

# LAW UPDATE

## From the Editor's Corner



Seth I. Rubin

*The RMF Corporate and Securities Law Update is designed to give you an overview of important topics facing the business world today. This issue focuses on a new data security and notification law*

*recently passed in New York State and on new IRS – deferred compensation rules. It also provides important information on the SEC's recent extension of compliance requirements in connection with Section 404 of the Sarbanes-Oxley Act. We encourage you to e-mail us with your questions so we can devote future articles to the issues you deem critical in our field. I hope to hear from you at [srubin@rmfpc.com](mailto:srubin@rmfpc.com).*

## Inside Update

- 2 SEC Votes to Extend Section 404 Compliance Deadline for Small Companies
- 3 Attention Employers: New Guidelines on Deferred Compensation Rules

## New York is Latest State to Adopt Security Breach Notification Law

by Barry R. Carus



Barry R. Carus

Many states have implemented data security and notification laws as a means to ensure accountability among the overwhelming number of businesses and governmental agencies that rely on databases containing the personal information of individuals. New York recently became the latest state to pass such a law as Governor George Pataki, on August 10, 2005, signed a bill that has been cited as the strictest security breach law yet. The New York law, known as the Information Security Breach and Notification Act, applies to any company, large or small, that maintains personal data, and makes no exceptions for small data breaches or breaches unlikely to result in identity theft, or for companies that have adopted their own disclosure policies.

Security breach laws have been enacted by many states in response to the occurrence of highly publicized personal data security breaches such as Choice Point, a data mining company, and DSW shoe outlet, which faced the theft of customer credit card information during last year's holiday season, exposing thousands of New York consumers and over a million customers in the U.S.

The new law took effect on December 8, 2005. In passing the law, the legislature was clear that its purpose is to "guarantee state residents the right to know what information was exposed during a breach, so that they can take the necessary steps to both prevent and repair any damage they may incur because of a public or private sector entity's failure to make proper notification."

While the Security Breach Law contains new notification requirements affecting both state entities and businesses, the primary focus of this article will be on the new requirements on businesses. Upon discovery or notification of a breach in the security of their system – either an unauthorized acquisition, or an acquisition without valid authorization of computerized data that compromises the security, confidentiality or integrity of personal information maintained by a business – a company (which owns or licenses computerized data, which includes private information) must provide personal notification to any New York resident whose private information was, or is reasonably believed to have been, acquired by a person without valid authorization. This notification must be made in the most expedient time possible and without delay.

Personal notification can be in one of several forms, including written notice, or electronic or telephone notice, provided the business (i.e., the notifier) follows certain procedures described in the law. However, if the business can demonstrate to the New York State

*Continued on Page 2*

*Continued from page 1*

Attorney General that the cost of providing personal notice exceeds \$250,000, or that the affected class of people to be notified exceeds \$500,000, an alternative method of notice may be provided consisting of e-mail notice (when the business has an e-mail address for the subject persons); conspicuous posting of the notice on the businesses' web site; and notification to major statewide media.

Regardless of how the notice is provided, it must include certain specific information for the business making the notification, including its contact information, a description of the categories of information comprising the security breach and specifics as to what personal or private information may have been acquired. In the event of a breach requiring any New York residents to be notified, the law also requires the business to notify the New York State Attorney General, the Consumer Protection Board and the State Office of Cyber Security, and further requires "critical infrastructure coordination as to the timing, content and distribution of the notices and approximate number of affected persons." The notification requirements become stricter if more than 500,000 New York residents are to be notified at one time – this would require the business to also provide consumer reporting agencies with all the same information.

### **Taking the Initiative to Limit or Avoid a Security Breach**

Because of these strict notification requirements, businesses have a strong incentive on various levels to adopt or improve their precautionary security and encryption procedures to ensure they do not face the penalties of noncompliance with the law. First, there is the cost of providing the notifications, which increases in scope depending upon the level of breach. Next, there is the cost in terms of loss of business reputation which results from the required public disclosures. Furthermore, the New York Attorney General may sue a business that violates the law and seek to recover damages for actual costs or losses incurred by a person entitled to notice, including consequential financial losses. These damages will likely multiply as the number of people affected by the breach of security rises. Finally, the law authorizes a court to impose a civil penalty, up to a maximum of \$150,000.

While management and IT departments of companies face many competing challenges for their time, all companies, including consumer-related companies in particular, should (if they have not already done so) commit the necessary time and resources to create and adopt a plan of action in the event of a security breach in order to limit the damage they may face if such an unfortunate event occurs. In considering compliance with the law, companies should develop a comprehensive series of best practices to ensure their security procedures are designed to limit the vulnerability of their systems to security breaches, and that their notification policy meets or exceeds the standards set forth in the law. Companies should undertake this important initiative by coordinating their efforts with their IT professionals (to design appropriate strategies for security and compliance of all information technology, including personal and private information), auditors (to ensure proper internal controls and Sarbanes-Oxley compliance) and attorneys (to ensure compliance with State and Federal standards on limiting identity theft).

## **SEC Votes to Extend Section 404 Compliance Deadline for Small Companies**

by Seth I. Rubin

On September 21, 2005, the Securities and Exchange Commission (SEC) granted a one-year extension to smaller companies to comply with reporting requirements of Section 404 of the Sarbanes Oxley Act of 2002 (SOX). Section 404, as implemented by the SEC, requires that each public company provide a report of management's assessment of the company's internal control over financial reporting. The report by management is to be accompanied by an auditor's report on the subject, and the combined reports are to be filed as part of the company's annual report on Form 10-K.

The SEC's announcement impacts nearly 6,000 companies and means that non-accelerated filers now have until their first fiscal year ending on or after July 15, 2007 to file internal control reports. Non-accelerated filers are companies that have, among other things, public equity float of less than \$75 million, have been a registrant for at least twelve months, and are not eligible to file reports with the SEC under the small business issuer rules. The decision to extend the compliance deadline was intended to provide additional time for the release of guidance on how smaller public companies should comply with Section 404 requirements, and to give the SEC additional time to evaluate the impact of Section 404 on smaller public companies.

The cost of implementing Section 404 of SOX has been a major source of complaint by companies large and small ever since SOX was enacted three years ago. The SEC's decision to once again extend the compliance deadline for smaller companies was driven, in large part, by the continuing cacophony of horror stories coming from business leaders around the country who bemoan the adverse impact Section 404 is having on their companies.

One of the main complaints is that smaller businesses are paying a significantly higher percentage of their revenues for SOX compliance than their large company counterparts because auditors are treating all companies alike in their internal controls assessments.

Evidence of the overwhelming cost of Section 404 compliance can be seen in the vastly increased number of companies that have already been taken private, or have announced plans to go private in the future. Several hundred companies have been taken private or announced plans to do so since the passage of SOX and many of them specifically list SOX compliance costs as justification for going private. This cannot be viewed as a healthy situation for the companies involved, nor for the shareholders of these companies who may face the possibility of owning shares in private companies not bound by the public reporting requirements of the Securities Exchange Act of 1934.

While the most recent extension is certainly good news for those smaller companies which would have been required to comply with Section 404 in fiscal year 2006, it should also be viewed as a wake-up call to those companies that have not yet begun to address their Section 404 deficiencies. Achieving compliance with Section 404 will not occur overnight but will take several months. Most non-accelerated filers lack the infrastructure to comply with Section 404 and require significant time to determine which processes require documentation and testing, and which ones show evidence of weakness and require correction.

Small companies would be well advised not to count on the SEC for additional extensions of Section 404 compliance requirements. While this is not the first extension of time given by the SEC in connection with Section 404, it may well be the last. As such, companies must decide whether it is worthwhile to remain public and, if so, to move quickly to begin the compliance process.

**Seth I. Rubin** is a senior associate in the firm's Corporate & Securities Department and Corporate Governance Practice Group. He can be reached at [srubin@rmfpc.com](mailto:srubin@rmfpc.com) or 516-663-6691.

## Attention Employers: New Guidelines on Deferred Compensation Rules

by Adam Silvers and Michael Schnipper



**Adam Silvers**



**Michael Schnipper**

With the adoption of the American Jobs Creation Act of 2004, and more particularly, Section 409A, Congress heavily regulated deferred compensation plans. Section 409A prohibits acceleration of payments of deferred compensation, provides detailed rules as to the date upon which an election to defer compensation must be made, and limits the events upon which payments under a deferred compensation plan may be made. Due to the complexity and comprehensiveness of the new rules, the IRS has released guidelines and extended the deadline for compliance with Section 409A to December 31, 2006. However, the IRS did not extend the December 31, 2005 deadline for termination of existing plans and the immediate good faith compliance requirement. Therefore, employers must immediately consider and act on the new law and the related regulations.

Section 409A covers any “nonqualified deferred compensation plan,” which includes any plan or agreement providing for the deferral of compensation. The IRS takes a broad approach in defining deferred compensation plans but exceptions do exist. Section 409A does not apply to amounts deferred prior to December 31, 2004, as long as the amounts were earned and vested as of December 31, 2004 and the plan is not materially changed after October 3, 2004.

---

*“Failure to comply with the provisions of Section 409A may result in the acceleration of tax assessments, as well as imposition of a 20% penalty, which must be paid by the employee.”*

---

Under the new law, the assessment of taxes will not be deferred unless a deferred compensation plan satisfies the following requirements:

- 1) Distribution of amounts under the plan may not be made until (a) there is a separation from service; (b) the employee is disabled; (c) the death of the employee; (d) a specified time or a time designated by the plan at the date the compensation is deferred; (e) the occurrence of a change in control of the employer; or (f) an unforeseeable emergency, whichever shall occur first.
- 2) Participants in the plan must elect to defer compensation before the beginning of the tax year in which compensable services will be provided. Newly eligible participants will have a thirty (30) day period to make the election.
- 3) If under the terms of a plan, restrictions are placed on certain assets of the employer when the employer’s financial condition is adversely impacted so as to make those assets only available for the payment of benefits, participants in the plan will be taxed as of (a) the date of the agreement which provides for such restrictions even if contingent on the financial condition of the employer; or (b) the date the assets actually become restricted, whichever occurs earlier.

Failure to comply with the provisions of Section 409A may result in the acceleration of tax assessments, as well as imposition of a 20% penalty, which must be paid by the employee. The IRS has noted that its auditors will be reviewing the terms of deferred compensation arrangements and comparing them to the new statute and related guidelines for compliance when conducting their audits. Until recently, much of the effect of the new statute on deferred compensation was unknown. However, on September 29, 2005, the IRS issued proposed regulations under Section 409A. The proposed regulations are the most detailed discussion of the new statute to date.

The proposed regulations also served to extend the deadline for compliance with Section 409A. IRS guidance issued in 2004 allowed companies to bring their deferred compensation plans within compliance of Section 409A by December 31, 2005.

## About the Firm

Founded in 1968, Ruskin Moscou Faltischek, P.C. has emerged as Long Island's preeminent law firm. As specialized as we are diverse, we have built cornerstone groups in all of the major practice areas of law, and service a diverse and sophisticated clientele. With more than 60 attorneys, superior knowledge of the law, polished business acumen and proven credentials, Ruskin Moscou Faltischek has earned a reputation for excellence and success. It is this ongoing achievement that makes us an acknowledged leader among our peers and the preferred choice among business leaders.

The strength of Ruskin Moscou Faltischek's resources greatly enhances what we can accomplish for our clients – to not only solve problems, but to create opportunities. We take pride in going beyond what is expected from most law firms. The invaluable contacts and relationships we have nurtured in the business community and our multidisciplinary approach heighten our value-added services.

*Continued from page 3*

The September 29, 2005 regulations extend this deadline to December 31, 2006. All terminations of plans and cancellations of existing deferral elections must have been completed by December 31, 2005 or Section 409A will apply. It must be noted that companies must comply with Section 409A in good faith throughout the extension. Good faith compliance requires employers to administer a plan in a manner which is consistent with Section 409A, even though formal amendment of the plan is not required until the effective date.

The best practice for employers is to begin reviewing all deferred compensation plans as soon as possible and to consult with their legal and tax advisors to determine if Section 409A will govern. Of particular concern are individual employment agreements that may contain provisions classified as a deferred compensation plan under Section 409A. Any plans governed by Section 409A should be closely scrutinized to confirm compliance with the new rules and be modified as needed to comply with the law.

**Adam Silvers** is a partner and a member of the Corporate & Securities Department and Intellectual Property Group. He also chairs the firm's Technology Practice Group. He can be reached at [asilvers@rmfpc.com](mailto:asilvers@rmfpc.com) or 516-663-6519.

**Michael Schnipper** is an associate in the Corporate & Securities Department. He can be reached at [mschnipper@rmfpc.com](mailto:mschnipper@rmfpc.com) or 516-663-6674.

The Corporate & Securities Update is published to provide information about developments in corporate and securities matters. It is not a substitute for legal advice and should not be construed as imparting legal advice generally or on specific matters. Please contact newsletter editor Seth Rubin or a specific author if you have comments or questions, or if you have suggestions for future issues.

Copyright © 2005 Ruskin Moscou Faltischek, P.C. All Rights Reserved.

Sandra McGrath - Paralegal

William A. Ubert

Adam P. Silvers

Stuart M. Sieger

Michael I. Schnipper

Molly M. Rush

Harold M. Rothstein

Arthur "Jerry" Kremer

Michael L. Faltischek

Barry R. Carus

Leora F. Arlizzzone

Seth I. Rubin, Editor

Irvin Brum, Chair

516.663.6600 ▲ [www.rmfpcc.com](http://www.rmfpcc.com)

New York City ▲ Uniondale ▲ Hauppauge

1425 Reckson Plaza, Uniondale, NY 11556-1425

East Tower, 15th Floor

Smart Counsel. Straight Talk.

RUSKIN MOSCOU FALTISCHEK P.C.



PRSRRT STD  
U.S. POSTAGE  
PAID  
Permit 135  
Smithtown, NY