

## Coming Soon to a Data File Near You! — *Security and Encryption Requirements*

Companies that handle electronic data may soon find themselves subject to strict and expensive data security and encryption requirements under a Massachusetts regulation scheduled to take effect March 1, 2010.

The Massachusetts regulations by their terms apply to anyone who “owns or licenses” electronic data containing “personal information.” “Personal information” is a Massachusetts resident’s last name *plus* first name or initial *plus* social security number, driver’s license number or financial account number, with or without PIN code. “Owns or licenses” means storing, processing or accessing personal information. Whether your company is inside or outside Massachusetts, if you own or license electronic personal information of a Massachusetts resident, Massachusetts says you must comply.

Many of the data security requirements are just common sense, like having an appropriate comprehensive information security program, authentication and password standards, and updated virus and security software, evaluating risks and improving safeguards, staffing, training and discipline, overseeing vendors who handle the personal information for you and making sure they implement a proper security program themselves. Most companies will already be in compliance.

However, the regulations also require encryption of personal information residing on laptops and other portable devices or transmitted by wireless or across public networks. This includes e-mail but probably not faxes or internal networks. The encryption requirements apply to everything from huge financial data files to a single email containing a Massachusetts resident’s name and social security number.

This could require major changes because even confidential emails are usually not encrypted today. Email encryption technology is available and feasible, but can be expensive, impede workflow, and clash with your business needs and record retention protocols (for instance) by automatically deleting attachments prematurely.

Is there any relief? The regulations allow some leeway through “technically feasible” and “appropriate to the company” standards. In addition, many legal experts doubt that Massachusetts can force out-of-state companies to comply. However, these factors may not provide meaningful legal relief. If you fail to comply and later suffer a security breach, your failure is likely to lead to a 20-20 hindsight claim that the breach was easily avoidable.

Accordingly, we urge you to reexamine your data security practices – especially regarding encryption of notebooks, portable devices, emails and web-based data transmission functions – and determine if you have large amounts of personal data that could be better protected. Purging unnecessary personal information from your systems and storage is the first and best protection. You should consult with a competent IT vendor regarding the feasibility and cost of encryption where personal information is essential.

We are ready to assist you. Contact the Stevens & Lee attorney with whom you regularly speak, or any one of the following, skilled in privacy and data security matters:

- David Richie – 610.478.2127 or [dr@stevenslee.com](mailto:dr@stevenslee.com)
- Elliott J. Stein – 609.987.7050 or [ejs@stevenslee.com](mailto:ejs@stevenslee.com)
- Paul Schieber – 215.751.2868 or [phs@stevenslee.com](mailto:phs@stevenslee.com)
- Amy Coll – 610.205.6023 or [afc@stevenslee.com](mailto:afc@stevenslee.com)
- Christine Beyer Savoca – 609.734.6197 or [cbs@stevenslee.com](mailto:cbs@stevenslee.com)