Incidents Which Trigger a Legal Obligation to Notify Guests

State Data Breach Laws Differ

What do you do when you learn that someone has stolen credit card account data[1] from your hotel? You probably already know that you may have to give notice to the affected cardholders and that if you don't do it in time or in the right way, you could face significant consequences. But what are the specific notice requirements that apply to your situation? And are there other legal requirements that apply?

Typically, a merchant must comply with the law of the state of residence of the person whose data was stolen, and where a hotel is victimized, that could mean complying with multiple state notification laws for a single breach. Most states require that the state attorney general or a consumer protection agency also be notified, but there are key differences among state notification laws. A quick and accurate understanding of the legal requirements that apply to a data security breach is critical. The following two examples of data thefts, both true stories, illustrate some key differences between certain state notice laws.

Theft by Electronic Hack. In 2008, a hacker invaded the central reservations system of a major hotel brand. The hacker then used the franchisor's system to access electronic data stored by approximately 50 franchised hotels across the country. Before he was detected, the hacker stole data from tens of thousands of individual credit card accounts.

Theft of Paper Data. In 2010, a man entered the lobby of a hotel, reached behind the front desk, grabbed a thick binder and ran. The binder contained pages with faxed reservation confirmations. The faxed pages contained credit card numbers intended to hold room blocks. Approximately 175 sets of credit card account information were contained in the binder. It was an inside job; the thief had been told by a hotel employee what the binder contained and where it would be.

After the 2008 incident involving the electronic hack, individual notices had to be sent to virtually every one of the many thousands of cardholders. This required sizeable expenditures for matching card data to cardholder addresses, formulating the proper text for the notices and mass mailing. Affected cardholders were offered a period of free fraud monitoring. Finally, consumer protection agencies in most states were provided with separate notices of the breach.[2] All told, the expense of responding to the 2008 breach have been monumental and costs are still being incurred.

Most states' data breach laws are written to apply only to electronically stored, computerized data. Only a few states' laws consider non-electronic data theft to be a breach.

The 2010 theft of the binder produced quite a different result. Of the 175 affected account holders from 25 different states, only four notices were required to be sent to affected cardholders, and only one state's attorney general had to be notified. The costs incurred were relatively miniscule, yet the hotel was in compliance with all 25 states' data breach laws.

Why the difference? It comes down to the fact that most states' data breach laws are written to apply only to electronically stored, computerized data. Only a few states' laws consider non-electronic data theft to be a breach. For example, Connecticut's law defines a breach as unauthorized access to or acquisition of electronic or computerized personal information. In contrast, Hawaii's notification law defines breach as, "unauthorized access to and acquisition of unencrypted or un-redacted records or data (computerized, paper or otherwise) ..." Only six states currently have laws that either fail to make any distinction in the type of data taken or specify that non-electronically stored data (e.g., paper) triggers notification responsibilities.

This is not to suggest that hotel managers and owners should ignore thefts of non-electronic personal information. Several states are amending their data breach laws to be more comprehensive, and Congress has been looking at passing comprehensive federal data breach notification laws for some time. Moreover, as a matter of customer service, good public relations and plain ethical behavior, hotels should carefully consider issuing voluntary notifications to affected guests, even if notice is not technically required under applicable state law. In any case, it is important to act quickly to understand the requirements and comply in a timely fashion.

SANDY B. GARFINKEL *is a member of the law firm of Eckert Seamans Cherin & Mellott, LLC. He has substantial experience in responding to thefts of personal information and data security breaches, including the application of state notification laws, required forensic investigation, security assessment and certification, compliance with PCI-DSS, and addressing fines issued by credit card brands. He can be reached at sgarfinkel@eckertseamans.com, 412.566.6868. This information is general and educational and is not legal advice. For more information, please visit www.hospitalitylawyer.com.*

[1] Credit card account information is "personal information," a term defined by state laws, which usually includes a person's name along with credit card account numbers, social security numbers, driver's license numbers or account passwords and possibly other types of information.

[2] There were a number of other consequences to the hotel owners and the franchisor following this incident, including card brand compliance investigations, fines issued by the credit card brands, etc. However, this article is only intended to address state law notification requirements.