
MEMORANDUM

TO: MEMBERS OF THE JCOTS PRIVACY ADVISORY COMMITTEE
FROM: LISA WALLMEYER, DIRECTOR
SUBJECT: DATABASE BREACH NOTIFICATION LEGISLATION
DATE: 10/21/2005

As you likely remember, the Privacy Advisory Committee requested at its October 12, 2005 meeting that staff prepare a document summarizing the alternatives that have thus far been discussed relating to HB 2721, and to database breach notification legislation generally. Accompanying this memo you will find a draft bill that lays out both substantive language for a potential bill, as well as alternative language for each element. This memo is meant to present the major issues that you will note in that draft bill in a quick and concise manner to aid in your review, and that will likely be topics of discussion at the Privacy Advisory Committee meeting scheduled for November 16 at 2:00 p.m.

DEFINITIONS

Definitions are key to a database breach bills, as they will set the parameters as to what breaches are subject to the disclosure requirements of the act. Issues to be considered include:

- Whether the legislation should apply to breaches affecting computerized data, or any sort of breach where personal information is obtained, whether in computerized or hard copy formula;
- Whether the legislation should apply when data is acquired, or when it is both acquired and accessed;
- Whether the legislation should apply only to unencrypted data;
- What parameters apply to giving substitute notice; and
- Whether the substance of what must be included in notice should be set forth in the definition.

NOTICE

The main issue relating to when notice of a breach must be given revolves around the circumstances of the breach. Some proposals would require notice to be given if a breach takes place at all; other proposals only require a breach if it is determined that the unauthorized access to the personal information is reasonably likely to lead to identity theft or other injury. These two examples are perhaps the two extreme ends of a continuum along which possible solutions may lie. In order to determine the proper standard, policy issues to be considered include the motivation behind such a

bill, the relative burden on the various standards place on entities in complying with the bill, and the effect on and benefit to residents of the Commonwealth in receiving the notice.

LAW-ENFORCEMENT EXEMPTION

All bills that I have reviewed relating to database breach notification include a provision that would allow an entity to delay notification if instructed by law-enforcement that notification would impede an investigation. Outstanding questions include whether notice may be delayed for impeding just criminal investigations or also civil actions, whether an entity must receive a determination in writing from a law-enforcement agency that an investigation would be impeded, and whether language relating to good-faith need be included in such a provisions.

CONSUMER REPORTING AGENCY NOTIFICATION

Some database breach notification bills include a requirement that national consumer reporting agencies be made aware of notifications being sent out under such legislation. The reasoning behind such a provision is that the reporting agencies need to be able to prepare for the potential deluge of calls and credit report requests it might receive from affected individuals. The question as to whether to include this requirement is closely coupled with the question as to whether an entity must let individuals know in its notice that they may want to contact a credit reporting agency to monitor his credit report, and/or provide contact information for the reporting agencies. Alternatively, absent specific language requiring that reporting contact information be made available in the notice, a bill might require the entity giving notice to make reporting agencies aware of the notice only if the entity chooses to include the reporting agency information in the notice. Finally, several bills do not include any language relating to consumer reporting agencies.

EXCLUSIONS FROM THE PROVISIONS.

Some bills allow for entities already regulated by state and/or federal law concerning breach notification to be exempt from these new requirements. This would apply to entities such as the banking industry (regulated by the Grahams Leech Bliley Act), or the health care industry (regulated by HIPAA). The argument for exemption is that requiring compliance with an additional law would create an additional burden on these already-regulated entities, and that compliance with multiple privacy and notification standards might be confusing. In addition to these regulated-entities, some bills also exempt any entity that has its own procedures and policies for addressing privacy and security breaches that comply with these new provisions.

REMEDIES

The issue of remedies is a key policy issue. Several bills allow for a private right of action for a person aggrieved by the bill, which may allow for recovery of actual damages or a baseline fine (\$100 per violation, for example), or whichever amount is greater. However, some entities advocate that enforcement should be left to the Office of the Attorney General. Where there is no private right of action, the fines are generally steeper -- such as \$150,000 per incident.