

FEDERAL RESERVE BANK OF SAN FRANCISCO  
101 MARKET STREET, SAN FRANCISCO, CALIFORNIA 94105

November 13, 2002

**BANKING SUPERVISION AND REGULATION:  
SARBANES-OXLEY ACT OF 2002**

To State Member Banks, Bank  
Holding Companies, U.S. Branches  
and Agencies of Foreign Banks,  
and Others Concerned,  
in the Twelfth Federal Reserve District

**The Sarbanes-Oxley Act of 2002 (SR 02-20)**

The recently enacted Sarbanes-Oxley Act of 2002 includes provisions addressing audits, financial reporting and disclosure, conflicts of interest, and corporate governance at public companies. The Act also establishes new supervisory mechanisms, including the new Public Company Accounting Oversight Board, for accountants and accounting firms that conduct external audits of public companies. This SR letter describes the most important provisions of the Act that examiners should be aware of when conducting examinations and inspections of banking organizations that are subject to the Act and supervised by the Federal Reserve. It also provides a general overview of the Act for affected domestic and foreign banking organizations.

Supervisory staff and banking organizations are encouraged to remain current on guidance implementing the Sarbanes-Oxley Act provided by the Securities and Exchange Commission through its regulations and releases. In addition, the Federal Reserve will issue further supervisory guidance as appropriate to assist banking organizations supervised by the Federal Reserve in complying with the Act. As soon as the SEC completes the issuance of all of the rules and guidance required by the Act, additional examination procedures addressing the Act's and SEC's requirements will be developed and disseminated to supervisory staff at the Reserve Banks.

**Publicly Held Banking Organizations**

In general, the Sarbanes-Oxley Act applies to public companies, that is, companies (including banks and bank holding companies) that have a class of securities registered under section 12 of the Securities Exchange Act of 1934 (the 1934 Act), or are otherwise required to file periodic reports (*e.g.*, 10-Ks and 10-Qs) under section 15(d) of the 1934 Act.<sup>1</sup> Bank holding companies, state member banks, and foreign banks that meet these qualifications (referred to herein as public banking organizations) are subject to the requirements of the Act, as well as any rules and regulations that the SEC may adopt to implement the Act.<sup>2</sup> Some of the Act's provisions are currently effective, while others will become effective on a specified future date or upon the issuance of implementing rules by the SEC.

**Audit Committee Structure and Responsibilities**

Section 301 of the Act requires that each public company have an audit committee composed entirely

---

<sup>1</sup> 15 U.S.C. 78l and 78o(d).

<sup>2</sup> Section 12(i) of the 1934 Act, as amended by the Sarbanes-Oxley Act, gives the Board of Governors the authority to administer and enforce certain provisions of the Act and the 1934 Act with respect to state member banks that have securities registered under the 1934 Act. The Board's Regulation H generally requires this limited number of state member banks to comply with any rules adopted by the SEC under the relevant provisions of the Act and the 1934 Act (12 CFR 208.36, as amended by 67 FR 57938 [September 13, 2002]).

of independent directors. If the company's board does not establish a separate audit committee, the full board may serve that function so long as each director is independent. In order to be independent for these purposes, a director may not (other than in his or her capacity as a director) accept any consulting, advisory, or other compensatory fee from the company, or be an "affiliated person" of the company or any of its subsidiaries.<sup>3</sup>

Section 301 also imposes several specific responsibilities on the audit committees of public companies. The audit committee must be directly responsible for the appointment and compensation of the company's outside auditor, as well as for overseeing the auditor's work. In addition, the audit committee must establish procedures for receiving and addressing any complaints about the company's accounting, internal accounting controls, or auditing, as well as for the anonymous and confidential submission of employee concerns regarding questionable accounting or auditing matters. Finally, the audit committee must have the authority to retain and compensate independent counsel and other advisers, as necessary to carry out the audit committee's duties.

### **Insider Lending**

Section 402 of the Act generally prohibits a public company and its subsidiaries from extending credit, or arranging for another entity to extend credit, in the form of a personal loan to any director or executive officer of the public company.<sup>4</sup> This provision is not retroactive, so it does not apply to extensions of credit made on or before July 30, 2002, the date of enactment of the Act, so long as the loan is not renewed or materially modified after that date.

Two exceptions to this loan prohibition exist. First, the prohibition does not apply to any loan made by an insured depository institution to a director or executive officer if the loan is subject to the insider lending restrictions of section 22(h) of the Federal Reserve Act (12 U.S.C. 375b), as implemented by the Board's Regulation O (12 CFR part 215). Accordingly, it is anticipated that loans by an insured depository institution to the directors and executive officers of its publicly traded parent bank holding company will be exempt from the prohibition, but will remain subject to the existing restrictions of Regulation O. It should be noted that this exception covers only loans made by banks and other insured depository institutions and does not cover loans made by a public bank holding company (or its nonbank subsidiaries) to the directors and executive officers of the public bank holding company.

The second exception permits the directors and executive officers of a public company to obtain home improvement and manufactured home loans, consumer loans, and loans under open-end credit plans or charge cards from their company or its subsidiaries so long as the credit (i) is extended in the ordinary course of the company's consumer credit business, (ii) is a kind of credit generally made available to the public by the company, and (iii) is made on market terms or on terms that are no more favorable than those offered to the general public.<sup>5</sup>

The SEC has authority to interpret the scope of the lending prohibition in section 402 of the Act and may issue guidance in the future concerning the scope of the lending prohibition and exceptions in section 402.

### **Outside Auditors**

- 1. Registration and Standards.** Title I of the Act provides for the establishment of the Public Company Accounting Oversight Board by April 26, 2003. All accounting firms that conduct audits of public companies (i.e., registered accounting firms) must register with the Oversight

---

<sup>3</sup> "Affiliated person" is defined by reference to the Investment Company Act of 1940 (15 U.S.C. 80-2(a)(3)), and includes any officer or employee of the company or its subsidiaries and any other person that owns five percent or more of the voting securities of the company or any of its subsidiaries.

<sup>4</sup> It is important to note that the Act does not prohibit a public company and its subsidiaries, including a bank holding company, a nonbank subsidiary of a bank holding company, and a bank, from making loans to non-executive level officers as well as to other employees of the company or bank.

<sup>5</sup> The Act also does not prohibit a registered broker-dealer that is a public company, or a subsidiary of a public company, from providing margin credit to its employees to buy, trade or carry securities so long as the credit is made in accordance with the Board's margin rules, is not made to purchase the stock of the public company, and complies with the requirements in (i), (ii) and (iii) above.

Board within 180 days of its establishment and become subject to its supervision. The Act gives the Oversight Board the authority (subject to SEC review) to establish auditing standards for registered accounting firms.

**2. Independence.** The Act includes several provisions designed to ensure that external auditors remain independent from the public companies (including public banking organizations) they audit. For example, section 206 prohibits a registered accounting firm from performing audit services for a public company if a senior executive (i.e., the CEO, CFO, chief accounting officer, comptroller or equivalent) of the company was employed by the accounting firm and participated in the audit of the company within the previous year. Section 203 of the Act also requires registered accounting firms to rotate the lead or reviewing partner for each public company so that no partner has primary responsibility for the engagement for more than five consecutive years.

In addition, section 201 of the Act prohibits registered accounting firms from contemporaneously providing audit and certain non-audit services to a public company. The eight enumerated prohibited non-audit services include bookkeeping and other services related to accounting records or financial statements; financial information system design and implementation; appraisals, valuations, and fairness opinions; actuarial services; internal audit outsourcing; management and human resources functions; broker, dealer, investment advisory and investment banking services; and legal and other non-audit expert services. The Oversight Board may add additional services to this list of prohibited non-audit services, and may prescribe additional rules relating to auditor independence. A registered accounting firm may provide non-audit services that are not otherwise prohibited, such as tax services, to a public company so long as the company's audit committee gives advance approval of the service arrangement.<sup>6</sup>

## Financial Disclosure and Reporting Obligations

**1. Certification Requirements.** Pursuant to section 302 of the Act, the SEC has adopted final rules that require the principal executive officer(s) and principal financial officer(s) of public companies to include certain certifications in the annual and quarterly reports filed by the company under the 1934 Act. These final rules require each officer to certify, with respect to each report filed, the following:

- a. The certifying officer has reviewed the report
- b. Based on the certifying officer's knowledge, the report does not contain any material misstatement or omit any material facts necessary to prevent any statement in the report from being misleading, and fairly presents the company's financial condition, results of operations and cash flows
- c. The certifying officers (i) are responsible for maintaining disclosure controls and procedures for the company, (ii) have designed such controls and procedures to ensure that material information is reported to the officers, (iii) have evaluated the effectiveness of the disclosure controls and procedures within the past 90 days, and (iv) have included in the report their conclusions about the effectiveness of such controls and procedures and any significant changes (including corrective actions) to the company's internal controls that have occurred subsequent to the officer's evaluation
- d. The certifying officers have disclosed to the company's auditor and audit committee any significant deficiencies or material weaknesses in the company's internal controls relating to financial reporting, as well as any fraud (whether material or not) involving the company's management or employees that have a significant role in the company's internal controls.<sup>7</sup>

<sup>6</sup> This prior approval requirement is waived if the company did not realize the services were non-audit services at the time of the auditor's engagement, and the aggregate amount of the non-audit services provided is less than five percent of the total amount paid to the auditor by the company in that fiscal year. In such circumstances, however, the non-audit services must be promptly brought to the attention of the company's audit committee and approved by the audit committee (or a designated member) before the conclusion of the audit.

<sup>7</sup> The precise wording for these certifications may be found in the SEC's final rules, which became effective on August 29, 2002. (1934 Act Release No. 34-46427 [August 28, 2002]).

A separate certification requirement is included in section 906 of the Act, which became effective on July 30, 2002. Section 906 requires that all periodic reports containing financial statements filed by a public company under sections 13(a) or 15(d) of the 1934 Act include a written certification by the CEO and CFO (or equivalent) that the report complies with the requirements of the 1934 Act and fairly presents, in all material respects, the financial condition and results of operations of the company. Persons that knowingly or willfully file false certifications under section 906 are subject to criminal penalties.

**2. Reports Must Reflect Material Correcting Adjustments.** Section 401 of the Act requires that all periodic reports filed by public companies that are required to include GAAP financial statements must reflect all material correcting adjustments identified by the company's auditor

**3. Management Assessment of Internal Controls.** Section 404 of the Act directs the SEC to issue rules requiring the annual reports filed by public companies to include a statement that management is responsible for maintaining an adequate internal control structure and procedures for financial reporting and contain an assessment of the effectiveness of these controls and procedures. The company's external auditor also must attest to, and report on, management's assessment.<sup>8</sup> On October 16, 2002, the SEC requested comment on proposed rulings to implement section 404. These rules should soon be available on the SEC's web site at <http://www.sec.gov>.

**4. Additional Disclosure Requirements.** By January 26, 2003, the SEC must issue final rules that require all quarterly and annual reports filed by public companies to disclose all material off-balance sheet transactions, arrangements, obligations and other relationships with unconsolidated entities or persons. In addition, by January 26, 2003, the SEC must issue final rules that prohibit public companies from including misleading *pro forma* financial information in their press releases, filings with the SEC or other public disclosures, and that require any *pro forma* information included in such documents to be reconciled with the company's GAAP financial statements. Section 409 of the Act also authorizes the SEC to issue additional rules requiring public companies to disclose material changes in their financial condition or operations to the public on a rapid and current basis.

### **Other Provisions Affecting Public Banking Organizations**

The Act contains a variety of other provisions affecting public companies and their officers, directors, and auditors. Some of these provisions are self-executing, *i.e.*, they are or will become effective without the adoption of implementing regulations. These include a requirement that CEOs and CFOs of public companies reimburse their company for specified types of compensation and profits if the company is forced to restate its financial statements as a result of misconduct (section 304), and a provision prohibiting executive officers and directors of public companies from purchasing or selling equity securities of the company acquired in connection with their service as an officer or director during any "blackout period" involving the security (section 306(a)).<sup>9</sup>

The SEC also has already adopted rules implementing (i) section 403, which accelerated the timeframe for officers, directors, and significant shareholders of a public company to disclose any purchases or sales of the company's equity securities;<sup>10</sup> (ii) section 303, which prohibits officers and directors of a public company from fraudulently coercing or misleading the company's auditors for the purpose of creating materially misleading financial statements; (iii) section 406 which requires public companies to disclose whether the company has adopted a code of ethics for their senior financial officers and, if not, the reasons why not; and (iv) section 407, which requires public companies to disclose whether the company's audit committee includes a "financial expert" and, if not, the reasons why not.<sup>11</sup>

<sup>8</sup> The requirements of section 404 closely mirror those established by section 112 of the Federal Deposit Insurance Corporation Improvement Act (12 U.S.C. 1831m) and part 363 of the FDIC's regulations, which include internal control, management assertion and accountant attestation requirements for insured depository institutions with total assets of \$500 million or more.

<sup>9</sup> Section 304 became effective on July 30, 2002, while section 306(a) will not become effective until January 26, 2003.

<sup>10</sup> 1934 Act Release No. 34-46421 (August 27, 2002).

<sup>11</sup> SEC Press Release 2002-150 (October 16, 2002).

## **Foreign Banking Organizations**

The provisions of the Act generally apply to any public company, regardless of where the company is based. Therefore, foreign banking organizations that have securities listed on a U.S. national securities exchange, or that are otherwise required to file periodic reports with the SEC under sections 12 or 15(d) of the 1934 Act, generally must comply with the Act's requirements.

## **Non-Publicly Held Banking Organizations**

Banking organizations that are not public companies generally are not covered by the provisions of the Act, but may be subject to similar requirements under other laws or Federal Reserve or FDIC regulations. For example, top-tier bank holding companies that are required to file Forms FR Y-6 and that have total assets of \$500 million or more must have an annual audit of their consolidated financial statements conducted by an independent public accountant. In addition, insured depository institutions with total assets of \$500 million or more must have an annual audit conducted by an independent public accountant and must have an audit committee composed entirely of directors that are independent of management. (12 U.S.C. 1831m; 12 CFR part 363).

## **SEC Regulations and Federal Reserve Supervisory Guidance**

The SEC has begun and will continue to implement the Act and provide guidance to public companies through its regulations and releases. Examination staff and public banking organizations are encouraged to remain current on SEC issuances in this area, which are generally available through the SEC's web site <http://www.sec.gov>. Supervisory staff and banking organizations should refer to the Act and the SEC's releases for additional guidance concerning the effective dates of the Act's provisions.

Federal Reserve staff, together with staff of the other federal banking agencies, currently are reviewing existing regulations and guidance to determine whether modifications to these regulations and guidance are appropriate in light of the Act. As part of this review, the agencies are working to develop policies for non-public banking organizations that are in accord with the purposes and provisions of the Act.

## **E-Notification**

The Federal Reserve Bank of San Francisco will notify depository institutions by e-mail of new Banking Supervision and Regulation circular letters recently posted on the Twelfth District Federal Reserve Bank web site. We will e-mail a summary of the letter as well as a link to the full text of the letter and its attachments to view and print. We will discontinue hard copy mailings at the end of the year. We will be discontinuing hard copy mailings at the end of the year. To subscribe to this free service, simply visit our web site at <http://www.frbsf.org/banking/> and click on the E-Notification logo.

## **Additional Information**

All circulars and documents are available on the Internet through the Federal Reserve Bank of San Francisco's Internet site, at <http://www.frbsf.org/banking/letters>. Paper copies of the notice (**SR 02-20**) are available from our Corporate Services Department. To request copies to be sent by mail, please call (415) 974-2060.

For additional information about the Sarbanes-Oxley Act of 2002, please contact our Banking Supervision and Regulation Department at (415) 974-2936.