DAVIS MALM & D'AGOSTINE P.C.

ATTORNEYS AT LAW

---

**REGULATORY AND ADMINISTRATIVE LAW ALERT**
**APRIL 2016**

---

## "RED FLAGS" IN DATA BREACH NOTICES THAT GET THE ATTENTION OF THE ATTORNEY GENERAL'S OFFICE

During the March 23, 2016 "Protecting Data and Dealing with Breaches" panel that I chaired for Massachusetts Continuing Legal Education (MCLE),[1] Assistant Attorney General Sara Cable identified some "red flags" that the Office's Data Privacy and Security Unit looks for when reviewing data breach notices under Massachusetts law.

All companies (including non-Massachusetts based) holding personal information of Massachusetts residents should know that the presence of any of these "flags" may increase the likelihood of agency inquiries (by email, phone or letter) or formal investigations (typically by a Civil Investigative Demand) under Massachusetts consumer protection statutes (including G.L. c. 93A), data breach statutes (including G.L. c. 93H and 93I) and its toughest in the nation data security rules (at 201 CMR 17.00).

Based on my reading of Assistant Attorney General Cable's remarks – speaking in her personal rather than official capacity – key triggers may include:

1. **Size of Breach.**

   The larger the number of affected consumers, the greater the likelihood that the Attorney General will inquire as to compliance with applicable data breach or consumer protection laws and rules.

2. **Nature of Affected Consumers.**

   Irrespective of the number of affected consumers, if a breach involves consumers who are members of disadvantaged or vulnerable groups such as children, the elderly, the disabled community, or racial, ethnic or religious minorities, then the Attorney General is likely to pay particular attention.

3. **Nature of Breach.**

   The Attorney General is likely to inquire as to breaches that appear to have been avoidable through reasonable diligence, such as repeated breaches involving the same or similar defective practice or policy (e.g., multiple losses of unencrypted laptops) or losses caused by a well-known system vulnerability that should have been long remedied.

---

[1] Information on ordering from MCLE the full "Protecting Data and Dealing with Breaches 2016" webinar and supporting materials can be found here.

**4. Quality (or Lack Thereof) of the Breach Notice.**

A usually vague or patently noncompliant breach notice, or a failure to provide the required notice at all, is likely to trigger follow up inquiries, especially when combined with one of the above flags.

**5. Speed of Breach Notice.**

Even though companies experiencing a breach are afforded "reasonable time" (a term with substantial flexibility under applicable law) to meet breach reporting obligations, the Attorney General may undertake investigations when a response appears to be unusually slow relative to the extent of potential harms – commonly flagged when the Attorney General begins receiving consumer complaints in advance of any required reporting.

## CONTACT

If you have questions about this alert, please contact Robert J. Munnelly, Jr. or a member of our Regulatory and Administrative Law Practice.

---



One Boston Place, Boston, Massachusetts 02108 | phone 617.367.2500 | fax 617.523.6215 | info@davismalm.com.