crowell moring

CLIENT ALERT

To Notify or Not to Notify - 2006 Update

Apr.07.2006

Following in the footsteps of the California legislature, twenty-three other states have now passed security breach notification laws, and there are similar laws pending in several more states. Additionally, as we march into the second quarter of 2006, several states are considering legislation to expand their existing security breach notification laws to broaden the types of entities covered by the law, to eliminate exemptions under the law (including some exemptions for HIPAA-covered or Graham-Leach-Bliley-covered entities) and to regulate the use of social security numbers, among other things.

Each of the recently enacted laws, like the California law, generally requires entities to promptly notify the residents of that state if the security, confidentiality or integrity of their personal information (defined similarly by most states with some notable exceptions) has been compromised.

However, the new state security laws don't just require notification of breaches after the fact. Some states require businesses to take measures now to prevent the occurrence of breaches. Depending on where you do business, you could be required by state law to:

- Implement and maintain security procedures and practices to protect personal information.
- Adopt measures to ensure transfers of personal information to third parties are subject to contractual safeguards.
- Review existing document destruction policies to ensure appropriate timing and methods for the destruction of personal information.
- Utilize encryption to ensure the safe transfer of personal information to third parties.

The best way to avoid disclosure under the new laws is to avoid the breach in the first place. Therefore, corporations are well-advised to adopt procedures for handling the security of personal information generally, and prepare a response plan which includes an established method for notifying individuals when and if their personal information is compromised. In addition to enforcement by the State Attorneys General and private litigants, the FTC is actively enforcing privacy laws through the general unfair act or practices portion of the FTC Act.

The FTC brought a number of high profile enforcement actions involving security breach incidents in 2005 and the trend continues in 2006, increasing the pressure for businesses to implement and maintain adequate security procedures and practices that closely mirror those found in the Safeguards Rules of the Gramm-Leach-Bliley Act. Most notably, the FTC recently issued the largest fine in FTC history against ChoicePoint, with $10 million in civil penalties, and $5 million in consumer redress.

For more information, please contact the professional(s) listed below, or your regular Crowell & Moring contact.

Kris D. Meade
Partner – Washington, D.C.
Phone: +1 202.624.2854

Email: kmeade@crowell.com