Financial Alert

Management & Compliance Solutions for Financial Institutions

May 2004

Regulation B: spousal signature rules revised

by Sean Kulczycki, St. Louis, skulczycki @bkd.com

Many lenders are familiar with Regulation B's (*Equal Credit Opportunity Act of 1989*) signature requirements, as well as the limitations they place on who can be asked to sign a promissory note or loan guaranty.

In fact, this issue has been a frequent source of contention between lenders and compliance professionals. After April 15, 2004, these long-standing requirements will undergo significant change.

Recent revisions to Regulation B and the Federal Reserve Board's **Official Staff Commentary on Regulation B** go into effect April 15 and will significantly affect critical steps in the lending process.

Even for financial institutions that either opt to or currently use a commercial credit application, adding a separate affirmation of intent is recommended.

Note that the Federal Reserve Board has made such revisions to the model application forms included in Appendix B of the regulation.

How to interpret revisions

The primary revision is the result of language added to the regulation: "A creditor shall not deem the submission of a joint financial statement or other evidence of jointly held assets as an application for joint credit."

In addition, the **Official Staff Commentary** says, "the method used to establish intent must be distinct from the means used by individuals to affirm the accuracy of information."

In other words, consumer and commercial loans require a separate affirmation of the co-applicant's intent.

For commercial loans, a commercial credit application or modification to existing personal financial statement forms may be required.

Institutions will need to modify financial statement forms to include wording about borrowers who intend to apply for joint credit. Consider adding a separate signature line for the applicants to sign or initial.

When are spousal signatures required?

Failing to obtain a spouse's signature on documents establishing intent does not necessarily create a violation of Regulation B.

If the expressed intent of an applicant's spouse is not obtained, the spouse can only be required to sign a credit instrument if the individual applicant does not qualify.

(continued on page 3)

SOX 404: SEC & PCAOB issue new rules & deferrals

by Travis Webb, Indianapolis, twebb@bkd.com

The rules and regulations of the *Sarbanes-Oxley Act of 2002* (the Act) continue to evolve nearly two years after the law's passage. With recent changes, some entities will escape the most time-consuming provision for two more years.

Implementation delayed

You are likely aware of the February decision by the Securities and Exchange Commission (SEC) to extend effective dates for the Act's controversial Section 404.

404 requires management (and the external auditor) to assess and report on the effectiveness of the institution's internal control over financial reporting.

The regulations originally required accelerated filers to comply for fiscal years ending on or after June 15, 2004; the date has been deferred to fiscal years ending on or after November 15, 2004.

While only a five-month delay in the effective date has been granted, an institution with a fiscal year falling between June and November 15 has an additional year to complete the documentation and testing process.

SOX 404

For other filers, the effective date was deferred from fiscal years ending on or after April 15, 2005, to ending on or after July 15, 2005.

Similarly, a June 30 fiscal year-end nonaccelerated filer has an additional year to meet Section 404's requirements.

Accelerated filers take note

There has been some confusion determining accelerated-filer status. Entities have been caught by

(continued on page 4)

In this issue

- ✔ Regulation B: spousal signature rules revised
- ✔ SOX 404: SEC & PCAOB issue new rules & deferrals
- ✔ Financial institutions need IT risk assessment
- ✔ Comparing SOX & FDICIA: Do you know the difference?
- ✔ New currency transaction report

Financial institutions need IT

by Jerry Lowrance, BKD Technologies, jlowrance@bkd.com

The need for risk assessment is a common theme in recent information technology (IT) regulatory examinations at financial institutions.

What is risk assessment, and how is it done? How detailed should it be? Should an independent third party perform it?

Guidelines require risk assessment

The *Gramm-Leach-Bliley Act of 1999* (GLBA) and the Federal Financial Institutions Examination Council's (FFIEC) guidelines require a risk assessment to be performed.

The assessment should identify risks to the security of an institution's information systems, risks resulting from anything that could compromise the confidentiality of sensitive information or the availability of critical systems.

An institution's information security program must be designed to protect its most critical systems and sensitive information, and a risk assessment is the program's foundation.

The first step in a risk assessment is to conduct a business impact analysis (BIA). This identifies the institution's core business functions, the information systems that support them and the impact systems loss would have.

Assess each asset

Information systems are collections of assets, such as application software, hardware, data and networks. Each asset is subject to different threats.

For example, a server located in a public area and one located in a secure area are subject to different threats; however, all servers located in secure areas may be subject to similar threats.

For this reason, risks should be assessed for each asset or group of similar assets rather than for the system as a whole.

The process can be quite detailed when taken to the extreme. Each modem, workstation and server could be assessed individually.

While this would make the risk assessment more complete, the goal is to identify and assess threats to critical assets and sensitive information.

If those assets are essential to the operation of a critical system or contain sensitive information, then they should be assessed individually. If not, the assets should not be included in the risk assessment.

Foresee threats

No single list of threats applies to all institutions. All reasonably foreseeable threats should be considered and are defined by factors, such as the institution's location and its technical environment.

For example, a hurricane is not a reasonably foreseeable threat to an institution located in Kansas, nor would a hacker threaten an institution that does not have an Internet connection.

IT threats are commonly categorized as one of the following:

Natural - Tornado, earthquake, etc.

Human - Accidental or intentional human acts

Technical - Equipment failure, communication failure, etc.

Define a scenario for each threat, such as a natural threat like a tornado: A destructive (Type 2 or greater) tornado strikes the institution's operation center where its main computer servers are located, causing major damage and destruction.

The scenario describes the threat in terms of its outcome, which is necessary for assessing the likelihood and impact of the threat.

How to assess risk

An asset can be open to risk for a variety of reasons, including:

Threats to the asset - Different threats apply to different assets.

Existing controls - Various measures may already be in place to reduce the likelihood of a threat or its impact on the institution.

Vulnerability to threats - Weaknesses or conditions may exist that make the asset vulnerable to threats.

For example, an institution that does not conduct background checks on employees with access to sensitive data is vulnerable to unauthorized insider activity.

Once an institution understands how and where it is vulnerable, it must assess the likelihood of various threat scenarios, as well as their potential impact, *e.g.,* financial, reputation, compliance, etc.

While this could be based on historical statistical evidence and a detailed financial analysis, more subjective approaches are acceptable and more practical.

Likelihood and impact can both be rated high, medium or low, and each rating can be numerically weighted, then multiplied to produce a risk score for each threat to each asset. Scores are accumulated per asset and business function, then ranked accordingly.

Process is ongoing

Your institution's management is responsible for initiating the process and should be involved with rating the likelihood and the impact of threats.

A consultant can provide an independent perspective and bring the necessary skills, experience and tools to efficiently handle the assessment. For multiple perspectives, include technical and nontechnical personnel on the team.

REGULATORY COMPLIANCE

New currency transaction report

by Sean Kulczycki, St. Louis, skulczycki@bkd.com

The Financial Crimes Enforcement Network (FinCEN) has recently issued a revised **Currency Transaction Report (CTR)**.

The new form (FinCEN 104) — available at **http://www.fincen.gov/ fin104_ctr.pdf** — went into effect December 1, 2003; however, the earlier version (Internal Revenue Service Form 4789) will be accepted until August 31, 2004.

FinCEN Form 104 contains three additional fields in Part II: Item 26a (Foreign cash in), Item 27a (Foreign cash out) and Item 29 (Foreign country).

Instructions for completing FinCEN Form 104 state, "if foreign currency is exchanged, enter the amount of foreign currency in items 26a and 27a."

In addition, the instructions state the country of origin should be listed in Item 29. If currency is exchanged from multiple countries, the bank should mark Item 36 and "identify the additional country(s) and/or currency(s) involved."

Other than the aforementioned changes, banks should continue completing and reporting large currency transactions as they have done in the past.❏

risk assessment

Risk assessment is an ongoing process. Update the information any time changes occur. For example, assess risk if a new server is installed or when new controls are implemented.

Implement results

The risk assessment will identify and, to a degree, quantify risks. GLBA requires an institution's management and board of directors be made aware of them.

After comparing the risk to the cost of controlling it, management decides which controls to implement and should document decisions and the rationale behind them.

Assessment results also can be the basis of your institution's business continuity plan. Assessing risk requires subjective judgment, decisions that can only be made by management.

Because assessments produce considerable data to analyze and report, an automated tool designed especially for this purpose can help simplify the process and produce more meaningful reports.

BKD's consultants use a proprietary database software tool to help produce management reports and to make the risk assessment process more efficient.

In addition, financial institutions soon will be able to purchase software from BKD Technologies that will assist them in the risk assessment process. Ask your BKD advisor for details.❑

Comparing SOX & FDICIA: Do you know the difference?

FDIC issued FIL No. 17-203 on March 5, 2003, which addresses the "Applicability of Selected Provisions of the *Sarbanes-Oxley Act of 2002* to FDIC Supervised Banks with Less Than $500 Million Total Assets That Are Not Public Companies."

Generally, FDIC has taken the position that many components of SOX are relevant and appropriate considerations for financial institutions regardless of size.

However, the *Federal Deposit Insurance Corporation Improvement Act of 1991* (FDICIA) and SOX are not the same, and the jurisdiction of the related bodies is separate.

FDICIA applies to financial institutions with $500 million or more in assets; SOX applies only to public companies. A financial institution might be subject to FDICIA and not to SOX, or vice versa, or may be subject to both acts.

Documentation methods and the extent of testing FDICIA compliance will drive how much work is necessary to comply with SOX.

There is a somewhat universally understood expectation that the stakes are higher with SOX and that the level of effort can be significantly higher as well.

The degree of documentation is likely to be a higher threshold for SOX than it is for FDICIA. Talk to your BKD advisor about specific considerations.❑

Regulation B: spousal signature. . .

(continued from page 1)

This will require an analysis of the primary applicant's individual assets and their individual interest in jointly owned assets.

As stated in FDIC's recently issued FIL-6-2004, "the creditor must determine (and not presume) the actual form of ownership of the property prior to or at consummation of the credit transaction. The possibility of subsequent changes in the form of ownership, *e.g.*, by transfer or divorce, may not be considered."

Different rules for married applicants

Different rules apply to married applicants who reside in community property states—or if the property the applicant is relying on is located in such a state.

To satisfy the debt in the event of default, the creditor (acting in accordance with applicable state law) may require the signature of the applicant's spouse on any instrument necessary to make the community property available provided:

- ▲ Applicable state law denies the applicant power to manage or control sufficient community property to qualify for the amount of credit requested, and
- ▲ The applicant lacks sufficient separate property to qualify for the amount of credit requested

How state laws affect individuals

If an individual applicant requests secured credit, a creditor may require the signature of the applicant's spouse only on instruments necessary under applicable state law to make the property being offered as security available to satisfy the debt in the event of default.

Generally, a signature is only needed on a security instrument; however, applicable state law may require both spouses to sign the promissory note (or other credit instrument) to create an enforceable security interest.

The above applies equally in the business-lending environment, including instances where a business loan is applied for by an individual or by an entity that requests individuals as guarantors.

Use new guidelines

Even if a corporation or other entity is creditworthy, a creditor may require the personal guarantees of those who have qualifying business relationships—partners, directors or officers, as well as closely held corporation shareholders.

Creditors are prohibited from automatically requiring the signature of a guarantor's spouse if one of the aforementioned qualifying relationships is absent.

Use the new guidelines in such circumstances: The spouse should be requested to document intent to "apply" as a guarantor.

Take steps as soon as possible to modify your forms for personal financial statements and credit applications (both consumer and commercial).

In addition, educate all appropriate personnel on the revised spousal signature rules, as well as state-law requirements for individual and joint property.❑

Check out. . .

Financial Alert @ bkd.com

SOX 404: new rules & deferrals. . .

(continued from page 1)
recent market recoveries that improved their stock prices and caused them to become accelerated filers for Section 404 purposes; this also resulted in an earlier effective date.

Accelerated filers (defined by regulation 17CFR240.12b-2) include:

- Those who have filed for the last 12 months and
- Those with an aggregate market capitalization of $75 million or more at the end of the last business day of the second quarter of the fiscal year based on voting and nonvoting common equity held by nonaffiliates

For entities close to the $75 million market-capitalization level, taking a close look at affiliate holdings is critical to determining the effective date.

Plan to go private?

Nationally, entities are evaluating the continuing cost of participating in the public market. Going private can reduce costs and provide benefits, such as:

- Eliminates Act compliance and SEC reporting
- Increases control by insiders or large shareholders
- Provides liquidity to small shareholders through buy-outs

Every benefit has a price:

- Decreases liquidity and shareholder base
- Reduces access to capital
- Weakens stock option liquidity

To become qualified to deregister, some entities are seeking to reduce their total number of shareholders to fewer than 300 by such means as buy-outs, tender offers and other transactions.

For entities close to the $75 million market-capitalization level, taking a close look at affiliate holdings is critical. . .

PCAOB's final rules

On March 9, 2004, the Public Company Accounting Oversight Board (PCAOB) released its final rules for the external auditor's attestation related to Section 404.

While many questions remain, issuance of the final rule (pending SEC approval) provides registrants an improved barometer for what it will take to achieve a "clean opinion" from their external auditor.

Highlights of the changes from the originally proposed rules include:

- Relaxed provisions allow auditors to rely more on others' work, *e.g.,* internal auditors
- Compromises on issues were made to reduce duplicative efforts of external and internal audit and to address concerns about inappropriate reductions in internal audit departments
- Auditor walk-throughs of transactions (from start to finish) were reaffirmed as required, but thresholds were reduced
- Audit committee effectiveness remains relevant for auditor consideration but as part of the overall evaluation rather than a separate test

The changes should reduce the overall cost of compliance; however, the required effort and resulting cost remains substantial. Auditors must perform sufficient testing themselves to provide the principal evidence for their opinion.

Your external auditors' ability to assist you is constrained. To maintain their independence to opine on your internal control, your auditors' involvement in your efforts to document, test and assess internal control is severely limited.

Getting started

Even if you are among those enjoying a new deferral, it may be beneficial to step up efforts to complete Section 404 activities.

Improvement efforts can be substantial, yet many entities are finding the time and resources necessary to complete initial evaluations of internal control and resulting remediation.

Take the following steps to move your process forward:

- Identify who in management will lead the project (often the CFO or controller)
- Assess system complexity and existing resources, including consideration of existing documentation and testing
- Evaluate potential outside resources
- Evaluate whether to use as your criteria the **Internal Control–Integrated Framework** report from the Committee of Sponsoring Organizations of the Treadway Commission (available at **www.coso.org**)
- Develop a compliance timeline that recognizes the impact of testing and any necessary remediation and improvement efforts
- Create project teams, provide training and execute your documentation plan

* * *

Contact your BKD Financial Institutions Group advisor for more information about Section 404 and how it will affect your institution.❑

How to Reach BKD

For a complete list of our offices and subsidiaries and their contact information, go to bkd.com or call Director of Communications at 417 831-7283.

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

PRSRT STD
US POSTAGE PAID
SPRINGFIELD MO
PERMIT #801

Address Service Requested

inFinet RESOURCES
Independent Financial Institution Network

bkd.com