Montgomery Bar Association | Montgomery County PA

SIDEBAR

MAGAZINE

OF THE PEOPLE, BY THE PEOPLE, FOR THE PEOPLE:

A Unique Countywide Arts Initiative & Courthouse Improvement Project

Attorney General

KATHLEEN KANE

Joins our bar!

THE CENTER FOR MEDIATION & ARBITRATION

MBA's new dispute resolution center launches to rave reviews

BYOD

Policies...Scary Liabilities For the Uninformed Employer

By Robert W. Small, Esq.

The phone rings. It is 10:30 p.m. on a Friday. Calls at this hour rarely bring good news; and this one is no exception. Gloria, a newly hired agent in the Benefits Department of your insurance brokerage and financial services company, informs you that her personal laptop computer was stolen from her car. At first you wonder why Gloria is sharing this unfortunate news with you; but she quickly reminds you that under the company's newly adopted "Bring Your Own Device" (BYOD) Program, Gloria was using her personal laptop for company business. Residing on her now missing, computer are the full names, addresses, social security numbers, account numbers, and account balances of plan participants for 15 client benefit plans for which you act as plan administrator and for several other plans to which your clients serve that role. That same information and health histories for the client health plans that your company administers are also on the laptop. Gloria informs you that the same information for all 75 of your own company's employees resides on her computer. All told, personal information of more than 2500 individuals, living in all fifty states, potentially has been breached.

The news gets worse when you speak with your lawyer. You learn that because some information is health information, you will have to notify those individuals whose information has been compromised under the Federal Health Insurance Portability and Accountability Act. (HIPAA) and the Health Information Technology for Economic and Clinical Health Act (HITECH), this will require your lawyer to review regulations issued by the Department of Health and Human Services and the Federal Trade Commission to determine who must be notified and what information must be given.

As you are considered a financial institution, you will have reporting responsibilities under the Financial Services Modernization Act of 1999 (aka Gramm-Leach-Bliley Act). This will require review of regulations issued by the Office of the Comptroller of the Currency, the Federal Reserve Board and the Federal Deposit Insurance Corporation as well as the Office of Thrift Supervision to determine what regulations might apply to that aspect of your business.

Furthermore, your lawyer tells you that if any of the employees work for your affiliated radio station he will also have to spend time visiting the Federal Communications Act 1934 and Regulations issued under that Act by the Federal Communications Commission which relate to data breach notification.

But then the really bad news comes. At least 46 states have legislation dealing with the breach of personal information. Although he is familiar with the laws of your state, he and a team of associates will have to "blue sky" the other 45 state laws.

Your lawyer tells you that "personal information" subject to breach notification statutes include social security numbers, drivers licenses numbers, account numbers, credit card or debit card numbers, along with security and or access codes or passwords that would permit access to an individual account, medical information, health insurance information, date of birth, mother's maiden name, biometric data, DNA data, passport number, taxpayer identification numbers, and account numbers even disassociated from passwords or PIN numbers.

Anticipating a large legal fee and notification costs, you ask if notification is required. He responds that many states have risk of harm thresholds which require notification only if the breach of personal information poses, or is likely to pose, a significant risk of harm to the affected individuals. In response to his questions you inform your lawyer that, while a password is required to open the files on the stolen laptop, the data is not encrypted. With this information your lawyer tells you that this probably rises to the level of a significant risk of harm to the individuals whose personal information is on the computer triggering your notification obligations.

You ask what you have to tell your employees and what your clients will have to tell their employees as you are certain your clients will be looking to you for guidance as to their obligations. Your lawyer tells you that the information you must provide depends on each state statute. You ask if the company could simply provide all of the information required by the most comprehensive statute which would save time with the blue sky exercise. Your lawyer responds that what some states require you to put in employee notifications, other states prohibit. Therefore, there can be no "one size fits all" notification letter.

Furthermore, it is not as simple as notifying plan participants or your own employees. Some states require notification to state officials such as the State Attorney General. Some states permit you to delay notification if the law enforcement agency investigating the breach requests that of you so as not to impede its investigation. Additionally, at least one state requires that you notify them before notifying plan participants or employees and have your notification letter approved.

Your lawyer will have 4 associates begin the blue sky process immediately. By the end of the day he lets you know that the good news is only 11 states' statutes create a private right of action for individuals to sue you for

Continued on page 12