

R. Michael Murphy

Getting a Grip on Identity Theft: Emerging Trends in Data Security Obligations

As businesses increasingly maintain electronic records about their customers and employees, the risks associated with data security breaches also increase. Data security breaches can take the form of anything from a stolen laptop or disk drive to sophisticated breaches of vast data networks.

The Identity Theft Resource Center (ITRC), a nonprofit organization based in California, maintains an updated list of identity theft breaches that are reported in the United States. As of April 14, 2009, the ITRC documented 155 breaches that resulted in the exposure of the personal information of 1,733,069 individuals.

In response to this growing threat, federal agencies and states are enacting new laws, rules and regulations intended to increase the security of personal information. This movement began at the federal level and initially concerned only certain sectors, such as the financial and health care industries. However, following the federal government's

lead, numerous states now require companies to provide "reasonable security" to protect the confidentiality of personal information, including Arkansas, Connecticut, Maryland, Massachusetts, Nevada, Rhode Island, Texas and Utah. This type of regulation is expected to continue to be adopted at the state level in the years to come, and many commentators are calling for the federal government to pre-empt these state requirements by enacting personal data security requirements that would be applicable nationwide. What follows is a summary of the evolution of the legal obligation to safeguard sensitive digital information, as well as late-2008 state-level developments relating to information data security.

Personal information

As an initial matter, it is important to examine what type of information is protected under the data security obligations being imposed by regulators. Protected data is commonly referred to as "personal information." States have different statutory definitions in place, but in general, personal information includes sensitive information about individuals that is not publicly available. The following definition from Connecticut is representative of the approach taken by other states:

"Personal information" means information capable of being associated with a particular individual through one or more identifiers, including, but not limited to, a Social Security Number

(SSN), a driver's license number, a state identification card number, an account number, a credit or debit card number, a passport number, an alien registration number or a health insurance identification number, and does not include publicly available information that is lawfully made available to the general public from federal, state or local government records or widely distributed media.

Development of legal obligation

The legal obligation to provide security for personal information has evolved during the past several years with much of the activity taking place at the federal level. The obligation to develop and implement a comprehensive, written information-security program first appeared in legislation and regulations governing the financial and health care sectors. The first such requirement was the Gramm-Leach-Bliley Act issued by the Federal Reserve, the Office of the Comptroller of the Currency, the FDIC and the Office of Thrift Supervision on Feb. 1, 2001, which required financial institutions to adopt information security plans. This was followed on Feb. 20, 2003 by the issuance of HIPAA Security Standards requiring comprehensive written information security plans in the healthcare sector. The Federal Trade Commission has since adopted the view that a comprehensive information security program is a "best practice" applicable to all businesses and all industries, and has begun pursuing companies in non-regulated industries based on an alleged failure to provide adequate security for their data.

Beginning in 2004, the requirement for companies to implement an information security program began evolving on the state level. The first state to act was California, which enacted legislation requiring all businesses to "implement and maintain reasonable security procedures and practices" to protect personal information about California residents from unauthorized access, destruction, use, modification or disclosure. However, the California legislature failed to further define what constitutes "reasonable security." Numerous states followed California's lead, imposing similar obligations on companies to adopt "reasonable" security practices.

Most recently, on Sept. 19, 2008, the Massachusetts Office of Consumer Affairs and Business Regulation (OCA-BR) issued a new set of regulations requiring businesses that own, license, store or maintain personal information to create a comprehensive, written information-security program (Massachusetts Regulations). These regulations constitute the most comprehensive plan for regulation of data security that has been issued by a state to date. The Massachusetts Regulations specifically require companies to implement a written information security program similar to the type described by the federal Gramm-Leach-Bliley Act and HIPAA regulations. However, the Massachusetts Regulations go further and require companies to comply with certain specific computer system security requirements (including the encryption of data). Commentators expect similar regulations to be ad-

opted by other states nationwide. The spread of this type of obligation can already be seen. On Dec. 5, 2008, New Jersey released a "pre-proposal" for regulations very similar to those issued in Massachusetts.

Recent state developments in data security

Connecticut

Effective Oct. 1, 2008, a new Connecticut privacy law (Connecticut Law) requires companies to: 1) create and display a "privacy protection policy" concerning the collection and use of SSNs; and 2) safeguard and properly dispose of personal information. The Connecticut Law requires companies to create a privacy protection policy if they collect SSNs in the course of business. These privacy policies must: 1) protect the confidentiality of SSNs; 2) prohibit unlawful disclosure of SSNs; and 3) limit access to SSNs. The Connecticut Law requires the privacy protection policy to be published or "publicly displayed," which includes posting the policy on an Internet webpage. The Connecticut Law also requires any person in possession of the personal information of another person to: 1) safeguard the data, computer files and documents containing the personal information from misuse by third parties; and 2) "destroy, erase or make unreadable such data, computer files and documents prior to disposal."

Nevada

As of Oct. 1, 2008, the State of Nevada enacted legislation (Nevada Law) that

Jennifer M. Miller and Kelly B. Roney

Erring on the Side of Caution Responding to Qualified Written Requests under RESPA

The Real Estate Settlement Practices Act of 1974 (RESPA) represents a response by Congress to perceived abuses in the real estate settlement process and an attempt to protect consumers from unnecessarily high settlement charges resulting from those abuses. One of the three general requirements imposed on mortgage servicers under RESPA is a requirement to respond to written inquiries from the borrower. In order to elicit the mandated response from the mortgage servicer, however, the borrower's inquiry must be a qualified written request under the RESPA statute. When a mortgage servicer receives

“Because RESPA is a remedial act that is designed to protect consumers, erring on the side of caution in situations where a servicer is faced with a lengthy inquiry that is purported to be a qualified written request is probably the best response.”

a qualified written request, RESPA sets forth specific statutory requirements that the servicer must comply with in responding to the request, or face penalties for noncompliance.

A qualified written request is a written correspondence that contains or enables the servicer to identify the name and account of the borrower. It must also either include a statement

concerning the reasons the borrower believes his account is wrong, or provide details to the servicer regarding “other information sought by the borrower.” RESPA makes clear that even this “other information” must relate to the servicing of the loan in order to classify the inquiry as a qualified written request. Servicing can be loosely defined as receiving any payments from the borrower due under the loan.

Servicers have begun to receive written requests containing more than just inquiries into the servicing of the loan; many requests also demand documentation and details regarding the mortgage application process and origination of the loan, as well as other demands that do not appear related to the servicing of the loan. While some requests, or portions of the requests, may certainly contain legitimate servicing inquiries, these especially lengthy written requests appear to be a tactic borrowers use to effectively forestall an impending foreclosure. These delays, however, can be very costly and time consuming for servicers, who typically must postpone the foreclosure proceedings and incur additional legal fees in order to adequately address the requests and reschedule the foreclosure sale.

Servicers are required to address a qualified written request, by providing acknowledgement of receipt of the borrower's correspondence within 20 days, and taking certain substantive actions within 60 days of receipt of a qualified written request, including: 1) making appropriate corrections to the borrower's account; 2) conducting an investigation and providing the borrower with a written explanation or clarification, including the reasons the servicer believes the borrower's

account is correct, and specific contact information of an individual, office or department that can provide assistance to the borrower; or 3) conducting an investigation and providing the borrower with a written explanation or clarification that explains why the requested information is unavailable or cannot be obtained, and the specific contact information of an individual, office or department that can provide assistance to the borrower.

Most, if not all, cases interpreting violations of RESPA deal with the failure to respond within a timely manner or to determine whether written or oral communication between the borrower and servicer constitutes a qualified written request. The courts have failed thus far to substantively address whether a servicer is required to respond to inquiries contained in an otherwise legitimate qualified written request that do not relate to the servicing of the loan. For example, it has been held that merely providing pay-off quotes containing an itemization of charges to the account, but providing no explanation of each charge, will not constitute a sufficient response to a legitimate qualified written request.

Because RESPA is a remedial act that is designed to protect consumers, erring on the side of caution in situations where a servicer is faced with a lengthy inquiry that is purported to be a qualified written request is probably the best response. Servicers must be sure, however, that any such response meets the statutory requirements set forth in RESPA, as a failure to do so could leave the servicer subject to the variety of penalties available to borrowers under RESPA. **C**



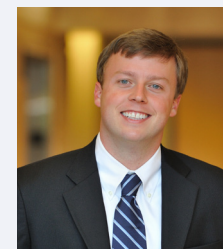
Jennifer M. Miller

Jenny practices in the area of Litigation at Sirote. She received her J.D. from Indiana University School of Law in 2008. Jenny received her M.A. in 2003 and her B.A. in 2001 from the University of Alabama-Birmingham.



Kelly B. Roney

Kelly practices in the areas of Corporate and Real Estate Law as well as Business and Financial Services. She received her J.D. from The University of Alabama School of Law in 2008 and her B.S. in Finance from The University of Alabama in 2001.



R. Michael Murphy

Mike practices in the area of Corporate Law. He received his J.D. from Vanderbilt University School of Law in 2007 and his B.A. from Vanderbilt University in 2004.

Continued from page 3

Getting a Grip on Identity Theft

requires that a business in the State of Nevada shall not transfer any personal information of a customer through an electronic transmission, other than a fax, to a person outside of the secure system of the business unless the business uses encryption to ensure the security of the electronic transmission. The Nevada Law defines encryption broadly to mean “any protective or disruptive measure, including, without limitation, cryptography, enciphering, encoding or a computer contaminant, to prevent access, make the information unusable or disrupt the use of the network.” As a result of the passage of the Nevada Law, any business that operates in that state is obligated to encrypt all of its customers' personal information when it will be sent electronically, unless the transmission is by fax.

Massachusetts

On Sept. 19, 2008, the OCABR issued the comprehensive Massachusetts Regulations, which require businesses that own, license, store or maintain personal information of Massachusetts residents to create a comprehensive, written information security program and establish and maintain a computer security system. The Massachusetts Regulations apply to all businesses that possess personal information about a Massachusetts resident even if the business is not located in the state. The effective date for compliance with the Massachusetts Regulations was originally set for Jan. 1, 2009, but has been pushed back until Jan. 1, 2010.

Each company's security program will be evaluated on a case by case basis taking into consideration: 1) the size, scope and type of business of the company obligated to safeguard the personal information under such comprehensive information security program; 2) the amount of resources available to the company; 3) the amount of stored data; and 4) the need for security and confidentiality of both consumer and employee information. It is also important to note that the obligations imposed by the Massachusetts Regulation include the responsibility to ensure that third-party service providers that do business with a covered entity are applying security measures at least as stringent as those required of the covered entity.

Conclusion

The emerging legal trend is clear. Regulators are placing increasing obligations on businesses to provide security for sensitive data. The multi-state scope of many companies and the nature of electronic commerce may effectively make laws like those of Massachusetts applicable nationwide. If a company is not currently subject to a legal obligation to implement information security procedures, it probably will be in the near future. Businesses that collect personal information of customers or employees should be aware of these requirements and consider taking steps to implement an information security program. **C**