

Customer Data Security: Privacy Compliance Becomes Yet More Costly

By Susan Barbieri Montgomery, Esq. and Sam Hudson, Esq.
Foley Hoag LLP

With effect from January 1, 2005, many U.S. businesses that collect personal information from their customers will face increased data security requirements. The new requirements add yet more regulation to the area of consumer privacy, an area that saw substantial legislative activity in 2004.

Even though the new data security requirements are found in a California law¹, they will have nationwide effect because they apply to any business that owns or licenses “personal information” about California residents. In addition, companies will continue to be held responsible for protecting personal data in compliance with the promises they have made to their customers, such as in privacy policies published on websites. The effect of existing promises and the new law means that many companies face stricter data security requirements than they realize.

New California Law

The new law defines “personal information” as an individual’s first name or initial and surname and any of the following, when either the name or any of the following elements are not encrypted or redacted:

- § credit or debit card number or account number, together with any code required for access to an individual’s account;
- § Social Security Number;
- § driver’s license number or California identification number; or
- § information relating to the individual’s medical history, treatment or diagnosis.

Based on this definition, any business that, by way of example, has California-resident employees or that may collect the name and credit card details of a California resident should review its data security to determine whether it needs to meet the standards of the new law. The law will not apply to financial institutions and health care entities that are already regulated by federal laws such as the Gramm-Leach-Bliley Act and the Health Insurance Portability and Accountability Act (HIPAA).

The data security standard imposed by the new law is very general in nature, and so it will need to be interpreted by businesses and ultimately by the courts. The relevant standard is that businesses must implement and maintain “reasonable security procedures”, appropriate to the nature of the information, to protect it from unauthorized access, destruction, use, modification or disclosure. The law also requires that the business impose reasonable security requirements by contract on any third party to whom personal information of a California resident is disclosed.

Reviewing Security Standards

Although the “reasonable security procedures” standard may seem so general as to be impossible to implement, in fact there are a number of guideposts available. In assessing what is reasonable in their particular circumstances, businesses should consider the information security standards that have been established by the Federal Trade Commission for financial information², and by the Department of Health and Human Services for medical information³. These standards will not always be appropriate, depending on the nature of the particular information being retained, but they provide guidelines against which courts may be expected to assess the reasonableness of any particular security procedures. For example, the FTC requires financial institutions that hold customer information to implement and maintain an information security program that, in summary:

- § is in writing;
- § has a designated employee to coordinate it;
- § includes an assessment of the risks to information security in areas such as employee training and management and information systems design; and
- § provides safeguards against identified risks, and regularly tests that the safeguards are effective.

The Security Standards Rule issued under HIPAA⁴ sets out a much more detailed set of security standards, requiring entities covered by the rule to address such specific issues as unique user IDs, automatic log-offs, encryption and data integrity controls. In addition, the terms of settlement in recent FTC enforcement actions over information security, such as the Tower Records settlement announced in April, 2004⁵, provide further guidance on appropriate security standards. It would seem prudent for businesses that are subject to the new California law to make a considered assessment of the technical, administrative and physical safeguards that the business has in place for customer information, as compared to the standards set out in sources such as these.

Your Privacy Policy: A Complicating Factor

The advent of the new law may also warrant a re-examination of the information security promises that you make in published materials such as your privacy policy. Many businesses offer customer assurances or adopt website privacy policies that expose them to additional liability because of customer-friendly promises, such as “We take customer privacy seriously” and “We will always safeguard customer information”. As Tower Records discovered, the FTC takes the view that such promises imply that the business has adopted rigorous software solutions and administrative procedures to back them up. Companies should ask whether they are making promises in their privacy policies that impose upon themselves higher standards than the “reasonable security procedures” soon to be required by California, and if so, verify that they are meeting those promises.

Those businesses that have not adopted a privacy policy should also be aware of another California law, effective July 1, 2004, that requires the operator of a website that collects

personal information (defined more broadly than in the definition above) about California residents to conspicuously post a privacy policy⁶. The privacy policy must:

- § identify the categories of personally identifiable information collected by the website operator;
- § identify the categories of third parties with whom the operator may share the information;
- § describe the process by which the website operator notifies consumers of material changes to the privacy policy;
- § if the website operator has a process for allowing consumers to review and request changes to the consumer's personally identifiable information, a description of that process; and
- § the effective date of the policy.

As there is no federal law that requires a company to have a privacy policy, this law may provide another example of California enacting a law which has effects outside California. However, the greatest legal risk in connection with privacy policies remains the risk that companies will make promises to which they do not adhere. Many enforcement actions in the area of consumer privacy have been based on a company's misleading representations, not on the company's failure to comply with a particular privacy law.

For more information about privacy and data security issues, please contact Susan Montgomery, Partner, Foley Hoag LLP, at (617) 832 1222 or Sam Hudson, Associate, at (617) 832 1741.

¹ California Civil Code § 17985.81.5.

² 16 C.F.R. 314.

³ 45 C.F.R. 164.

⁴ Ibid.

⁵ In the matter of MTS, Inc. and Tower Direct, LLC. Consent Order dated April 21, 2004.

⁶ California Business and Professions Code §22575-22579.