Attorneys General continue to increase legal standards for data privacy compliance

Massachusetts Attorney General penalizes company for failing to comply with PCI standards

Many have written about it and several have contemplated it -- whether states will adopt private data security standards, such as the Payment Card Industry Data Security Standards (PCI DSS), and use them as legal standards that owners and holders of personal information (PI) must comply with. That's exactly what the Massachusetts Attorney General did when it recently filed suit against Briar Group, LLC and alleged, among several other things, that Briar was not PCI compliant at the time of its data breach in November 2009, affecting 53,000 MasterCard and 72,000 Visa accounts.

PCI DSS are private data security standards created by the Payment Card Industry Security Standards Council that apply to all organizations collecting credit cards. The Complaint alleged that Briar's failure to implement basic data security measures on its computer system allowed hackers to gain access to Briar's customers' credit and debit card information.

Briar ultimately settled with Massachusetts through a consent judgment with the following penalties, in part:

- Briar Group to pay State of Massachusetts $110,000;
- Establish a Written Information Security Program;
- Maintain PCI compliance and verify same within fourteen days;
- Revise password management process; and
- Implement various network system changes.

It's too early to tell whether other attorneys general will follow suit, but we may very well see a new trend of requiring organizations with PI to comply with state, federal and now private data security standards, such as PCI DSS. What is not hard to tell is that now, more than ever, businesses must meet strict requirements to protect PI or face severe penalties.

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.