

## ONPOINT

A publication of Schneider Downs &amp; Co., Inc.



INSIGHT ■ INNOVATION ■ EXPERIENCE

Summer 2010 • Volume 28 • Issue 3

## &gt;&gt; IN THIS ISSUE

- 1 Costly Mistakes: What We Can Learn From the Five Largest Data Breaches Reported Under HITECH
- 1 Key Tax Dates
- 3 Key Fundamentals of Reviewing and Assessing Service Auditor Reports
- 4 The Future of E-Filing is Here: It's Mandatory!
- 4 Wealth Management: Question of the Quarter
- 5 Around Schneider Downs
- 5 New Hires
- 5 Benefit Plan Due Dates
- 6 Professional News

## KEY TAX DATES

## OCTOBER

15

**Individuals.** Last day for filing 2009 Form 1040 for individuals who obtained automatic six-month filing extension.

31 (due November 1)

**Employers.** Employers of nonagricultural and nonhousehold employees must file return on Form 941 to report income tax withholding and FICA taxes for the third quarter of 2010.

## DECEMBER

15

**Estimated Tax.** Payment of last installment of 2010 estimated tax by calendar-year corporations.

See Page 5 for additional key dates

## Costly Mistakes: What We Can Learn from the Five Largest Data Breaches Reported Under HITECH

by Christopher Watson, Manager, Internal Audit and Risk Advisory Services

Data breaches involving private healthcare information have been high-profile news stories lately. With recent changes to HIPAA enforcement, as well as notification requirements, organizations are beginning to clearly see the impact of data breaches and the risks and costs associated with them.

In September of 2009, the HITECH Act put forth a data breach notification rule that requires all healthcare providers to report breaches affecting more than 500 individuals. Since February 22, 2010, when the official federal list of reported data breaches was launched, there have been 99 reported breaches involving nearly 3.5 million individuals.

The most shocking aspect of this listing is not the number of breaches, or even the number of records involved, but the ease with which they could have been prevented. Of the five largest breaches reported, three were related to the theft of unencrypted hard drives, one was related to the theft of an unencrypted laptop, and another was related to the unencrypted storage of information on leased copiers.

In its fifth annual study, the Ponemon Institute found that the average financial

cost of a breached customer record has risen to almost \$204. These numbers come from a detailed analysis of 45 specific data breach cases ranging from 5,000 to 101,000 affected records per incident. In addition to these hard costs, there are soft costs associated with a breach that must also be taken into consideration, such as reputational damage and loss of patient privacy.

Take a look at the five largest breaches that have been reported to the U.S. Department of Health and Human Services Office for Civil Rights:

### AvMed Health Plan

The theft of two laptops containing patient information was reported by AvMed in February of 2010. One of the laptops was encrypted and later recovered; however, the other was not encrypted and is still missing. A potential 1.2 million records were involved.

### BlueCross BlueShield of Tennessee

A theft of 57 unencrypted hard drives from servers at a leased facility in Chattanooga, Tennessee that was a former call center has resulted in nearly one million individuals being affected.

Continued on Page 2

## Data Breaches *continued from Page 1*

### Affinity Health Plan

The managed care plan provider notified more than 409,000 customers about a breach related to returned leased copy machines that contained hard drives with unencrypted patient information stored on them. The issue was discovered by CBS News during its investigation of the contents of four copy machines that had been purchased from a leasing company.

### Emergency Healthcare Physicians Ltd.

An emergency physician group notified 180,000 of its patients after an unencrypted portable hard drive was stolen from a billing service.

### Providence Hospital

Close to 84,000 patients were affected when an unencrypted hard drive was stolen from a locked office.

All of these breaches were easily preventable through the implementation of appropriate information security standards. It is important to realize that, while the encryption of sensitive data is a good practice, it is not the only step that should be taken in order to mitigate the risk of potential data breaches. The implementation of an appropriate compliance and information security program could have mitigated, or even prevented, the risk to these affected organizations altogether.

Here are some initial steps to follow:

- Assign formal responsibilities. Designate personnel to spearhead the effort, and involve multiple business units in the direction of the Information Security Program such as IT, HR,

Payroll, Legal, etc. Communicate the philosophy that information security resides in all aspects of the organization, not just IT.

- Conduct an Information Security Risk Assessment. This assessment should answer the following questions:

- What data do I have that is at risk, and where is it located? Ensure that data is classified throughout the organization, including in test environments, at key vendors, etc.; that its storage and transmittal is evaluated; and that owners of the data are assigned.

- What is the potential impact of a data breach, and what are my financial, operational, regulatory and reputational risks?

- What are the potential threats and exposures?

- What steps can be taken to mitigate my risk and overall exposure?

- Develop appropriate policies for the organization to follow, such as a Portable Media Device Policy,

Encryption Policy, Data Destruction Policy, Data Retention Policy, Vendor Management Policy, Incident Response Policy, etc.

- Train your employees on these policies and appropriate best practices, and ensure that they understand how to comply with your policies. Training not only provides users

with the tools to identify, prevent and escalate potential incidents, but it also sends a message to potential internal threats that there are people watching and that there will be

penalties to violations of the policies.

- Implement controls and security layers around your data in order to reduce your risks.
- Test your controls and ensure that they are operating effectively.
- Test your incident response process and ensure that, in the event of a breach, the appropriate steps would be followed.

Following these steps will put your organization on the path to an effective Information Security Program that just may keep you from being another example of how costly a data breach can become. ■



**CHRISTOPHER WATSON**  
INTERNAL AUDIT AND RISK  
ADVISORY SERVICES  
*Manager*



OnPoint is a publication of Schneider Downs & Co., Inc.

The matters highlighted in this newsletter are presented in broad, general terms and, accordingly, cannot be applied without consideration of all the circumstances. The firm will provide additional details on matters discussed in this newsletter upon request, and will be pleased to discuss with clients or their attorneys the possible effects of these matters in specific situations.

A number of clients and friends of the firm have requested permission to reprint articles from OnPoint. We are pleased that our readers find the articles informative, and encourage reproduction with acknowledgment of the source.

© 2010 Schneider Downs & Co., Inc.

PLEASE RECYCLE  
THIS NEWSLETTER.



# FEATURE ARTICLE

## Key Fundamentals of Reviewing and Assessing Service Auditor Reports

by Holly Russo, Senior Manager, and Heather Haemer, Manager, Internal Audit and Risk Advisory Services

A Service Auditor Report (sometimes called a SAS 70 or SSAE 16) is typically required by companies (“user organizations”) and their auditors (“user auditors”) that obtain significant services from another organization (“service organization”). Service organizations provide services to another corporation. Service organizations often handle sensitive or private data, and potentially conduct transactions with this data. Examples of service organizations include: application service providers, claims processing centers, real estate title and closing companies, bank trust departments, payroll and billing service providers, investment management firms, data centers or other data processing service bureaus.



The auditors of the service organization’s customers can use the Service Auditor Report to gain an understanding of the internal controls in operation at the service organization. Service Auditor Reports can be used by the user organizations’ auditors to assess internal control risk for the purposes of planning and executing a financial audit. There are numerous steps that users should perform to review and assess Service Auditor Reports. While there may be additional elements to consider, the following are key factors that users should include in their assessments:

### Identify the Type of Report

A Type I Service Auditor Report is issued as of a particular date, and states that the control objectives are in operation and that the supporting controls are suitably designed to achieve the objectives

as of that date. However, the service auditor does NOT test the operating effectiveness of controls. Thus, a Type I Service Auditor report is limited in that the *user auditor* cannot rely on the report to reduce assessment of control risk below the maximum, and they cannot reduce their independent testing.

A Type II Service Auditor Report is issued covering a period of time, and states that the control objectives are in operation as of a specified date, and that the supporting controls are suitably designed to achieve the objectives. It also states that the controls were tested and were operating with sufficient effectiveness to provide reasonable assurance that control objectives were achieved during the specified period.

Type II Service Auditor Reports may be used by *user auditors* to reduce assessment of control risk below the maximum and thus reduce their independent testing.

Type II examination periods are most useful to user auditors when the examination period includes as many months as possible within user organizations’ fiscal years. Typically, a Service Auditor Report will cover a period six months to one year in length.

### Review the Opinion

When the service auditor concludes that the description is fairly presented and that the controls are suitably designed and operating effectively for the audit period, the service auditor renders an “unqualified opinion.” If the service auditor’s procedures reveal exceptions or control deficiencies,

the service auditor may conclude that one or more control objectives could not be achieved due to a deficiency in design or operating effectiveness. When this occurs, the service auditor “qualifies” the opinion.

Whether the opinion is qualified or unqualified, the service auditor is required to document all relevant exceptions in Section III of the Service Auditor Report. Users should understand the nature of any exceptions noted in the Service Auditor Report to determine whether they raise any concerns or result in additional risk exposure to user organizations.

### Evaluate the Report for Reliance

Users should review the quality and completeness of the control objectives covered by the report and assess whether the scope of the report is adequate for reliance. The control objectives should typically cover information technology and core processes impacting users’ financial statements.

Another item in assessing the adequacy of the Service Auditor Report is to consider who performed the work. Some due diligence is required to research the service auditor’s qualifications, to determine whether the firm has adequate skill sets and assess the competency of the auditor.

### Assess the User Control Considerations

Finally, users should review and assess the user control considerations noted in the Service Auditor Report. If the user organization does not have the noted controls in place, it may warrant action by the user organization to implement suggested controls and/or determine if the user has other controls in place to mitigate the associated risks. ■



# NEWS YOU NEED

## The Future of E-Filing is Here! It's Mandatory

by Ronald A. Kramer, Director of Strategic Tax Planning

It seemed like only yesterday when the IRS introduced the technology to file returns electronically.

"E-filing" was phased in slowly at first; large partnerships were the first entities required to file this way. Electronic filing for corporations, S corporations and large nonprofits was subsequently mandated, and later, many states followed suit and instituted their own "e-filing" requirements.

For several years now, Schneider Downs has offered individual taxpayers "e-filing" as an enhancement to our standard tax preparation services. Electronic filing is simple, it reduces the IRS's error rate, it saves postage, and it's "green" – it saves massive amounts of paper. Congress apparently agrees; it recently passed the Worker, Homeownership, and Business Assistance Act of 2009, requiring specified tax return preparers to file all individual, trust and estate returns electronically. The provision is phased in over two years. Larger-volume tax preparers must comply in 2011, and smaller practitioners must comply by 2012.

Our individual clients who are familiar with this process definitely prefer e-filing to the old-fashioned method of paper filing. However, not all of our clients have embraced this new technology, and to those clients, we say: Welcome to the electronic world! For 2010 returns filed in 2011, all federal individual returns we prepare are mandated by law to be filed electronically. Currently, there is no option to elect out.

A number of states have introduced similar

*continued on Page 5*

## Q & A

### Schneider Downs Wealth Management Advisors, LP *Question of the Quarter*

#### **Q. I can't turn on the television or radio without hearing about why I should be buying gold. Is gold a good investment?**

Many investors believe that gold is a safe asset that retains its value regardless of financial market volatility, and that the value of gold increases in times of economic stress or high inflation. Marketers of gold bullion and gold coins are definitely playing upon those beliefs today. Like any advertiser, the gold salesperson is focusing on a specific message with the intent to entice the consumer to buy.



Why gold? Gold has long been used as a form of money and a store of value. Unlike many commodities, it is not consumed, it does not tarnish and it is relatively scarce. But has investing in gold provided the safe haven and inflation protection that it is credited with?

According to a recent article published by the investment management firm Payden & Rygel, the reality of investing in gold is much less attractive than the perception. For example, gold has been viewed as a safe haven in a financial crisis. However, when the market melted down in the fall of 2008, so did the price of gold. Between July 2008 and November 2008, gold lost 30% of its value. Gold recovered from this loss in 2009, but the equity market also staged a major recovery.

Another perception is that gold is a reliable store of value and a hedge against inflation. According to Payden & Rygel's research, when adjusted for inflation, gold prices are still at only half of their 1981 peak. Additionally, gold does not pay interest or dividends.

Gold prices are also not stable. Like the prices of other commodities and equities, the price

of gold can fluctuate wildly. Gold prices have been up or down in value on an average of 20% per year over the past decade.

There are some other points one might consider before climbing into the gold vault. In order for an asset class to provide enough weight to "protect" a portfolio or accrete a noticeable boost from positive performance, one should invest at least 3%

to 5% of the portfolio into that asset class. That could be a large bag of coins or bars, and the cost to safely store the investment impacts the return. Additionally, the purchase and sale of gold bullion and coins involve a bid/ask spread. This is the difference between what you must pay the seller to buy the gold and what the seller will pay you in order to take the load off your hands. Therefore, any profits are also clipped by transaction costs.

An alternative to buying gold in its metal form, is to invest in gold-related stocks or an Exchange Traded Fund (ETF) that tracks the price of gold. Both choices have their own specific pros and cons. Before jumping onto the gold bandwagon, an investor should understand the risks and rewards of the asset. As with any asset that has had a recent profitable run, the investor must remember that the performance of gold over the last several months in no way predicts its future performance. ■

*Source: Payden & Rygel Point of View, Third Quarter 2010 – Gold Myth vs Reality*

Written by Nancy L. Skeans, CPA, CFP®, Partner/Managing Director, Schneider Downs Wealth Management Advisors, LP.

## E-Filing *continued from Page 4*

filing requirements; among them are Pennsylvania, Ohio, New York and New Jersey, and we will be compliant with their regulations. Other states in which you file may also mandate electronic filing, and we will assist you in meeting this obligation.

Finally: didn't we all know this day would arrive? Once "e-file" was introduced, we knew this would be the future. Luckily, we here at Schneider Downs have become quite experienced with electronic filing, and we believe the transition will be seamless. For more information about the new "e-file" requirements and how it will affect you, please contact your Schneider Downs representative. ■



**RONALD A. KRAMER**  
**TAX ADVISORS**

*Director of Strategic Tax Planning*

## Around Schneider Downs



The Pittsburgh office fielded a team of 26 walkers to march in Walk Now for Autism 2010, held on a beautiful day on June 26. The team helped raise more than \$1,800 to help fight autism. This is the second year that Schneider Downs has participated in the event.

This summer, both offices held their second annual Summer Leadership Program for undergraduate accounting majors. The Pittsburgh group ended the program with a land and water tour of Pittsburgh on the Just Ducky vehicle.



Summer means Schneider Downs picnics! The Columbus office celebrated at Huntington Park, as they watched the Columbus Clippers take on the Pawtucket Red Sox. The Pittsburgh office's picnic was held at the Pittsburgh Zoo and PPG Aquarium on one of the hottest days of the year!

Practice Unit Fridays. That is what we have dubbed our summer Fridays. Each practice unit is given the opportunity to highlight its services in unique ways. The Business Advisors had a mini-golf and Wii golf competition. Pictured: Brad Tobe concentrates before his putt. Joel Rosenthal shows off his Wii golf prowess.



## CALENDAR - BENEFIT PLAN DUE DATES

### Forms 5500, Annual Return/Report of Employee Benefit Plan.

Year-End	Due Date	With 5558 Extension
5/31	12/31/10	3/15/11
6/30	1/31/11	4/15/11
7/31	2/28/11	5/16/11

### Processing of corrective distributions relative to failed 401(k) ADP/401(m) ACP discrimination testing, so as to avoid a 10% excise tax imposed on the employer.

Year-End	Due Date
9/30	12/15/10
10/31	1/17/11
11/30	2/15/11

## New Hires

Our people are our greatest strength. We welcome our April, May and June new hires:

Laura K. Colby      David M. Edwards  
Cathleen A. Condrac      Peyton A. Wagner  
Megan K. Dunleavy      Frank A. Wiseshart

WELCOME


# ONPOINT

## Schneider Downs

1133 Penn Avenue  
Pittsburgh, PA 15222-4205  
TEL 412.697.5200  
FAX 412.261.4876

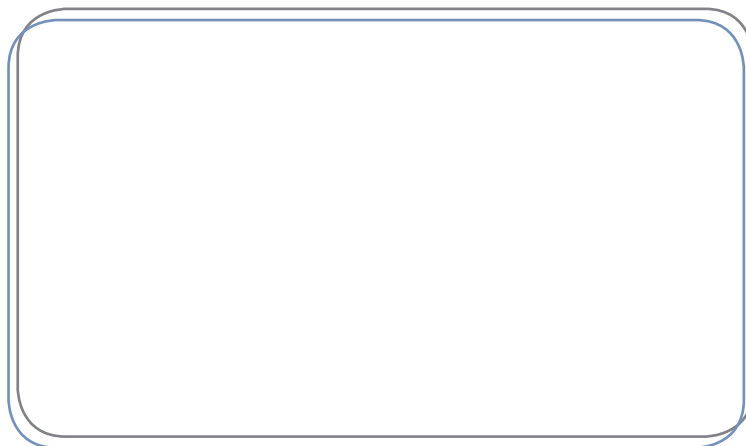
Huntington Center, Suite 2100  
41 South High Street  
Columbus, OH 43215-6102  
TEL 614.586.7200  
FAX 614.621.4062

[www.schneiderdowns.com](http://www.schneiderdowns.com)

 Follow us on Twitter!  
@Schneider\_Downs

CHANGE SERVICE REQUESTED

PRSRT STD  
U.S. POSTAGE  
PAID  
PERMIT NO. 830  
PITTSBURGH, PA



## Interested in receiving email updates?

Are you on our email list? Schneider Downs frequently issues email messages with news, information and updates on topics that are important to our clients' industries. If you would like to receive periodic updates via email, please visit [www.schneiderdowns.com](http://www.schneiderdowns.com) and click on Subscriptions. We'll be sure to keep in touch.



## PROFESSIONAL NEWS

**Donald B. Applegarth**, Audit Shareholder, **Brian C. O'Brien**, Audit Shareholder, and **Michael A. Renzelman**, Audit Shareholder attended the AICPA's 2010 National Advanced Accounting and Auditing Technical Symposium in July in Orlando, FL.

**Richard X. McKenna**, Business Advisors Manager, received his Certified Supply Chain Professional (CSCP) certification from APICS - The Association for Operations Management.

**John H. Stafford**, Technology Shareholder, was quoted in the August 6 issue of *Information Technology Advisor* on the topic of using help desks to solve technology issues.

**Karlye N. Rowles**, Marketing Manager, was appointed to the Joseph M. Katz Graduate School of Business Alumni Board.

**Steven D. Thompson**, Audit Shareholder, and **Holly L. Russo**, Internal Audit and Risk Advisory Senior Manager, presented during a Strafford webinar entitled "Mastering SAS 70 Audit Reports for Service Organizations" on June 16.

**Melanie M. LaSota**, Director of Estate and Tax Trust Services, attended the AICPA Estate Planning conference in Washington, DC in July. Melanie was also elected to Secretary of the Pittsburgh Youth Symphony Orchestra.

**Jeffery A. Acheson**, Partner and Managing Director of SD Retirement Plan Solutions, was quoted in the August 18 *Pittsburgh Post-Gazette* article, "New rules order thorough disclosures of 401(k) fees."

**Matthew M. McKinnon**, Tax Senior Manager, presented at the Small Business Tax Credit for Health Insurance Expenses of Tax-Exempt Organizations webinar presented by the Ohio Grantmakers in August in Columbus, OH.

**Roy M. Lydic**, Audit Shareholder, spoke at the Ohio Society of Certified Public Accountant's Auditor of State Conference in May in Columbus, OH.

**Don A. Linzer**, CEO of Schneider Downs Wealth Management Advisors, was quoted in the August 5 *Pittsburgh Post-Gazette* article, "What's next for the estate tax?"

**Donald R. Owens**, Internal Audit and Risk Advisory Services Director, presented "Fraud Avoidance - Reducing Fraud Risk by Assessing and Strengthening Internal Controls" for the Ohio Society of Certified Public Accountants in August in Columbus, OH.

**Staci L. Brogan**, Audit Senior Manager, presented at The Forbes Funds' Financial Management Series in August in Pittsburgh, PA. The focus of the session was Data Analysis.

**Susan M. Kirsch**, Tax Shareholder, was quoted in the August 4 *Pittsburgh Post-Gazette* article, "Small nonprofits could lose tax-exempt status."

**James B. Yard**, Internal Audit and Risk Advisory Shareholder, was appointed Vice Chairman and Chairman Elect for Junior Achievement of Western Pennsylvania.

**Gennaro J. DiBello**, Tax Shareholder, was appointed to Assistant Treasurer for YPO Pittsburgh.