program for Examination Handbook Section 341 to reflect the addition of six examination procedures for Section 615(e) of FCRA, Duties Regarding the Detection, Prevention, and Mitigation of Identity Theft. These duties are codified in 12 CFR § 571.90.

1300 Fair Credit and Reporting Act

The update to Examination Handbook Section 1300 incorporates the examination procedures for FCRA Sections 615(e), Duties Regarding the Detection, Prevention, and Mitigation of Identity Theft, 12 CFR § 571.90; § 615(e), Duties of Card Issuers Regarding Changes of Address, 12 CFR § 571.91; and § 605(h), Duties of Users of Credit Reports Regarding Address Discrepancies, 12 CFR § 571.82.

FCRA Section 615(e), as amended by the FACT Act, requires associations that have covered accounts to develop and implement a written Identity Theft Prevention Program (Program) for combating identity theft in connection with new and existing accounts. The Program must include reasonable policies and procedures for detecting, preventing, and mitigating identity theft and enable an association to do the following:

- Identify relevant patterns, practices, and specific forms of activity that are “red flags” signaling possible identity theft and incorporate those red flags into the Program.
- Detect red flags that have been incorporated into the Program.
- Respond appropriately to any red flags that are detected to prevent and mitigate identity theft.
- Ensure the Program is updated periodically to reflect changes in risks from identity theft.

FCRA Section 615(e) also requires credit and debit card issuers to develop reasonable policies and procedures to assess the validity of a request for a change of address that is followed closely by a request for an additional or replacement card. FCRA Section 605(h) requires users of consumer reports to develop and apply reasonable policies and procedures when they receive a notice of address discrepancy from a consumer reporting agency.

OTS examiners will conduct the Examination Handbook 341 and 1300 procedures on comprehensive examinations commencing on or after November 1, 2008. To facilitate this, OTS is updating its Preliminary Examination Response Kit to request materials for Identity Theft Red Flags and Address Discrepancies consistent with these new examination procedures.

Timothy T Ward

–Timothy T. Ward
Deputy Director
Examinations, Supervision, and Consumer Protection

Information Technology Risks and Controls

This Handbook Section presents the agency's examination guidance and program for assessing information technology (IT) risks in comprehensive examinations of savings associations that do not undergo a separate IT examination. OTS uses this section to evaluate technology risks in an association and to assess the strength of an association's internal controls for information technology. The Handbook section focuses on the important control activities of proactive management oversight for information security, business continuity, and vendor management, as well as technology-related audit work.

Technology has revolutionized daily operations in savings associations. Associations have moved away from mainframe-oriented computer processing environments and toward increased reliance on decentralized or distributed technological environments, for example, networks, the Internet, and enterprise-wide processing. This examination guidance reflects these changes. Examiners assess the risks of the association's usage of technology, the overall resulting exposure to technology risks, and the adequacy of controls to mitigate those risks.

LINKS

Program

If the savings association does not properly identify and mitigate technology risks, there can be serious adverse consequences to its reputation. Examples of technology risks that can substantially damage an association's reputation include unauthorized access to corporate data and customer records, identity theft, inadequate business continuity planning, or fraud. These can also cause significant financial losses to an association. Use this Handbook Section to determine, on a risk-focused basis, whether an association's use of technology is consistent with a safe, sound, and secure operating environment. This Handbook guidance and program complements Section 340, Internal Controls.

OVERVIEW

Increasingly, associations are using technology to develop and deliver financial products and services, with the goals of improving customer service and reducing operating costs. Even the most traditional, conservative associations have embraced technology. Associations have made, and continue to make, huge investments in technology to maintain and upgrade their infrastructure, to provide new electronic information-based services, to manage their risk positions and pricing, and to monitor transactions to detect and prevent money laundering and terrorist financing under the Bank Secrecy Act and the PATRIOT Act. At the same time, new electronic products, such as online banking, make it possible for small associations to take advantage of newer technologies at lower costs.

Improved processes, such as automated underwriting and credit scoring, have given borrowers the opportunity to obtain credit cards, mortgages, and small business loans from more financial services providers. Automated underwriting and credit scoring substantially reduce the time and costs involved in making sound credit decisions. These tools have also improved the ability of lenders to evaluate and price credit risk, which allows extensions of credit to a wider range of borrowers. Individuals can easily obtain their credit reports and credit scores and verify the information. They can contact the credit bureau if information in the report is incorrect, and thereby, improve their credit standing.

Information technology has made other significant contributions to associations' profitability. In mortgage lending, credit decisions are made in minutes rather than days and at a much lower cost than a decade ago. New technology has also enhanced competition, making it easier for local associations to offer new products and compete successfully with out-of-market associations. In addition, securitization, which is also highly dependent on advances in information technology, has broadened the pool of mortgage lenders and made the primary and secondary markets far more efficient.

Associations use software and computers in operations due to the volume and complexity of transactions processed each day; in fact, almost every aspect of operations within an association is able to use some technology. Savings associations use technology to develop budgets and business plans, underwrite loans, measure and model interest rate risk, track trust accounts, and monitor suspicious activities; in short, to manage almost every aspect of their operations. As technology evolves, and associations continue to increase their reliance on it, risks increase. The increased risks require effective controls to ensure the integrity, confidentiality, and availability of data.

Risks are inherent in using any technology, and threats to associations come from both internal and external sources. Hackers, disgruntled employees, and errors can adversely affect reliability. Unauthorized parties might access networked systems that are connected to an association's database, and obtain sensitive, nonpublic customer information. Association websites may be inappropriately altered. Electronic mail containing confidential, proprietary corporate information may be distributed in error.

> An association's board of directors and management should establish policies, procedures, and controls to ensure confidentiality, integrity and availability of information.

Clearly, this increased reliance on technology has significantly increased the risks of financial and reputation losses due to unauthorized access to customer and corporate financial records, interruption of services to customers, and fraud. Associations must make choices regarding how to manage and control these risks.

Associations must establish and maintain adequate control systems so management can identify, measure, monitor, and control IT risks that could adversely affect performance or pose safety and soundness concerns. Similar to basic internal controls, associations should design IT risk controls to prevent, to mitigate, and/or to detect and address errors and problems. This process should involve representation from all functional areas, for example, audit, finance, legal, lending, marketing, and IT. These areas should all be involved from the beginning of the process to assess collectively the effects on the association. However, ultimately the board of directors and management are responsible for

developing and implementing the processes, policies, and controls that ensure confidentiality, integrity, and availability for an association's data and systems:

- Confidentiality: Customer and corporate information is protected from unauthorized access or use.
- Integrity: Information is not altered without permission.
- Availability: Authorized users have prompt and continuous access.

The level of technical knowledge required by boards of directors and senior managers varies and is dependent on the size and nature of the association's operations and the degree of complexities within its technology environment. Nonetheless, at a minimum, directors and senior officers should have a clear understanding of the risks posed by technology, provide clear guidance on risk management practices, and take an active oversight role in monitoring risk mitigation activities.

EXAMINATION OVERSIGHT ACTIVITIES

In conducting risk-focused reviews of information technology in comprehensive examinations, examiners:

- Review the association's IT environment.
- Determine the association's significant technology risks.
- Evaluate management's technology oversight activities, including any technology audit work.
- Assess the strengths of the association's control activities.

You should always consider the level of IT risks and adequacy of the control environment when scoping for examinations and assigning the Management and, as appropriate, the composite CAMELS ratings.

Consistent with a risk-focused approach, you should use judgment in determining the depth of the technology review in comprehensive examinations. The examination work should be consistent with the characteristics, size, complexity, and business activities of the association. To determine the appropriate review, close coordination is needed between the Examiner-in-Charge (EIC), other members of the examination team, and examiners who review the IT risks and controls.

Examination Coverage

IT examiners review technology risks and controls at associations that have complex operations and activities. Safety and soundness examiners review IT risks and controls during comprehensive examinations, using this examination guidance and its related examination procedures. To supplement

the examination guidance in this Section, we encourage you to refer to the FFIEC IT Examination Handbook Booklets, if necessary.

Regional managers determine whether to assign an IT examiner to review an association's information technology. They consider the most recent information available regarding the association's technology environment and the strength of IT controls. As complexity within an association's technology environment stabilizes or decreases, examination responsibilities for some associations may move from IT examiners to non-IT examiners.

Factors suggesting an IT examiner may need to review this area include the following:

- Recent, pending, or proposed system conversions.
- Recent or pending mergers and acquisitions.
- Problems and concerns at previous examinations.
- Volume and type of internal processing conducted.
- Complex applications, systems, networks, or equipment.
- Volume of loan servicing.

While these factors suggest a need for an IT examiner, they are not determinative. In scoping, the EIC should consult with the Regional IT Examination Manager regarding IT concerns. Such consultation helps ensure proper evaluation and consistent regulatory treatment.

Significant internal control weaknesses warrant expanded investigation and analysis. In those situations, the examiner completing this program, the EIC, the Regional IT Examination Manager, and the regional Caseload Management team will determine what additional procedures are needed, who should perform them, and whether to conduct them at the current examination or at a future comprehensive or IT examination.

Information Technology and Management Ratings

The strength of the information technology control environment is one of the factors considered in assigning a rating to the Management component of CAMELS. As stated in Examination Handbook Section 070, the Management component rating must reflect the board's and management's ability and effectiveness in managing all aspects of an association's risks, including the findings and conclusions for IT risks and controls.

The Management rating should always reflect serious control deficiencies for technology risks. Generally, if you identify serious deficiencies with the technology controls, you should rate Management no higher than 2.

Ratings: IT Concerns

> The EIC should select Yes for IT Concerns whenever the exam findings disclose significant IT weaknesses.

For comprehensive regular examinations, the EIC completes the data field in the OTS Examination Data System (EDS) for the technology examination work. The data field is not available in EDS for type 17 comprehensive special examinations. You should detail significant IT weaknesses for type 17 examinations in the Examination Conclusions and Comments. **Note:** This data field is available for examination types 11 (State) and 46 (Comprehensive Limited). We encourage its use, but it is not required.

This data field prompts the EIC to answer Yes or No to the question:

- Were significant IT concerns noted in the Report of Examination (ROE)?

The EIC should select Yes whenever the examination findings disclose significant IT weaknesses. A significant weakness is one that the EIC concludes is at least partially the cause for lowering the Management rating. A significant weakness could also be something that significantly impacts the association, and management lacks the will or ability to resolve it. If the IT program did not disclose any significant weaknesses, the EIC should answer No.

Examination Comments and Conclusions

You should incorporate IT examination comments and conclusions into the Management comments, either on the formal report page for Management, or in the Management-related comments summarized under overall Examination Conclusions and Comments. You should present findings under the caption or heading, Information Technology.

Examiners conducting this program assess an association's compliance with the Interagency Guidelines Establishing Information Security Standards (Security Guidelines), 12 CFR Part 570 Appendix B, including Supplement A. The Security Guidelines implement Section 501(b) of the Gramm-Leach-Bliley Act of 1999 (GLB Act), and Section 216 of the Fair and Accurate Credit Transactions Act of 2003 (FACT Act).

The ROE comments should include a brief description of the association's IT environment, significant technology risks, and an overall conclusion as to the adequacy of controls. The report comments should also clearly state whether or not the association is in compliance with the requirements of the Security Guidelines. You must note material instances of noncompliance in the ROE.

You should present significant adverse findings in sufficient detail to identify the specific conditions that require corrective action. Whenever possible, these should include mutually agreeable deadlines for completion of corrective actions. Present corrective actions and deadlines in the Management page comments, or integrate them into the Management-related comments in the Examination Conclusions and Comments. Include significant findings, for example, violations of laws or regulations, on the Matters Requiring Board Attention page.

When examining a state-chartered association, you should also refer to state regulations and follow supplemental regional examination policies and procedures.

Information Technology Database

OTS developed and maintains the Information Technology Database (IT Database), a national system that provides agency management with information on the thrift industry's data processing activities and technology service providers. The Director, Information Technology Examinations, is the IT Database system owner. IT Examinations works with OTS Information Systems to maintain and enhance the system, oversee its operations, and update system standards, policies and procedures.

A staff person in IT Examinations serves as the IT Database National Administrator. In addition to the National Administrator, the regional IT Examination Managers have designated Regional IT Database Administrators. The Regional IT Database Administrators ensure that data collected from the associations, and reviewed by the safety and soundness examiners, are entered into the IT Database, as required.

The IT Database contains information on service providers used by associations, such as names, addresses, significant applications processed, and processing locations, domestic or foreign. The IT Database also collects information about significant applications processed internally by associations. Examiners and Caseload Managers use this information to produce reports that identify technology-related risks, which can be addressed in examinations, off-site monitoring, and other regulatory oversight activities.

The examiner completing the IT procedures collects and reviews the IT Database information for accuracy and completeness, and then provides the information to the regional office for input. The information in the IT Database must be updated every 18 months. If these examination procedures are not conducted within the 18-month timeframe, regional staff must obtain the IT Database information directly from the association.

Information Technology Environments in Associations

Background

Associations have a number of choices available to meet their IT needs. Many OTS-regulated associations outsource a significant amount of their information processing functions to one or more third-party service providers. Others maintain internal data centers to run software licensed from vendors or developed in-house. Mixes or hybrids of these basic approaches are common. An association might contract with one service provider for its general ledger and deposit systems, and with other service providers for loan servicing or its website. Associations also might use licensed software for investments and interest rate risk analysis, and spreadsheets developed in-house for asset quality and board reports.

In addition to outsourcing significant business operations to service providers, most associations are interconnected with various other entities, such as ATM networks and automated clearing houses (ACHs), to process daily business. Associations also maintain one or more internal networks, Local Area Networks, or Wide Area Networks. Each of these arrangements requires a different type and level of management involvement with regard to data integrity, security measures, and business continuity plans.

OTS expects associations to develop and maintain strong control environments for the information technologies they use. A strong control environment enables management to identify, evaluate, and control risks associated with the business activities. In complex technology environments, it is critical that associations have effective risk management practices and strong internal controls to ensure that all of the technology risks are identified and appropriately addressed. Associations should have effective policies and procedures in place commensurate with the complexity of the IT environment. They also should identify the risks of using technology prior to deploying it, and ensure adequate controls are in place.

Components of Information Technology Environments

Personal Computers

The personal computer is the most prominent tool in an association's business environment. The power of personal computers has enabled information processing in associations to evolve from the traditional, centralized environment to a decentralized or distributed environment. In addition to its use as a word processor and terminal access device to other computers, a personal computer operates as a powerful standalone computer or within a network of computers. Most associations have at least one internal network, whether it uses third-party service providers, processes internally, or uses a combination of these arrangements.

Using personal computers, association staff can create applications to supplement those provided by third-party service providers or internally operated data centers. For example, staff can use personal computers to originate data, download and manipulate information from an association's databases, and upload the data back into the databases. Each of these activities creates information, which management uses to make decisions that affect business strategies, customer relationships, and regulatory reporting. Management should implement and maintain controls over these activities to ensure confidentiality, integrity, and availability of the information processed and produced.

Networks

A computer network is an arrangement in which multiple computers are connected to share information, applications, and equipment. By design, networks can increase efficiency, convenience, and access; however, the design also directly affects the specific risks that users must address and control.

Network access can be provided through a combination of devices such as personal computers, telephones, interactive television equipment, and card devices with imbedded computer chips. The connections are completed principally though telephone lines, cable systems, or wireless technology. It is important to note that not all networks are equally critical, vulnerable, or contain data that is equally sensitive. Every association must evaluate the risks it faces and address those risks.

The Internet is a public network that can be accessed by any computer equipped with a modem. While not centrally managed, the Internet is given order through the World Wide Web (Web), which facilitates visual interfaces and links or electronic connections to other information. The Web also provides multimedia capabilities such as text, graphics, audio, and video.

Intranets are private networks built on the infrastructure and standards of the Internet and the Web. Intranets allow access to databases and electronic documents by defined user groups that are generally limited to internal personnel.

Associations must review and address the security of internal networks, whether private, or configured as local or wide area networks. Internal attacks are potentially more damaging than attacks from outsiders because an association's personnel, who can include consultants as well as employees, have authorized access to critical computer resources. An internal attacker could exploit trusted relationships in networked systems to gain a level of access that allows the attacker to circumvent established security controls. After circumventing the security controls, the attacker could potentially access sensitive customer or corporate information.

Public networks pose additional risks over those of internal networks. Transmitting confidential data over public networks through the use of dedicated or leased lines may provide an inappropriate sense of security. These lines use the infrastructure of public networks; therefore, they are vulnerable to the same attacks as the public networks themselves. Confidential data transmitted via public networks may be intercepted or compromised by individuals for whom the data is not intended. It is therefore important to encrypt sensitive data transmitted via public network infrastructure.

Local and Wide Area Networks

A local area network (LAN) is a network that interconnects systems within a small geographic area, for example, a building or a floor within a building. Using personal computers or other terminals, users communicate via electronic mail, share printers, and access common systems, databases, and software. A wide area network (WAN) connects users in larger geographic areas. An association might have a LAN within its headquarters, and a WAN for its branches or lending offices to communicate with each other and the headquarters.

LANs and WANs provide substantial benefits in productivity and information access. They facilitate interaction among association staff and between the association and its service providers. Examples of services that associations can offer through their networks include telephone banking, banking by personal computer, ATMs, automatic bill payments, and automated clearinghouse systems for direct deposits or payments. Such access, however, requires that the association apply controls to the personal computers.

Associations that use LAN, WAN, or other network technologies should have policies and procedures that govern purchase and maintenance of hardware and software. Associations must also establish and maintain sound controls that limit access to data and applications based upon job responsibilities, and protect the data's confidentiality and integrity.

Firewalls

Firewalls are a combination of hardware and/or software placed between networks that regulate traffic that passes through them. They provide protection against unauthorized individuals gaining access to an association's network. Associations should consider firewalls for any system connected to an outside network.

A firewall does not ensure that a system is impenetrable. Firewalls must be configured for specific operating environments and the association must review and update firewall rules regularly to ensure their effectiveness.

Internet Activities

Association management should have policies, procedures, and controls to govern employee Internet activities. These should address the following:

- Minimizing viruses or other damaging program code associated with downloading files.
- Appropriate use of Internet facilities and services by employees.
- Using encryption to protect sensitive information in transit, for example, electronic mail messages.

Electronic Banking

Electronic banking is the delivery of information products and services between a customer and an association using electronic access devices such as telephones, automated teller machines, and personal computers. Typically, the devices are connected through a telecommunication line or the Internet.

Internet Banking

Internet banking refers to the systems that enable customers to access their accounts and information regarding the association's products and services from the association's website via a personal computer or similar communication device.

Transactional Websites

Transactional websites, as defined in CEO Memo 109, allow customers to do any of the following:

- Open an account.
- Access an account.
- Obtain an account balance.
- Transfer funds.
- Process bill payments.
- Apply for or obtain a loan.
- Purchase other authorized products or services.

CEO Memo 109, Transactional Web Sites, states that OTS-regulated associations planning to establish a transactional website must file a Notice with OTS at least 30 days in advance of opening the website to transact business with customers. The examiner conducting the IT examination procedures should determine that the association filed the required Notice with the appropriate regional office.

If the Notice was not timely and properly filed, the EIC should notify the regional caseload management team to determine appropriate remediation. If the Notice was filed pursuant to CEO Memo 109, the examiner reviewing IT risks and controls should contact the regional office to determine if there were any issues that require onsite follow-up review.

Transactional websites also pose specific consumer protection and privacy issues associations should address. See Handbook Section 1375, Privacy, for additional guidance.

Transactional websites that provide for electronic mail between the association and customers require additional controls, for example, encryption, to protect the confidentiality of customer accounts and other sensitive data. Associations should clearly caution customers about sending sensitive data, for example, account numbers, in electronic mail messages to the association or anyone else. For additional guidance see CEO Memo 228, Interagency Guidance on Authentication in an Internet Banking Environment.

Informational Websites

Informational websites provide general information about an association's products and services. Informational websites often highlight loan and deposit programs, branch locations, and operating hours. These may also provide electronic mail addresses for contacting the association and its employees.

Some informational websites provide links to other websites that provide community interest information or other related product information. Thrift Bulletin 83 provides guidance regarding these web-linking arrangements.

CONTROL ACTIVITIES FOR INFORMATION TECHNOLOGY RISKS MANAGEMENT OVERSIGHT

Responsibilities of the Board of Directors

Boards of directors have the ultimate responsibility for all technology deployed in their associations. They should approve their associations' overall business and technology strategies. The board of directors and management cannot delegate responsibility for technology controls to service providers, software vendors, or even internal staff. The board of directors must ensure that strong controls for technology risks exist throughout the association.

The level of knowledge required by boards of directors and management is dependent on the size and nature of an association's operations and the degree of complexity within its technology environment. Nevertheless, association directors and management should have a clear understanding of the risks posed by using specific technology, provide clear guidance on risk management practices, and take a proactive role in overseeing technology risk mitigation activities. An association's board of directors and management must effectively plan for using technology, establish a strong control environment, including audit or other independent review of the controls, and educate and support the association's technology users.

To manage effectively the risks associated with complex technology environments, some associations have established a senior management Information Technology committee. This committee is responsible for overseeing the relevant technology control functions throughout the association, for example, in the auditing, legal, and financial divisions, and ensuring these controls are integrated into a framework of risk management for information technology. This senior management committee regularly reviews new products and activities and provides final approval of transactions. Such senior management committees can serve as an important part of an effective information technology control infrastructure.

Strategic Planning for Information Technology

Deficiencies in planning for deploying technology significantly increase the risks posed to an association and its ability to respond effectively. Therefore, regardless of asset size, associations should have an appropriate plan for technology that outlines the framework for the uses of technology. The substance and form of such a plan will vary from association to association and be dependent on the complexity of the association's operations. The key elements are whether and how well the technology planning process meets the association's needs.

Associations should update their technology plans annually. A satisfactory technology plan coordinates the technology initiatives and activities to the overall business planning process. It should also address the technology strategy used, for example, a combination of internal and outsourced processing that supports delivery of the selected products and services.

Associations intending to implement a transactional website should address this in the technology plan. Management should consider the implications of a transactional website on the association's long-term goals and strategies, and obtain input from the affected business line and technology managers. Planning for a transactional website should address the required advance notice to OTS and include a thorough review of the risks posed by a transactional website to information security, business continuity, and vendor management.

Training Information Technology Users

Associations must properly educate and support employees and customers to achieve user acceptance of, and confidence in, the association's information systems and technology. Associations should provide training to employees and customers to use applications properly. Associations must also support users with prompt responses to problems. If an association fails to provide reasonable training and support for customers and staff, commitment to the system and its applications deteriorates, administrative costs increase, and avoidable errors may occur. Training deficiencies also raise the risks of information security problems and increases potential for identity theft.

Associations should fully inform staff of any changes or updates to systems. Associations should also train staff on how to respond to and execute the business continuity plan. If the association chooses to outsource this function, it must carefully evaluate the third-party vendor's qualifications prior to signing any contracts. Management should also provide backup training for key job functions.

For additional guidance on Management control activities, see Examination Handbook Sections 310, Oversight by the Board of Directors, and 330, Management Assessment, CEO Memo 201, FFIEC IT Examination Handbook, Management Booklet, and CEO Memo 245, Director's Responsibility Guide and Guide to Management Reports.

Audits and Other Independent Reviews

All associations should adopt and maintain an audit program. An effective audit function is essential to an association's safe and sound operations. It provides the framework for assessing the effectiveness of the association's risk management practices. It also facilitates reporting to the board of directors and management on the strengths and weaknesses within the association's internal controls. To ensure adequate audit coverage, associations may use internal audit work, external audit work, or a combination of both depending on the association's audit risk assessment. Effective audit coverage substantially improves an association's ability to detect potentially serious problems.

The audit work may be completed internally or externally, however, someone that is qualified and independent of the process or function reviewed must complete the work. This independent person can conduct the audit work separately, as an audit of a specific technology activity, or incorporate it into the audit work for a specific operating department or business line.

The complexity of financial products, services, and delivery channels makes the inclusion of risk-based IT audit coverage an important consideration in establishing an effective overall audit program. Effective audit coverage of technology risks requires personnel that have the skills and experience to

identify and report on compliance with the association's policies and procedures. These skills and experience should include strong abilities to understand technology risks, as well as a detailed understanding of the association's IT policies and procedures.

Audit procedures are most effective when designed into the technology or system during development. When combined with a strong risk management program, a comprehensive, ongoing audit program allows the association to protect its interests and those of customers. In developing an audit program for technology, an association should consider how each application protects fully the financial and informational assets, system reliability and availability, and user confidence.

See Thrift Bulletin 81, Interagency Policy Statement on the Internal Audit Function and Outsourcing, for additional guidance on OTS expectations for an internal audit program.

Technology Audit Plan

An association's audit plan should provide for reviewing its technology risks. It is the responsibility of the board of directors and management to determine how much auditing will effectively monitor the internal control system, taking into account the audit function's costs and benefits. For associations that are large or have complex operations, the benefits derived from a full-time manager of audit or an auditing staff will likely outweigh the costs. For small associations with few employees and less complex operations, these costs may outweigh the benefits. Nevertheless, even a small association without an internal auditor can ensure it maintains an objective internal audit function by implementing a comprehensive set of independent reviews of significant internal controls.

Generally, a technology audit will:

- Review technology policies, standards, and procedures.
- Assess how technology affects association operations.
- Determine if technology activities are consistent with management policies and procedures.
- Substantiate the integrity of employee activities and appropriateness of user access rights.

Audit work for technology should validate that all the business lines are complying with the association's standards for technology usage, and appropriately identify any exceptions. This validation should include transaction testing that confirms policy compliance, existence of proper approvals, adequacy of documentation, and integrity of management reporting.

Technology audit work should have clear procedures for when and how to expand the scope of audit activities. There should also be procedures for reporting audit findings directly to the association's board of directors or audit committee, as well as management in the audited area. Associations should implement follow-up procedures to ensure that management resolved all audit findings satisfactorily and the business unit or department implemented audit recommendations in a timely manner.

The complexity of the association's technology environment may cause some associations to retain outside consultants, accountants, or lawyers to review this area. The retention of independent expertise may be an appropriate method to control effectively the overall risk. For example, associations may employ external auditors to test the technology environment and ensure compliance with policies and procedures. The resulting reports can provide valuable insight to the association in improving its risk controls and oversight.

Additional guidance regarding External and Internal Audit is found in Handbook Sections 350 and 355, and CEO Memo 182, FFIEC IT Examination Handbook, Audit Booklet.

Information Security Risks and Controls

An association's corporate data and customer information must be available, accurate, complete, valid, and secure. Information security is the process or methodology an association uses to protect its corporate and customer information. Strong and effective information security is essential to an association's safety and soundness, and should be commensurate with the complexity of its operations and IT environment. The most effective information security has strong board of directors and management support and controls implemented throughout the association's business operations.

Effective information security is not a judgment or conclusion about the condition of IT controls at a particular point in time. Rather, effective information security is an ongoing and evolving process. An association has effective information security when it successfully integrates its processes, people, and technology to mitigate risks to acceptable levels in accordance with its risk assessment.

An effective information security program serves as the overall framework that identifies risks, develops and implements a security strategy, tests key controls, and monitors the risk environment. This framework stresses the important roles of senior management and boards of directors by emphasizing their responsibility to recognize security risks in their associations and effectively mitigate security risks by assigning appropriate roles and responsibilities to management and employees. OTS expects an association's information security program will have an incident response component for responding to specific risks, for example, unauthorized access attempts. The information security program should also provide for regular testing as well as security training of employees and other users.

The scope of an association's information security program should address all technology activities, for example, personal computers, Internet-based banking, and processing by the association's service providers. Effective security does not rely on one solution; rather it requires several measures, which, taken together, serve to identify, monitor, control, and mitigate potential risks to that information. Associations should use several differing controls to manage and ensure information security. Among these commonly found in associations are controls for authentication, passwords, user identification (ID), user access, system log-on and log-off, virus protection, and encryption.

Information Security Controls

Authentication

Savings associations use authentication controls to verify and recognize the identity of parties to a transaction. Typically, such controls include computerized logs, digital signatures, edit checks, and separation of duties. Weak authentication controls can allow the accuracy and reliability of data to be compromised from unauthorized access and fraud, errors introduced into the systems, or corruption of data and information. Associations should use effective authentication controls to restrict access and preserve integrity of data.

Authentication procedures for access to sensitive data minimally require a password. Maintenance procedures should ensure that only the user has knowledge of the user's password. Associations should have procedures that allow only users to change their own passwords. Password controls should have all of the following:

- Length of at least six characters, preferably more.
- A mixture of alphabetic, numeric, or other characters.
- Expiration dates that require users to change passwords frequently.
- Restrictions on reuse of previous passwords.
- Automatic lockouts after a defined number of failed log-on attempts.
- Suppression over the display of user passwords in any form.
- Encryption of password files.

OTS and the other federal financial regulators issued guidance on risks and risk management controls to authenticate identity of customers accessing an association's Internet-based financial services. This guidance, distributed in CEO Memo 228, Authentication in an Internet Banking Environment, addresses the increased risks to associations and their customers from the growth of Internet banking and other electronic financial services, and the increased incidents of identity theft and fraud. As this guidance relates, associations need effective authentication systems to comply with requirements for safeguarding customer information, prevent money laundering and terrorist financing, and reduce fraud and theft of sensitive customer information.

The level of authentication an association uses should be commensurate with the risks of the Internet-based products and services offered. Associations should conduct a risk assessment to identify the types and levels of risk associated with their Internet banking applications. Where an association's risk assessment indicates the use of single-factor authentication – only a log-on ID or password – is inadequate, the association should implement multifactor authentication, layered security, or other controls reasonably calculated to mitigate these risks. OTS considers single-factor authentication

inadequate as the only control mechanism for higher-risk transactions involving access to customer information or movement of funds to others.

Additional guidance regarding enhanced authentication is found in CEO Memo 242, Frequently Asked Questions on Authentication in an Internet Banking Environment.

User Access Rights and Controls

Associations should also establish controls to limit user access. For example, associations should limit access to the Security Administrator account to the smallest number of persons practical without adversely affecting operations. Security Administrators should not have access to customer records. In addition, the association may grant contractors and consultants access to an association's systems. The association should tightly control these access rights.

Access rights to a system enable transaction processing and information retrieval. For outsourced systems, service providers typically set up generic access profiles for common job categories, for example, teller profiles. Associations should not accept and use the vendor access profiles without reviewing them. This increases the risk of inappropriate user access and weakens the control environment for sensitive data. To ensure user access is appropriate, associations should:

- Assign job responsibilities to provide for segregation of duties and dual control.
- Assign user retrieval and information processing capability profiles, based on job responsibilities.
- Ensure separate access profiles for their different systems.

User identification controls should require:

- Management approval to issue a new user ID.
- A unique user ID for each user. Multiple users should not be assigned to one user ID unless there are mitigating controls.
- Restrictions on issuing multiple identifications unless there are mitigating controls.
- Effective procedures to delete, disable, or change access rights promptly for terminated or reassigned employees.

Inappropriate user access assignments could be caused by control deficiencies in granting these rights or by weaknesses in the system security controls. System security control weaknesses can result from software rules that permit inappropriate grouping of user access rights. Weaknesses also arise when software capabilities are not properly invoked. Not enabling the supervisory override capability over dormant accounts is an example of such a weakness.

Management should periodically conduct independent reviews of user access rights to ensure user access assignments are appropriate and properly controlled. Management should document the findings of these reviews and resolution of any recommendations. Regardless of the cause, you should comment in the ROE on inappropriate user access rights.

Other Information Security Controls

System log-on and log-off controls should limit the number of unsuccessful log-on attempts to a user account. Associations should consider a control that notifies users of unsuccessful attempts since the user's last log-on. Associations should also require that personal computers and system access terminals automatically log-off after a brief period of inactivity.

Associations should install virus protection software on all personal computers and servers to prevent corruption of data or systems. Virus protection controls should include both association policies and installed software. An association's policies should restrict employees from adding software to their personal computers. The policy should also provide for periodic review or audit of the employees' personal computers to ensure conformance with association policies. Anti-virus software should be updated regularly to protect against new viruses.

Acknowledgement controls, such as batch totaling, sequential numbering, and one-for-one checking against a control file, verify proper completion of electronic transactions. For example, if an electronic transmission is interrupted, the association should have controls in place to notify the sender of the incomplete transaction and prevent duplication during re-submission.

Encryption technology scrambles data and information so it cannot be read or understood without the proper codes for unscrambling. Confidential or sensitive data and information in transit should always be encrypted. This includes email containing confidential or sensitive information, as well as Internet banking transactions. As part of performing its risk assessment, association management should identify the strength of encryption needed for specific categories of information.

For additional guidance regarding information security, see CEO Memo 241, FFIEC IT Examination Handbook, Information Security Booklet.

INTERAGENCY GUIDELINES ESTABLISHING INFORMATION SECURITY STANDARDS

12 CFR Part 570 Appendix B and Supplement A Security Guidelines and Association Responsibilities

The Interagency Guidelines Establishing Information Security Standards implement:

- Section 501(b) of the GLB Act, which requires the federal financial regulators, including OTS, to establish standards for administrative, technical, and physical safeguards to ensure the security, confidentiality, integrity, and proper disposal of customer information.

- Section 216 of the FACT Act, which requires the federal financial regulators to issue regulations directing associations to ensure the proper disposal of consumer information. See Examination Handbook Section 1300, Fair Credit Reporting Act, for guidance on the FACT Act.

For additional guidance on an association's compliance obligations for the Security Guidelines, see CEO Memo 231, Compliance Guide for the Interagency Guidelines Establishing Information Security Standards.

Differences Between Security Guidelines and Privacy Rule

The requirements of the Security Guidelines, 12 CFR Part 570 Appendix B and Supplement A, and the Privacy Rule, 12 CFR Part 573, both relate to confidentiality of customer information. However, they have different focuses:

- The Security Guidelines address safeguarding confidentiality and security of a customer's information and ensuring proper disposal. The focus of the Security Guidelines is preventing or responding to foreseeable threats against, or unauthorized access or use of, that information. Further, the Security Guidelines state that associations must contractually require their service providers that have access to customer information to protect that information.

- The Privacy Rule limits disclosure of nonpublic personal information. The Privacy Rule prohibits disclosure of a consumer's nonpublic personal information unless certain notice requirements are satisfied and the consumer does not elect to opt out of the disclosure. The Privacy Rule does not impose any obligations with respect to safeguarding information. The Privacy Rule only requires associations to provide privacy notices to customers and consumers that describe their policies and practices to protect the confidentiality and security of nonpublic personal information.

Role of Board of Directors

The Security Guidelines require the association's board of directors, or an appropriate committee of the board, to develop, implement, and maintain a written information security program. Initially, the board or a committee must approve the written information security program. Thereafter, the board, or an appropriate committee, must oversee implementation and maintenance of the program. These duties include assigning specific responsibility for implementing the program and reviewing reports prepared by management. Management must provide a report to the board, or an appropriate committee, at least annually that describes the overall status of the information security program and the association's compliance with the Security Guidelines.

> An association's board of directors is responsible for developing, implementing, and maintaining a written information security program.

Information Security Program

Under the Security Guidelines, each association must develop and maintain an effective written information security program tailored to the complexity of its operations. Associations must identify and evaluate risks to its customers' information, including the risk of improper disposal of customer and consumer information. An association must also develop plans to mitigate these risks and implement appropriate controls, including proactive oversight and monitoring of its service providers that have access to the association's customer information.

Additionally, the Security Guidelines require that associations test, monitor, and update the information security program, as needed. Management should report the status of the information security program to the board of directors at least annually. The reports should discuss material issues such as risk assessment, risk management and control decisions, service provider arrangements, results of testing, security breaches or violations and management's responses, and recommendations for changes in the information security program.

Objectives

As detailed in the Security Guidelines, the objectives of a written information security program are:

- Security and confidentiality of customer information.
- Protection against anticipated threats or hazards to the security or integrity of customer information.
- Protection against unauthorized access to or use of such information that could result in substantial harm or inconvenience to customers.
- Proper disposal of customer and consumer information.

Risk Assessment

A written information security program begins with conducting an assessment of the reasonably foreseeable risks. Like the other elements of its information security program, the association's risk assessment should be documented. The Security Guidelines recommend the following steps in conducting a satisfactory risk assessment:

- Identifying reasonably foreseeable internal and external threats that could result in unauthorized disclosure, misuse, alteration, or destruction of customer information or customer information systems.

- Assessing the likelihood and potential damage of the identified threats, taking into consideration the sensitivity of customer information.

- Evaluating the sufficiency of the policies, procedures, customer information systems, and other arrangements an association has in place to control risks identified.

- Applying the preceding three steps in connection with disposal of customer information.

For additional guidance regarding conducting an information security risk assessment, see the FFIEC IT Examination Handbook, Information Security Booklet.

Managing and Controlling Risk

Managing and controlling information security risk is an ongoing process. An association should review its policies and procedures on an ongoing basis to ensure they are adequate to safeguard customer information and customer information systems, and to ensure proper disposal of customer and consumer information. The association should include the review and findings in reports on the written information security program. The association should also update its risk assessment for new products and services and before implementing system changes.

The Security Guidelines provide a list of control measures associations must consider and adopt, as appropriate. For example, an association must consider controls to restrict access to sensitive or nonpublic customer information. These controls should restrict access only to individuals who have a need to know such information. Associations must also consider whether encryption of customer information maintained in electronic form is warranted in light of its information risk assessment. If so, the association should adopt appropriate encryption measures to protect information in transit, storage, or both.

Associations should train staff to implement and maintain the written information security program. Associations should provide specialized training to ensure personnel protect customer information in accordance with requirements of the information security program. For example, they should train staff to recognize and respond to attempted fraud and identify theft, guard against pretext calling, and dispose properly of customer and consumer information.

Associations also should test key controls, systems, and procedures of the information security program. The association's risk assessment should determine the scope, sequence, and frequency of testing. OTS expects testing to be done periodically at a frequency that takes into account the rapid evolution of threats to information security. Independent third parties or staff other than those who develop and maintain the information security program should perform and review the testing.

An association should adjust its written information security program to reflect the results of the ongoing risk assessment and tests of its key controls. An association should adjust the program to take into account changes in technology; the sensitivity of customer information maintained; internal or external threats to information; and its own changing business arrangements, such as mergers, acquisitions, alliances and joint ventures, outsourcing arrangements, and changes in customer information systems.

Security Guidelines and Service Providers

The Security Guidelines have specific requirements that apply to service providers. In addition to exercising due diligence in selecting a service provider, an association must enter into and enforce a contract that requires the service provider to implement appropriate measures designed to meet the objectives of the Security Guidelines. The contract guidance in the Security Guidelines applies to all service providers, affiliated and nonaffiliated.

Consistent with OTS and interagency outsourcing guidance, the Security Guidelines also require an association to monitor its service providers to confirm they satisfy all contractual obligations to the association. Among other things, these obligations include protecting against unauthorized access to or use of customer information maintained by the service provider that could result in substantial harm or inconvenience to any customer, and proper disposal of customer and consumer information.

The Security Guidelines do not impose specific requirements regarding methods used or frequency of monitoring service providers to ensure they are fulfilling their obligations under contracts. An association must monitor each service provider in accordance with its risk assessment for potential risks posed by the service provider. These activities could include reviewing audits or summaries of test results conducted by a qualified party independent of management and personnel responsible for development and maintenance of the service provider's security program. An association should document its reviews of service providers in the written information security program.

Security Guidelines and Disposal Rule

The Security Guidelines direct associations to require in contracts that their service providers implement appropriate measures designed to meet the obligations of the guidelines regarding the proper disposal of consumer information. Although the Security Guidelines do not prescribe a specific method of disposal, OTS expects associations to have appropriate risk-based disposal procedures for records. As indicated in their risk assessments, associations should ensure that paper records containing customer or consumer information are rendered unreadable. Associations should also recognize that computer-based records present unique disposal problems.

Supplement A to 12 CFR Part 570 Appendix B

Incident Response Program

OTS and the other federal financial regulators issued guidance regarding programs to respond to unauthorized access to customer information and when to provide customer notice (Incident Response Guidance). According to this guidance, an association should develop and implement a response program to address unauthorized access to or use of customer information that could result in substantial harm or inconvenience to a customer. The components of an effective response program include:

- Assessment of the nature and scope of the incident and identification of what customer information has been accessed or misused.
- Prompt notification to OTS once an association becomes aware of an incident involving unauthorized access to or use of sensitive customer information.
- Notification to appropriate law enforcement authorities in situations involving federal criminal violations requiring immediate action.
- Filing a timely Suspicious Activity Report, consistent with OTS regulations and instructions.
- Measures to contain and control the incident to prevent further unauthorized access to or misuse of customer information, while preserving records and other evidence.
- Notification to customers, when warranted.

Customer Notification

The Incident Response Guidance describes when and how associations should provide notice to customers affected by unauthorized access or misuse of their information. In particular, once an association becomes aware of an incident of unauthorized access to sensitive customer information, it should conduct a reasonable investigation to determine the likelihood the information has been or will be misused. If it determines that misuse of customer information has occurred, or is reasonably possible, the association should notify the affected customer as soon as possible.

Sensitive customer information means a customer's name, address, or telephone number, in conjunction with the customer's social security number, driver's license number, account number, credit or debit card number, or a PIN or password that would permit access to the customer's account. It also includes any combination of components of customer information that would allow an unauthorized third party to log onto or access the customer's account electronically, such as user name and password or password and account number.

The Incident Response Guidance also states that an association's contract with its service provider should require the service provider to take appropriate actions to address incidents of unauthorized

access to customer information, including notification to the association as soon as possible following any incident. For additional guidance on response programs for security breaches and notifying affected customers, see CEO Memo 214, Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice.

If OTS finds an association's performance is deficient under the Security Guidelines, it may take appropriate corrective action. The agency could require the association to file a compliance plan in accordance with the regulations implementing the Prompt Corrective Action provisions of the Federal Deposit Insurance Act. Or, OTS could initiate an enforcement action under 12 CFR § 568.5 for noncompliance with the Security Guidelines.

Identity Theft Red Flags Regulation and Interagency Guidelines

12 CFR Part 571.90, Duties Regarding Detection, Prevention, and Mitigation of Identity Theft; Interagency Guidelines on Identity Theft Detection, Prevention, and Mitigation

OTS and the other federal financial regulators and the Federal Trade Commission issued a regulation and interagency guidelines on Identity Theft Red Flags (Red Flags) implementing part of Section 114 of the FACT Act. The Red Flags regulation requires associations to develop and implement a comprehensive, written identity theft prevention program (ID Program) designed to detect, prevent, and mitigate identity theft in connection with opening covered accounts and existing covered accounts. For purposes of the Red Flags regulation and guidelines, covered accounts mean:

- An account that an association offers or maintains, primarily for personal, family, or household purposes, that involves or is designed to permit multiple payments or transactions, such as a credit card account, mortgage loan, automobile loan, margin account, checking account, or savings account.

- Any other account that the association offers or maintains for which there is a reasonably foreseeable risk to customers or to the safety and soundness of the association from identity theft, including financial, operational, reputation, or litigation risks.

Identity Theft Prevention Program

The ID Program must be appropriate to the association's size and complexity and the nature and scope of its activities. The ID Program must also include reasonable policies and procedures to:

- Identify relevant patterns, practices, and specific forms of activity that are red flags signaling possible identity theft and incorporate those red flags into the ID Program.

- Detect red flags that have been incorporated into the ID Program.

- Respond appropriately to any red flags that are detected to prevent and mitigate identity theft.
- Ensure the ID Program is updated periodically to reflect changes in risks from identity theft.

The ID Program must initially be approved by the association's board of directors, or an appropriate committee of the board. Staff must also be trained to implement effectively the ID Program and the association must exercise appropriate oversight of its service providers.

> An association's board of directors or board committee must approve the initial written identity theft prevention program.

In addition to the Red Flags regulation, OTS and the other federal financial regulators and the Federal Trade Commission issued guidelines to assist associations in developing their ID Programs. Associations must consider the Red Flags guidelines and include those that are appropriate. The guidelines include Supplement A, which provides 26 examples of red flags associations may consider incorporating into their ID Programs.

Identity Theft Risk Assessment

Associations must periodically determine whether they offer or maintain covered accounts. To make that determination, an association must conduct a risk assessment, considering the methods it uses to open and access accounts, and the association's previous experiences with identity theft. As with other aspects of the association's ID Program, the association should document the risk assessment.

For additional guidance on risk assessment see the FFIEC IT Examination Handbook, Information Security Booklet.

Role of Board of Directors

In addition to initially approving the ID Program, the regulation requires ongoing involvement by an association's board of directors, an appropriate committee of the board, or a designated senior management official. This includes oversight, development, implementation, and administration of the ID Program. As provided in the guidelines, oversight should include assigning specific responsibility for implementation of the ID Program, approving material changes to the ID Program, and annually reviewing reports prepared by staff regarding the association's compliance with the regulation.

Reports should address material matters and evaluate:

- Effectiveness of the association's policies and procedures in addressing identity theft in opening covered accounts or existing covered accounts.
- Service provider arrangements.
- Significant incidents involving identity theft and management's response.

- Recommendations for material changes to the ID Program.

Information Security Programs and Identity Theft Prevention Programs

In designing its ID Program to comply with the Red Flags regulation, associations may incorporate existing policies, procedures, programs, and other arrangements to control risks of identity theft to customers or the safety and soundness of the association. For example, associations may use all or parts of their written information security programs in the ID Program. Among the components of an effective information security program that associations may wish to use in their ID Programs are:

- Warnings or alert notices from service providers to identify red flags.
- Authentication methods to detect red flags.
- Response programs for unauthorized access to customer accounts to prevent and mitigate identity theft.

For additional guidance on the Red Flags regulation and guidelines, see CEO Memo 270, Identity Theft Red Flags Final Rule and Guidelines.

Business Continuity Risks and Controls

Board of Directors and Management Responsibilities

Associations must be capable of restoring critical information systems, operations, and services quickly after an adverse event. Effective business continuity planning can ensure associations are prepared to respond to events such as natural disasters, human error, terrorist activities, or a pandemic. For additional guidance on preparations for a pandemic, see CEO Memo 237, Interagency Advisory on Influenza Pandemic Preparedness, and CEO Memo 269, FFIEC IT Examination Handbook, Business Continuity Planning Booklet, Appendix D, Pandemic Planning.

> The board of directors is responsible for developing and annually reviewing test results and approving the association's Business Continuity Plan.

An association's board of directors and management are responsible for all of the following:

- Establishing policies and procedures, and assigning responsibilities to ensure that comprehensive business continuity planning, including testing, takes place.
- Annually reviewing the adequacy of the association's business continuity plan and test results.
- Documenting such reviews and approval in the board minutes.
- Evaluating adequacy of contingency planning and testing by service providers.

- Ensuring that the association's business continuity plan is compatible with that of its service providers.

Business continuity plans can minimize disruptions caused by problems that impair or even destroy the association's processing and delivery systems. Extended disruptions to the association's business operations pose substantial risks of financial losses, and could lead to the failure of an association. Effective business continuity planning requires a comprehensive, association-wide approach, not a narrow focus on recovery of the association's systems and technology.

Business Continuity Planning Process

Business continuity planning is the process of reviewing all of an association's departments and business lines and assessing the importance of each to the association and its customers. Association management then develops and maintains a written business continuity plan that addresses all significant products and services, and the outsourced and internally operated information systems and technology that support these.

The complexity of an association's IT environment should dictate the level of detail contained in the business continuity plan. As the association adds new information systems and technology to its environment, it should revise the business continuity plan. The beginning point should be a business impact analysis. This assesses the risks posed to each system, and then identifies the principal departments, resources, activities, and users potentially affected by a problem. This includes assessing the response capability of the association, the alternate processing site, transportation and storage of backup media, and third-party vendors who can provide alternate processing locations.

If the association has contracted with a third-party vendor, management must obtain, review and determine adequacy of the service provider's business continuity plan and testing. The vendor's plan should be compatible with, and integrated into, the association's business continuity plan. However, merely maintaining the vendor's business continuity plan, and participating in its periodic connectivity testing, is not adequate to satisfy this requirement. An association must have its own business recovery and continuity plan specifically designed for its operating profile and IT environment.

Business Continuity Plan Development

A business continuity plan should define the roles and responsibilities for recovery team members. The detail will vary among associations, depending on the degree of risk inherent in operations, the level and complexity of information technology used, and the association's available resources. However, the business continuity plan should be in sufficient detail so an association can respond effectively to a problem situation.

Typically, an association's business continuity plan should:

- Designate the individual(s) responsible for coordinating all activities in responding to a disaster when the business continuity plan is invoked.

- Define roles and responsibilities for each team member.
- State clearly how potential disasters could affect the association's departments, products, services, employees, and customers.
- Provide details on potential risks and describe strategies, resources, and procedures for recovery.
- Establish the periodic frequency for testing and ongoing training of employees.
- Specify a clear timeline for recovering significant operations.

A clear timeline for recovery is critical to the business continuity plan. Recovery does not mean when an affected system becomes available again. In achieving full recovery, the association may have to correct or resubmit transactions that were in process when the disaster or disruption occurred. This could involve a full day's transactions or more.

Additionally, an association's business continuity plan should address the differing requirements posed by outsourced and internally operated systems. For outsourced systems, the association's business continuity plan should address the following for each significant service provider:

- Categories and sources of data input, for example, branch transactions entered by personal computers or terminals.
- Work steps or processes to recover for resubmission data previously input.

For each internally operated system, the association's business continuity plan should address:

- Recovery of lost data, for example, day-of-disaster online input.
- Replacement of damaged hardware and software resources.
- Alternate processing locations.

Business Continuity Plan Monitoring and Testing

An association should test its business continuity plan at least annually. Acceptable testing methodologies include tabletop drills, walk-through exercises, and simulations. An association should modify its business continuity plan to reflect testing results and any changes to the association's information systems and technology environment.

The association's business continuity plan should also designate an incident response team. Generally this team would consist of a small number of staff from the departments and functions designated as

critical to recovery of operations. Collectively, the team provides the resources necessary to respond quickly and decisively to problems.

For additional guidance on business continuity planning, see CEO Memo 239, Hurricane Katrina: Industry Lessons Learned, and CEO Memo 269, FFIEC IT Examination Handbook, Business Continuity Planning Booklet.

VENDOR MANAGEMENT RISKS AND CONTROLS

An association's board of directors and management should develop and approve policies for overseeing its service providers.

Associations use outsourcing to reduce costs and achieve strategic goals more efficiently. More and more, associations use third parties to conduct business operations associations previously conducted directly. Given current technology environments, these outsourcing arrangements are becoming increasingly complex, and may involve foreign-based entities. **Note:** Outsourcing is use of a third party, either affiliated or nonaffiliated, to perform activities on a continuing basis, that the association would normally handle.

Outsourcing can be the initial transfer of an activity or function from the association to a third party, or from the original third party to another third-party service provider, which is sometimes referred to as subcontracting. Another major trend in outsourcing is offshore outsourcing or moving processing activities outside the United States.

Offshore outsourcing introduces country risk for associations. In offshore outsourcing, associations must also monitor foreign government policies, and political, social, economic, and legal conditions in the country where it has a contractual relation with the service provider. Because of this, an association should develop appropriate contingency plans and an exit strategy for foreign outsourcing relationships. The association should have a strategy to transfer the processing activities back to the United States should it become necessary.

Examples of commonly outsourced operations include accounting, human resources administration, and customer call centers. Associations may also determine that use of a specific technology is too sophisticated or dynamic to be supported effectively within the association. These associations may determine that some or all of such technology should be outsourced to a third-party vendor.

As stated in Thrift Bulletin 82a, Third Party Arrangements, the Home Owners' Loan Act (HOLA) requires associations to notify OTS of arrangements with all third-party providers. HOLA requires such notice regardless of whether or not there is a contract. Generally, associations must provide notice to a Regional Director, for both domestic and foreign third-party arrangements, within 30 days after the earlier of:

- The date the association enters into the contract with the third party.

- The date the third party initiates performing the services.

Service Provider Due Diligence

The association must also conduct adequate due diligence in selecting its service providers. Prior to the formal selection, it should develop specific criteria to assess a third-party service provider's capacity and ability to perform the outsourced activities effectively. Appropriate due diligence includes selecting those service providers that are qualified and have adequate resources to perform the work. It also involves ensuring the service provider understands and can meet the association's requirements. It is also important that an association verifies the service provider's financial soundness to fulfill its obligations.

Prior to outsourcing any aspect of its operations, the association should establish specific policies and procedures. Management should demonstrate a comprehensive understanding of outsourcing's expected benefits and costs. Management also should develop and implement a formal program to monitor the service provider relationship. A comprehensive vendor management oversight program should provide for ongoing monitoring and controlling of all relevant aspects of the service provider relationship.

If a service provider fails, or is otherwise unable to perform the outsourced activities, it may be costly and problematic to find alternative solutions. The association should consider transition costs and potential business disruptions. An association should not outsource activities to a service provider that does not meet all of an association's due diligence criteria.

Service Provider Contracts

A clearly written contract should govern all outsourcing arrangements. Associations can mitigate outsourcing risks by carefully negotiating and reviewing service provider contracts, including contract renewals, prior to signing. Legal counsel should always review the vendor contracts to determine that the association's interests are adequately protected. Associations should actively monitor vendor performance, and verify performance level reports periodically.

Key contract provisions should:

- Define clearly outsourced activities and expected service and performance levels.
- Provide for continuous monitoring and assessment of the service provider so the association can take timely corrective action.
- Include a termination clause and time period or conditions under which it would be exercised.
- Address issues related to subcontracting for all or part of the outsourced activity.

- Cover requirements detailed in the Security Guidelines that are contained in the association's written information security program.

- Address recommendations in the Identity Theft Red Flags guidelines that service providers have policies and procedures to detect and either report or mitigate identity theft.

Service Provider Management and Monitoring

Typically, the association forwards data to the service provider's processing center, usually via on-line data entry terminals; output reports are available at the association's on-line terminals and printers. For those portions of the service provider's systems that are within the association, the association has responsibility for establishing and maintaining appropriate controls. For example, an association should develop controls that restrict access to teller terminals to tellers and other specifically authorized personnel. An association should also develop controls for balancing and reconciling items processed by the third-party vendor. The contract should address these responsibilities.

An association that is part of a holding company structure may have an affiliated company provide its technology needs. The affiliated service provider could be a department within the parent holding company, or a separate affiliate of the association. This type of arrangement typically reduces costs and achieves enterprise-wide economies of scale. However, contracts among affiliated entities may raise supervisory concerns. See the Holding Company Handbook for additional guidance on transactions with affiliates.

Vendor contracts should specify performance measures; two key metrics are online up time and terminal response time. Up time refers to the hours and days online services will be available. Often, these are the hours the association's branches operate, plus two or three additional hours daily. Contracts should state the vendor's performance commitment, for example, 99 percent up time. Terminal response time refers to the customary elapsed time between transaction initiation, when the enter key is pressed, and delivery of information to the screen. Response time should be measured in seconds.

Service provider contracts should also address non-production or non-processing products and services. Examples of these are audited financial statements for the vendor, third-party audits of the service provider, or summaries of the vendor's disaster recovery testing results. An association should obtain and review these as part of a proactive vendor management program.

An association should obtain IT ROEs for its significant service providers. An association should also obtain third-party reviews of its significant service providers. A third-party review is an independent evaluation the service provider obtains to meet the needs of client associations. A qualified auditor who is independent of the service provider conducts the third-party review. The scope of this audit should be broad enough to satisfy the audit objectives of the service provider and the client associations.

The American Institute of Certified Public Accountants' Statement of Auditing Standards 70 (SAS 70) provides guidance for auditors performing the service provider review and to auditors of client financial associations. The SAS 70 reviews should determine the adequacy of controls in areas such as the service

provider's data center, systems and programming, and input/output controls. The controls reviewed at the service providers should have reciprocal controls at the individual client associations. In the SAS 70 review, the auditor will address these corresponding controls, in a section typically referred to as "client control considerations." An association should obtain and review these reports, and take appropriate actions for any client control considerations or weaknesses discussed. It is also important that an association understand the scope of the SAS 70 review to determine if it adequately assesses all relevant control areas.

For additional guidance on vendor management oversight activities, see Thrift Bulletin 82a, Third Party Arrangements, and CEO Memo 201, FFIEC IT Examination Handbook Outsourcing Technology Services Booklet.

Other Association Controls for Information Technology Risks

Input and Output Controls

An association should require additional controls for technology used to process information, which has direct monetary effects on either the association or its customers. These controls should include requirements that there be segregation of duties between input of information and review of that information post-processing. Such controls should also require the post-processing reviewer to reconcile the processed information.

For large dollar transactions, for example, funds transfers, associations should require that all phases of the transaction be performed under dual controls. For mortgage loan set-ups, verification procedures should consist of manually comparing a sample of source documents against system reports. The association's written policies and procedures should describe these controls in full detail.

Change Control Management

An association must prepare to adapt activities and information technology to meet changing requirements and circumstances. Association management should ensure that changes to existing technology undergo the same due diligence as new technology selections. An important consideration in technology changes is that there be thorough testing. Additionally, an association should maintain accurate and complete records describing the changes, reasons for the changes, and those responsible for making them.

Conversion Project Management

Any association that uses IT to perform operations or provide services must commit to update continuously its activities to keep current with technological changes. For example, if an association experiences a corporate merger or acquisition, wants to reduce or more effectively control costs, or offer new products or services, it must plan to convert its operations and systems to accommodate these changes.

In highly technological environments, it is likely that an association will experience at least one or more systems conversion. A systems conversion is the process of replacing existing applications with new ones developed internally, or with third-party vendor software through an outsourcing agreement. The association should conduct planning, testing, and monitoring of new activities as part of its risk mitigation processes.

A conversion presents significant risks to an association, which can be mitigated with adequate project management controls. Flawed or failed conversions are very costly, and can compromise the integrity and reliability of books and records, causing unsafe and unsound conditions within the association. For example, in a flawed check processing conversion, an association could be forced to charge-off significant, unresolved bookkeeping differences. In a flawed deposit conversion, management could have unreconciled deposits requiring adjustments and write-offs. These can cause significant financial losses and waste management resources.

The board of directors should monitor planning and implementation of major system conversions. The directors should also hold management accountable for the success or failure of these conversions. Management should develop and oversee the successful completion of tasks and milestones by both the vendor and association personnel. User testing, debugging, and staff and customer training should occur before implementation or conversion of any system.

Regulatory Guidance and References

Code of Federal Regulations (12 CFR)

§ 555	Electronic Operations
§ 563.161	Management and Financial Policies
§ 563.170	Examinations and Audits; Appraisals; Establishment and Maintenance of Records
§ 568	Security Procedures
Part 570 Appendix A	Safety and Soundness Guidelines and Compliance Procedures Interagency Guidelines Establishing Standards for Safety and Soundness
Part 570 Appendix B	Interagency Guidelines Establishing Information Security Standards
Part 570 Appendix B Supplement A	Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice

§571.90	Duties Regarding Detection, Prevention, and Mitigation of Identity Theft
§571.90 Appendix J	Interagency Guidelines on Identity Theft Detection, Prevention, and Mitigation
§571.90 Appendix J Supplement A	Illustrative Examples of Red Flags

Office of Thrift Supervision Guidance

CEO Memoranda

No. 109	Transactional Web Sites
No. 139	Identity Theft and Pretext Calling
No. 176	Information Technology Examination Handbook – Supervision of Technology Service Providers Booklet
No. 179	Request for Comment on Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice
No. 182	FFIEC Information Technology Examination Handbook – Audit Booklet and Electronic Banking Booklet
No. 193	'Phishing' and E-mail scams
No. 196	Information Technology Examination Handbook – Retail Payment Systems Booklet
No. 199	Information Technology Examination Handbook – Development and Acquisition Booklet
No. 201	Information Technology Examination Handbook – Management Booklet and Outsourcing Technology Services Booklet
No. 204	Information Technology Examination Handbook – Operations Booklet and Wholesale Payment Systems Booklet
No. 205	'Phishing' Customer Brochure
No. 207	Interagency Guidance – Risk Management of Free and Open Source Software

No. 214	Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice
No. 228	Interagency Guidance on Authentication in an Internet Banking Environment
No. 231	Compliance Guide for Interagency Guidelines Establishing Information Security Standards
No. 237	Interagency Advisory on Influenza Pandemic Preparedness
No. 239	Hurricane Katrina: Industry Lessons Learned
No. 241	Information Technology Examination Handbook – Information Security Booklet
No. 242	Frequently Asked Questions on Authentication in an Internet Banking Environment
No. 245	Director's Responsibility Guide and Guide to Management Reports
No. 269	Information Technology Examination Handbook – Business Continuity Planning Booklet
No. 270	Identity Theft Red Flags Final Rule and Guidelines

Thrift Bulletins

TB 81	Interagency Policy Statement on the Internal Audit Function and Its Outsourcing
TB 82a	Third Party Arrangements
TB 83	Interagency Guidance on Weblinking: Identifying Risks and Risk Techniques

Handbook Sections

Section 340	Internal Controls
Section 1300	Fair Credit Reporting Act
Section 1370	Electronic Banking
Section 1375	Privacy

Information Technology Risks and Controls Program

Examination Objectives

To determine whether management effectively identifies and mitigates the association's information technology (IT) risks.

To determine whether the board of directors adopted adequate policies, procedures, and operating strategies appropriate for the size and complexity of the association's IT environment.

To determine whether the association has a written information security program to comply with the requirements of the Interagency Guidelines Establishing Information Security Standards (Security Guidelines), which implement Sections 501(b) of the Gramm-Leach-Bliley Act of 1999 (GLB Act) and 216 of the Fair and Accurate Credit Transactions Act of 2003 (FACT Act).

To determine whether the association has a written identity theft prevention program to comply with the requirements of the Identity Theft Red Flags regulation, which implements Section 114 of the FACT Act.

To initiate corrective action when policies, procedures, or controls are deficient or when you note violations of laws or regulations.

Examination Procedures

WKP. REF.

Level I

Level I procedures assess the association's processes for identifying and managing IT risks. Level I procedures are sufficient when an association has an effective internal control environment for IT risks, and there are no findings, which would cause you to expand your scope.

1. Review the association's response to the PERK 05, previous examination reports, including IT Reports of Examination, internal and external audit reports, and supervisory correspondence. After verifying completeness and accuracy of the IT database information, provide this information to your regional office for processing and input.

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

WKP. REF.

2. Determine that the association implemented effective corrective actions for all previously cited IT exceptions, criticisms, or violations. This includes any matters cited in IT Reports of Examination.

3. Determine the complexity of the association's information technology environment. Identify the association's significant systems. Significant means those critical to ensure information security, satisfactory customer service, and continuity of operations. Review the association's networks. Determine what significant applications are processed on the networks.

4. In conjunction with the Examiner-in-Charge (EIC) or examiner(s) performing the other Management programs, review board of directors' minutes of regular, special, and committee meetings for discussion and approval of significant IT matters. Examples of significant IT matters would include the association's written information security program, its written identity theft prevention program, new or ongoing service provider relationships, and the association's business continuity plan.

5. In conjunction with the examiner(s) performing the reviews of Management and Earnings, determine the effectiveness of the board of directors and senior management in implementing strategic planning for IT. Evaluate plans for any significant changes. Review the association's strategic or business plan for IT-related activities.

6. Review the association's policies and procedures for IT. Determine whether these are effective for monitoring and controlling the association's IT risks considering the complexity of its IT environment.

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

WKP. REF.

7. In conjunction with the examiner(s) performing the review of the audit function, assess the adequacy of the association's audit coverage for IT risks. Verify that audit policies, practices, and programs for IT audits or other independent reviews are adequate for the size and complexity of the association's IT environment.

8. Review IT audits or other independent reviews completed since the preceding examination. Determine that IT audit work products are adequate for the size and complexity of the association's IT environment.

9. Assess management's responsiveness to IT audit concerns. Review the timeliness and adequacy of corrective actions. Confirm that the board of directors is informed of significant audit concerns, and that the board ensures completion of corrective actions.

10. Determine that IT audit expertise and training are sufficient for the complexity of the IT risks of the association.

11. Determine the association's compliance with the objectives of the interagency Security Guidelines implementing Sections 501(b) of the GLB Act and 216 of the FACT Act. The Security Guidelines require associations to have a comprehensive, written information security program that includes the administrative, technical, and physical safeguards to achieve the following objectives:

    - Ensure the security and confidentiality of customer information.
    - Protect against any anticipated threats or hazards to the security or integrity of customer information.
    - Protect against unauthorized access to or use of such information that could result in substantial harm or inconvenience to any customer.
    - Ensure proper disposal of customer and consumer information.

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

WKP. REF.

To meet the objectives and comply with the Security Guidelines, an association must:

- Implement a written information security program that the board of directors approved.
- Conduct and prepare a written information security risk assessment.
- Require in contracts that service providers implement appropriate information security programs designed to meet the objectives of the Security Guidelines.
- Monitor, evaluate, and adjust the information security program for changes in the association's IT environment.
- Report to the board of directors annually regarding the association's compliance with the Security Guidelines and the status of the written information security program.

12. Review measures the association has implemented in its written information security program to manage and control risks. Determine that the association considered and adopted, as appropriate:

- Access controls on customer information systems, including controls to authenticate and permit access only to authorized individuals.
- Controls and procedures to prevent employees from providing customer information to unauthorized individuals through pretext calling or other fraudulent methods.
- Access restrictions at physical locations containing customer information, such as buildings, computer facilities, and records storage facilities to permit access only to authorized individuals.
- Encryption of electronic customer information, including while in transit or in storage, or on networks or systems, to ensure unauthorized individuals do not gain access.

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

WKP. REF.

- Procedures designed to ensure that modifications to customer information systems are consistent with the association's written information security program.
- Dual control procedures, segregation of duties, and employee background checks for employees with access to customer information to minimize risk of misuse of customer information.
- Monitoring systems and procedures to detect actual and attempted attacks or other intrusions into customer information systems.
- Response programs that specify actions to take when the association suspects or detects that unauthorized individuals have gained access to customer information systems, including appropriate reports to regulatory and law enforcement agencies.
- Measures to protect against destruction, loss, or damage of customer information due to potential environmental hazards, such as fire and water damage or technological failures.

13. Confirm that the association has ongoing training for employees that implement and maintain the information security program. Review guidance to association employees for protecting customer and corporate information. Such guidance should describe the employee's responsibilities and consequences of improper actions.

14. Determine that the association has an incident response program consistent with the guidance in CEO Memo 214. Evaluate the effectiveness of the association's program for responding to incidents of unauthorized access to sensitive customer information and providing notification, as required. Confirm that the association's response program contains measures to:

- Assess the nature and scope of the incident.
- Notify OTS, either directly or through the association's service providers.
- Notify law enforcement agencies.
- File Suspicious Activity Reports when required.

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

WKP. REF.

- Control the incidents of unauthorized access.
- Notify customers, when necessary.

15. If the association had incidents of unauthorized access to sensitive customer information, determine that it:

- Conducted a prompt investigation to determine the likelihood the information accessed has been or will be misused.
- Notified customers when the investigation determined misuse of sensitive customer information has occurred or is reasonably probable.
- Delivered notification to customers, when warranted, by means the customer can reasonably be expected to receive, for example, by telephone, mail, or electronic mail.

16. Review the association's customer notice and determine it contains:

- A description of the incident, including type of information subject to unauthorized access.
- Measures taken by the association to protect customers from further unauthorized access.
- Telephone numbers customers can call for information and assistance.
- Reminders to customers to review account statements over a reasonable period – 12-to-24 months – and to report immediately suspicious activity and suspected identity theft incidents.
- A description of a fraud alert and how to place one in a customer's report.
- Recommendations to obtain credit reports from each nationwide credit-reporting agency and have information related to fraudulent transactions deleted.
- An explanation of how customers can obtain free credit reports.

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

WKP. REF.

- Information concerning availability of online guidance by the Federal Trade Commission regarding steps the consumer can take to protect against identity theft.

17. Evaluate the effectiveness of the association's measures to authenticate customers accessing Internet-based services and other electronic banking activities. Ensure that the association's authentication methods and controls specifically address the need for risk-based assessments, customer awareness, and security measures consistent with the guidance in CEO Memo 228. An association should:

- Ensure its information security program identifies and assesses risks associated with Internet-based products and services, identifies risk mitigation actions, and evaluates customer awareness efforts.
- Adjust its information security program for changes in IT, sensitivity of customer information, and internal or external threats to information.
- Implement appropriate risk mitigation strategies.

18. Verify that the association periodically[1] identifies covered accounts it offers or maintains.[2] Verify that the association:

- Included accounts for personal, family, and household purposes that permit multiple payments or transactions; and
- 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 association's previous experiences with identity theft.

[1] 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.

[2] A "covered account" includes: (i) an account primarily 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 association offers or maintains for which there is a reasonably foreseeable risk to customers or the safety and soundness of the association from identity theft.

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

WKP. REF.

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

20. Review any reports, such as audit reports and annual reports prepared by staff for the Board of Directors,[3] or an appropriate committee thereof or a designated senior management employee, on compliance with the Red Flags Rule, including reports that address the following:

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

21. Verify that the association 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 association and the nature and scope of its activities. Conduct the following procedures:

- Verify that the association 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.

[3] 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.

- 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. Associations may, but are not required to use the illustrative examples of Red Flags to identify relevant Red Flags Questions as shown in Supplement A to the Guidelines.
- Determine whether the association uses technology to detect Red Flags. If it does, discuss with management the methods by which the association confirms the technology is working effectively to detect, prevent, and mitigate identity theft.
- 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 association from identity theft.
- Verify that (i) the Board of Directors, or an 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.

22. Verify that the association trains appropriate staff to effectively implement and administer the Program.

23. Determine whether the association exercises appropriate and effective oversight of service providers that perform activities related to covered accounts.

24. Review password controls used on the association's operating systems and significant applications. Confirm these address password length, change intervals, composition, history, and reuse or lockout. Assess effectiveness of these controls.

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

WKP. REF.

25. Assess the association's user access assignment policies and procedures for its information systems. Determine that these policies and procedures:

    - Provide for proper segregation of duties and dual controls.
    - Assign processing capabilities according to job responsibilities.
    - Limit system administrator capabilities appropriately.
    - Create user access profiles or user access assignments that are differentiated according to job duties.
    - Ensure that the association periodically reviews and updates user access assignments for job changes and terminations.

26. Review user access profiles or user access assignments for at least one of the association's significant systems, for example, lending, deposits, general ledger, or funds transfers. Determine that system access rights are consistent with the association's policies and procedures for assigning system access.

27. Confirm that the association has current written procedures to ensure security over its funds transfer activities, and that personnel are adequately trained to follow these procedures.

28. Confirm that each authorized user involved in the association's funds transfer activities maintains a unique password known only to the user. Verify that system users change passwords frequently.

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

WKP. REF.

29. Review the association's business continuity plan. Verify that the business continuity plan is based on a business impact analysis and that it identifies recovery priorities. Confirm that the association tested the business continuity plan within the past twelve months and that the board of directors annually approves testing results and the business continuity plan.

30. Review the association's back-up procedures. Determine what data are backed up, the rotation schedule, where the back-up media are stored, and how soon the back-up media are taken offsite.

31. Ensure that the association excercises appropriate due diligence in selecting, managing, and monitoring its service providers. Determine the association has established adequate policies and procedures to manage its service provider or vendor relationships.

32. Determine that the association's contracts with its service providers have clauses that require the vendors to implement measures designed to meet the objectives of the Security Guidelines. Review the association's policies, procedures, and practices used to confirm that its service providers satisfied obligations under the contract regarding customer information.

33. Determine that the association's board of directors, or an appropriate committee, approves new service provider relationships, or significant changes to existing oursourcing arrangements. These changes should be supported by a written risk analysis consistent with the association's business plan and the proposed or planned activity.

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

WKP. REF.

34. Determine that association management and the board of directors periodically review significant service provider contracts and service level agreements.

35. If the association created a transactional website since the previous exam determine that it provided the notice to OTS as required by CEO Memo 109. If the Notice was not timely and satisfactorily filed, contact the regional office to discuss appropriate remediation actions. Discuss with the regional office the need for follow-up review to ensure compliance with the requirements set forth in the CEO memo.

36. Review the association's website to determine there are no inappropriate or misleading website links.

37. Discuss with your EIC any planned or pending system conversion, transactional website plans not previously communicated to or filed with OTS, system-generated errors that affect integrity of management information or regulatory reports, or any other significant IT issues or concerns. After discussion with your EIC, notify your regional IT Examination Manager, as appropriate.

LEVEL II

After you complete the Level I examination procedures, if you need additional review to support an examination conclusion for a particular IT risk, you should review examination guidance and procedures in the FFIEC Information Technology Examination Handbook for the specific subject matter. These FFIEC Information Technology Examination Handbook procedures are considered Level II procedures for Examination Handbook Section 341.

You should complete the examination procedures in the FFIEC Information Technology Examination Handbook you deem necessary to test, support, and present conclusions derived from performing Level I procedures. Level II procedures provide additional verification regarding the level of technology

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

WKP. REF.

risk and the effectiveness of a savings association's risk management processes and controls. You can use the FFIEC examination procedures in their entirety or selectively, depending on the examination scope and need for additional verification.

EXAMINER'S SUMMARY, RECOMMENDATIONS, AND COMMENTS

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

Fair Credit Reporting Act

Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003

Telephone Consumer Protection Act and Junk Fax Act

This Handbook Section contains background information, regulatory guidance, and examination programs for the following three laws:

- The Fair Credit Reporting Act
- Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003
- Telephone Consumer Protection Act and Junk Fax Act

FAIR CREDIT REPORTING ACT

Background and Summary

LINKS

Program

Appendix A

The Fair Credit Reporting Act (FCRA)[1] became effective on April 25, 1971. The FCRA is a part of a group of acts contained in the Federal Consumer Credit Protection Act[2] such as the Truth in Lending Act and the Fair Debt Collection Practices Act.

Congress substantively amended FCRA upon the passage of the Fair and Accurate Credit Transactions Act of 2003 (FACT Act)[3]. The FACT Act created many new responsibilities for consumer reporting

[1] 15 USC §§ 1681-1681u.

[2] 15 USC § 1601 *et seq.*

[3] Pub. L. No. 108-159, 117 Stat. 1952.

agencies and users of consumer reports. It contained many new consumer disclosure requirements as well as provisions to address identity theft. In addition, it provided free annual consumer report rights for consumers and improved access to consumer report information to help increase the accuracy of data in the consumer reporting system.

The FCRA contains significant responsibilities for business entities that are consumer reporting agencies and lesser responsibilities for those that are not. Generally, financial institutions are not consumer reporting agencies; however, depending on the degree to which their information sharing business practices approximate those of a consumer reporting agency, they can be deemed as such.

In addition to the requirements related to financial institutions acting as consumer reporting agencies, FCRA requirements also apply to financial institutions that operate in any of the following capacities:

- Procurers and users of information (for example, as credit grantors, purchasers of dealer paper, or when opening deposit accounts).
- Furnishers and transmitters of information (by reporting information to consumer reporting agencies, other third parties, or to affiliates).
- Marketers of credit or insurance products.
- Employers.

Structure and Overview of Examination Modules

We structured the examination procedures as a series of modules, grouping similar requirements together. The modules contain general information about each of the requirements:

- Module 1 Obtaining Consumer Reports.
- Module 2 Obtaining Information and Sharing Among Affiliates.
- Module 3 Disclosures to Consumers and Miscellaneous Requirements.
- Module 4 Financial Institutions as Furnishers of Information.
- Module 5 Consumer Alerts and Identity Theft Protections

Financial institutions are subject to a number of different requirements under the FCRA. The statute contains some of the requirements, while others are in regulations issued jointly by the FFIEC agencies or in regulations issued by the Federal Reserve Board and/or the Federal Trade Commission. Appendix A contains a matrix of the different statutory and regulatory cites applicable to financial institutions that are not consumer reporting agencies.

Important Definitions

The FCRA uses a number of definitions. Key definitions include the following:

Consumer

A consumer is defined as an individual.

Consumer Report

A consumer report is any written, oral, or other communication of any information by a consumer reporting agency that bears on a consumer's creditworthiness, credit standing, credit capacity, character, general reputation, personal characteristics, or mode of living that is used or expected to be used or collected, in whole or in part, for the purpose of serving as a factor in establishing the consumer's eligibility for any of the following:

- Credit or insurance to be used primarily for personal, family, or household purposes.
- Employment purposes.
- Any other purpose authorized under § 604 (15 USC 1681b).

The term consumer report does not include any of the following:

- Any report containing information solely about transactions or experiences between the consumer and the institution making the report.
- Any communication of that transaction or experience information among entities related by common ownership or affiliated by corporate control (for example, different institutions that are members of the same holding company, or subsidiary companies of an insured institution).
- Communication of other information among persons related by common ownership or affiliated by corporate control if:
  - — It is clearly and conspicuously disclosed to the consumer that the information may be communicated among such persons; and
  - — The consumer is given the opportunity, before the time that the information is communicated, to direct that the information not be communicated among such persons.
- Any authorization or approval of a specific extension of credit directly or indirectly by the issuer of a credit card or similar device.

- Any report in which a person who has been requested by a third party to make a specific extension of credit directly or indirectly to a consumer, such as a lender who has received a request from a broker, conveys his or her decision with respect to such request, if the third party advises the consumer of the name and address of the person to whom the request was made, and such person makes the disclosures to the consumer required under section 615 (15 USC § 1681m), Requirements On Users Of Consumer Reports.

- A communication described in subsection (o) or (x) of section 603 (15 USC § 1681a(o)) (which relates to certain investigative reports and certain reports to prospective employers).

Person

A person means any individual, partnership, corporation, trust, estate, cooperative, association, government or governmental subdivision or agency, or other entity.

Investigative Consumer Report

An investigative consumer report means a consumer report or portion thereof in which information on a consumer's character, general reputation, personal characteristics, or mode of living is obtained through personal interviews with neighbors, friends, or associates of the consumer reported on or with others with whom he is acquainted or who may have knowledge concerning any such items of information. However, such information does not include specific factual information on a consumer's credit record obtained directly from a creditor of the consumer or from a consumer reporting agency when such information was obtained directly from a creditor of the consumer or from the consumer.

Adverse Action

The term adverse action has the same meaning as used in § 701(d)(6) (15 USC1691(d)(6)) of the Equal Credit Opportunity Act (ECOA). Under the ECOA, it means a denial or revocation of credit, a change in the terms of an existing credit arrangement, or a refusal to grant credit in substantially the same amount or on terms substantially similar to those requested. Under the ECOA, the term does not include a refusal to extend additional credit under an existing credit arrangement where the applicant is delinquent or otherwise in default, or where such additional credit would exceed a previously established credit limit.

The term has the following additional meanings for purposes of the FCRA:

- A denial or cancellation of, an increase in any charge for, or a reduction or other adverse or unfavorable change in the terms of coverage or amount of, any insurance, existing or applied for, in connection with the underwriting of insurance.

- A denial of employment or any other decision for employment purposes that adversely affects any current or prospective employee.

- A denial or cancellation of, an increase in any charge for, or any other adverse or unfavorable change in the terms of, any license or benefit described in section 604(a)(3)(D) (15 USC § 1681b(a)(3)(D)).

- An action taken or determination that is:

  — Made in connection with an application made by, or transaction initiated by, any consumer, or in connection with a review of an account to determine whether the consumer continues to meet the terms of the account.

  — Adverse to the interests of the consumer.

Employment Purposes

The term employment purposes when used in connection with a consumer report means a report used for the purpose of evaluating a consumer for employment, promotion, reassignment or retention as an employee.

Consumer Reporting Agency

The term consumer reporting agency means any person that, for monetary fees, dues, or on a cooperative nonprofit basis, regularly engages in whole or in part in the practice of assembling or evaluating consumer credit information or other information on consumers for the purpose of furnishing consumer reports to third parties, and that uses any means or facility of interstate commerce for the purpose of preparing or furnishing consumer reports.

MODULE 1: OBTAINING CONSUMER REPORTS

Overview

Consumer reporting agencies have a significant amount of personal information about consumers. This information is invaluable in assessing a consumer's creditworthiness for a variety of products and services, including loan and deposit accounts, insurance, and utility services, among others. The FCRA governs access to this information to ensure that a prospective user of the information obtains it for permissible purposes and does not exploit it for illegitimate purposes.

The FCRA requires any prospective user of a consumer report, for example, a lender, insurer, landlord, or employer, among others, to have a legally permissible purpose to obtain a report.

Permissible Purposes of Consumer Reports (Section 604) and Investigative Consumer Reports (Section 606)

Legally Permissible Purposes. The FCRA allows a consumer reporting agency to furnish a consumer report for the following circumstances and no other:

- In response to a court order or Federal Grand Jury subpoena.
- In accordance with the written instructions of the consumer.
- To a person, including a financial institution, that the agency has reason to believe intends to use the report as information for any of the following reasons:
  - — In connection with a credit transaction involving the consumer (includes extending, reviewing, and collecting credit).
  - — For employment purposes.[4]
  - — In connection with the underwriting of insurance involving the consumer.
  - — In connection with a determination of the consumer's eligibility for a license or other benefit granted by a governmental instrumentality that is required by law to consider an applicant's financial responsibility.
  - — As a potential investor or servicer, or current insurer, in connection with a valuation of, or an assessment of the credit or prepayment risks associated with, an existing credit obligation.
  - — Otherwise has a legitimate business need for the information:
    - ✓ In connection with a business transaction that the consumer initiates; or
    - ✓ To review an account to determine whether the consumer continues to meet the terms of the account.
- In response to a request by the head of a State or local child support enforcement agency (or authorized appointee) if the person certifies various information to the consumer reporting agency regarding the need to obtain the report. (Generally, this particular purpose does not impact a financial institution that is not a consumer reporting agency.)

[4] Use of consumer reports for employment purposes requires specific advanced authorization, disclosure, and adverse action notices. Module 3 of the examination procedures contains these issues.

Prescreened Consumer Reports. Users of consumer reports, such as financial institutions, may obtain prescreened consumer reports to make firm offers of credit or insurance to consumers, unless the consumers elected to opt out of being included on prescreened lists. The FCRA contains many requirements, including an opt out notice requirement when prescreened consumer reports are used. In addition to defining prescreened consumer reports, Module 3 covers these requirements.

Investigative Consumer Reports (Section 606). This section on Investigative Consumer Reports contains specific requirements for use of an investigative consumer report. This type of consumer report contains information about a consumer's character, general reputation, personal characteristics, or mode of living obtained in whole or in part through personal interviews with neighbors, friends, or associates of the consumer. If a financial institution procures an investigative consumer report, or causes the preparation of one, the institution must meet the following requirements:

- The institution clearly and accurately discloses to the consumer that it may obtain an investigative consumer report.
- The disclosure contains a statement of the consumer's right to request other information about the report and a summary of the consumer's rights under the FCRA.
- The disclosure is in writing and is mailed or otherwise delivered to the consumer not later than three business days after the date on which the report was first requested.
- The financial institution procuring the report certifies to the consumer reporting agency that it has complied with the disclosure requirements and will comply in the event that the consumer requests additional disclosures about the report.

Institution Procedures. Given the preponderance of electronically available information and the growth of identity theft, financial institutions should manage the risks associated with obtaining and using consumer reports. Financial institutions should employ procedures, controls, or other safeguards to ensure that they obtain and use consumer reports only in situations for which there are permissible purposes. Management should deal with information access, storage, and destruction under an institution's Information Security Program; however, management must comply with FCRA in initially obtaining consumer reports.

MODULE 2: OBTAINING INFORMATION AND SHARING AMONG AFFILIATES

Overview

The FCRA contains many substantive compliance requirements for consumer reporting agencies designed to help ensure the accuracy and integrity of the consumer reporting system. As noted in the definitions section, a consumer reporting agency is a person that generally furnishes consumer reports

to third parties. By their very nature, banks, credit unions, and savings associations have a significant amount of consumer information that could constitute a consumer report, and thus communication of this information could cause the institution to become a consumer reporting agency. The FCRA contains several exceptions that enable a financial institution to communicate this type of information, within strict guidelines, without becoming a consumer reporting agency.

Rather than containing strict information sharing prohibitions, the FCRA creates a business disincentive such that if a financial institution shares consumer report information outside of the exceptions, then the institution is a consumer reporting agency and will be subject to the significant, substantive requirements of the FCRA applicable to those entities. Typically, a financial institution will structure its information sharing practices within the exceptions to avoid becoming a consumer reporting agency. This examination module generally covers the various information sharing practices within these exceptions.

If upon completion of this module, you determine that the financial institution's information sharing practices fall outside of these exceptions, you should consider the financial institution a consumer reporting agency and complete Module 6 of the examination procedures.

Consumer Report and Information Sharing (Section 603(d))

This section on Consumer Report and Information Sharing defines a consumer report to include information about a consumer such as that which bears on a consumer's creditworthiness, character, and capacity among other factors. Communication of this information may cause a person, including a financial institution, to become a consumer reporting agency. The statutory definition contains key exemptions to this definition that enable financial institutions to share this type of information under certain circumstances, without becoming consumer reporting agencies. Specifically, the term consumer report does not include:

- A report containing information solely as to transactions or experiences between the consumer and the financial institution making the report. A person, including a financial institution, may share information strictly related to its own transactions or experiences with a consumer (such as the consumer's payment history, or an account with the institution) with any third party, without regard to affiliation, without becoming a consumer reporting agency. The Privacy of Consumer Financial Information regulations that implement the Gramm-Leach-Bliley Act (GLBA) may restrict this type of information sharing because it meets the definition of nonpublic personal information under the Privacy regulations. Therefore, sharing it with nonaffiliated third parties may be subject to an opt out under the privacy regulations. In turn, the FCRA may also restrict activities that the GLBA permits. For example, the GLBA permits a financial institution to share a list of its customers and information such as their credit scores with another financial institution to jointly market or sponsor other financial products or services. This communication may be a consumer report under the FCRA and could potentially cause the sharing financial institution to become a consumer reporting agency.

- Communication of such transaction or experience information among persons, including financial institutions related by common ownership or affiliated by corporate control.

- Communication of other information (for example, other than transaction or experience information) among persons and financial institutions related by common ownership or affiliated by corporate control, if it is clearly and conspicuously disclosed to the consumer that the information will be communicated among such entities, and before the information is initially communicated, the consumer is given the opportunity to opt out of the communication. This allows a financial institution to share other information (that is, information other than its own transaction and experience information) that could otherwise be a consumer report, without becoming a consumer reporting agency under both of the following circumstances:

  — The sharing of the "other" information is done with affiliates.

  — Consumers are provided with the notice and an opportunity to opt out of this sharing before the information is first communicated among affiliates.

  For example, "other" information can include information a consumer provides on an application form concerning accounts with other financial institutions. It can also include information a financial institution obtains from a consumer reporting agency, such as the consumer's credit score. If a financial institution shares other information with affiliates without providing a notice and an opportunity to opt out, the financial institution may become a consumer reporting agency subject to all of the other requirements of the FCRA.

  GLBA and its implementing regulations require that a financial institution's Privacy Notice contain the Consumer Report (Section 603(d)) opt out right.

Other Exceptions

Specific extensions of credit. In addition, the term consumer report does not include the communication of a specific extension of credit directly or indirectly by the issuer of a credit card or similar device. For example, this exception allows a lender to communicate an authorization through the credit card network to a retailer, to enable a consumer to complete a purchase using a credit card.

Credit Decision to Third Party (for example, auto dealer). The term consumer report also does not include any report in which a person, including a financial institution, who has been requested by a third party to make a specific extension of credit directly or indirectly to a consumer, conveys the decision with respect to the request. The third party must advise the consumer of the name and address of the financial institution to which the request was made, and such financial institution makes the adverse action disclosures required by section 615 of the FCRA. For example, this exception allows a lender to communicate a credit decision to an automobile dealer who is arranging financing for a consumer purchasing an automobile and who requires a loan to finance the transaction.

Joint User Rule. The Federal Trade Commission staff commentary discusses another exception known as the "Joint User Rule." Under this exception, users of consumer reports, including financial institutions, may share information if they are jointly involved in the decision to approve a consumer's request for a product or service, provided that each has a permissible purpose to obtain a consumer report on the individual. For example, a consumer applies for a mortgage loan that will have a high loan-to-value ratio, and thus the lender will require private mortgage insurance (PMI) in order to approve the application. An outside company provides the PMI. The lender and the PMI company can share consumer report information about the consumer because both entities have permissible purposes to obtain the information and both are jointly involved in the decision to grant the products to the consumer. This exception applies to entities that are affiliated or nonaffiliated third parties. It is important to note that the GLBA will still apply to the sharing of nonpublic, personal information with nonaffiliated third parties; therefore, financial institutions should be aware the GLBA may still limit or prohibit sharing under the FCRA joint user rule.

Protection of Medical Information (Section 604(g))

Section 604(g) generally prohibits creditors from obtaining and using medical information in connection with any determination of the consumer's eligibility, or continued eligibility, for credit. The statute contains no prohibition on creditors obtaining or using medical information for other purposes that are not in connection with a determination of the consumer's eligibility, or continued eligibility for credit.

Section 604(g)(5)(A) requires the federal banking agencies and NCUA to prescribe regulations that permit transactions that are determined to be necessary and appropriate to protect legitimate operational, transactional, risk, consumer, and other needs (including administrative verification purposes), consistent with the Congressional intent to restrict the use of medical information for inappropriate purposes. On November 22, 2005, the FFIEC Agencies published final rules in the Federal Register (70 FR 70664). The rules contain the general prohibition on obtaining or using medical information, and provide exceptions for the limited circumstances when medical information may be used. The rules define "credit" and "creditor" as having the same meanings as in section 702 of the Equal Credit Opportunity Act (15 USC 1691a).

Obtaining and Using Unsolicited Medical Information. A creditor does not violate the prohibition on obtaining medical information if it receives the medical information pertaining to a consumer in connection with any determination of the consumer's eligibility, or continued eligibility, for credit without specifically requesting medical information. However, the creditor may only use this medical information in connection with a determination of the consumer's eligibility, or continued eligibility, for credit in accordance with either the financial information exception or one of the specific other exceptions provided in the rules. We discuss these exceptions below.

Financial Information Exception. The rules allow a creditor to obtain and use medical information pertaining to a consumer in connection with any determination of the consumer's eligibility or continued eligibility for credit, so long as:

- The information is the type of information routinely used in making credit eligibility determinations, such as information relating to debts, expenses, income, benefits, assets, collateral, or the purpose of the loan, including the use of the loan proceeds.

- The creditor uses the medical information in a manner and to an extent that is no less favorable than it would use comparable information that is not medical information in a credit transaction.

- The creditor does not take the consumer's physical, mental, or behavioral health, condition or history, type of treatment, or prognosis into account as part of any such determination.

The financial information exception is designed in part to allow creditors to consider a consumer's medical debts and expenses in the assessment of that consumer's ability to repay the loan according to the loan terms. In addition, the financial information exception also allows a creditor to consider the dollar amount and continued eligibility for disability income, worker's compensation income, or other benefits related to health or a medical condition that is relied on as a source of repayment.

The creditor may use the medical information in a manner and to an extent that is no less favorable than it would use comparable, nonmedical information. For example, a consumer includes on an application for credit information about two $20,000 debts. One debt is to a hospital; the other is to a retailer. The creditor may use and consider the debt to the hospital in the same manner in which it considers the debt to the retailer, such as including the debts in the calculation of the consumer's proposed debt-to-income ratio. In addition, the consumer's payment history of the debt to the hospital may be considered in the same manner as the debt to the retailer. For example, if the creditor does not grant loans to applicants who have debts that are 90-days past due, the creditor could consider the past-due status of a debt to the hospital, in the same manner as the past-due status of a debt to the retailer.

A creditor may use medical information in a manner that is more favorable to the consumer, according to its regular policies and procedures. For example, if a creditor has a routine policy of declining consumers who have a 90-day past due installment loan to a retailer, but does not decline consumers who have a 90-day past due debt to a hospital, the financial information exception would allow a creditor to continue this policy without violating the rules because in these cases, the creditor's treatment of the debt to the hospital is more favorable to the consumer.

A creditor may not take the consumer's physical, mental, or behavioral health, condition or history, type of treatment, or prognosis into account as part of any determination regarding the consumer's eligibility, or continued eligibility for credit. The creditor may only consider the financial implications as discussed above, such as the status of a debt to a hospital, continued eligibility for disability income, etc.

Specific Exceptions for Obtaining and Using Medical Information. In addition to the financial information exception, the rules also provide for the following nine specific exceptions under which a creditor can obtain and use medical information in it's determination of the consumer's eligibility, or continued eligibility for credit:

- To determine whether the use of a power of attorney or legal representative that is triggered by a medical condition or event is necessary and appropriate, or whether the consumer has the legal capacity to contract when a person seeks to exercise a power of attorney or act as a legal representative for a consumer based on an asserted medical condition or event. For example, if Person A is attempting to act on behalf of Person B under a Power of Attorney that is invoked based on a medical event, a creditor is allowed to obtain and use medical information to verify that Person B has experienced a medical condition or event such that Person A is allowed to act under the Power of Attorney.

- To comply with applicable requirements of local, state, or Federal laws.

- To determine, at the consumer's request, whether the consumer qualifies for a legally permissible special credit program or credit related assistance program that is:

  — Designed to meet the special needs of consumers with medical conditions; AND

  — Established and administered pursuant to a written plan that:

    ✓ Identifies the class of persons that the program is designed to benefit; and

    ✓ Sets forth the procedures and standards for extending credit or providing other credit-related assistance under the program.

- To the extent necessary for purposes of fraud prevention or detection.

- In the case of credit for the purpose of financing medical products or services, to determine and verify the medical purpose of the loan and the use of the proceeds.

- Consistent with safe and sound banking practices, if the consumer or the consumer's legal representative requests that the creditor use medical information in determining the consumer's eligibility, or continued eligibility, for credit, to accommodate the consumer's particular circumstances, and such request is documented by the creditor. For example, at the consumer's request, a creditor may grant an exception to its ordinary policy to accommodate a medical condition that the consumer has experienced. This exception allows a creditor to consider medical information in this context, but it does not require a creditor to make such an accommodation nor does it require a creditor to grant a loan that is unsafe or unsound.

- Consistent with safe and sound practices, to determine whether the provisions of a forbearance practice or program that is triggered by a medical condition or event apply to a consumer. For example, if a creditor has a policy of delaying foreclosure in cases where a consumer is experiencing a medical hardship, this exception allows the creditor to use medical information to determine if the policy would apply to the consumer. Like the exception listed in the bullet above, this exception does not require a creditor to grant forbearance, it merely provides an exception so that a creditor may consider medical information in these instances.

- To determine the consumer's eligibility for the triggering of, or the reactivation of a debt cancellation contract or debt suspension agreement, if a medical condition or event is a triggering event for the provision of benefits under the contract or agreement.

- To determine the consumer's eligibility for the triggering of, or the reactivation of a credit insurance product, if a medical condition or event is a triggering event for the provision of benefits under the product.

Limits on redisclosure of information. If a creditor subject to the medical information rules receives medical information about a consumer from a consumer reporting agency or its affiliate, the creditor must not disclose that information to any other person, except as necessary to carry out the purpose for which the information was initially disclosed, or as otherwise permitted by statute, regulation, or order.

Sharing medical information with affiliates. In general, the exclusions from the definition of "consumer report" in section 603(d)(2) of the FCRA allow the sharing of non-medical information among affiliates. With regard to medical information, section 603(d)(3) of the FCRA provides that the exclusions in section 603(d)(2) do not apply when a person subject to the medical information rules shares any of the following information with an affiliate:

- Medical information.

- An individualized list or description based on the payment transactions of the consumer for medical products or services.

- An aggregate list of identified consumers based on payment transactions for medical products or services.

If a person who is subject to the medical rules shares with an affiliate the type of information discussed above, the exclusions from the definition of "consumer report" do not apply. Effectively, this means that if a person shares medical information, that person becomes a consumer reporting agency, subject to all of the other substantive requirements of the FCRA.

The rules provide exceptions to these limitations on sharing medical information with affiliates. A person, such as a bank, thrift, or credit union, may share medical information with its affiliates without becoming a consumer reporting agency under any of the following circumstances:

- In connection with the business of insurance or annuities (including the activities described in section 18B of the model Privacy of Consumer Financial and Health Information Regulation issued by the National Association of Insurance Commissioners, as in effect on January 1, 2003).

- For any purpose permitted without authorization under the regulations promulgated by the Department of Health and Human Services pursuant to the Health Insurance Portability and Accountability Act of 1996 (HIPAA).

- For any purpose referred to in section 1179 of HIPAA.

- For any purpose described in section 502(e) of the Gramm-Leach-Bliley Act.

- In connection with a determination of the consumer's eligibility, or continued eligibility, for credit consistent with the financial information exceptions or specific exceptions.

- As otherwise permitted by order of the appropriate federal agency or NCUA, as applicable.

Affiliate Marketing Opt Out (Section 624)

Section 624 gives a consumer the right to restrict an entity, with which it does not have a pre-existing business relationship, from ***using*** certain information obtained from an affiliate to make solicitations to that consumer. This provision is distinct from Section 603(d)(2)(A)(iii) which gives a consumer the right to restrict the ***sharing*** of certain consumer information among affiliates.[5]

Under Section 624, an entity may not use information received from an affiliate to market its products or services to a consumer, unless the consumer is given notice and a reasonable opportunity and a reasonable and simple method to opt out of the making of such solicitations. The affiliate marketing opt-out applies to both transaction or experience information and "other" information, such as information from credit reports and credit applications. On November 7, 2007, the federal financial institution regulators published final regulations in the Federal Register to implement this section (72 FR 62910).[6]

Exceptions to the notice and opt out requirements apply when an entity uses eligibility information in certain ways, as described later in these procedures.

[5] See Module 2, Section 603(d) Consumer Report and Information Sharing, for provisions pertaining to the sharing of consumer information. Under Section 603(d)(2)(A)(iii) of the FCRA, entities are responsible for complying with the affiliate *sharing* notice and opt-out requirement, where applicable. Thus, under the FCRA, certain consumer information will be subject to two opt-outs, a sharing opt-out (Section 603(d)) and a marketing use opt-out (Section 624). These two opt-outs may be consolidated.

[6] See 12 CFR 571.20(a) for the scope of entities covered by Subpart C of 12 CFR 571.

Key Definitions (12 CFR 571.20)[7]

- *Eligibility information (12 CFR 571.20(b)(3))* includes not only transaction and experience information, but also the type of information found in consumer reports, such as information from third party sources and credit scores. Eligibility information does not include aggregate or blind data that does not contain personal identifiers such as account numbers, names, or addresses.[8]

- *Pre-existing business relationship (12 CFR 571.20(b)(4))*[9] means a relationship between a person, such as a financial institution (or a person's licensed agent), and a consumer based on:

  — A financial contract between the person and the consumer which is in force on the date on which the consumer is sent a solicitation covered by the affiliate marketing regulation;

  — The purchase, rental, or lease by the consumer of the person's goods or services, or a financial transaction (including holding an active account or a policy in force, or having another continuing relationship) between the consumer and the person, during the 18-month period immediately preceding the date on which the consumer is sent a solicitation covered by the affiliate marketing regulation; or

  — An inquiry or application by the consumer regarding a product or service offered by that person during the three-month period immediately preceding the date on which the consumer is sent a solicitation covered by the affiliate marketing regulation.

- *Solicitation (12 CFR 571.20(b)(5))* means the marketing of a product or service initiated by a person, such as a financial institution, to a particular consumer that is:

  — Based on eligibility information communicated to that person by its affiliate; and

  — Intended to encourage the consumer to purchase or obtain such product or service.

  Examples of a solicitation include a telemarketing call, direct mail, e-mail, or other form of marketing communication directed to a particular consumer that is based on eligibility information received from an affiliate. A solicitation does not include marketing communications that are directed at the general public (e.g., television, general circulation magazine, and billboard advertisements).

[7] See 12 CFR 571.20 for other definitions.

[8] Specifically, "eligibility information" is defined in the affiliate marketing regulation as "any information the communication of which would be a consumer report if the exclusions from the definition of "consumer report" in Section 603(d)(2)(A) of the [Fair Credit Reporting] Act did not apply."

[9] See 12 CFR 571.20(b)(4)(ii) and (iii) for examples of pre-existing business relationships and situations where no pre-existing business relationship exists.

Initial Notice and Opt-out Requirement (12 CFR 571.21(a), 571.24, and 571.25). A financial institution and its subsidiaries (financial institution) generally may not use eligibility information about a consumer that it receives from an affiliate to make a solicitation for marketing purposes to the consumer, unless:

- It is clearly and conspicuously disclosed to the consumer in writing or, if the consumer agrees, electronically, in a concise notice that the financial institution may use eligibility information about that consumer that it received from an affiliate to make solicitations for marketing purposes to the consumer;

- The consumer is provided a reasonable opportunity and a reasonable and simple method to "opt out" (that is, the consumer prohibits the financial institution from using eligibility information to make solicitations for marketing purposes to the consumer);[10] and

- The consumer has not opted out.

For example, a consumer has a homeowner's insurance policy with an insurance company. The insurance company shares eligibility information about the consumer with its affiliated depository institution. Based on that eligibility information, the depository institution wants to make a solicitation to the consumer about its home equity loan products. The depository institution does not have a pre-existing business relationship with the consumer and none of the other exceptions apply. The depository institution may not use eligibility information it received from its insurance affiliate to make solicitations to the consumer about its home equity loan products unless the insurance company gave the consumer a notice and opportunity to opt out and the consumer does not opt out.

Making Solicitations (12 CFR 571.21(b)).[11] A financial institution (or a service provider acting on behalf of the financial institution) makes a solicitation for marketing purposes if:

- The financial institution receives eligibility information from an affiliate, including when the affiliate places that information into a common database that the financial institution may access;

- The financial institution uses that eligibility information to do one or more of the following:

  — Identify the consumer or type of consumer to receive a solicitation;

  — Establish criteria used to select the consumer to receive a solicitation; or

[10] See 12 CFR 571.24 and 571.25 for examples of "a reasonable opportunity to opt out" and "reasonable and simple methods for opting out."

[11] See 12 CFR 571.21(b)(6) for examples of making solicitations.

— Decide which of the financial institution's products or services to market to the consumer or tailor the financial institution's solicitation to that consumer; and

- As a result of the financial institution's use of the eligibility information, the consumer is provided a solicitation.

  A financial institution does ***not*** make a solicitation for marketing purposes (and therefore the affiliate marketing regulation, with its notice and opt-out requirements, does not apply) in the situations listed below, commonly referred to as "constructive sharing." Constructive sharing occurs when a financial institution provides criteria to an affiliate to use in marketing the financial institution's product and the affiliate uses the criteria to send marketing materials to the affiliate's own customers that meet the criteria. In this situation, the financial institution is not *using* shared eligibility information to make solicitations.

- The financial institution provides criteria for consumers to whom it would like its affiliate to market the financial institution's products. Then, based on this criteria, the affiliate uses eligibility information that the affiliate obtained in connection with its own pre-existing business relationship with the consumer to market the financial institution's products or services (or directs its service provider to use the eligibility information in the same manner and the financial institution does not communicate with the service provider regarding that use).

- A service provider, applying the financial institution's criteria, uses information from an affiliate, such as that in a shared database, to market the financial institution's products or services to the consumer, so long as it meets certain requirements, including all of the following.

  — The affiliate controls access to and use of its eligibility information by the service provider under a written agreement between the affiliate and the service provider.

  — The affiliate establishes, in writing, specific terms and conditions under which the service provider may access and use the affiliate's eligibility information to market the financial institution's products and services (or those of affiliates generally) to the consumer.

  — The affiliate requires the service provider, under a written agreement, to implement reasonable policies and procedures designed to ensure that the service provider uses the affiliate's eligibility information in accordance with the terms and conditions established by the affiliate relating to the marketing of the financial institution's products or services.

  — The affiliate is identified on or with the marketing materials provided to the consumer.

  — The financial institution does not directly use its affiliate's eligibility information in the manner described above under "Making Solicitations (12 CFR 571.21(b))," item 2.

Exceptions to Initial Notice and Opt-out Requirements (12 CFR 571.21(c)).[12] The initial notice and opt-out requirements do not apply to a financial institution if it uses eligibility information that it receives from an affiliate:

- To make a solicitation for marketing purposes to a consumer with whom the financial institution has a pre-existing business relationship;
- To facilitate communications to an individual for whose benefit the financial institution provides employee benefit or other services pursuant to a contract with an employer;
- To perform services on behalf of an affiliate (but this would not allow solicitation where the consumer has opted out);
- In response to a communication about the financial institution's products or services initiated by the consumer;
- In response to a consumer's authorization or request to receive solicitations; or
- If the financial institution's compliance with the affiliate marketing regulation would prevent it from complying with State insurance laws pertaining to unfair discrimination in any state in which the financial institution is lawfully doing business.

Contents of Opt-out Notice (12 CFR 571.23). A financial institution must provide to the consumer a reasonable and simple method for the consumer to opt out. The opt-out notice must be clear, conspicuous, and concise, and must accurately disclose specific information outlined in 12 CFR 571.23(a), including that the consumer may elect to limit the use of eligibility information to make solicitations to the consumer. See Appendix C to the regulation for the model notices contained in the affiliate marketing regulation.

Alternative contents. An affiliate that provides a consumer a broader right to opt out than that required by the affiliate marketing regulation may satisfy the regulatory requirements by providing the consumer with a clear, conspicuous, and concise notice that accurately discloses the consumer's opt-out rights.

Coordinated, consolidated, and equivalent notices. Opt-out and renewal notices may be coordinated and consolidated with any other notice or disclosure required under any other provision of law, such as the Gramm-Leach-Bliley Act (GLBA), 15 USC 6801 et seq. Renewal notices, which have additional required content (12 CFR 571.27), may be consolidated with the annual GLBA privacy notices.

[12] See 12 CFR 571.21(d) for examples of exceptions to the initial notice and opt-out requirement.

Delivery of the Opt-out Notice (12 CFR 571.21(a)(3) and 571.26).[13] An affiliate that has or previously had a pre-existing business relationship with the consumer must provide the notice either individually or as part of a joint notice from two or more members of an affiliated group of companies. The opt-out notice must be provided so that each consumer can reasonably be expected to receive actual notice. A consumer may not reasonably be expected to receive actual notice if, for example, the affiliate providing the notice sends the notice via e-mail to a consumer who has not agreed to receive electronic disclosures by e-mail from the affiliate providing the notice.[14]

Scope of Opt-out (12 CFR 571.22(a) and 571.23(a)(2)).[15] As a general rule, the consumer's election to opt out prohibits any affiliate covered by the opt-out notice from using eligibility information received from another affiliate, described in the notice, to make solicitations to the consumer. If two or more consumers jointly obtain a product or service, any of the joint consumers may exercise the right to opt out. It is impermissible to require all joint consumers to opt out before implementing any opt-out direction.

Menu of alternatives. A consumer may be given the opportunity to choose from a menu of alternatives when electing to prohibit solicitations, such as by:

- Electing to prohibit solicitations from certain types of affiliates covered by the opt-out notice but not other types of affiliates covered by the notice.
- Electing to prohibit solicitations based on certain types of eligibility information but not other types of eligibility information.
- Electing to prohibit solicitations by certain methods of delivery but not other methods of delivery.

One of the alternatives, however, must allow the consumer to prohibit all solicitations from all of the affiliates that are covered by the notice.

Continuing relationship. If the consumer establishes a continuing relationship with a financial institution or its affiliate, an opt-out notice may apply to eligibility information obtained from one or more continuing relationships (such as a deposit account, a mortgage loan, or a credit card), if the notice adequately describes the continuing relationships covered. The opt-out notice can also apply to future continuing relationships if the notice adequately describes the continuing future relationships that would be covered.

[13] See 12 CFR 571.26(b) and (c) for examples of "reasonable expectation of actual notice" and "no reasonable expectation of actual notice."

[14] For opt-out notices provided electronically, the notice may be provided in compliance with either the electronic disclosure provisions of 12 CFR 571.24(b)(2) and 571.24(b)(3) or the provisions in section 101 of the Electronic Signatures in Global and National Commerce Act, 15 USC 7001 et seq.

[15] See 12 CFR 571.22(a) for examples of the scope of the opt-out, including examples of continuing relationships.

Special rule for a notice following termination of all continuing relationships. After all continuing relationships with a financial institution or its affiliate(s) are terminated, a consumer must be given a new opt-out notice if the consumer later establishes another continuing relationship with the financial institution or its affiliate(s) and the consumer's eligibility information is to be used to make a solicitation. The consumer's decision not to opt out after receiving the new opt-out notice would not override a prior opt-out election that applies to eligibility information obtained in connection with a

No continuing relationship (isolated transaction). If the consumer does not establish a continuing relationship with a financial institution or its affiliate, but the financial institution or its affiliate obtains eligibility information about the consumer in connection with a transaction with the consumer (such as an ATM cash withdrawal, purchase of traveler's checks, or a credit application that is denied), an opt-out notice provided to the consumer only applies to eligibility information obtained in connection with that transaction.

Time, Duration, and Renewal of Opt-out (12 CFR 571.22(b) and (c) and 571.27). A consumer may opt out at any time. The opt-out must be effective for a period of at least five years beginning when the consumer's opt-out election is received and implemented, unless the consumer later revokes the opt-out in writing or, if the consumer agrees, electronically. An opt-out period may be set at more than five years, including an opt-out that does not expire unless the consumer revokes it.

Renewal after opt-out period expires. After the opt-out period expires, a financial institution may not make solicitations based on eligibility information it receives from an affiliate to a consumer who previously opted out, unless:

- The consumer receives a renewal notice and opportunity to opt out, and the consumer does not renew the opt-out; or
- An exception to the notice and opt-out requirements applies.[16]

Contents of renewal notice. The renewal notice must be clear, conspicuous, and concise, and must accurately disclose most of the elements of the original opt-out notice, as well as the following information as applicable:

- The consumer previously elected to limit the use of certain information to make solicitations to the consumer.
- The consumer's election has expired or is about to expire.
- The consumer may elect to renew the consumer's previous election.

[16] See 12 CFR 571.21(c) for exceptions.

- If applicable, that the consumer's election to renew will apply for the specified period of time stated in the notice and that the consumer will be allowed to renew the election once that period expires.

See 12 CFR 571.27(b) for all the content requirements of a renewal notice.

Renewal period. Each opt-out renewal must be effective for a period of at least five years.

Affiliate who may provide the notice. The renewal notice must be provided by the affiliate that provided the previous opt-out notice, or its successor; or as part of a joint renewal notice from two or more members of an affiliated group of companies, or their successors, that jointly provided the previous opt-out notice.

Timing of the renewal notice. A renewal notice may be provided to the consumer either a reasonable period of time before the expiration of the opt-out period[17] or any time after the expiration of the opt-out period but before solicitations are made to the consumer that would have been prohibited by the expired opt-out.

Prospective application (12 CFR 571.28(c)). A financial institution may use eligibility information received from an affiliate to make solicitations to a consumer if it received such information prior to October 1, 2008, the mandatory compliance date of the affiliate marketing regulation. An institution is deemed to have received eligibility information when such information is placed into a common database and is accessible by the institution prior to that date.

Model forms for opt-out notices (12 CFR 571, Appendix C). Appendix C of the affiliate marketing regulation contains model forms that may be used to comply with the requirement for clear, conspicuous, and concise notices. The five model forms are:

C-1 Model Form for Initial Opt-out Notice (Single-Affiliate Notice)

C-2 Model Form for Initial Opt-out Notice (Joint Notice)

C-3 Model Form for Renewal Notice (Single-Affiliate Notice)

C-4 Model Form for Renewal Notice (Joint Notice)

C-5 Model Form for Voluntary "No Marketing" Notice

[17] An opt-out period may not be shortened by sending a renewal notice to the consumer before expiration of the opt-out period, even if the consumer does not renew the opt-out. If a financial institution provides an annual privacy notice under the Gramm-Leach-Bliley Act, providing a renewal notice with the last annual privacy notice provided to the consumer before expiration of the opt-out period is a reasonable period of time before expiration of the opt-out in all cases (12 CFR 571.27(d)).

Use of the model forms is not required and a financial institution may make certain changes to the language or format of the model forms without losing the protection from liability afforded by use of the model forms. These changes may not be so extensive as to affect the substance, clarity, or meaningful sequence of the language in the model forms. Institutions making such extensive revisions will lose the safe harbor that Appendix C provides. Examples of acceptable changes are provided in Appendix C to the regulation.

MODULE 3: DISCLOSURES TO CONSUMERS AND MISCELLANEOUS REQUIREMENTS

Overview

The FCRA requires financial institutions to provide consumers with various notices and information under a variety of circumstances. This module contains examination responsibilities for these various areas.

Use of Consumer Reports for Employment Purposes (Section 604(b))

This section on the Use of Consumer Reports for Employment Purposes has specific requirements for financial institutions that obtain consumer reports of its employees or prospective employees prior to, and/or during, the term of employment. The FCRA generally requires the written permission of the consumer to procure a consumer report for "employment purposes." Moreover, the financial institution must provide to the consumer in writing a clear and conspicuous disclosure that it may obtain a consumer report for employment purposes prior to procuring a report.

Prior to taking any adverse action involving employment that is based in whole or in part on the consumer report, the user generally must provide to the consumer:

- A copy of the report.
- A description in writing of the rights of the consumer under this title, as FTC prescribes under § (609)(c)(3).

At the time a financial institution takes adverse action in an employment situation, § 615 requires that it must provide the consumer with an adverse action notice described later in this module.

Prescreened Consumer Reports and Opt out Notice (Sections 604(c) and 615(d)) (and Parts 642 and 698 of Federal Trade Commission Regulations)

The sections on Prescreened Consumer Reports and Opt Out Notice allows persons, including financial institutions, to obtain and use consumer reports on any consumer in connection with any

credit or insurance transaction that the consumer does not initiate, to make firm offers of credit or insurance. This process, known as prescreening, occurs when a financial institution obtains a list from a consumer reporting agency of consumers who meet certain predetermined creditworthiness criteria and who have not elected to be excluded from such lists. These lists may only contain the following information:

- The name and address of a consumer.
- An identifier that is not unique to the consumer and that the person uses solely for the purpose of verifying the identity of the consumer.
- Other information pertaining to a consumer that does not identify the relationship or experience of the consumer with respect to a particular creditor or other entity.

Each name appearing on the list is considered an individual consumer report. In order to obtain and use these lists, financial institutions must make a "firm offer of credit or insurance" as defined in § 603(l) to each person on the list. An institution is not required to grant credit or insurance if the consumer is not creditworthy or insurable, or cannot furnish required collateral, provided that the financial institution determines the underwriting criteria in advance, and applies it consistently.

> Example 1: Assume a home mortgage lender obtains a list from a consumer reporting agency of everyone in County X, with a current home mortgage loan and a credit score of 700. The lender will use this list to market a second lien home equity loan product. The lender's other nonconsumer report criteria, in addition to those used in the prescreened list for this product, include a maximum total debt-to-income ratio (DTI) of 50 percent or less. The consumer reporting agency can screen some of the criteria but must determine other criteria individually, such as the DTI, when consumers respond to the offer. If a consumer responds to the offer, but already has a DTI of 60 percent, the lender does not have to grant the loan.

In addition, the financial institution is allowed to obtain a full consumer report on anyone responding to the offer to verify that the consumer continues to meet the creditworthiness criteria. If the consumer no longer meets those criteria, the financial institution does not have to grant the loan.

> Example 2: On January 1, a credit card lender obtains a list from a consumer reporting agency of consumers in County Y who have credit scores of 720, and no previous bankruptcy records. The lender mails solicitations offering a pre-approved credit card to everyone on the list on January 2. On January 31, a consumer responds to the offer and the lender obtains and reviews a full consumer report that shows a bankruptcy record was added on January 15. Since this consumer no longer meets the lender's predetermined criteria, the lender is not required to issue the credit card.

These basic requirements help prevent financial institutions from obtaining prescreened lists without following through with an offer of credit or insurance. The financial institution must maintain the criteria used for the product (including the criteria used to generate the prescreened report and any

other criteria such as collateral requirements) on file for a period of three years, beginning on the date that the financial institution made the offer to the consumer.

Technical Notice and Opt Out Requirements (Section 615(d)). This section contains consumer protections and technical notice requirements concerning prescreened offers of credit or insurance. The FCRA requires nationwide consumer reporting agencies to jointly operate an "opt out" system, whereby consumers can elect to be excluded from prescreened lists by calling a toll-free number.

When a financial institution obtains and uses these lists, it must provide consumers with a Prescreened Opt Out Notice with the offer of credit or insurance. This notice alerts consumers that they are receiving the offer because they meet certain creditworthiness criteria. The notice must also provide the toll-free telephone number operated by the nationwide consumer reporting agencies for consumers to call to opt out of prescreened lists.

The FCRA contains the basic requirement to provide notices to consumers at the time the prescreened offers are made. The Federal Trade Commission (FTC) published an implementing regulation containing the technical requirements of the notice at 16 CFR Parts 642 and 698. This regulation is applicable to anyone, including banks, credit unions, and saving associations, that obtains and uses prescreened consumer reports. These requirements became effective on August 1, 2005; however, the requirement to provide a notice containing the toll-free opt out telephone number has existed under the FCRA for many years.

Short and Long Notice. FTC regulations 16 CFR 642 and 698 require that the financial institution give a "short" notice and a "long" notice of the prescreened opt out information with each written solicitation made to consumers using prescreened consumer reports. These regulations also contain specific requirements concerning the content and appearance of these notices. The requirements are listed within the following paragraphs of these procedures. The regulations were published on January 31, 2005, in 70 Federal Register 5022, and took effect August 1, 2005.

The short notice must be a clear and conspicuous, simple, and easy-to-understand statement as follows:

- Content. The short notice must state that the consumer has the right to opt out of receiving prescreened solicitations. It must provide the toll-free number and direct consumers to the existence and location of the long notice. It should also state the title of the long notice. The short notice may not contain any other information.

- Form. The short notice must be in a type size larger than the principal text on the same page, but it may not be smaller than 12-point type. If the financial institution provides the notice by electronic means, it must be larger than the type size of the principal text on the same page.

- Location. The short form must be on the front side of the first page of the principal promotional document in the solicitation. If provided electronically, it must be on the same page and in close proximity to the principal marketing message. The statement must be located

so that it is distinct from other information, such as inside a border, and must be in a distinct type style, such as bolded, italicized, underlined, and/or in a color that contrasts with the principal text on the page, if the solicitation is provided in more than one color.

The long notice must also be a clear and conspicuous, simple, and easy-to-understand statement as follows:

- Content. The long notice must state the information required by § 615(d) of the FCRA and may not include any other information that interferes with, detracts from, contradicts, or otherwise undermines the purpose of the notice.

- Form. The notice must appear in the solicitation, be in a type size that is no smaller than the type size of the principal text on the same page, and, for solicitations provided other than by electronic means, the type size may not be smaller than 8-point type. The notice must begin with a heading in capital letters, underlined, and identifying the long notice as the "PRESCREEN & OPT OUT NOTICE." It must be in a type style that is distinct from the principal type style used on the same page, such as bolded, italicized, underlined, and/or in a color that contrasts from the principal text, if the solicitation is in more than one color. The notice must be set apart from other text on the page, such as by including a blank line above and below the statement, and by indenting both the left and right margins from other text on the page.

The FTC developed model Prescreened Opt Out Notices, which are contained in Appendix A to 16 CFR 698 of the FTC's regulations. Appendix A contains complete sample solicitations for context. The prescreen notice text is contained below:

Sample Short Notice:

You can choose to stop receiving "prescreened" offers of (credit or insurance) from this and other companies by calling toll-free (toll-free number). See PRESCREEN & OPT-OUT NOTICE on other side (or other location) for more information about prescreened offers.

Sample Long Notice:

PRESCREEN & OPT-OUT NOTICE: This "prescreened" offer of (credit or insurance) is based on information in your credit report indicating that you meet certain criteria. This offer is not guaranteed if you do not meet our criteria (including providing acceptable property as collateral). If you do not want to receive prescreened offers of (credit or insurance) from this and other companies, call the consumer reporting agencies (or name of consumer reporting agency) toll-free, (toll-free number); or write: (consumer reporting agency name and mailing address).

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

This section on Truncation of Credit and Debit Card Account Numbers provides that persons, including financial institutions that accept debit and credit cards for the transaction of business will be prohibited from issuing electronic receipts that contain more than the last five digits of the card number, or the card expiration date, at the point of sale or transaction. This requirement applies only to electronically developed receipts and does not apply to hand-written receipts or those developed with an imprint of the card.

For Automatic Teller Machines (ATMs) and Point-of-Sale (POS) terminals or other machines that were put into operation before January 1, 2005, this requirement took effect on December 4, 2006. For ATMs and POS terminals or other machines that were put into operation on or after January 1, 2005, the effective date was the date of installation.

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

This section on Disclosure of Credit scores by Certain Mortgage Lenders requires financial institutions that make or arrange mortgage loans using credit scores to provide the score with accompanying information to the applicants.

Credit score. For purposes of this section, the term "credit score" is defined as a numerical value or a categorization derived from a statistical tool or modeling system used by a person who makes or arranges a loan to predict the likelihood of certain credit behaviors, including default (and the numerical value or the categorization derived from such analysis may also be referred to as a "risk predictor" or "risk score"). The credit score does not include either of the following:

- Any mortgage score or rating by an automated underwriting system that considers one or more factors in addition to credit information, such as the loan-to-value ratio, the amount of down payment, or the financial assets of a consumer.

- Any other elements of the underwriting process or underwriting decision.

Covered transactions. The disclosure requirement applies to both closed-end and open-end loans that are for consumer purposes and are secured by one- to four-family residential real properties, including purchase and refinance transactions. This requirement will not apply in circumstances that do not involve a consumer purpose, such as when a borrower obtains a loan secured by his or her residence to finance his or her small business.

Specific required notice. Financial institutions in covered transactions that use credit scores must provide a disclosure containing the following specific language, which is contained in § 609(g)(1)(D):

Notice to The Home Loan Applicant

In connection with your application for a home loan, the lender must disclose to you the score that a consumer reporting agency distributed to users and the lender used in connection with your home loan, and the key factors affecting your credit scores.

The credit score is a computer generated summary calculated at the time of the request and based on information that a consumer reporting agency or lender has on file. The scores are based on data about your credit history and payment patterns. Credit scores are important because they are used to assist the lender in determining whether you will obtain a loan. They may also be used to determine what interest rate you may be offered on the mortgage. Credit scores can change over time, depending on your conduct, how your credit history and payment patterns change, and how credit scoring technologies change.

Because the score is based on information in your credit history, it is very important that you review the credit-related information that is being furnished to make sure it is accurate. Credit records may vary from one company to another.

If you have questions about your credit score or the credit information that is furnished to you, contact the consumer reporting agency at the address and telephone number provided with this notice, or contact the lender, if the lender developed or generated the credit score. The consumer reporting agency plays no part in the decision to take any action on the loan application and is unable to provide you with specific reasons for the decision on a loan application.

If you have questions concerning the terms of the loan, contact the lender.

The notice must include the name, address, and telephone number of each consumer reporting agency that provided a credit score that was used.

Credit score and key factors disclosed. In addition to the notice, financial institutions must also disclose the credit score, the range of possible scores, the date that the score was created, and the "key factors" used in the score calculation. "Key factors" are all relevant elements or reasons adversely affecting the credit score for the particular individual, listed in the order of their importance, and based on their effect on the credit score. The total number of factors the financial institution should disclose must not exceed four. However, if one of the key factors is the number of inquiries into a consumer's credit information, then the total number of factors must not exceed five. These key factors come from information the consumer reporting agencies supplied with any consumer report that was furnished containing a credit score (Section 605(d)(2)).

This disclosure requirement applies in any application for a covered transaction, regardless of the final action the lender takes on the application. The FCRA requires a financial institution to disclose all of the credit scores used in these transactions. For example, if two joint applicants apply for a mortgage loan to purchase a single-family residence and the lender uses both credit scores, then the financial

institution needs to disclose both. The statute specifically does not require more than one disclosure per loan. Therefore, if the financial institution uses multiple scores, it can include all of them in one disclosure containing the Notice to the Home Loan Applicant.

If a financial institution uses a credit score that it did not obtain directly from a consumer reporting agency, but may contain some information from a consumer reporting agency, the financial institution may satisfy this disclosure requirement by providing a score and associated key factor information that a consumer reporting agency supplied. For example, certain automated underwriting systems generate a score used in a credit decision. These systems are often populated by data obtained from a consumer reporting agency. If a financial institution uses this automated system, it may satisfy the disclosure requirement by providing the applicants with a score and key factors a consumer reporting agency supplied based on the data, including credit score(s) imported into the automated underwriting system. This will provide applicants with information about their credit history and its role in the credit decision, in the spirit of this section of the statute.

Timing. With regard to the timing of the disclosure, the statute requires that the financial institution provide it as soon as is reasonably practicable after using a credit score.

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

This section requires users of consumer reports to make certain disclosures when they take adverse actions with respect to consumers, based on information received from third parties. Specific disclosures are required depending upon whether the source of the information is: a consumer reporting agency, a third party other than a consumer reporting agency, or an affiliate. The disclosure requirements are discussed separately below.

Information Obtained From a Consumer Reporting Agency

Section 615(a), Duties of Users Taking Adverse Actions on the Basis of Information Contained in Consumer Reports, provides that when adverse action is taken with respect to any consumer based in whole or in part on any information contained in a consumer report, the financial institution must:

- Provide oral, written, or electronic notice of the adverse action to the consumer.
- Provide to the consumer orally, in writing, or electronically:
  - The name, address, and telephone number of the consumer reporting agency from which it received the information (including a toll-free telephone number established by the agency, if the consumer reporting agency maintains files on a nationwide basis).
  - A statement that the consumer reporting agency did not make the decision to take the adverse action and is unable to provide the consumer the specific reasons why the adverse action was taken.

- Provide the consumer an oral, written, or electronic notice of the consumer's right to obtain a free copy of the consumer report from the consumer reporting agency within 60 days of receiving notice of the adverse action, and the consumer's right to dispute the accuracy or completeness of any information in the consumer report with the consumer reporting agency.

Information Obtained from a Source Other Than a Consumer Reporting Agency

Section 615(b)(1), Adverse Action Based on Information Obtained from Third Parties Other than Consumer Reporting Agencies, provides that if a financial institution:

— Denies credit for personal, family, or household purposes involving a consumer, or;

— Increases the charge for such credit,

Partially or wholly on the basis of information obtained from a person other than a consumer reporting agency and bearing upon the consumer's creditworthiness, credit standing, credit capacity, character, general reputation, personal characteristics, or mode of living, the financial institution:

- At the time it communicates an adverse action to a consumer, must clearly and accurately disclose the consumer's right to file a written request for the reasons for the adverse action.

- If it receives such a request within 60 days after the consumer learns of the adverse action, must disclose, within a reasonable period of time, the nature of the adverse information. The financial institution should sufficiently detail the information to enable the consumer to evaluate its accuracy. The financial institution may, but need not, disclose the source of the information. In some instances, it may be impossible to identify the nature of certain information without also revealing the source.

Information Obtained from an Affiliate

Section 615(b)(2), Duties of Taking Certain Actions Based on Information Provided by Affiliate, provides that if a person, including a financial institution, takes an adverse action involving credit (taken in connection with a transaction initiated by a consumer), insurance or employment, based in whole or in part on information provided by an affiliate, the financial institution must notify the consumer that the information:

- Was furnished by a person related to the financial institution by common ownership or affiliated by common corporate control.

- Bears upon the consumer's creditworthiness, credit standing, credit capacity, character, general reputation, personal characteristics, or mode of living.

- Does not pertain solely to transactions or experiences between the consumer and the person furnishing the information.

- Does not include information in a consumer report.

The notification must inform the consumer of the action and that the consumer may obtain a disclosure of the nature of the information relied upon by making a written request within 60 days of transmittal of the adverse action notice. If the consumer makes such a request, the user must disclose the nature of the information received from the affiliate not later than 30 days after receiving the request.

Debt Collector Communications Concerning Identity Theft (Section 615(g))

This section, Debt Collector Communications Concerning Identity Thefts, has specific requirements for financial institutions that act as debt collectors, whereby they collect debts on behalf of a third party that is a creditor or other user of a consumer report. The requirements do not apply when a financial institution is collecting its own loans. When a financial institution is notified that any information relating to a debt that it is attempting to collect may be fraudulent or may be the result of identity theft, the financial institution must notify the third party of this fact. In addition, if the consumer, to whom the debt purportedly relates, requests information about the transaction, the financial institution must provide all of the information the consumer would otherwise be entitled to if the consumer wished to dispute the debt under other provisions of law applicable to the financial institution.

Risk-Based Pricing Notice (Section 615(h))

This section, Risk-Based Pricing Notice, 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. The agencies will provide this section of the examination procedures upon publication of final rules.

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

DUTIES OF USERS OF CREDIT REPORTS REGARDING ADDRESS DISCREPANCIES (12 CFR 571.82) (SECTION 605(H))

Section 605(h)(1) requires that, when providing a consumer report to a person that requests the report (a user), a nationwide consumer reporting agency (NCRA) must provide a notice of address discrepancy to the user if the address provided by the user in its request "substantially differs" from the address the NCRA has in the consumer's file. Section 605(h)(2) requires the federal banking agencies and the NCUA (the Agencies), and the FTC to prescribe regulations providing guidance regarding reasonable policies and procedures that a user of a consumer report should employ when such user has received a notice of address discrepancy. On November 9, 2007, the Agencies and the FTC published final rules in the Federal Register implementing this section (72 FR 63718).

Definitions

- Nationwide consumer reporting agency (NCRA). Section 603(p) defines a NCRA as one that compiles and maintains files on consumers on a nationwide basis and regularly engages in the practice of assembling or evaluating and maintaining the following two pieces of information about consumers residing nationwide for the purpose of furnishing consumer reports to third parties bearing on a consumer's credit worthiness, credit standing, or credit capacity:

  — Public record information.

  — Credit account information from persons who furnish that information regularly and in the ordinary course of business.

- Notice of address discrepancy (12 CFR 571.82(b)). A "notice of address discrepancy" is a notice sent to a user by an NCRA (section 603(p)) that informs the user of a substantial difference between the address for the consumer that the user provided to request the consumer report and the address(es) in the NCRA's file for the consumer.

Requirement to form a reasonable belief (12 CFR 571.82(c)). A user must develop and implement reasonable policies and procedures designed to enable the user to form a reasonable belief that the consumer report relates to the consumer whose report was requested, when the user receives a notice of address discrepancy in connection with a new or existing account.

The rules provide the following examples of reasonable policies and procedures for forming a reasonable belief that a consumer report relates to the consumer whose report was requested:

- Comparing information in the consumer report with information the user

  — has obtained and used to verify the consumer's identity as required by the Customer Identification Program rules (31 CFR 103.121);

  — maintains in its records; or

  — obtains from a third party; or

- Verifying the information in the consumer report with the consumer.

Requirement to furnish a consumer's address to an NCRA (12 CFR 571.82(d)). A user must develop and implement reasonable policies and procedures for furnishing to the NCRA an address for the consumer that the user has reasonably confirmed is accurate when the user does the following:

- Forms a reasonable belief that the report relates to the consumer whose report was requested.

- Establishes a continuing relationship with the consumer (i.e., in connection with a new account).

- Regularly, and in the ordinary course of business, furnishes information to the NCRA that provided the notice of address discrepancy.

  A user's policies and procedures for furnishing a consumer's address to an NCRA must require the user to furnish the confirmed address as part of the information it regularly furnishes to the NCRA during the reporting period when it establishes a continuing relationship with the consumer.

The rules also provide the following examples of how a user may reasonably confirm an address is accurate:

- Verifying the address with the consumer whose report was requested.

- Reviewing its own records.

- Verifying the address through third-party sources.

- Using other reasonable means.

FINANCIAL INSTITUTIONS AS FURNISHERS OF INFORMATION

Overview

The FCRA contains many responsibilities for financial institutions that furnish information to consumer reporting agencies. These requirements generally involve ensuring the accuracy of the data that is placed in the consumer reporting system. This examination module includes reviews of the various areas associated with furnishers of information. This module will not apply to financial institutions that do not furnish any information to consumer reporting agencies.

Furnishers of Information – General (Section 623)

We will amend this subsection, Furnishers of Information, upon completion of inter-agency guidance for institutions regarding the accuracy and integrity of information furnished to consumer reporting agencies. The FACT Act requires this guidance. An interagency working group will develop and publish guidance for comment, and will finalize this guidance at a later date. The agencies will also write rules regarding when furnishers must handle direct disputes from consumers.

In the interim period, institutions that furnish information to consumer reporting agencies must comply with the existing requirements in the FCRA. These requirements generally require accurate reporting and prompt investigation and resolution of accuracy disputes. The examination procedures within this subsection are based largely on the procedures last approved by the FFIEC Task Force on Consumer Compliance in March 2000, but have been revised to include new requirements under the 2003 amendments to the FCRA that do not require implementing regulations. Upon completion of the interagency guidance for the accuracy and integrity of information furnished to consumer reporting agencies, we will significantly revise this subsection.

Duties of furnishers to provide accurate information (Section 623(a)). This section states that a person, including a financial institution, may, but need not, specify an address for receipt of notices from consumers concerning inaccurate information. If the financial institution specifies such an address, then it may not furnish information relating to a consumer to any consumer reporting agency, if (a) the consumer notified the financial institution, at the specified address, that the information is inaccurate, and (b) the information is inaccurate. If the financial institution does not specify an address, then it may not furnish any information relating to a consumer to any consumer reporting agency if the financial institution knows or has reasonable cause to believe that the information is inaccurate.

When a financial institution that (regularly and in the ordinary course of business) furnishes information to one or more consumer reporting agencies about its transactions or experiences with any consumer determines that any such information is not complete or accurate, the financial institution must promptly notify the consumer reporting agency of that determination. The financial institution must provide corrections to that information or any additional information necessary to make the information complete and accurate to the consumer reporting agency. Further, the financial institution

thereafter must not furnish any information that remains incomplete or inaccurate to the consumer reporting agency.

If a consumer disputes the completeness or accuracy of any information a financial institution furnishes to a consumer reporting agency, that financial institution may not furnish the information to any consumer reporting agency without notice that the consumer disputes the information.

Voluntary closures of accounts (Section 623(a)(4)). This section requires a person, including a financial institution, who regularly and in the ordinary course of business furnishes information to a consumer reporting agency regarding one of its consumer credit accountholders, to notify the consumer reporting agency of the consumer's voluntary account closure. This notice is to be furnished to the consumer reporting agency as part of the regularly furnished information for the period in which the account is closed.

Notice involving delinquent **accounts** (Section 623(a)(5)). This section requires that a person, including a financial institution, that furnishes information to a consumer reporting agency about a delinquent account placed for collection, charged off, or subjected to any similar action, must, not later than 90 days after furnishing the information to the consumer reporting agency, notify the consumer reporting agency of the month and year of the commencement of the delinquency that immediately preceded the action.

Duties upon notice of dispute (Section 623(b)). This section requires that whenever a financial institution receives a notice of dispute from a consumer reporting agency regarding the accuracy or completeness of any information the financial institution provided to a consumer reporting agency pursuant to section 611 (Procedure in Case of Disputed Accuracy), that financial institution must, pursuant to § 623(b):

- Conduct an investigation regarding the disputed information.
- Review all relevant information the consumer reporting agency provided along with the notice.
- Report the results of the investigation to the consumer reporting agency.
- If the investigation finds the information is incomplete or inaccurate, report those results to all nationwide consumer reporting agencies to which the financial institution previously provided the information.
- If the disputed information is incomplete, inaccurate, or not verifiable by the financial institution, it must promptly, for purposes of reporting to the consumer reporting agency do one of the following:

  — Modify the item of information.

— Delete the item of information.

— Permanently block the reporting of that item of information.

The financial institution must complete the required investigations, reviews, and reports within 30 days. The financial institution may extend the time period for 15 days if a consumer reporting agency receives additional relevant information from the consumer.

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

This section, Prevention of Re-Pollution of Consumer Reports, has specific requirements for furnishers of information, including financial institutions, to a consumer reporting agency that received notice from a consumer reporting agency that furnished information may be fraudulent as a result of identity theft. Section 605B, Block of Information Resulting From Identity Theft, requires consumer reporting agencies to notify furnishers of information, including financial institutions, that the information may be the result of identity theft, an identity theft report has been filed, and that a block has been requested. Upon receiving such notice, § 623(a)(6) requires financial institutions to establish and follow reasonable procedures to ensure that it does not re-report this information to the consumer reporting agency, thus "re-polluting" the victim's consumer report.

Section 615(f), Prohibition on Sale or Transfer of Debt Caused by Identity Theft, also prohibits a financial institution from selling or transferring debt caused by an alleged identity theft.

Negative Information Notice (Section 623(a)(7))

This section, Negative Information Notice, requires a financial institution to provide consumers with a notice either before it provides negative information to a nationwide consumer reporting agency, or within 30 days after reporting the negative information.

Negative information. For these purposes, negative information means any information concerning a customer's delinquencies, late payments, insolvency, or any form of default.

Nationwide consumer reporting agency. Section 603(p) of the FCRA defines a nationwide consumer reporting agency as a "consumer reporting agency that compiles and maintains files on consumers on a nationwide basis." It defines this type of consumer reporting agency as one that regularly assembles or evaluates, and maintains, each of the following regarding consumers residing nationwide for the purpose of furnishing consumer reports to third parties bearing on a consumer's creditworthiness, credit standing, or credit capacity:

- Public Record Information.

- Credit account information from persons who furnish that information regularly and in the ordinary course of business.

Institutions may provide this disclosure on or with any notice of default, any billing statement, or any other materials provided to the customer, as long as the notice is clear and conspicuous. Institutions may also choose to provide this notice to all customers as an abundance of caution. However, financial institutions may not include this notice in the initial disclosures provided under § 127(a) of the Truth in Lending Act.

Model text. As required by the FCRA, the Federal Reserve Board developed the following model text that institutions can use to comply with these requirements. The first model contains text an institution can use when it provides a notice before furnishing negative information. The second model form contains text to use when an institution provides notice within 30 days after reporting negative information:

Notice prior to communicating negative information (Model B-1):

"We may report information about your account to credit bureaus. Late payments, missed payments, or other defaults on your account may be reflected in your credit report."

Notice within 30 days after communicating negative information (Model B-2):

"We have told a credit bureau about a late payment, missed payment, or other default on your account. This information may be reflected in your credit report."

Use of the model form(s) is not required; however, proper use of the model forms provides a financial institution with a safe harbor from liability. A financial institution may make certain changes to the language or format of the model notices without losing the safe harbor from liability provided by the model notices. The changes to the model notices may not be so extensive as to affect the substance, clarity, or meaningful sequence of the language in the model notices. A financial institution making extensive revisions will lose the safe harbor from liability that the model notices provide. Acceptable changes include:

- Rearranging the order of the references to "late payment(s)," or "missed payment(s)."
- Pluralizing the terms "credit bureau," "credit report," and "account."
- Specifying the particular type of account on which it may furnish information, such as "credit card account."
- Rearranging in Model Notice B-1 the phrases "information about your account" and "to credit bureaus" such that it would read, "We may report to credit bureaus information about your account."

MODULE 5: CONSUMER ALERTS AND IDENTITY THEFT PROTECTIONS

Overview

The FCRA contains several provisions for both consumer reporting agencies and users of consumer reports, including financial institutions, that are designed to help combat identity theft. This module applies to financial institutions that are not consumer reporting agencies, but are users of consumer reports.

Two primary requirements exist: first, a user of a consumer report that contains a fraud or active duty alert must take steps to verify the identity of an individual to whom the consumer report relates, and second, a financial institution must disclose certain information when consumers allege that they are the victims of identity theft.

Fraud and Active Duty Alerts (Section 605A(h))

Initial fraud and active duty alerts. Consumers who suspect that they may be the victims of fraud including identity theft may request nationwide consumer reporting agencies to place initial fraud alerts in their consumer reports. These alerts must remain in a consumer's report for no less than 90 days. In addition, members of the armed services who are called to active duty may also request that active duty alerts be placed in their consumer reports. Active duty alerts must remain in these service members' files for no less than 12 months.

Section 605A(h)(1)(B), Limitations on Use of Information for Credit Extensions, requires users of consumer reports, including financial institutions, to verify a consumer's identity if a consumer report includes a fraud or active duty alert. Unless the financial institution uses reasonable policies and procedures to form a reasonable belief that it knows the identity of the person making the request, the financial institution may not:

- Establish a new credit plan or extension credit (other than under an open-end credit plan) in the name of the consumer.
- Issue an additional card on an existing account.
- Increase a credit limit.

Extended Alerts. Consumers who allege that they are the victim of an identity theft may also place an extended alert, which lasts seven years, on their consumer report. Extended alerts require consumers to submit identity theft reports and appropriate proof of identity to the nationwide consumer reporting agencies.

Section 605A(h)(2)(B), Limitation on Users, requires a financial institution that obtains a consumer report that contains an extended alert to contact the consumer in person or by the method the consumer lists in the alert prior to performing any of the three actions listed above.

Information Available to Victims (Section 609(e))

This section, Information Available to Victims, requires a financial institution to provide records of fraudulent transactions to victims of identity theft within 30 days after the receipt of a request for the records. These records include the application and business transaction records under the control of the financial institution whether maintained by the financial institution or another person on behalf of the institution (such as a service provider). The financial institution should provide this information to any of the following:

- The victim.
- Any federal, state, or local government law enforcement agency or officer specified by the victim in the request.
- Any law enforcement agency investigating the identity theft that was authorized by the victim to take receipt of these records.

The victim must make the request for the records in writing and send it to the financial institution at the address specified by the financial institution for this purpose. The financial institution may ask the victim to provide information, if known, regarding the date of the transaction or application, and any other identifying information such as an account or transaction number.

Unless the financial institution has a high degree of confidence that it knows the identity of the victim making the request for information, the financial institution must take prudent steps to positively identify the person before disclosing any information. Proof of identity can include any of the following:

- A government-issued identification card.
- Personally identifying information of the same type that was provided to the financial institution by the unauthorized person.
- Personally identifiable information that the financial institution typically requests from new applicants or for new transactions.

At the election of the financial institution, the victim must also provide the financial institution with proof of an identity theft complaint, which may consist of a copy of a police report evidencing the claim of identity theft and a properly completed affidavit. The affidavit can be either the standardized

affidavit form prepared by the Federal Trade Commission (published in April 2005 in 70 Federal Register 21792), or an "affidavit of fact" that is acceptable to the financial institution for this purpose.

When these conditions are met, the financial institution must provide the information at no charge to the victim. However, the financial institution is not required to provide any information if, acting in good faith, the financial institution determines any of the following:

- Section 609(e) does not require disclosure of the information.
- The financial institution does not have a high degree of confidence in knowing the true identity of the requestor, based on the identification and/or proof provided.
- The request for information is based on a misrepresentation of fact by the requestor.
- The information requested is Internet navigational data or similar information about a person's visit to a web site or online service.

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

Section 615(e) requires the federal banking agencies and the NCUA (the Agencies) as well as the FTC to prescribe regulations and guidelines for financial institutions and creditors[18] regarding identity theft. On November 9, 2007, the Agencies published final rules and guidelines in the Federal Register implementing this section (72 FR 63718).

Definitions (12 CFR 571.90(b). The following regulatory definitions pertain to the regulations regarding identify theft red flags.

- An "**account**" is a continuing relationship established by a person with a financial institution to obtain a product or service for personal, family, household or business purposes. An account includes the following:
  - An extension of credit, such as the purchase of property or services involving a deferred payment.
  - A deposit account.
- The "**board of directors**" includes, for a branch or agency of a foreign bank, the managing official in charge of the branch or agency and, for any other creditor that does not have a board of directors, a designated employee at the level of senior management.

[18] For purposes of these examination procedures, "financial institutions and creditors" are referred to jointly as "financial institutions."

- A "**covered account**" is:

  — An account that a financial institution offers or maintains, primarily for personal, family, or household purposes, that involves or is designed to permit multiple payments or transactions, such as a credit card account, mortgage loan, automobile loan, margin account, cell phone account, utility account, checking account or savings account.

  — Any other account offered or maintained by the financial institution for which there is a reasonably foreseeable risk to customers or the safety and soundness of the financial institution from identity theft, including financial, operational, compliance, reputation or litigation risks.

- A "**customer**" is a person that has a "covered account" with a financial institution.

- "**Identity theft**" means a fraud committed or attempted using the identifying information of another person without authority. "Identifying information" means any name or number that may be used alone or in conjunction with any other information to identify a specific person (16 CFR 603.2).

- A "**red flag**" is a pattern, practice or specific activity that indicates the possible existence of identity theft.

- A "**service provider**" is a person that provides a service directly to a financial institution.

Periodic identification of covered accounts (12 CFR 571.90(c)). Each financial institution must periodically determine whether it offers or maintains covered accounts. As part of this determination, the financial institution must conduct a risk assessment to determine whether it offers or maintains covered accounts taking into consideration:

- The methods it provides to open its accounts.

- The methods it provides to access its accounts.

- Its previous experiences with identity theft.

Establishment of an identity theft prevention program (Program) (12 CFR 571.90 (d)). A financial institution must develop and implement a written Program designed to detect, prevent, and mitigate identity theft in connection with the opening of a "covered account" or any existing "covered account." The Program must be tailored to the financial institution's size and complexity and the nature and scope of its operations and must contain "reasonable policies and procedures" to:

- Identify red flags for the covered accounts the financial institution offers or maintains and incorporate those red flags into the Program.

- Detect red flags that have been incorporated into the Program.
- Respond appropriately to any red flags that are detected to prevent and mitigate identity theft.
- Ensure the Program (including the red flags determined to be relevant) is updated periodically, to reflect changes in risks to customers and to the safety and soundness of the financial institution from identity theft.

Administration of the Program (12 CFR 571.90 (e)). A financial institution must provide for the continued administration of the Program by doing all of the following:

- Obtaining approval of the initial written Program by the board of directors or an appropriate committee of the board.
- Involving the board of directors, a committee of the board, or an employee at the level of senior management, in the oversight, development, implementation, and administration of the Program.
- Training staff, as necessary, to implement the Program effectively.
- Exercising appropriate and effective oversight of service provider arrangements.

Guidelines (12 CFR 571.90(f)). Each financial institution that is required to implement a program also must consider the guidelines in Appendix J of the regulation and include in its Program guidelines that are appropriate. The guidelines are intended to assist financial institutions in the formulation and maintenance of a Program that satisfies the regulatory requirements. A financial institution may determine that a particular guideline is not appropriate to incorporate into its Program; however, the financial institution must have policies and procedures that meet the specific requirements of the rules.

A financial institution may incorporate into its Program, as appropriate, its existing policies, procedures, and other arrangements that control reasonably foreseeable risks to customers and to the safety and soundness of the financial institution from identity theft.

Illustrative examples of red flags are located in Supplement A to Appendix J of the regulation. A financial institution is not required to use the examples, nor will it need to justify its failure to include in its Program a specific red flag from the list of examples. However, the financial institution must be able to account for the overall effectiveness of its Program that is appropriate to its size and complexity and the nature and scope of its activities.

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

Section 615(e)(1)(C) requires the Agencies and the FTC to prescribe regulations for debit and credit card issuers regarding the assessment of the validity of address changes for existing accounts. The regulations require card issuers to have procedures to assess the validity of an address change if the card issuer receives a notice of change of address for an existing account, and within a short period of time (during at least the first 30 days) receives a request for an additional or replacement card for the same account. On November 9, 2007, the Agencies and the FTC published final rules in the Federal Register implementing this section (72 FR 63718).

Definitions (12 CFR 571.91(b)). The following definitions pertain to the rules governing the duties of card issuers regarding changes of address:

- A "**cardholder**" is a consumer who has been issued a credit or debit card.

- "**Clear and conspicuous**" means reasonably understandable and designed to call attention to the nature and significance of the information presented.

Address validation requirements (12 CFR 571.91(c)). A card issuer must establish and implement 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. In such situations, the card issuer must not issue an additional or replacement card until it assesses the validity of the change of address in accordance with its policies and procedures.

The policies and procedures must provide that the card issuer will:

- Notify the cardholder of the request for an additional or replacement card

  — at the cardholder's former address; or

  — by any other means of communication that the card issuer and the cardholder have previously agreed to use; and

- Provide to the cardholder a reasonable means of promptly reporting incorrect address changes; or

  — Assess the validity of the change of address according to the procedures the card issuer has established as a part of its Identity Theft Prevention Program (12 CFR 571.90).

Alternative timing of address validation (12 CFR 571.91(d)). A card issuer may satisfy the requirements of these rules prior to receiving any request for an additional or replacement card by validating an address when it receives an address change notification.

Form of notice (12 CFR 571.91(e)). Any written or electronic notice that a card issuer provides to satisfy these rules must be clear and conspicuous and provided separately from its regular correspondence with the cardholder.

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

Background

The Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003 (CAN-SPAM or Act)[19], charged the Federal Trade Commission (FTC) with issuing implementing regulations.[20] The FTC issued regulations, which became effective March 28, 2005, that provide criteria to determine the *primary purpose* of electronic mail (e-mail) messages. The FTC also issued regulations that contain criteria pertaining to warning labels on sexually oriented materials, which became effective May 19, 2004.

The goals of the Act are to:

- Reduce spam and unsolicited pornography by prohibiting senders of unsolicited commercial e-mail messages from disguising the source and content of their messages.

- Give consumers the choice to cease receiving a sender's unsolicited commercial e-mail messages.

Section 8 of the Federal Deposit Insurance Act grants compliance authority to the Federal Deposit Insurance Corporation, the Office of the Comptroller of the Currency, the Federal Reserve Board, and the Office of Thrift Supervision. The Federal Credit Union Act 12 USC 1751 grants authority to the National Credit Union Association.

The FTC researched and determined that a "Do Not Spam" registry (similar to the highly effective "Do Not Call" registry) would not be effective or practicable at this time.

Key Definitions

Affirmative consent (usage: commercial e-mail messages):

- The recipient expressly consents to receive the message, either in response to a clear and conspicuous request for such consent or at the recipient's own initiative; and

[19] 15 USC 7701 - 7713

[20] Final rules relating to the established criteria for determining when the primary purpose of an e-mail message is commercial were published in the *Federal Register* on January 19, 2005 (70 FR 3110). Final rules relating to governing the labeling of commercial e-mail containing sexually oriented material were published in the *Federal Register* on April 19, 2004 (69 FR 21024). A notice of proposed rulemaking relating to definitions, implementation and reporting requirements under the CAN-SPAM Act was published in the *Federal Register* on May 12, 2005 (70 FR 25426).

- If the message is from a party other than the party to which the recipient communicated such consent, at which time the recipient was given clear and conspicuous notice that the recipient's e-mail address could be transferred to such other party for the purpose of initiating commercial e-mail messages.

Commercial e-mail message: Any e-mail message the *primary purpose* of which is to advertise or promote for a commercial purpose, a commercial product or service (including content on the Internet). An e-mail message would not be considered to be a commercial e-mail message solely because such message includes a reference to a commercial entity that serves to identify the sender, or a reference or link to an Internet Web site operated for a commercial purpose.

Dictionary attacks: Obtaining e-mail addresses by using automated means to generate possible e-mail addresses by combining names, letters, or numbers into numerous permutations.

Harvesting: Obtaining e-mail addresses using automated means from an Internet Web site or proprietary online service operated by another person, where such service/person, at the time the address was obtained, provided a notice stating that the operator of such Web site or online service would not give, sell, or otherwise transfer electronic addresses.

Header information: The source, destination, and routing information attached to the beginning of an e-mail message, including the originating domain name and originating e-mail address.

Hijacking: The use of automated means to register for multiple e-mail accounts or online user accounts from which to transmit, or enable another person to transmit, a commercial e-mail message that is unlawful.

Initiate: To originate, transmit, or to procure the origination or transmission of such message but shall not include actions that constitute routine conveyance. For purposes of the Act, more than one person may be considered to have initiated the same message.

Primary purpose: The FTC's regulations provide further clarification regarding determination of whether an e-mail message has "commercial" promotion as its *primary purpose*: (16 CFR 316.3)

- The primary purpose of an e-mail message is deemed commercial if it contains only the commercial advertisement or promotion of a commercial product or service (commercial content).

- The primary purpose of an e-mail message is deemed commercial if it contains both commercial content and "transactional or relationship" content (see below for definition) if either of the following occurs:

  — A recipient reasonably interpreting the subject line of the e-mail message would likely conclude that the message contains commercial content.

— The e-mail message's "transactional or relationship" content does not appear in whole or substantial part at the beginning of the body of the message.

- The primary purpose of an e-mail message is deemed commercial if it contains both commercial content as well as content that is not transactional or relationship content if a recipient reasonably interpreting either:

  — The subject line of the e-mail message would likely conclude that the message contains commercial content.

  — The body of the message would likely conclude that the primary purpose of the message is commercial.

- The primary purpose of an e-mail message is deemed transactional or relationship (noncommercial) if it contains only "transactional or relationship" content.

Recipient: An authorized user of the electronic mail address to which the message was sent or delivered.

Sender: A person who initiates an e-mail message and whose product, service, or Internet website is advertised or promoted by the message.

Sexually oriented material: Any material that depicts sexually explicit conduct unless the depiction constitutes a small and insignificant part of the whole.

Transactional or relationship e-mail message: An e-mail message with the primary purpose of facilitating, completing, or confirming a commercial transaction that the recipient previously agreed to enter into; to provide warranty, product recall, or safety or security information; or subscription, membership, account, loan, or other information relating to an ongoing purchase or use.

General Requirements of the CAN-SPAM Statute:

- Prohibits the use of 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 because the person initiating the message knowingly uses another protected computer to relay or retransmit the message for purposes of disguising its origin.

- Prohibits the use of deceptive subject headings (Section 7704(a)(2)).

- Requires a functioning e-mail return address or other Internet-based response mechanism (Section 7704(a)(3)).

- Requires the discontinuation of commercial e-mail messages within 10 business days after receipt of opt-out notification from recipient (Section 7704(a)(4)).

- Requires 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)).

- Prohibits address harvesting and dictionary attacks (Section 7704(b)(1)).

- Prohibits hijacking (Section 7704(b)(2)).

- Prohibits any person from knowingly relaying or retransmitting a commercial e-mail message that is unlawful (Section 7704(b)(3)).

- Requires warning labels (in the subject line and within the message body) on commercial e-mail messages containing sexually oriented material (Section 7704(d)).

- Prohibits a person from promoting, or allowing the promotion of, that person's trade or business, or goods, products, property, or services in an unlawful commercial e-mail message (Section 7705)(a)).

TELEPHONE CONSUMER PROTECTION ACT AND JUNK FAX PREVENTION ACT

BACKGROUND

The Federal Communications Commission (FCC) issued regulations that establish a national "Do-Not-Call" registry[21] and other requirements pursuant to the Telephone Consumer Protection Action of 1991 (TCPA)[22]. The FCC regulations detail certain requirements for entities making telemarketing calls, such as complying with do-not-call list requirements, keeping to a maximum number of abandoned calls, and transmitting caller ID information. The regulations also detail the FCC's unsolicited facsimile advertising requirements, which were modified by the Junk Fax Prevention Act of 2005 and became effective on July 9, 2005. The FCC regulations were generally effective as of October 1, 2003.

The FCC regulations apply to banks, insurance companies, credit unions, and savings associations. The Federal Trade Commission's (FTC) telemarketing regulations parallel the FCC regulations[23] and apply to all other business entities, including third parties acting as agent or on behalf of a financial institution.

Key Definitions

Abandoned call – A telephone call that is not transferred to a live sales agent within two seconds of the recipient's completed greeting.

Automatic Telephone Dialing System and Autodialer – Equipment that has the capacity to store or produce telephone numbers to be called using a random or sequential number generator and the capability to dial such numbers.

Established business relationship for the purpose of telephone solicitations – A prior or existing relationship between a person or entity and a residential subscriber based on the subscriber's purchase or transaction with the entity within the 18 months immediately preceding the date of the telephone call or on the basis of the subscriber's inquiry or application regarding products or services offered by the entity within the three months immediately preceding the date of the call, and neither party has previously terminated the relationship. The established business relationship does not extend

[21] The Federal Trade Commission (FTC) maintains the national Do-Not-Call registry adopted by the FCC.

[22] 47 USC 227; The Federal Communications Commission's final regulations were published in the *Federal Register* on July 25, 2003 (68 FR 44144). The regulations were modified several times. *See* 68 FR 59131 (Oct. 14, 2003); 69 FR 60311 (Oct. 8, 2004); 70 FR 19337 (Apr.13, 2005); 71 FR 25977 (May 3, 2006); 71 FR 56893 (Sept. 28, 2006); 71 FR 75122 (Dec. 14, 2006).

[23] The Federal Trade Commission final regulations were published in the *Federal Register* on January 29, 2003 (68 FR 4580).

to an affiliate unless the subscriber would reasonably expect them to be included given the nature and type of goods or services offered by the affiliate and the identity of the affiliates.

Established business relationship for purposes of sending of facsimile advertisements – A prior or existing relationship formed by a voluntary two-way communication between a person or entity and a business or residential subscriber, on the basis of an inquiry, application, purchase, or transaction by the business or residential subscriber regarding products or services offered by such person or entity, which relationship has not been previously terminated by either party.

Facsimile broadcaster – A person or entity that transmits messages to telephone facsimile machines on behalf of another person or entity for a fee.

Residential Subscriber – An individual who has contracted with a common carrier to provide telephone exchange service at a personal residence.

Seller – The person or entity on whose behalf a telephone call or message is initiated for the purpose of encouraging purchase or rental of, or investment in, property, goods, or services that is transmitted to any person.

Telemarketer – The person or entity that initiates a telephone call or message for the purpose of encouraging the purchase or rental of, or investment in, property, goods, or services that is transmitted to any person.

Telemarketing – The initiation of a telephone call or message for the purpose of encouraging the purchase or rental of, or investment in, property, goods, or services that is transmitted to any person.

Telephone facsimile machine – Equipment which has the capacity to transcribe text or images, or both, from paper into an electronic signal and to transmit that signal over a regular telephone line, or to transcribe text or images (or both) from an electronic signal received over a regular telephone line onto paper.

Telephone solicitation – The initiation of a telephone call or message for the purpose of encouraging the purchase or rental of, or investment in, property, goods, or services that is transmitted to any person. Telephone solicitation *does not* include a call or message to any person with that person's prior express permission, to any person with whom the caller has an established business relationship, or on behalf of a tax-exempt nonprofit organization.

Unsolicited advertisement – Any material that advertises the commercial availability or quality of any property, goods, or services that is transmitted to any person without that person's prior express invitation or permission.

General Requirements of TCPA

The FCC regulations that implement the Telephone Consumer Protection Act of 1991 provide consumers with options to avoid unwanted telephone solicitations. The regulations address the following:

- The FCC's adoption of a national "Do-Not-Call" registry expands coverage to entities not regulated by the FTC.[24]

- Under the FCC's rules, no seller, or entity telemarketing on behalf of the seller, can initiate a telephone solicitation to a residential telephone subscriber who has registered his or her telephone number on the national *do-not-call* registry. A safe harbor exists for an inadvertent violation of this requirement if the telemarketer can demonstrate that the violation was an error and that its routine practices include:

  — Written procedures.

  — *Training of personnel.*

  — Maintenance and recording of a list of telephone numbers excluded from contact.

  — Use of a version of the national *do-not-call* registry obtained no more than 31 days prior to the date any call is made (with records to document compliance).

  — *A process* to ensure that it does not sell, rent, lease, purchase, or use the do-not-call database in any manner except in compliance with FCC regulations (47 CFR 64.1200(c)(2)(i)) and applicable state or federal law.

- Companies must maintain company-specific do-not-call lists reflecting the names of customers with established business relationships who have requested to be excluded from telemarketing. Such requests *must be honored* for five years (47 CFR 64.1200(d)(6)).

- Telemarketing calls can be made only between the hours of 8 a.m. and 9 p.m. (local time at the called party's location) (47 CFR 64.1200(c)(1)).

- All telemarketers must comply with limits on "abandoned calls" and employ other consumer-friendly practices when using automated telephone-dialing equipment. A telemarketer must abandon no more than three percent of calls answered by a person and must deliver a

[24] By doing so, the FCC asserts its considerably broader jurisdiction over telemarketing than the FTC. Specifically, telemarketing by in-house employees of banks, savings associations, and credit unions, as well as other areas of commerce, are covered by the FCC's authority.

prerecorded identification message when abandoning a call. Two or more telephone lines of a multi-line business are not to be called simultaneously. Telemarketers must not disconnect an unanswered telemarketing call prior to at least 15 seconds or four rings. All businesses that use autodialers to sell services must maintain records documenting compliance with call abandonment rules (47 CFR 64.1200(a)(4),(5),(6)).

- All prerecorded messages, whether delivered by automated dialing equipment or not, must identify the name of the entity responsible for initiating the call, along with the telephone number of that entity (this cannot be a 900 number or other number for which charges exceed local or long distance transmission charges) and must provide a valid number for the subscriber to call that can be used during normal business hours to *request* not to be called again (47 CFR 64.1200(b)).

- All persons or entities that initiate calls for telemarketing purposes to a residential telephone subscriber must have procedures for maintaining a list of persons who request not to receive telemarketing calls made by or on behalf of that person or entity. The procedures must meet the following minimum standards.

  — *Written policy* – The institution must have a written policy, available on demand, for maintaining a do-not-call list.

  — *Training of personnel* – The institution must train personnel engaged in telemarketing about the existence and use of the do-not-call list.

  — *Recording and honoring of do-not-call requests* – The institution must start honoring do-not-call requests within 30 days after they are made. 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.

  — *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.

  — *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.

  — *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)(1)-(6)).

- All telemarketers must transmit caller ID information, when available, and must refrain from blocking any such transmission(s) to the consumer (47 CFR 64.1601(e)).[25]

- Unsolicited fax transmissions must not be sent unless the sender has *both* (a) an established business relationship with the recipient; and (b) the number of the facsimile machine, received through the recipient's voluntary communication of that number or through a directory, advertisement or Internet site to which the recipient voluntarily made its facsimile number available for public dissemination (47 CFR 64.1200(a)(3)).

- Such fax transmissions must contain a notice informing the recipient of the right to opt out of receiving future unsolicited fax advertisements and the means by which the recipient may do so (47 CFR 64.1200(a)(3)(iii)).

- The sender must honor requests to opt out that meet the criteria detailed in the regulation (47 CFR 64.1200(a)(3)(v), (vi)).

- Tax-exempt nonprofit organizations are not required to comply with the do-not-call provisions of the TCPA (47 CFR 64.1200(d)(7)).

REFERENCES

Law

15 USC 1681 et seq.	Fair Credit Reporting Act
15 USC 7701 – 7713	Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003
47 USC 227	Telephone Consumer Protection Act and Junk Fax Protection Act

Regulations

12 CFR Part 571	Fair Credit Reporting
16 CFR Part 310	Telemarketing Sales Rule
16 CFR Part 316	Rules Implementing the CAN –SPAM Act of 2003

[25] The rule sets forth the technical information that must be made available (subject to differing technologies). The FCC stated that Caller ID information should also increase accountability and provide an important resource for the FCC and FTC in pursuing enforcement actions against TCPA violators (68 FR 44166, July 25, 2003).

47 CFR Parts 64 and 68	Rules and Regulations Implementing the Telephone Consumer Protection Act of 1991

Examination Handbook

Section 1100	Compliance Oversight Examination Program

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 #:	

FCRA Statutory and Regulatory Matrix

The table below contains the statutory or regulatory cites for each provision of the FCRA applicable to financial institutions that are not consumer reporting agencies[1]. Some of the requirements are self-executing by the statute, while others are contained in interagency regulations, while others still are contained in regulations published by only one or two of the regulatory agencies. One requirement is subject to regulations that are not yet finalized and thus is listed as to-be-determined (TBD) in the table below. The regulatory agencies are listed in the first horizontal line and the various compliance responsibilities are presented in the order that they appear in the various examination modules in the first column. Financial institutions are subject to the list of cites in the column containing their primary federal regulator.

Compliance Responsibility	Federal Reserve Board	FDIC	OCC	OTS	NCUA
Module 1					
Obtaining Consumer Reports	§604 and §606 of the FCRA	§604 and §606 of the FCRA	§604 and §606 of the FCRA	§604 and §606 of the FCRA	§604 and §606 of the FCRA
Module 2					
Information Sharing & Affiliate Sharing Opt Out	§603(d) of the FCRA	§603(d) of the FCRA	§603(d) of the FCRA	§603(d) of the FCRA	§603(d) of the FCRA
Protection of Medical Information	Part 222 of FRB Regulation V	Part 334 of FDIC Regulations	Part 41 of OCC Regulations	Part 571 of OTS Regulations	Part 717 of NCUA Regulations
Affiliate Marketing Opt Out	Part 222 of FRB Regulation V	Part 334 of FDIC Regulations	Part 41 of OCC Regulations	Part 571 of OTS Regulations	Part 717 of NCUA Regulations
Module 3					
Employment Disclosures	§604(b)(2) of the FCRA	§604(b)(2) of the FCRA	§604(b)(2) of the FCRA	§604(b)(2) of the FCRA	§604(b)(2) of the FCRA
Prescreened Consumer Reports	§604(c) & §615(d) of the FCRA and FTC Regulations Parts 642 and 698	§604(c) & §615(d) of the FCRA and FTC Regulations Parts 642 and 698	§604(c) & §615(d) of the FCRA and FTC Regulations Parts 642 and 698	§604(c) & §615(d) of the FCRA and FTC Regulations Parts 642 and 698	§604(c) & §615(d) of the FCRA and FTC Regulations Parts 642 and 698
Truncation of Credit and Debit Card Account Numbers	§605(g) of the FCRA	§605(g) of the FCRA	§605(g) of the FCRA	§605(g) of the FCRA	§605(g) of the FCRA
Credit Score Disclosures	§609(g) of the FCRA	§609(g) of the FCRA	§609(g) of the FCRA	§609(g) of the FCRA	§609(g) of the FCRA
Adverse Action Disclosures	§615 of the FCRA	§615 of the FCRA	§615 of the FCRA	§615 of the FCRA	§615 of the FCRA
Debt Collector Communications	§615(g) of the FCRA	§615(g) of the FCRA	§615(g) of the FCRA	§615(g) of the FCRA	§615(g) of the FCRA
Risk-Based Pricing Notice	TBD	(NA)	(NA)	(NA)	(NA)
Module 4					
Duties of Users of Credit Reports Regarding Address Discrepancies	§605(h) of the FCRA	§605(h) of the FCRA	§605(h) of the FCRA	§605(h) of the FCRA	§605(h) of the FCRA
Furnishers of Information – General	§623 of the FCRA	§623 of the FCRA	§623 of the FCRA	§623 of the FCRA	§623 of the FCRA
Prevention of Re-Pollution of Reports	§623(a)(6) of the FCRA	§623(a)(6) of the FCRA	§623(a)(6) of the FCRA	§623(a)(6) of the FCRA	§623(a)(6) of the FCRA
Negative Information Notice	§623(a)(7) of the FCRA and Appendix B of Part222 of FRB Regulation V	§623(a)(7) of the FCRA and Appendix B of Part222 of FRB Regulation V	§623(a)(7) of the FCRA and Appendix B of Part222 of FRB Regulation V	§623(a)(7) of the FCRA and Appendix B of Part222 of FRB Regulation V	§623(a)(7) of the FCRA and Appendix B of Part222 of FRB Regulation V

[1] Other FCRA provisions applicable to non-consumer reporting agency banks, thrifts, and credit unions are covered in other examinations, such as risk management, information technology, etc. and are thus not part of this guidance. These provisions include Section 628 (Disposal Rules).

Compliance Responsibility	Federal Reserve Board	FDIC	OCC	OTS	NCUA
Module 5					
Fraud & Active Duty Alerts	§605A(h)(2)(B) of the FCRA	§605A(h)(2)(B) of the FCRA	§605A(h)(2)(B) of the FCRA	§605A(h)(2)(B) of the FCRA	§605A(h)(2)(B) of the FCRA
Information Available to Victims	§609(e) of the FCRA	§609(e) of the FCRA	§609(e) of the FCRA	§609(e) of the FCRA	§609(e) of the FCRA
Duties Regarding the Detection, Prevention, and Mitigation of Identify Theft	§615(e) of the FCRA	§615(e) of the FCRA	§615(e) of the FCRA	§615(e) of the FCRA	§615(e) of the FCRA