CLIENT ALERT: January 20, 2011

DATA SECURITY UPDATE: ATTORNEY GENERAL'S OFFICE REQUESTS COPIES OF WRITTEN INFORMATION SECURITY PLANS (WISPs) UPON BREACH NOTIFICATION

The Massachusetts Attorney General's Office ("AG's Office"), which is charged with enforcing the Massachusetts data privacy laws (M.G.L. c. 93H&I; 201 CMR 17.00 et seq.), is now asking for additional information when it receives notification of a security breach under state law. In particular, the AG's Office has begun requesting a copy of the Written Information Security Plan (WISP) of the organization that experienced the security breach.

Since March 2010, every organization that stores "personal information" of Massachusetts residents is required to develop and implement a WISP. A WISP is an internal policy and procedure document setting forth the administrative, technical and physical safeguards used by an organization to ensure the security and confidentiality of records that contain personal information of Massachusetts residents. Until recently, there was no indication that the AG's Office would require an organization to submit its WISP after a breach notification. Now, however, organizations are being required to submit WISPs.

There is concern that under certain circumstances, WISPs submitted to the AG's Office may become records subject to public disclosure. However, under Massachusetts public records law, several exemptions authorize the state to withhold a document from public disclosure. If it receives a request under the public records law for an organization's WISP, the AG's Office has indicated that it will endeavor to withhold the document and prevent its release if a state law exemption applies.

To further ensure that such documents do not become public, Krokidas & Bluestein attorneys have recommended to the AG's Office that it invoke the investigatory exemption provision of the Massachusetts public records law. This exemption covers investigatory materials that are compiled by the state out of the public view, the disclosure of which would not be in the public's interest. Krokidas & Bluestein attorneys also recommend to clients that WISP submissions made to the AG's Office after a breach notification include a statement regarding the applicability of specific exemptions from public record disclosure, as well as a request that the organization be notified if the WISP becomes subject to a public records request.

If you do not have a WISP in place, need advice about your current WISP, experience a privacy breach pursuant to the Massachusetts data privacy laws, have been requested by the Attorney General to submit a copy of your WISP, or have any other questions regarding this topic, please contact Attorney Anjali Waikar at awaikar@kb-law.com.