Massachusetts Attorney General says you must practice what you preach

Having a WISP is not enough to comply with data security standards

In the first public settlement of its kind related to violations of the new Massachusetts Standards for the Protection of Personal Information of Residents of the Commonwealth, 201 C.M.R. 17.00, Belmont Savings Bank has entered into a settlement with the Massachusetts Attorney General following a data breach in which an unencrypted backup tape containing the names, Social Security numbers, and account numbers of more than 13,000 Massachusetts residents was lost after a Belmont employee failed to follow the bank's own Written Information Security Program ("WISP").

In May 2011, a Belmont employee left an unencrypted backup tape on a desk rather than storing it in a vault for the night, which was then inadvertently thrown away by the evening cleaning crew. Although Belmont had a WISP, which met the new Massachusetts data security standards, Belmont failed to comply with the WISP in practice. Specifically, Belmont failed to encrypt portable devices, such as the backup tape, which contained personal information.

The Attorney General's settlement with Belmont provides for a civil penalty of $7,500 as well as injunctive relief to mitigate the risk of future data breaches at Belmont. Under the terms of the settlement, Belmont must comply with the provisions of its own WISP, including:

1. Ensuring the proper transfer and inventory of backup computer tapes containing personal information;
2. Storing backup computer tapes containing personal information in a secure location; and
3. Effectively training the members of its workforce on the policies and procedures with respect to maintaining the security of personal information.

Attorney General Martha Coakley noted that, "Consumers expect businesses to not only develop policies and procedures to safeguard their sensitive personal information, but to follow these procedures as well." Bottom line, it is no longer enough for businesses to just have a WISP relative to treatment and protection of its personal information. Organizations must actually put the safeguards in place that they set forth in their WISPs.

If you have any questions, contact:

James J. Giszczak
248.220.1354
jgiszczak@mcdonaldhopkins.com

Dominic A. Paluzzi
248.220.1356
dpaluzzi@mcdonaldhopkins.com

or any of our Data Privacy and Network Security attorneys by clicking on the link below:

Data Privacy and Network Security

McDonald Hopkins counsels businesses and organizations regarding all aspects of data privacy and network security, including proactive compliance with the numerous state, federal and private data security regulations (including PCI DSS and HITECH) relative to personal information and protected health information, training of employees and preventative measures to decrease the risk of data theft. We also counsel businesses and organizations through the data breach response process and coordinate notifications to affected individuals and state attorneys general, as well as advising on media related issues. Our attorneys can help you properly assess your risks to ensure compliance. After you complete the brief McDonald Hopkins Data Privacy and Network Security Review, your company will be provided with an assessment of the required areas of compliance which have the greatest need of attention and improvement.