

BKD Financial Alert

August 2008



by Thomas W. Grundy, tgrundy@bkd.com

Last November, the federal agencies that regulate financial institutions, along with the Federal Trade Commission, issued the final rule and guidelines pertaining to identity theft “Red Flags” and addressing discrepancies. The final rule and guidelines implement Sections 114 and 315 of the *Fair and Accurate Credit Transactions Act of 2003*.

This final rule requires each financial institution or creditor that offers or maintains one or more covered accounts to develop and implement a written identity theft prevention program.

This program must be designed to detect, prevent and mitigate identity theft in connection with the opening of a covered account or any existing covered account.

The final rule defines a covered account as the following:

“... an account that a financial institution or creditor 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; and ... any other account that the financial institution or creditor offers or maintains for which there is a reasonably foreseeable risk to customers or the safety

Financial institutions must implement “Red Flag” rule programs by November 1, 2008

and soundness of the financial institution or creditor from identity theft, including financial, operational, compliance, reputation or litigation risks.”

Each financial institution must periodically conduct a risk assessment to determine whether it offers or maintains a covered account, as described.

Content of the program

The program must include reasonable policies and procedures designed to:

- ▶ Identify relevant Red Flags for covered accounts and incorporate those Red Flags into the program. The final rule defines a Red Flag as “a pattern, practice or specific activity that indicates the possible existence of identity theft”
- ▶ Detect Red Flags that have been incorporated into the program
- ▶ Respond appropriately to any Red Flags that are detected and mitigate identity theft
- ▶ Update the program periodically to reflect changes in risks to customers and the safety and soundness of the financial institution or creditor

The appendix to the final rule provides guidelines to assist in developing and implementing a program, including an illustrative listing of Red Flags.

The guidelines detail expectations for the ongoing administration of the program. Specifically, the board of directors, an appropriate committee of the board or a member of senior management should perform the following:

- ▶ Assign specific responsibility for the program’s implementation
- ▶ Review compliance reports
- ▶ Approve material changes to the program as necessary to address changing identity theft risks

At least annually the staff responsible for administering the program should report to the board of directors, an appropriate committee of the board or a designated member of senior management on compliance. The report should address:

- ▶ Effectiveness of policies and procedures in addressing the risk of identity theft in connection with opening covered accounts or with respect to existing covered accounts
- ▶ Service provider arrangements
- ▶ Significant incidents involving identity theft and management’s response
- ▶ Recommendations for material changes to the program

continued on page 2

Inside

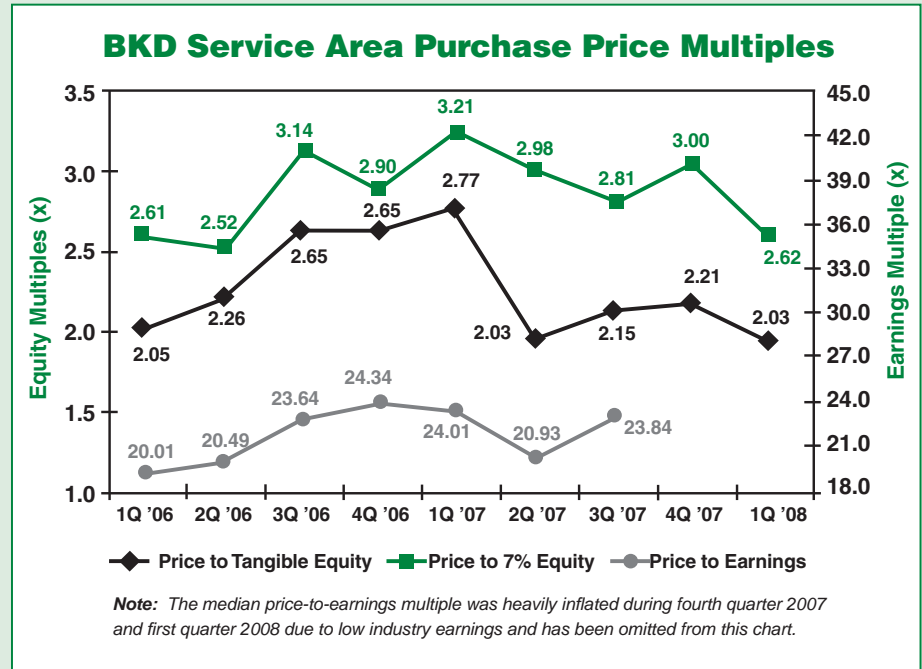
- ▶ **Merger activity in banking still strong, though valuations are down**
- ▶ **Make your information technology risk assessment work for you with careful planning, review**
- ▶ **Mark your calendar**

Merger activity in banking still strong, though valuations are down

by Patrick Hayes, phayes@bkd.com

Although BKD Corporate Finance continues to see mergers and acquisitions throughout the banking industry and BKD service area, valuations have been on the decline. The 17 announced transactions during the first quarter of 2008 are slightly down from the 20 announced in the same period a year ago, but up from the 15 announced in the fourth quarter of 2007. Transaction multiples for the first quarter of 2008 were far less favorable than multiples from the previous quarter as well as multiples from the same quarter a year ago. A median price to tangible equity multiple of 2.03 is 8.1% lower than that of the previous quarter and 26.7% lower than the first quarter of 2007. The median price to 7% equity multiple decreased 12.7% to 2.62 from the previous quarter and 18.4% from 3.21 during the same quarter in 2007.

Nationally, the total number of



announced transactions decreased significantly, with 36 announced in the first quarter of 2008 compared to 87 in the same quarter of 2007.

For a further breakdown of first quarter transactions, visit our Bank Merger Update at <http://www.bkd.com/docs/about/BankMergerUpdate.pdf>. ■

Financial institutions must implement Red Flag rule . . .

continued from page 1

When engaging a third-party service provider, the institution should determine the activity of the service provider is conducted in accordance with reasonable policies and procedures designed to detect, prevent and mitigate the risk of identity theft.

Finally, training for all affected staff will be crucial for the proper implementation and ongoing success of the program.

Card issuers and change of address requests

The final rule requires an issuer of credit and debit cards to implement reasonable policies and procedures to assess

the validity of a change of address if the issuer also receives a request for additional or replacement cards within 30 days of the change of address notification. Should this occur, the card issuer may not issue an additional or replacement card until it assesses the validity of the address change by:

- ▶ Notifying the cardholder of the request at the cardholder's former address or by any other previously established means of communication between the card issuer and the cardholder
- ▶ Assessing the validity of the change of address in accordance with the policies and procedures the card issuer has established as part of its program for

detecting, preventing and mitigating identity theft

Users of consumer reports address discrepancies

The final rule also requires users of consumer reports to develop reasonable policies and procedures to apply when they receive a notice of address discrepancy from a consumer reporting agency. These policies and procedures must allow the user to reasonably believe that a consumer report relates to the consumer about whom it has requested the report. Examples of reasonable policies and procedures are provided in the final rule. ■

Make your information technology risk assessment work for you with careful planning, review

by Kevin Sethman, ksethman@bkd.com

Now that you've created the information technology risk assessment that the regulators wanted you to have, what should you do? The three next steps should be these:

- ▶ Review your risk assessment
- ▶ Test your risk assessment
- ▶ Integrate your risk assessment

1 ■ Review your risk assessment

It is always better to have the external auditors catch a problem than the examiners, and it's even better to catch a problem internally before the external auditors find it. One of the best things you can do with your risk assessment is to ensure that your internal auditors are able to review it as soon as possible.

BKD has discovered significant issues while reviewing information technology risk assessments. Often assessments are deficient or they are not useful to management.

BKD has noted these key deficiencies in risk assessments:

- ▶ **Incomplete assessments**—In some instances, new or existing technology has been overlooked, critical vendors were not identified or the assessments failed to address all areas of the institution.
- ▶ **Risk was not rated**—Some of the assessments BKD has reviewed identify the risks, but don't assign a score (such as high, medium or low) to the risk. As a result, management may find it difficult to prioritize the assignment of resources to achieve the greatest return on investment.
- ▶ **Existing controls are not identified**—In some instances, the risk assessments failed to identify the existing control environment, or they fail to document that the residual risk is acceptable to management.

The result is the risk assessment leaves the impression risk management is either weak or non-existent, something the examiners will want to address.

Because of issues listed above, risk assessments are not useful to management. One additional item BKD has noted is the assessment is simply too complicated for non-technical people to use effectively and, as a result, it's pushed to the bottom of the pile. Therefore, it is a best practice to have the assessment reviewed or even prepared by someone who can bridge this communication gap.

2 ■ Test your risk assessment

First of all, this is about coordinating the testing of your risk assessment, rather than setting up a separate testing protocol for the IT risk assessment. For example, in your risk assessment, you will have documented risks that affect your business continuity plan or your ability to comply with the Gramm-Leach-Bliley Act (GLBA). You should already have testing/validation protocols established for most, if not all, of these areas.

Other testing is as simple as making sure your internal auditors are verifying your data backups are prepared and properly transported to the offsite storage location or that antivirus software is properly updated.

Additionally, make sure your line managers check work stations to ensure employees are properly controlling information. Any manager can look out for simple things, such as making sure employees don't keep their passwords on a note under the keyboard and terminals

are locked or turned off—whichever your policy requires. Your information security officer should follow-up on these items on a regular basis.

3 ■ Integrate your risk assessment

You've invested a lot of time and financial resources into the creation of your IT risk assessment and want to ensure you receive a return on this investment. The key question then is how to do that. The answer is to integrate the risk assessment into your planning process.

This can be done in several ways. You should use the risk assessment as the starting point for your IT strategic plan or to validate aspects of your business continuity plan and your GLBA compliance activities. More importantly, use your IT risk assessment as the starting point for addressing new regulatory mandates, whenever possible. For example, one of the mandates we're currently facing as

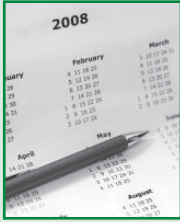
an industry is to address identity theft Red Flags. Your information technology will be an important part of this process; therefore, make sure the IT risk assessment is a starting point for and a critical

component of your identity theft risk assessment.

For guidance on preparing an information security risk assessment, go to www.bkd.com/docs/newsletters/FA/FinancialAlert2004-05.pdf. For more help with this issue, please contact your BKD advisor. ■



Mark Your Calendar



Brett Schimanski and Mark Wofford of BKD will present a free one-hour webcast *The "Red Flag" Compliance Deadline, Are You*

Ready? at 10 a.m. (CDT), Thursday, August 14. This webcast will cover the importance of the Red Flag rule and outline the core requirements of the identity theft prevention program, accounts covered by the regulation, the completion of a risk assessment and actions to be taken when Red Flags

are identified. Register at bkd.com/webcast.

John Bourquard of BKD will present a free one-hour webcast *Effective Credit Administration in a Challenging Environment* at 10 a.m. (CDT), Thursday, September 25. This informative webcast will address current credit trends, emerging risks, ideas to help mitigate risk in your portfolio and to improve the administration of your loans. Register at bkd.com/webcast.

About Financial Alert

This newsletter's content is written by qualified, experienced BKD professionals, but applying specific information to your situation requires careful consideration of facts and circumstances. Consult your BKD advisor before acting on any matter covered in this newsletter.

To change your mailing information, email instructions to newsletters@bkd.com. Include the mailing label code number that appears above your name. To add your name to our mailing list, contact a sales and marketing specialist at the BKD office nearest you. To inquire about information in this newsletter, contact your BKD advisor.

E-subscribe to **Financial Alert**. Follow the sign-up instructions at bkd.com/enews/.

bkd.com Your email address and personal information will never be sold to vendors or shared with anyone outside BKD.

© 2008 BKD, LLP.
All rights reserved.

Praxity
MEMBER
GLOBAL ALLIANCE OF
INDEPENDENT FIRMS

Address Service Requested

For a complete list of our offices and subsidiaries and their contacts, visit bkd.com or contact the sales & marketing specialist at the BKD office nearest you.

P.O. Box 1900
Springfield, MO 65801-1900

CPAs & Advisors

