

DAY PITNEY LLP

MEMORANDUM

TO: Altru, LLC
FROM: John P. Scordo, Esq.
DATE: June 1, 2010
RE: Data Breach Notification Costs and Insurance

Personal data security breaches are being reported with increasing regularity. During the past few years, there have been numerous examples of persons breaking into the computer systems of corporate, government, academic and charitable institutions and stealing personal data such as Social Security, bank account, credit card or driver's license numbers, as well as medical and student records. These breaches occur not only because of illegal or fraudulent attacks, but often because of careless business practices, such as lost or stolen laptop computers, or the inadvertent posting of personal data on public websites.

Since January 2005, data breaches have affected more than 345 million records in the United State containing personal information. *Privacy Rights Clearinghouse, as of 1-22-2010 at www.privacyrights.org/ar/ChronDataBreaches.htm*. Identity theft affects about 8.3 million adults annually. The average total per-incident cost of a data security breach, including third party liability and fines/penalties, was \$6.75 million. *Ponemon Institute 2009 Annual Study: Cost of a Data Breach, www.encryptionreports.com/download/Ponemon_COB_2009_US.pdf*. In 2009, the trend continued with two of the largest breaches in history. In January 2009, as many as 100 million credit card records were exposed when it was discovered that hackers broke into the network of a credit card processor. In October 2009, the personal information of more than

70 million U.S. military veterans was compromised when an improperly erased hard drive was sent out for repair.¹

Most states and several federal government agencies have enacted laws requiring organizations to protect personal information data, and inform individuals of security breaches involving such information. California passed the first data breach notification law in 2003. At present 46 states, and the District of Columbia and Puerto Rico, have laws in effect requiring notifications to the public if there has been a loss or unauthorized access to any personal information. The only states which do not yet have data breach protection laws are Alabama, Kentucky, New Mexico and South Dakota.

The average cost of issuing privacy breach notifications and offering credit monitoring has been reported by at least one source as approximately \$166,000 per 1,000 records lost. *See www.tech-404.com/calculator.html*. The average number of records lost in a typical data breach incident is approximately 100,000. *Id.*

Non-profit organizations are not exempt from data security laws and regulations and are particularly vulnerable if they collect and retain data on contributors, *see e.g.* www.nonprofit.about.com/od/fundraising/tp/protectdata.htm A security breach can quickly destroy a non-profit organization's well-earned reputation for integrity and professionalism. www.blog.grace-npc.com/2010/02/17/how-a-security-breach-can-take-down-your-

¹ The causes of privacy breach incidents reported to date can be summarized as follows: Stolen Laptop 20%; Hackers 16%; Web 13%; Fraud 8%; Stolen Computer 7%; Disposal Document 5%; Mail 4%; Unknown 4%; E-mail 4%; Lost Media 3%; Stolen Document 3%; Lost Tape 2%; Lost Document 2%; Lost Drive 2%; Stolen Tape 1%; Stolen Media 1%; Stolen Drive 1%; Lost Laptop 1%; Virus 1%; Disposal Tape 0%; Disposal Drive 0%; Lost Computer 0%; and Disposal Computer 0%. *datalossdb.org*

nonprofit.aspx See also Non-profit company says 3.3 million student loan records stolen,
infoworld.com/d/the-industry-standard/

All types of organizations are in possession of personal information because it is defined broadly.

It is almost impossible to not collect or hold some personally identifying information — names and addresses, Social Security numbers, credit card numbers, or other account numbers — about your customers, patrons, employees, business partners, students, or patients. Most state statutes broadly define “personal information” as any data that associates an individual’s name with either their Social Security number, driver’s license, or one of their financial account numbers. For example:

California:

"Personal information" means an individual's first name or first initial and last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted: (1) Social security number. (2) Driver's license number or California Identification Card number. (3) Account number, credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account.

Massachusetts:

Protected personal information includes the first name and last name or first initial and last name of a resident in combination with the resident's (i) social security number, (ii) driver's license number, (iii) state identification number, (iv) financial account, debit or credit card number in combination with or without any required security code, access code, or password that would permit access to a resident's account.

Ohio:

"Personal information" means an individual's name, consisting of the 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 the data elements are not encrypted, redacted, or altered by any method or technology in such a manner that the data elements are unreadable: (i) Social security number; (ii) Driver's license number or state identification

card number; and (iii) account number or credit or debit card number, in combination with and linked to any required security code, access code, or password that would permit access to an individual's financial account.

All Statutes Require Protection of Information and Notification of a Breach:

Data security breach disclosure laws have dramatically increased the risks associated with handling personal electronic records. As a result, organizations are spending millions of dollars reacting to data breaches involving the personal information of consumers and employees in both protecting against future breaches, as well as the notification and rectification of past breaches. Data breach notification laws typically require covered entities to implement a breach notification policy, and include requirements for incident reporting and handling external breach notification. The data breach notification statutes are intended to provide individuals with timely warning that their personal information may have fallen into the hands of an unauthorized person, giving them the opportunity to take action to protect themselves against identity theft or to minimize the effect of identity theft that has taken place. The state laws generally require entities to notify consumers when there has been a breach that exposes their personally identifiable information. Some states also require notification to credit bureaus and regulators.

Still, Ponemon's 2008 "Consumer Report Card on Data Breach Notification" indicated that "[d]ata breach notifications are a failure if individuals do not have a clear understanding of their level of risk, available support, and the steps they need to take to respond to the loss or theft of their personal information... research strongly suggests that legal compliance is the primary goal of many companies' notification efforts. This approach does not serve the best interests of consumers and contributes to a breakdown in trust that can impact a company monetarily as a result of an increase in customer defection." *Ponemon Institute, Consumers' Report Card on*

Data Breach Notification, (April 15, 2008), www.idexperts.com/breach/ponemon-study/ponemon_success.aspx.

Each state's law can vary about, for example: what constitutes personal information? what constitutes a breach that necessitates disclosure? who must be notified? when must the notification be issued and what should it contain?

Insurance For First-Party Loss As A Result of Incurring Data Breach Notification Expenses

We have reviewed the Supplementary Data Breach Expense Coverage (the "Endorsement") being offered as part of Old Republic Insurance Company's Non-Profit Organization Management Liability Insurance Policy. The additional coverage offered in the Endorsement will, in our view, provide a significant benefit to insureds. I am not aware of any other carrier that offers this benefit as a widely available option for an existing management liability policy. Based on the facts and law discussed above, and our own experience and knowledge in this area, we believe data breaches and the direct costs associated with them present a significant risk to almost any organization, including non-profit organizations, and we believe those risks will increase in the future. Coverage such as that offered in the Endorsement should be strongly considered by all of your firm's clients.

The Endorsement covers the organization directly, and offers reimbursement for reasonable and incurred costs and expenses in notifying third parties of a data breach, if required by State or Federal privacy laws, and costs and expenses of providing credit monitoring to the person receiving the notice, if required by such laws. The Endorsement also covers reasonable fees and costs to hire a public relations firm to restore the public's confidence in the organization's management and control of its computer, communications or file systems. The triggering event is any unauthorized access to data (existing in the files, as well as computer

systems, of the organization), or a malicious attack against the organization's systems, which results in notification obligations. The coverage afforded in the Endorsement addresses a significant risk applicable to almost all insureds. This coverage will become more and more necessary and commonplace in the future.

The coverage is subject to a sub-limit and other terms and conditions which should be reviewed by the insured. Third party liability, defense costs and fines or penalties are not covered. Separate coverage for all or some of these losses is available in other policies, usually referred to as network security policies, which should be considered by most insureds.

We would be happy to expand on any of the areas addressed herein. If you should require additional information, please let us know. Please note that this advice is intended only for Altru, LLC and is not intended as legal or other advice to any third party.