

Compliance Corner



FEDERAL RESERVE BANK OF PHILADELPHIA

Regulatory Expectations for Compliance with the Fair Credit Reporting Act

by Eddie L. Valentine, Supervising Examiner

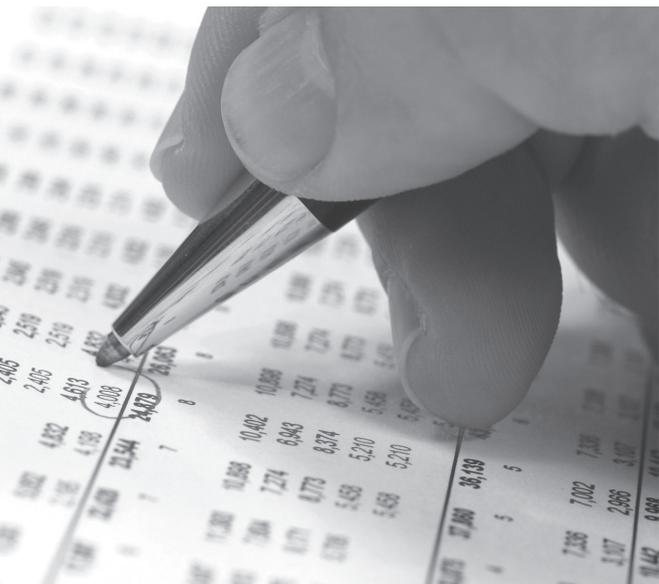
This article summarizes the revised examination procedures for the Fair Credit Reporting Act (FCRA) that the Federal Financial Institutions Examination Council (FFIEC) Task Force on Consumer Compliance approved on November 14, 2005. Among other things, the revised procedures address provisions of the FCRA that were substantially amended by the Fair and Accurate Credit Transactions Act of 2003 (FACT Act).¹ The revised examination procedures replace the interim guidance for reviewing compliance, which was effective December 1, 2004. This article will help financial institutions prepare for their next compliance examination by understanding the revised procedures examiners will be utilizing to verify compliance with the FCRA.

Background and Summary of FCRA and FACT Act

The FCRA imposes significant responsibilities on business entities that qualify as consumer reporting agencies and lesser responsibilities on those that do not. A consumer reporting agency is defined as any person who regularly engages in the practice of assembling or evaluating consumer credit information for the purpose of selling consumer reports to third parties. Financial institutions are generally not considered consumer reporting agencies; however, if they engage in certain types of information sharing practices, they can be deemed a consumer reporting agency.

In addition to the requirements for financial institutions acting as consumer reporting agencies, FCRA
continued on page CC8

¹ The full text of the revised procedures is available on the Board of Governors' website at <www.federalreserve.gov/board-docs/caletters/2005/0509/CA05-9Attach1.pdf>.



CC2

Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice

CC4

The New Intermediate Small Bank CRA Evaluation

CC7

Compliance Alert: Truth in Lending Appeals Court Decision

CC11

Educating Your Customer

Compliance Corner is published quarterly and is distributed via *SRC Insights* to institutions supervised by the Federal Reserve Bank of Philadelphia. *SRC Insights* is available on the Federal Reserve Bank's website at www.philadelphiafed.org. Suggestions, comments, and requests for back issues are welcome in writing, by telephone (215-574-3760), or by e-mail (cynthia.course@phil.frb.org). Please address all correspondence to: Cynthia L. Course, Federal Reserve Bank of Philadelphia, SRC - 7th Floor, Ten Independence Mall, Philadelphia, PA 19106-1574.

Editor.....Cynthia L. Course
Associate Editor.....Joanne Branigan
Designer.....Dianne Hallowell

The views expressed in this newsletter are those of the authors and are not necessarily those of this Reserve Bank or the Federal Reserve System.



Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice

by Kenneth J. Benton, *Consumer Regulations Specialist*

The Gramm-Leach-Bliley Act (GLB act), the landmark banking legislation that ended the Depression-era laws separating banking, insurance, and brokerage activities, also includes provisions designed to safeguard customer information held by financial institutions. Section 501(b) of the GLB act requires federal banking agencies—namely, the Board of Governors of the Federal Reserve System, the Office of the Comptroller of the Currency, the Federal Deposit Insurance Corporation, and the Office of Thrift Supervision—to establish standards for the financial institutions they supervise to protect the security and confidentiality of customer information and to implement safeguards to help prevent unauthorized access to the information. In response to this mandate, the agencies previously published the Interagency Guidelines Establishing Information Security Standards (the guidelines).

Last March, the agencies published an interpretation of the guidelines, *Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice* (final guidance), which establishes the procedures financial institutions should follow after they determine that customer information was accessed without authorization.¹ This article provides an overview of the final guidance for response programs.

Scope of the Guidance

The final guidance only applies to a financial institution's "customers." The GLB act distinguishes between a "consumer," who is defined as "an individual who obtains or has obtained a financial product or service... that is to be used primarily for personal, family, or household purposes," and a "customer," who is defined as "a consumer who has a customer relationship with [the financial institution]." The "customer relationship" is defined as "a continuing relationship between a consumer and [the financial institution] under which [the financial institution] provides one or more financial products or services to the consumer that are to be used primarily for personal, family, or household purposes." Generally, if the relationship between a financial institution and an individual is significant, then the individual is a customer. For example, a person who obtains a mortgage from a bank is considered a customer, while a person who only uses an ATM at a bank and has no other business

¹ CA Letter 05-10 and SR Letter 05-23 were issued to address Federal Reserve expectations related to the final guidance and are available on the Board of Governors' website at www.federalreserve.gov/boarddocs/srletters/2005/sr0523.htm.

there is a consumer. Strictly speaking, then, financial institutions are only required to implement the final guidance with respect to their customers.

As a practical matter, however, once a financial institution invests the time and resources to establish information security procedures, it would not make sense to only safeguard the information of customers. While financial institutions are not required to safeguard the information of noncustomers, institutions could expose themselves to liability for security breaches if they used weaker security standards for their noncustomer account holders.

The final guidance also defines the type of customer information to which it applies: nonpublic personal information, regardless of the format in which it is stored (electronic, paper, etc.), that is maintained by the institution or on behalf of the institution by a service provider. This definition is important because it clarifies that an institution is not liable for the loss of customer information not under its control. For example, if a customer divulged account information because of a phishing scam, in which a fraudulent website imitates a legitimate site, deceiving customers into divulging financial information, the financial institution would not be liable under the GLB act for resulting losses, because the information divulged was not under its control.²

The final guidance does not apply to a financial institution's foreign offices, branches, or affiliates. However, a financial institution covered by the final guidance is responsible for the security of its customer information, regardless of whether the information is maintained in the United States.

Procedures Following Unauthorized Access

The final guidance requires that financial institutions establish a five-pronged response program to deal with unauthorized access of customer information:

1. Assess the nature and scope of the incident, and identify what customer information has been accessed or misused

² The bank would likely still be responsible for most of the losses under Section 205.6 of Regulation E, the Board's implementing regulation for the Electronic Funds Transfer Act, if they occurred electronically and the customer gave timely notice of the loss.



2. Notify the primary federal regulator promptly
3. Notify law enforcement in situations involving federal criminal violations that require immediate attention
4. Take appropriate steps to contain and control the incident to prevent further unauthorized access, such as monitoring, freezing, or closing affected accounts, while preserving records and other evidence
5. Notify customers when warranted

Assess the Nature and Scope of Incident

When a financial institution learns of unauthorized access to information, it must first assess the nature and scope of the incident and identify what customer information systems and types of customer information have been accessed.

Notice to Federal Bank Regulator and Law Enforcement

After assessing the nature and scope of the incidents, the final guidance states that financial institutions should notify their primary federal regulator if "sensitive customer information" was accessed without authorization. Sensitive information is defined as "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 personal identification number or password that would permit access to the customer's account." It also includes any combination of components of customer information that would allow someone to log onto or access the customer's account, such as user name and password. Thus, if an institution learned of unauthorized access to customer information, but the information was not

continued on page CC6

The New Intermediate Small Bank CRA Evaluation

by Elizabeth Rozsa, Senior Examiner

Last quarter's issue of *Compliance Corner* contained an article summarizing recent amendments to the Community Reinvestment Act (CRA), including changes that expand the definition of community development and clarify illegal credit practices. This issue focuses on the new CRA classification for banks with assets between \$250 million and \$1 billion regardless of holding company affiliation: the intermediate small bank (ISB).

Banks within this asset threshold now have the option of being evaluated as either an ISB or a large bank. Because this change will impact many banks in the Third District, this article will review factors that banks should consider in determining whether to elect ISB or large bank procedures for their next CRA evaluation.

Who Is Eligible for the ISB Evaluation?

Banks with total assets of at least \$250 million as of December 31, 2005, for **both** of the two prior calendar years and with less than \$1 billion as of December 31, 2005, for **either** of the two prior calendar years are eligible to be evaluated as ISBs. These thresholds will be updated yearly based on the Consumer Price Index, and the new limits will be published in the Federal Register.

How Is the ISB Evaluation Conducted?

An ISB evaluation consists of a streamlined lending test and a community development test. The lending test evaluates all the elements of a small bank CRA evaluation, namely, a bank's loan-to-deposit ratio, the percentage of its loans located in the assessment area, the bank's record of lending to borrowers of different incomes and businesses of different sizes, the geographic distribution of the bank's loans, and the bank's record of response to written CRA-related complaints.

The community development test evaluates the following:

- The number and amount of community development loans
- The number and amount of qualified investments
- The extent to which the bank provides community development services
- The bank's responsiveness to community development lending, investment, and service needs (in the context of the bank's capacities, business strategy, the needs of the relevant community, and the number and types of opportunities for community development)

Basic Differences Between ISB and Large Bank Data Collection Procedures

Under the ISB evaluation, banks with assets between \$250 million and \$1 billion are no longer required to submit CRA small business and small farm data. However, if a bank chooses to be evaluated under the large bank procedures, it must have submitted at least one year of small business/small farm data. Conversely, if a bank has been evaluated as a large



bank in the past but now chooses the new ISB procedures, it is no longer required to submit data.

Evaluation of Community Development Lending.

Under the ISB procedures, community development lending is no longer evaluated under the lending test, but rather as part of the community development test, which includes *all* of the bank's community development activities. Retail banking services are no longer evaluated under the service test. Instead, examiners evaluate the extent to which banks provide community development services to low- and moderate-income people, including through branches and other facilities located in low- and moderate-income areas.

However, under the large bank procedures, community development activities are evaluated separately; community development loans are evaluated as part of the lending test, qualified investments as part of the investment test, and community development services as part of the service test.

It is important to understand how a bank's community development lending performance affects its overall CRA rating under the large bank and ISB procedures. With the large bank procedures, as long as a bank's lending test rating is satisfactory, it can still receive an overall satisfactory CRA rating—even if its performance under the investment or service test is rated “needs to improve.”

Under the ISB procedures, by contrast, a bank cannot receive a satisfactory rating overall unless its performance under *both* the lending and community development tests is satisfactory. In deciding which procedures to select for its next CRA evaluation, a bank must consider, therefore, its community development lending performance, either along with the rest of its lending as part of the lending test under the large bank procedures or along with the rest of its community development activities under the new ISB procedures.

Responsiveness Versus Innovation and Flexibility. Another important distinction between the ISB and large bank CRA procedures is that the large bank procedures evaluate banks on the innovation and flexibility of their products in meeting community development needs in their assessment areas. The ISB procedures, however, do not evaluate innovation and flexibility, but they place much greater emphasis on a bank's responsiveness to the specific community development needs in its assessment area. This determination will be based on the capacity and business strategy of the bank, actual community needs, and the number and type of opportunities for community development. While these criteria are ostensibly easier to meet, they require more research, thought, and planning on the part of both bankers charged

with meeting these criteria and examiners evaluating their performance. Examiners will consider the bank's assessment of community needs, along with information from community, government, civic, and other sources to gain a working knowledge of community needs.

Final Thoughts

Banks eligible to be evaluated under the new ISB procedures should review their last performance evaluation (and information on CRA performance since the last evaluation) to determine

their strengths and weaknesses and should examine their performance through the filter of the new ISB procedures. This process will enable banks to determine whether they would benefit from electing the new ISB procedures or whether it would be more advantageous to be evaluated under the large bank procedures.

The examination procedures for ISBs are available on the FFIEC website at <www.ffiec.gov/cra>. If you have further questions, however, please contact Senior Examiner Elizabeth Rozsa (elizabeth.rozsa@phil.frb.org) or Supervising Examiner John D. Fields (john.d.fields@phil.frb.org) through the Regulations Assistance Line at (215) 574-6568. □

It is important to understand how a bank's community development lending performance affects its overall CRA rating under the large bank and ISB procedures.

Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice

...continued from page CC3

sensitive, the institution would not have to notify law enforcement and its regulator.

The final guidance does not mandate any particular method for notifying regulators, but instead it emphasizes expeditious contact, such as via telephone. The final guidance also clarifies that it is the responsibility of financial institutions—not their service providers—to report unauthorized access to their regulators. However, in the interest of efficiency and timeliness, when a breach occurs, financial institutions may authorize their service providers to notify their regulator on the institution's behalf.

Regarding notice to law enforcement, the final guidance states that in addition to filing a timely Suspicious Activity Report (SAR), an institution should notify law enforcement by telephone when the unauthorized access involves violations of federal criminal laws. This is consistent with the federal banking agencies' SAR regulations.

Contain and Control Incident

After learning of unauthorized access, the next step is to contain and control the problem. The following measures can be taken in response to unauthorized computer access: 1) shut down applications or third party connections, 2) reconfigure firewalls, 3) ensure that all known vulnerabilities in the financial institution's computer systems have been addressed, 4) change computer access codes, 5) modify physical access controls, and 6) place additional controls on service provider arrangements.

Customer Notification

The guidance employs a pragmatic approach to identifying the circumstances in which institutions must notify their customers of unauthorized access. If sensitive customer information has been accessed

without authorization, the institution must determine whether it is likely the information has been or will be misused. If the institution reasonably believes that the information was or can be misused, it must notify the customer as soon as possible, unless a law enforcement agency believes that early notice to the customer might compromise a criminal investigation and notifies the institution in writing of its request to delay notice to the customer. But if the institution does not believe the information was misused or could be misused, it is not required to notify the customer.

When an institution determines that it must notify a customer of unauthorized access, the notice must:

- Be printed in a clear and conspicuous manner
- Describe the circumstances under which the unauthorized access occurred
- Specify the information that was accessed
- Identify the procedures the institution has undertaken to prevent further unauthorized access
- Provide a phone number the customer can call for information
- Advise customers to review their account statements for suspicious activity immediately
- Advise customers to monitor their credit report with the three major credit bureaus for the next 12 to 24 months
- Identify the procedure to obtain free credit reports under the Fair Credit Reporting Act³

In the interest of efficiency and timeliness, when a breach occurs, financial institutions may authorize their service providers to notify their regulator on the institution's behalf.

³ In conjunction with the three major credit reporting agencies, the FTC maintains a website that specifies the procedures for consumers to follow to obtain their annual free credit report from each of the three bureaus at <www.annualcreditreport.com/cra/index.jsp>.

- Describe how the customer can file “fraud alerts” with credit bureaus to alert the customers’ creditors that the customer may be a victim of fraud
- List the FTC’s identity theft website <www.consumer.gov/idtheft> and phone number (1-877-ID-THEFT)

The final guidance also encourages financial institutions to notify the three major credit bureaus.

Final Thoughts

In light of the final guidance, financial institutions

should promptly review their existing security procedures and response programs to determine whether they satisfy the requirements of the final guidance and make any necessary changes to their existing program to ensure that they are in compliance.

If you have any questions about this article, please contact Consumer Regulations Specialist Kenneth J. Benton (kenneth.j.benton@phil.frb.org) or Supervising Examiner John D. Fields (john.d.fields@phil.frb.org) through the Regulations Assistance Line at (215) 574-6568. □

The addresses and phone numbers of the credit fraud departments of the three major agencies are:

Equifax

P.O. Box 740241
Atlanta, GA 30374-0241
1-800-525-6285
www.equifax.com

Experian

P.O. Box 9532
Allen, TX 75013
1-888-397-3742
www.experian.com

TransUnion

Fraud Victim Assistance Division
P.O. Box 6790
Fullerton, CA 92834-6790
1-800-680-7289
www.transunion.com

Compliance Alert:

Truth in Lending Appeals Court Decision

Bank compliance departments should be aware of an important new decision from the United States Court of Appeals for the Third Circuit and the federal appeals court in Philadelphia, whose decisions are binding in the states of Pennsylvania, New Jersey, Delaware, and the U.S. Virgin Islands. In *Vallies v. Sky Bank*, 432 F.3d 493 (3d Cir. 2006), the Third Circuit interpreted the Truth in Lending Act (TILA) and Regulation Z, the implementing regulation for TILA published by the Board of Governors of the Federal Reserve System.

The issue in this class-action case is whether a creditor violates TILA and Regulation Z when a third party makes some of the required TILA disclosures in a credit transaction. In this case, a consumer had obtained bank financing to purchase a truck from a truck dealer. The financing included Guaranteed Auto Protection (GAP), a form of debt cancellation coverage subject to disclosure under Section 226.4(d)(3)(i) of Regulation Z. The bank made all of the required TILA and Regulation Z loan disclosures, except for the GAP insurance disclosure, which was made by the truck dealer.

The consumer sued the bank, alleging that the GAP financing disclosure by the dealer, instead of by the bank, violated TILA and Regulation Z. The trial court ruled in favor of the bank, finding that the identity of the person making the disclosures was irrelevant as long as the required disclosures were made. But the Third Circuit reversed the ruling, holding that the plain language of TILA and Regulation Z requires that the creditor must make all disclosures.¹ Banks operating in the Third Circuit should therefore ensure that all of their TILA and Regulation Z disclosures are made in the bank’s name.

¹ Regulation Z contains an exception in Section 226.5(d) regarding which creditor will make the required disclosures when a credit transaction has multiple creditors. That exception did not apply here because the truck dealer did not extend credit.

Regulatory Expectations for Compliance with the Fair Credit Reporting Act *...continued from page CC1*

requirements apply to financial institutions that engage in the following activities:

- Procuring and using information (e.g., as credit grantors, purchasers of dealer paper, or when opening deposit accounts)
- Furnishing and transmitting information (e.g., by reporting information to consumer reporting agencies, other third parties, or affiliates)
- Marketing credit or insurance products
- Employing people

Structure and Overview of Examination Procedures

The revised FCRA examination procedures are organized as a series of six modules. This structure allows examiners to risk-focus the FCRA review according to a financial institution's operations. Specifically, if a module is not applicable to a financial institution's operations, it is excluded from the examination scope. General information about each module's requirements is given below. The actual examination procedures for each of the modules are contained in Appendix A to the examination procedures, discussed later in this article.

Module 1: Obtaining Consumer Reports. Consumer reporting agencies retain a significant amount of financial information about consumers. This information

Banks, credit unions, and thrifts have a significant amount of consumer information that could constitute a consumer report.

is invaluable when assessing a consumer's creditworthiness for financial products and services, such as loans, deposit accounts, insurance, leases, and more. The FCRA regulates creditors' ability

to access this information to ensure that they use it for permissible purposes. It requires any prospective "user" of a consumer report (such as a lender, insurer, landlord, or employer) to have a legal purpose to obtain it.

Given the prevalence of electronically available information and the growth of identity theft, financial institutions must manage the risks associated with obtaining and using consumer reports. Module 1 verifies that financial institutions are employing procedures, controls, and other safeguards to ensure that consumer reports are obtained and used only for permissible purposes. Once the information is acquired, an institution's information security program governs the procedures to access, store, and destroy it. However, the procedures to obtain a consumer report must be

in compliance with the FCRA.

Module 2: Obtaining Information and Sharing Among Affiliates. The FCRA contains many substantive compliance requirements for consumer reporting agencies to ensure the accuracy and integrity of the consumer reporting system. Banks, credit unions, and thrifts have a significant amount of consumer information that could constitute a consumer report, and, thus, communicating this information could qualify the institution as a consumer reporting agency. However, the FCRA contains several exceptions that allow a financial institution to communicate this type of information, within strict guidelines, without being designated a consumer reporting agency.

Instead of containing strict information sharing prohibitions, the FCRA creates a business disincentive. If an institution shares consumer report information outside of the exceptions, it is considered a consumer reporting agency, and, therefore, it is subject to the significant compliance requirements under the FCRA. Consequently, most financial institutions structure their information sharing practices within



the exceptions to avoid being designated a consumer reporting agency.

This examination module covers various information sharing practices within these exceptions. If examiners determine that a financial institution's information sharing practices fall outside of these exceptions, it can be considered a consumer reporting agency, and examiners will have to complete the examination procedures specified in Module 6.²

Module 3: Disclosures to Consumers and Miscellaneous Requirements. The FCRA requires financial institutions to provide consumers with notices and information under a variety of circumstances. This module examines compliance in these areas.

Module 4: Financial Institutions as Furnishers of Information. The FCRA imposes many responsibilities on financial institutions that furnish information to consumer reporting agencies. These requirements generally involve ensuring the accuracy of the data that are placed in the consumer reporting system. Financial institutions that do not furnish any information to consumer reporting agencies will not be examined under this module.

Module 5: Consumer Alerts and Identity Theft Protections. The FCRA contains several provisions for both consumer reporting agencies and users of consumer reports that are designed to help combat identity theft. This module applies to financial institutions that are not consumer reporting agencies, but that are users of consumer reports.

To combat identity theft, the FCRA imposes two primary requirements. First, a user of a consumer report that contains a fraud or active duty alert must take steps to verify the identity of the individual to whom the consumer report relates. Second, a financial institution must disclose certain information when consumers allege they are victims of identity theft.

Module 6: Requirements for Consumer Reporting Agencies. The FFIEC will add the procedures

² The FFIEC has not yet written the procedures for Module 6, which will be added at a later date in a revised version of the examination procedures.

for Module 6 at a later date. Examiners will not review compliance with the consumer reporting agency requirements until the new procedures are developed.

Appendix A—FCRA Examination Procedures

The FCRA examination objectives are as follows:

- Determine the financial institution's compliance with the FCRA
- Assess the quality of the financial institution's compliance management systems and its policies and procedures for implementing the FCRA
- Determine the reliance that can be placed on the financial institution's internal controls and procedures for monitoring the institution's compliance with the FCRA
- Direct corrective action when violations of law are identified or when policies or internal controls are deficient

Initial Procedures. The initial procedures are designed to acquaint examiners with the operations and processes of the institution under examination. They focus on an institution's systems, controls, policies, and procedures, including audits and previous examination findings. The extent to which the FCRA and its implementing regulations apply depends on an institution's unique operations.

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, some of the individual compliance responsibilities are set forth directly in the statute, while others are within joint interagency regulations. Still others are included in regulations set by some of the regulatory agencies. The modules present examination responsibilities by subject matter versus the regulatory or statutory construction.

Examination Process. Examiners will follow the steps outlined below to determine which modules apply to each financial institution and which modules will be completed as part of their examination scope.

1. Determine whether the institution's internal controls are adequate to ensure compliance in the area under review through discussions with management and review of available information. The following data will be reviewed:

organization charts, flowcharts, policies and procedures, loan documentation, checklists, and computer program documentation (e.g., 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 any compliance audit material, including work papers and reports, to determine whether:
 - a. The scope of the audit addresses all provisions as applicable
 - b. Corrective actions were taken to follow up on previously identified deficiencies
 - c. The testing includes samples covering all product types and decision centers
 - d. The work performed is accurate
 - e. Significant deficiencies and their causes are included in reports to management and/or to the board of directors
 - f. The frequency of review is appropriate
3. Review the financial institution's training materials to determine whether:
 - a. Appropriate training is provided to individuals responsible for FCRA compliance and operational procedures
 - b. The training is comprehensive and covers the various aspects of the FCRA that apply to the individual financial institution's operations
4. Determine which portions of the six examination modules will apply.
5. Complete appropriate examination modules and document and form conclusions regarding the quality of the financial institution's compliance management systems and compliance with the FCRA.

Future Modifications to the Examination Procedures. Some provisions of the FACT Act require the regulators to enact implementing regulations before the requirements and their corresponding examination procedures apply. The revised examination procedures contain three sections that will be amend-

ed after the implementing regulations are enacted. Those sections are §604(g)—Protection of Medical Information, §624—Affiliate Sharing, and §615(h)—Risk-Based Pricing Notice.

As previously noted, Module 4 contains examination procedures for institutions that furnish information to consumer reporting agencies. The FFIEC will have to update this module after an interagency group issues guidance required by Section 312 of the FACT Act to enhance the accuracy of furnishing such information. In the interim, Module 4 will be used in examining financial institutions subject to the FCRA requirements for furnishers of information to consumer reporting agencies.

Financial institutions should review their compliance management programs to ensure that their FCRA policies and procedures reflect the revised provisions of the act.

Appendix B—Statutory and Regulatory Matrix

As previously noted, financial institutions are subject to a number of different requirements under the FCRA. Appendix B of the revised procedures contains a matrix that displays the different compliance obligations required of financial institutions under the FCRA and the citations

to the statutes and implementing regulations from which these obligations derive. This matrix is sorted by federal regulator.

Final Remarks

Examiners began utilizing the new FCRA examination procedures during the last quarter of 2005. Financial institutions should review their compliance management programs to ensure that their FCRA policies and procedures reflect the revised provisions of the act. The Federal Trade Commission (FTC) recently republished a booklet which contains the FCRA to reflect changes by the FACT Act. Instructions for ordering the booklet are available on the FTC's website at <www.ftc.gov/bcp/online/pubs/bulkordr.htm>.

If you have any questions about this article, please contact Supervising Examiner Eddie L. Valentine (eddie.valentine@phil.frb.org) or Supervising Examiner John D. Fields (john.d.fields@phil.frb.org) through the Regulations Assistance Line at (215) 574-6568. □

Educating Your Customer

As a financial institution, one of your biggest priorities is to ensure a secure banking environment for all of your customers. And with so many current threats to protecting consumer information, it is important for your institution to be proactive in taking protective measures. One of the best places to begin is through consumer awareness.

Many customers may not know their rights. They may not know what their credit report means. They may not understand the details of credit costs and terms. But you, as a financial institution, can help. If you can teach your customers how to protect themselves against fraud, then, in turn, your institution can be better able to detect and prevent threats to consumer protection.

The Federal Reserve System can help with your consumer awareness efforts. We publish consumer pamphlets on a variety of issues, including consumer credit, bank products, consumer rights, and more. The most recent pamphlets published by the Philadelphia Fed include "Preventing Payment Card Fraud: Dos and Don'ts," "Protecting Yourself Against Identity Theft," and "What You Need to Know About Payment Cards." All of our pamphlets are available for you to distribute to your customers—free of charge. To order, please contact Debbie Hemerka (debbie.hemerka@phil.frb.org) or visit our website at www.philadelphiafed.org.



Consumer Compliance Contact Information

Consumer Compliance/ CRA Examination Issues

Constance H. Wallgren (215) 574-6217
Robin P. Myers (215) 574-4182
David A. Center (215) 574-3457

Consumer Complaints

Denise Mosley (215) 574-3729
John D. Fields, III (215) 574-6044
Regulations Assistance Line (215) 574-6568



FEDERAL RESERVE BANK
OF PHILADELPHIA

Supervision, Regulation and Credit Department
Ten Independence Mall
Philadelphia, PA 19106

www.philadelphiafed.org

E-Mail Notification Service

Would you like to read *SRC Insights* and *Compliance Corner* on our website up to three weeks before they are mailed? Sign up for our e-mail notification service today at www.philadelphiafed.org/phil_mailing_list/dsp_user_login.cfm.