KROKIDAS & BLUESTEIN
ATTORNEYS

CLIENT ALERT

MARCH 1, 2012 DEADLINE:

THIRD PARTY SERVICE CONTRACTS MUST COMPLY WITH MASSACHUSETTS DATA SECURITY LAW

By March 1, 2012, Massachusetts entities – including both non-profit organizations and for-profit companies – must ensure that all third party service provider contracts comply with the Massachusetts Data Security Regulations ("Regulations"), 201 CMR 17.00, et seq.

Background

The Regulations require that all entities that receive, store, maintain, process or otherwise have access to personal information of Massachusetts residents ("entities") create and implement security plans and maintain appropriate security measures.[i] This requirement went into effect in March 2010.

In addition, the Regulations impose obligations on entities to ensure that their third-party service providers ("service providers") comply with the Regulations. Specifically, entities must:

1) take reasonable steps to select and retain service providers that are capable of maintaining appropriate security measures to protect personal information, and
2) require service providers to contract to implement and maintain such security measures.

The Regulations included a two year grace period for contracts entered into on or before March 1, 2010. **Therefore, by March 1, 2012, all service provider contracts must include a provision requiring the service provider to satisfy the state law, regardless of when the contract was executed.**

Notably, the law reaches all service provider contracts, including contracts with non-Massachusetts-based service providers. By way of example, a Rhode Island-based data storage company is subject to the Regulations if it stores documents that contain personal information of Massachusetts residents. And a California-based insurance company that administers a company's health insurance benefits is covered if it handles claims of the company's employees

who reside in Massachusetts. Failure to comply with the Regulations may result in monetary penalties.

What Steps You Should Take:

- Determine whether your service providers either use, receive, store, maintain or process personal information of Massachusetts residents, or have access to such information;

- Review all such service provider contracts to ensure that they contain language that meets the Regulations' requirements and, if they do not, revise such contracts; and

- Ensure that all new service provider contracts comply with the law.

For assistance with reviewing your service provider contracts, drafting amendments to such contracts, or for any other security or privacy related matter, please contact Attorney Anjali Waikar (awaikar@kb-law.com) or any other attorney at Krokidas & Bluestein.

[i] "Personal information" is defined as a Massachusetts resident's first and last name, or first initial and last name, in connection with any of the following: (1) Social Security number; (2) driver's license number or state-issued identification card number; or (3) financial account number, or credit or debit card number.