

PENNSYLVANIA
CPA JOURNAL

VOLUME 79, NUMBER 1

SPRING 2008



Accidents Happen

**Know Your Responsibilities
When Client Data Goes Missing**

By Jonathan S. Ziss, JD

In virtually every type of business, data is received, processed, stored, transported, and otherwise disseminated in digital form via electronic media. In the accounting profession, digital data is ubiquitous. As a result, laptops and hand-held PDAs are essential productivity tools of the trade. And due to advances in digitized memory, storage capacity is nearly beyond the realm of consideration; that is to say, the data CPAs use and decipher occupy, as a practical matter, virtually no space. The entire contents of a laptop can be stored on a device the size of a finger. Taking your practice with you wherever you may go is easy and convenient. There is, however, a darker side to this breakthrough in efficiency: losing your collection of critical data is now much easier.

According to the Web site www.privacyrights.org, numerous inadvertent data spills affected public accountants in 2006. Among the unintentional jetsam were the following:

- In the United Kingdom, an Ernst & Young laptop was stolen from an automobile. It contained Social Security numbers of 38,000 employees of BP, Sun Oil, Cisco Systems, and IBM. This was one of two Ernst & Young laptops with personal information to go missing that year in the United Kingdom.
- An external auditor with Deloitte lost a CD containing the names, Social Security numbers, and stock holdings in McAfee of 9,290 McAfee employees.
- An unencrypted hard drive containing names, addresses, and Social Security numbers of AICPA members was lost when it was shipped back to the organization by a computer repair company. Reportedly, 330,000 records were affected.
- A laptop was stolen from the trunk of the car of a law firm's auditor. It contained confidential employee pension plan information, including names, Social Security numbers, and 401(k) and profit-sharing information. This affected the records of 500 past and present employees.

The accounting profession is not alone, of course. Data losses affecting other industries and government branches are legion. Even a casual review of the listing of incidents makes the stomach churn.

So, what happens when a laptop is left in a taxi or is swiped from a desk after hours? Are there laws that explain culpability or prescribe certain responses? Are you at risk of an ethical breach? What about insurance coverage? This article will provide guidance on each of these points.

Growing Data Security Laws

Secured digital information has drawn the attention of federal- and state-level lawmakers in recent years. Beginning with personal health information, and then expanding to all records that involve the collection and communication of Social Security numbers or credit data, businesses now have affirmative obligations to safeguard this personal information. Breach notifications are now required, and becoming commonplace. Data destruction, too, has attracted legislative attention. This, however, is only the beginning. Federal and state legislators and regulators are continually drafting and debating new secured data laws.

It is imperative that practitioners and CPAs in all types of industries pay attention to these proposed secured data laws. Yes, they are more examples of the seemingly inevitable trend toward added complexity in the business world, but to ignore this facet of professional life would be perilous.

Federal Statutes

Most major pieces of federal data security legislation, and their implementing regulations, are fairly specialized. Regulations under the Health Insurance Portability and Accountability Act of 1996 (HIPAA), for example, are an early example of a comprehensive framework for protecting sensitive information. The law has proven both enduring and influential, having become a model for other legislation and a touchstone for courts when speaking of the standard of care for personal data.

The Financial Services Modernization Act of 1999 requires financial institutions to “ensure the security and confidentiality of customer records and information; protect against anticipated threats or hazards to the security or integrity of such records; and protect against unauthorized access to, or use of, such records or information which could result in substantial harm or inconvenience to any customer.” The Sarbanes-Oxley Act of 2002 requires retention of prescribed records, including work papers; peer review of audits; disclosure of auditors’ testing of issuers’ internal controls; monitoring of ethics and independence; consultation within auditing firms; supervision; hiring; acceptances of engagements; and internal inspections. The list of specialized federal laws goes on, including the Telephone Records and Privacy Protection Act of 2006, which criminalizes “pretexting,” the obtainment of phone records by false pretenses, and the Veterans Benefits, Health Care and Information Technology Act of 2006, which requires the Department of Veterans’ Affairs to improve data security policies in the wake of multiple breaches of its database.

The trend toward specialized acts may be over as we enter an era of secured data protection laws of a more general application. The 110th Congress is presently considering the Personal Data Privacy and Security Act. This bill applies to businesses engaged in interstate commerce, and establishes standards for developing and implementing administrative, technical, and physical safeguards to protect the security of sensitive personal information in electronic or digital form. As it stands, this requirement would apply only to entities holding information on more than 10,000 U.S. persons. In the event of a breach, those affected must receive notification within 45 days and a toll-free phone number must be established to take inquiries. Knowingly covering up a breach will be made a crime under the proposed legislation. This certainly would up the ante when considering whether a qualifying breach indeed occurred, and thus whether the notice requirement has been “triggered.”¹

A number of similar pieces of legislation are also before

Congress, so it is safe to assume that there will be new federal legislation enacted along these lines in the near future.²

State Statutes

The majority of states also have enacted laws that cover the protection of personal information. While personal information is described by a variety of definitions, these laws do have certain elements in common. These typically include the name of an individual in combination with the individual’s Social Security number, driver’s license number, state identification number, or financial account, debit or credit card number in combination with any required security code, access code, or password that would permit access to an individual’s account. These state laws require businesses to provide notification in the event of an unauthorized breach. Firms with multistate practices take note: personal information about an individual or business residing in another state could be subject to that other state’s security laws.

Pennsylvania’s Secured Data Laws

In June 2006, Pennsylvania enacted a pair of statutes known as the Breach of Personal Information Notification Act (PIN Act). The PIN Act requires that “an entity that maintains, stores, or manages computerized data that includes personal information shall provide notice of any breach of the security of the system, following discovery of the breach of the security of the system, to any resident of the Commonwealth whose unencrypted and unredacted personal information was, or is reasonably believed to have been, accessed and acquired by an unauthorized person. ...

The notice shall be made without unreasonable delay.” The act defines “personal information” as including an individual’s first name, or first initial, and last name in combination with and linked to any one or more of the following data elements when not encrypted or redacted: Social Security number; driver’s license number or a state identification card number; or financial account, credit card, or debit card num-

bers in combination with any required code that would permit access to an individual’s financial account.

The PIN Act defines breach of the security of the system as “the unauthorized access and acquisition of computerized data that materially compromises the security or confidentiality of personal information maintained by the entity as part of a database of personal information regarding multiple individuals and that causes or the entity reasonably believes has caused or will cause loss or injury to any resident of this Commonwealth.”

Having a cautious and well-considered electronic data collection, storage, security, dissemination, and destruction policy is the right place to begin.

The act also prescribes the form of notice to be given: e-mail notification if a prior business relationship exists; notice via telephone if the customer can be reasonably expected to receive it, and if the notice is given in a clear manner; or, if the cost of notice would exceed \$100,000 or the affected class exceeds 175,000, a substitute notice – such as a Web site posting – may be used. Written notification always fits the bill.

This statute leaves room for interpretation and the exercise of judgment in the event of a presumed or suspected breach of the system's security. Likewise, determining whether a triggering event has occurred under the PIN Act, or that of any other state, may not be easy. The facts surrounding the misplacement of a laptop or PDA, a suspected incident of hacking, or any other possible breach, may be murky and uncertain.

What to Do and When

When considering the content of the notice, as well as the more fundamental question of whether or not to send it, one must be careful and deliberate. The guidance of legal counsel and an experienced public relations person may be prudent. An example of the sensitive nature of this type of communication is available on the Federal Trade Commission's Web site, in the form of its "model letter for the compromise of Social Security numbers." The model letter calls attention to a "potential problem involving identity theft" and recommends that those affected "place a fraud alert on [their] credit file." The model letter can be found at www.ftc.gov/idtheft.

Beyond the challenge of complying with a state notification statute,³ one can also expect to fret over negative publicity, client complaints, loss of good will, and exposure to law suits.

A common question is, "What is the exposure to damages for the inadvertent loss of personal data?" The cost of credit monitoring for a limited time is not an infrequent remedy, and may be a well-received proffer in the event of a breach. Likewise, advice as to how to protect against identity theft distributed via one's Web site or via mail might help make amends.

Better yet, do not have a breach in the first place. This may sound trite, but having a cautious and well-considered electronic data collection, storage, security, dissemination, and destruction policy is truly the right place to begin. This is critical to your business, so don't throw it all on the laps of your IT people. IT professionals are not licensed, and there is considerable variability as to their capabilities. Do your homework, and choose your IT vendors and staff with due care, and be involved. Also note, many states require businesses to be proactive in safeguarding personal information. California's statute, for example, provides that: "A business that owns or licenses personal information about a California resident shall implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the personal information from unauthorized access, destruction, use, modification, or disclosure."⁴

The insurance industry has committed significant resources to the issue of secured data. Nowadays, there is coverage available to business owners and professionals that can respond specifically to both first-party and third-party identity protection and other technology exposures. Ask your insurance professional or legal advisor to explain the coverage and limits you now have in place. There may be coverage extensions that are well-suited to your practice. Bearing in mind that the loss of just one laptop can cost a company \$90,000 or more in credit monitoring, public relations damage control, litigation expense, and possible fines, insurance should be considered as part of your risk management.

Note that the legal landscape in this area remains dynamic. Among the laws currently before Congress, several data security acts would displace state laws on the same subject, and would impose civil penalties in excess of \$10,000 per violation, and aggregate penalties in the millions. Clearly, lawmakers take the problem of missing laptops seriously.

One final note, and not an especially pleasant one at that. The PICPA Code of Professional Conduct, Section 301 (Confidential Client Information), provides that "[a] member ... shall not disclose any confidential client information without the specific consent of the client." While drafted well in advance of today's wired work place and wired world, Section 301 sounds a sobering note if considered in terms of a data breach. Among other laws to ponder in this context are Pennsylvania's Accountant-Client Privilege statute⁵ and the tax practitioner privilege,⁶ both of which would cause any practitioner a fit if a disc or device containing tax returns and/or associated work papers were lost or stolen.

In a wireless world, data seemingly moves swifter than a breeze. That does not make your jobs any easier when it comes to meeting your growing obligations to safeguard electronic data from possible tempests. ■

¹ S. 495 would provide for an exemption to notice if the breached entity submits a risk assessment in writing to the U.S. Secret Service, and that risk assessment concludes that there is no significant risk that the breach has or will result in harm to those individuals whose information was subject to the security breach. When the data is encrypted or another method meeting effective industry standards has rendered the data indecipherable, this creates a presumption that no significant risk exists.

² S. 239, S. 806, S. 1178, S. 1260, and H. 958

³ Bear in mind that a breach affecting persons or businesses in multiple states will likely trigger the notification requirement of each such state.

⁴ Cal. Civ. Code Section 1798.81.5

⁵ 63 P.S. Section 9.11

⁶ IRC Section 7525

Jonathan S. Ziss, JD, is a partner with Margolis Edelstein in Philadelphia. He can be reached at jziss@margolisedelstein.com.



Jonathan S. Ziss, JD