Foster Garvey

Duff on Hospitality Law

Recent Developments in Data Privacy and Security Laws

on 5.28.10 | Posted in Data Privacy, Hotels, Technology

A pair of recently effected state laws makes clear that information security remains a significant issue that receives and will continue to receive considerable legislative and commercial attention. Hoteliers, restaurateurs and others in the hospitality industry use personally identifiable information (PII) of their guests and customers to improve services and create a personalized experience.

Greg and I attended the annual Hospitality Law Conference in Houston this February, which devoted an entire track to data privacy issues. It's the definition of a hot topic, and important, so please take note!

After the Breach: Now Banks Get Paid Too

Until now, state statutes treating the issue of data security have dealt exclusively with post-breach requirements—i.e. a business's duty to notify individuals whose personally identifiable information (PII) might be compromised—and creating a claim for individuals who want to sue for damages. The Washington law (H.B. 1149) continues in this vein; and under the revised law, financial institutions may now recover their costs from certain businesses for reissuing debit and credit cards after a data breach, if the businesses were negligent in protecting data. Now a hotelier not only has to worry about paying damages to guests whose data might have been breached, but she also needs to worry about paying the banks who have to reissue the cards.

Before the Breach: Required Security Measures

The administrative regulations arising from Massachusetts amended "Security Breaches" act are the first such regulations to directly impose an obligation on businesses to protect PII. Any business that owns or licenses PII about Massachusetts residents must take steps to prevent a breach, as set forth in the administrative code. For example, businesses must:

Encrypt all data, including on mobile devices (laptops, PDAs, etc,)

Restrict physical access to records containing PII

Develop written information security policies and adhere to them '

Regularly monitor networks for unauthorized activity

Compliance with PCI-DSS Standards

The Massachusetts attorney general has, to date, been ominously silent about how to interpret the new regulations. In the mean time, businesses would do well to become PCI-DSS compliant, whether or not credit card information is actually stored. These standards, promulgated by the PCI Council, set forth some "best practices" that will help data owners and licensors comply with various state legal obligations. In fact, PCI-DSS compliance provides a "safe harbor" from the recoveries made available under the amended Washington law.

What Does it all Mean?

Part of the total guest service experience often requires the creation of a guest folio or profile that allows the hotel or restaurant (or other hotels or restaurants under the same owner or manager) to "remember" that a guest likes the New York Times in the morning and eggs over-easy with a side of wheat toast. The folios may also "remember" credit card numbers, passports, addresses and phone numbers. This information is critical to the operation of the hotel or restaurant, but absolutely must be protected.

Aside from the legal penalties, a big data breach is embarrassing and can create a PR and guest services nightmare. Take a lesson from Wyndam, Radisson, and Starwood, and be sure to protect your data.

Tags: data privacy, PCI, PCI-DSS, Personally Identifiable Information (PII), Security