

Commentary

Sarbanes-Oxley & Internal Controls: The Not So Hidden Implications For Information Technology And Information Security

By
Ronald I. Raether Jr.
and
Brian D. Wright

[Editor's Note Mr Raether is a partner in the law firm of Faruki Ireland & Cox P.L.L. Mr Wright is an associate in that firm. Both have considerable experience with litigating and advising companies with technology-related matters, including information security and protection of personally identifiable information against data security breaches. Faruki Ireland & Cox serves as counsel in specific litigation matters for LexisNexis. Mealey Publications is owned by LexisNexis, which is a division of Reed Elsevier Inc. The views expressed in this article are those of the authors and not of Mealey Publications. Copyright 2006 by the authors. Responses are welcome.]

I Introduction And Summary

As the early-2000s may be defined as the era of accounting irregularities and the restatement of public filings, the mid-2000s are becoming widely viewed as the era of the data security breach. In 2005, over 100 data security breaches were reported, which affected some 50 million people.¹ In 2006, the reports of data security breaches continue. With every announcement of another security breach comes added public pressure for Congress to act to provide new legislation that requires more protection for consumers' personally identifiable information. Given the enormity of the task and political difficulty of preparing and passing such broad-based legislation, the public pressure has begun to shift away from seeking new legislation to seeking other avenues to provide protection of personally identifiable information.²

For example, companies such as ChoicePoint, Inc., BJ's Warehouse, DSW Inc., and CardSystems Solutions, Inc. may have felt the results of such pressure. Each of these companies has been the subject of a recent enforcement action or a consent agreement with the Federal Trade Commission ("FTC"). In a somewhat unconventional manner, the FTC has begun to use Section 5 of the Federal Trade Commission Act ("FTC Act") and the Gramm-Leach-Bliley Act ("GLB Act") to bring enforcement actions or enter into a consent agreement after data security breaches.³ Lesson learned — Regulators are seeking ways to expand their zone of regulation to meet the needs of changing technology, including the protection of personally identifiable information and information security.

In light of the mounting public pressure, almost daily announcement of another data security breach, and increase in the willingness of governmental agencies to look to existing legislation for added authority, lawyers (both outside and in-house) should take a fresh look at existing laws to examine them for possible new ways that their clients could come under scrutiny from governmental regulators. One possible place to start is the Sarbanes-Oxley Act of 2002 ("Sarbanes-Oxley Act"). Given the broad language used by both Congress in creating the Act and the Securities and Exchange Commission ("SEC") in drafting regulations as directed under the Act, it is possible that the SEC could attempt to use the Sarbanes-Oxley Act as

an avenue to address lapses in information security or to prevent (or react to) data security breaches that occur in publicly-owned companies

II Sarbanes-Oxley Act Of 2002

In the wake of the accounting and corporate governance scandals of the early 2000s, on July 29, 2002, Congress passed the Sarbanes-Oxley Act, which was signed by President Bush the next day⁴ Several high-profile public company bankruptcies (including Enron, WorldCom, and Global Crossing), and the negative stock market reaction to those bankruptcies are some of the well-known forces that drove Congress to rush to pass Sarbanes-Oxley The bankruptcies, which brought along with them the corporate governance and accounting scandals, shattered public confidence in the stock market, the boards of directors of public companies, and the government regulators that oversee those businesses, like the SEC In an attempt to ameliorate the damage caused to the public's confidence in public companies and the equities markets, Congress passed the Sarbanes-Oxley Act, which has been called "the most important securities legislation since the original federal securities laws of the 1930s"⁵

The Sarbanes-Oxley Act has six core initiatives (1) the creation of the Public Company Accounting Oversight Boards to watch over the audits of the public companies that are subject to securities laws,⁶ (2) the establishment of rules requiring the independence of public company auditors,⁷ (3) regulation of corporate governance,⁸ (4) the enhancement of financial disclosures,⁹ (5) regulation of securities analysts' conflicts of interest,¹⁰ and (6) creation of new substantive crimes and enhancement of penalties for violations of securities laws¹¹

While several of the above initiatives have had a major effect on how attorneys (both outside and in-house) advise their corporate clients, those same attorneys may want to take a closer look at Sections 302 and 404 (and their internal control components) as it is possible that those sections could have an unanticipated impact on information security and the information technology departments of public companies

A. Sections 302 And 404 And Internal Controls Requirements

The establishment and maintenance of internal controls are mandated by two separate sections under the Sar-

banes-Oxley Act (Sections 302 and 404), both of which require certification by executives or management¹²

Section 302 of the Sarbanes-Oxley Act requires companies to take more responsibility for the accuracy of their financial reports With this goal in mind, Section 302 requires, among other things, that the officers of publicly-held companies certify that the reports filed with the SEC do not "contain any untrue statement of a material fact" and that the reports "fairly present in all material respects the financial condition and results of operations of the issuer"¹³ Section 302 also requires certification and acknowledgement by the officers regarding the use of internal controls¹⁴

More specifically, "the signing officers" must certify that they — "(A) are responsible for establishing and maintaining internal controls, (B) have designed such internal controls to ensure that material information relating to the issuer and its consolidated subsidiaries is made known to such officers by others within those entities, particularly during the period in which the periodic reports are being prepared, (C) have evaluated the effectiveness of the issuer's internal controls as of a date within 90 days prior to the report; and (D) have presented in the report their conclusions about the effectiveness of their internal controls based on their evaluation as of that date"¹⁵

Section 404 of the Sarbanes-Oxley Act requires a company's management to assess the internal controls of the company and to provide "an internal control report" as part of each company's annual report¹⁶ The "internal control report" must "(1) state the responsibility of management for establishing and maintaining an adequate internal control structure and procedures for financial reporting, and (2) contain an assessment, as of the end of the most recent fiscal year of the issuer, of the effectiveness of the internal control structure and procedures of the issuer for financial reporting"¹⁷ While the above requires management to certify to the assessment of internal controls, Section 404 also requires public audit firms to provide a similar certification¹⁸

Sections 302 and 402 raise an interesting question — what exactly are internal controls? In the "Final Rule Management's Reports on Internal Control Over Financial Reporting and Certification of Disclosure in Exchange Act Periodic Reports" ("Final

Rule”),¹⁹ the SEC defines “internal control over financial reporting” as “[a] process designed by, or under the supervision of, the registrant’s principal executive and principal financial officers, or persons performing similar functions, and effected by the registrant’s board of directors, management and other personnel, to provide reasonable assurance regarding the prevention or timely detection of unauthorized acquisition, use or disposition of the registrant’s assets that could have a material effect on the financial statements”²⁰

In its Final Rule, the SEC made clear that “internal control is a broad concept that extends beyond the accounting functions of a company”²¹ The SEC further stated “that [the third] provision [above] is specifically included to make clear that, for purposes of our definition, the safeguarding of assets is one of the elements of internal control over financial reporting and it addresses the supplementation of the COSO Framework after it was originally promulgated”²²

The COSO (The Committee of Sponsoring Organizations, of the Treadway Commission or “COSO”)²³ developed its “Framework” in 1992 In the “supplementation of the COSO Framework,” the COSO defines “internal control over safeguarding of assets against unauthorized acquisition, use or disposition” as “[i]nternal control over safeguarding of assets against unauthorized acquisition, use or disposition is a process, effected by an entity’s board of directors, management and other personnel, designed to provide reasonable assurance regarding prevention or timely detection of unauthorized acquisition, use or disposition of the entity’s assets that could have a material effect on the financial statements”²⁴

Based upon the reasoning above, if a company does not have sufficient internal controls over its information security so that it can provide a “reasonable assurance regarding the prevention or timely detection of unauthorized acquisition, use or disposition of the entity’s assets” and that company finds itself the victim of a data security breach, then it is possible that the company could find itself subject to scrutiny from the SEC for violations of Sections 302 or 404 of the Sarbanes-Oxley Act

B. Data Breach Examples

Instead of examining recent FTC consent agreements and enforcement actions as unfair and deceptive trade

practice violations of Section 5 of the FTC Act, consider how the SEC could have attempted to bring an action against each of the involved companies to show violations of Sections 302 or 404 of the Sarbanes-Oxley Act Two recent enforcement actions brought by the FTC involving ChoicePoint, Inc (“ChoicePoint”) and CardSystems Solutions, Inc (“CardSystems Solutions”) provide interesting case studies for how the SEC could claim jurisdiction if a publicly-owned company suffers a serious data security breach²⁵

ChoicePoint, a publicly-traded company, settled with the FTC after the records of more than 163,000 consumers in its databases were compromised²⁶ ChoicePoint is in the business of providing identification and credential verification services to businesses, governments, and other entities²⁷ To perform such a service, ChoicePoint furnishes consumers’ personal information, in various combinations and product lines, to its customers²⁸ In sum, ChoicePoint’s major asset is consumers’ personal information

In February 2005, ChoicePoint announced that it may have disclosed the personal information of 145,000 consumers to persons that did not have a lawful purpose²⁹ Later in the same year, ChoicePoint announced that an additional 17,000 consumers may have been subject to an unauthorized disclosure³⁰ In its complaint, the FTC alleged that “ChoicePoint has fail[ed] to employ reasonable and appropriate security measures to protect consumers’ personal information”³¹ ChoicePoint agreed to pay \$10 million in civil penalties — the largest civil penalty in FTC history — and to provide \$5 million for consumer redress³²

There is little doubt that ChoicePoint’s breach had a material effect on its business Its stock fell 31 percent on the day the breach was reported, and then continued to fall³³ Moreover, ChoicePoint’s data breach also had a material effect on its financial statements On March 4, 2005, ChoicePoint filed a Form 8-K with the SEC disclosing the breach and stated that as a result of the breach that “[w]e cannot currently accurately estimate the impact on our operating results and financial condition”³⁴

In fact, ChoicePoint’s data security breach and unauthorized disclosure of information did get the attention of the SEC As ChoicePoint announced in its 8-K, “[w]e have received notice from the [SEC]

that [it] is conducting an informal inquiry into the circumstances surrounding any possible recent identify theft, recent trading in ChoicePoint stock by our Chief Executive Officer and Chief Operating Officer and related matters”³⁵ Although no Sarbanes-Oxley violations were announced as being found by the SEC as a result of the data security breach, such a finding by the SEC might have been supportable

The ChoicePoint matter is not the only example of a data security breach having a material effect on a business. In the CardSystems Solutions’ matter, the FTC entered into a consent agreement with CardSystems Solutions (and its successor, Solidus Networks, Inc. d/b/a Pay By Touch Solutions) after CardSystems Solutions announced in June 2005 that over 40 million consumers had their personally identifiable information exposed after a data security breach.³⁶ CardSystems Solutions is in the business of providing merchants with products and services used to process credit and debit card purchases.³⁷ CardSystems Solutions collects and stores personal information about each of the consumers whose credit or debit card was processed (including the card number and expiration date of the credit or debit card).³⁸

In its complaint, the FTC alleged that CardSystems Solutions engaged in a number of practices that “failed to provide reasonable and appropriate security for personal information.”³⁹ Eventually, CardSystems Solutions entered into a consent agreement with the FTC. In addition (and more significant — and material — to CardSystems’ business), several credit card companies, including Visa and American Express, ceased doing business with CardSystems Solutions.⁴⁰ The data breach and the resulting loss of the business, among other things, eventually led to the acquisition by its successor, Solidus Networks, Inc.⁴¹

If a publicly-owned company suffers a data security breach similar to ChoicePoint and CardSystems Solutions, then it is not a stretch to imagine that the SEC could attempt to use Sarbanes-Oxley as a way to find that those companies did not provide a reasonable assurance regarding prevention or timely detection of unauthorized acquisition, use or disposition of the entity’s assets that could have a material effect on the financial statements. In addition to the FTC action for violations of the FTC Act, publicly-owned companies faced with issues like those confronted by

ChoicePoint and CardSystems Solutions could also face additional scrutiny from the SEC for violations of the Sarbanes-Oxley Act

III Proactive And Affirmative Steps

It is difficult to predict the future. Absent new legislation, public pressure and future data security breaches could result in increased pressure on government regulators to use existing legislation to expand their zone of regulation to force companies to better protect consumers’ personally identifiable information. While the core purpose of Sarbanes-Oxley will always be to ensure accurate financial reporting, the lack of appropriate internal controls combined with a data security breach could result in additional scrutiny from the SEC on regulated companies that suffer a data breach. Even if such a result is deemed unlikely (as the case may be), companies should be proactive and should take affirmative steps to ensure that internal controls are in place to prevent any data security breaches or an unauthorized acquisition, use or disposition of the company’s assets. Such proactive steps are especially important when the company’s assets are the data itself.

In an effort to be proactive, internal control audits should include a review of the company’s data security elements and involve information technology experts. A thorough audit studies and assesses the company’s internal technology controls and information technology infrastructure. During the audit, the technology experts examine the company’s information systems, practices, and policies with the goal of determining whether the company’s systems adequately safeguard assets (including the personal information of its employees and customers). At the audit’s conclusion, an attestation from the technology experts is available to affirm the availability, confidentiality, and integrity of the company’s information technology systems.

In addition, since the legal standards continue to evolve, involvement of legal counsel who have expertise with not only Sarbanes-Oxley audits, but expertise in high-technology and privacy legislation and regulation becomes important. Optimization of the audit’s benefits is achieved when legal counsel work closely with the company and its information technology auditors to make sure that the company has the proper internal technology controls to safeguard