by Dick Hudak

Lessons learned from a hotel data breach

The criminals were good. They almost got away with the most elaborate data breach and identity theft scam I'd seen in all my years as an FBI agent and hotel security director.

The victim was a nationally branded hotel in Annapolis, Maryland. A gang of thieves from Baltimore infiltrated the hotel in 2004. An associate had applied for a front desk position, got it, and soon had access to the guest and accounting system.

The gang incorporated several businesses and opened bank accounts using previously stolen identities. They chose a bank based in New Mexico, certain that no one would fly 2,000 miles to check on a fake mailing address. Over the course of a few weeks, the group charged $850,000 to credit cards lifted from the hotel's accounting records. Charges ranged from $10,000 to $18,000 each.

When an out-of-state guest noticed the charge and told authorities of his only time in Maryland and where he stayed, the fraud was linked back to the hotel. Soon the front desk had a storm of phone calls to contend with. Local police arrived to interview the employees, and then the Secret Service took over.

Eventually, four criminals from Baltimore were identified and prosecuted. But with every victim, official and media inquiry, the general manager and his staff had to review the entire case—what had happened, what were the next steps. It was a logistical nightmare.

About 50 people had their credit cards defrauded. The hotel staff spent months on the phone giving interviews and processing paperwork.

When all was said and done, almost a year after the attack, they had learned a few hard lessons:

- Limit access to customer data on a need to know basis. Not all employees should have all access to guest and accounting systems.
- Only record the most necessary guest information. Before this incident took place, the hotel kept customers' full credit card numbers. Now that information is limited to only the last four digits.
- Create higher security access clearance for accounting records. Simply put, records with a higher level of personal information about guests or clients need a higher level of protection.
- Credit card companies and the law require hotels to save customer payment data for a certain amount of time, usually two or three years. After that period is up, destroy the records, and destroy them properly. In Massachusetts a hotel that used carbon copies simply threw them away and a group of dumpster-diving identity thieves found them.

- Background checks on employees are a must, whatever the job. Those with extra access to guest and accounting records should be thoroughly vetted.

Finally, consider an identity theft and data breach protection service. All those phone calls, all those police interviews, all that paperwork, could have been outsourced to a reputable company that's handled it all before. Services range from alerting customers of a breach, to dealing with law enforcement. The result is peace of mind. ✧

(Dick Hudak is a former FBI agent, Identity Theft 911 board member and managing partner of Resort Security Consulting Inc., a firm that provides security solutions to hotels and expert testimony in liability cases. This article was previously published by HospitalityLawyer.com in August 2011 and is reprinted with permission. E-mail: hudak@resortsecurity.com)