FOODSERVICE EAST | GUEST COLUMN | FEBRUARY 15, 2013

DATA SECURITY THREATS AND COMPLIANCE OBLIGATIONS IN THE FOODSERVICE INDUSTRY

BY, DAVID M. GOVERNO AND COREY M. DENNIS

Attorney David M. Governo is the founding partner of Governo Law Firm LLC, an 18-attorney law firm in Boston. For over three decades, he has advised companies on a range of risk management and compliance issues, and defended companies in complex litigation. He has attained Martindale-Hubbell's highest "AV" rating, is an active member of the Federation of Defense and Corporate Counsel, and has been voted a New England Super Lawyer for many years. He may be reached at dgoverno@governo.com.

Attorney Corey M. Dennis defends companies in complex litigation, and advises companies on risk management and compliance issues at Governo Law Firm LLC. He has counseled businesses on compliance with data privacy laws, is a Certified Information Privacy Professional (CIPP/US), and has published numerous legal articles in the areas of data privacy, civil litigation, social media, toxic tort, and employment law. He may be reached at cdennis@governo.com.

During recent years, over 1,800 data security breaches, resulting from both malicious hacking and unintentional loss of information, have affected more than 3.2 million Massachusetts residents. Given the quantity of customer financial information that restaurants, bars, and other businesses in the foodservice industry handle daily, they have become a prime target of cyber attacks. In fact, a recent report found that restaurants were "easily the most-targeted businesses, accounting for over half of all reported attacks."

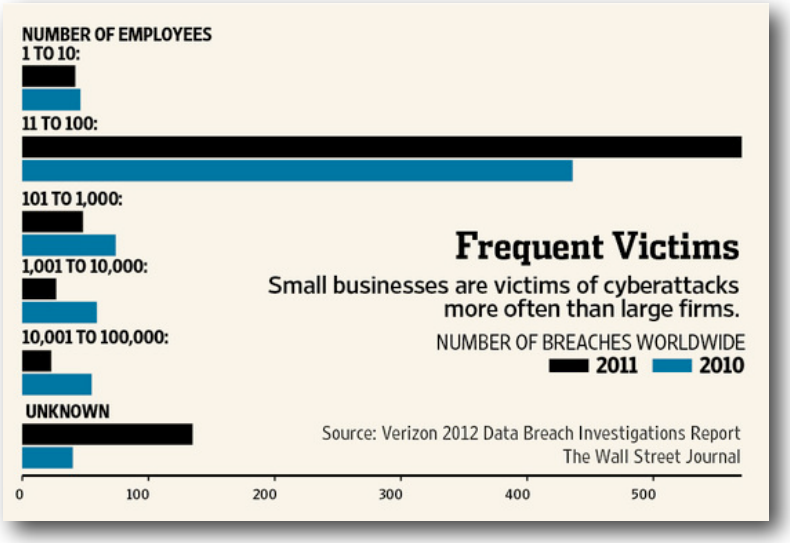
Data breaches are costly, with the potential to ruin a company's reputation and lead to legal liability. In 2011, a Boston-area restaurant group was fined $110,000 following a data breach enforcement action brought by the Massachusetts Attorney General, which was reported in major news outlets, including *The Boston Globe*. Other recent noteworthy restaurant data breaches include:

- In June 2012, Penn Station, Inc. reported a data breach affecting customers at 80 Penn Station East Coast Subs franchise restaurants throughout Pennsylvania and the Midwest.

- From 2008 to 2011, hundreds of merchants, including over 150 Subway restaurant franchises throughout the country, were subjected to a multimillion dollar fraud scheme, resulting in the compromise of over 146,000 customer payment cards and more than $10 million in fraud losses. In September 2012, two Romanian hackers pled guilty to perpetrating these crimes.

- From 2010 to 2011, seven waiters at high-end steakhouses in New York City—including The Capital Grille, Smith & Wollensky, JoJo, and Wolfgang's Steakhouse—stole credit card information from dozens of diners using high-tech devices to extract the information ("skimming"). In November 2011, 28 individuals who were members of the crime ring perpetrating the identity fraud were prosecuted in New York state court.

While data breaches affecting large companies frequently make the news headlines, small businesses are particularly vulnerable to cyber threats, as they lack the resources and budgets necessary to maintain adequate data security measures. In fact, recent articles in the *Wall Street Journal* reported that the majority of worldwide data breaches last year involved small companies (with 100 or fewer employees), and that the costs of these breaches are enough to "put a small company out of business."



To reduce the risk of legal liability, companies must be sure to comply with applicable data privacy laws and standards. Over the past few years, nearly all states in the U.S. have enacted data breach notification laws, requiring notification of affected residents and regulatory authorities in the event of a data breach. Many of these laws also require businesses to maintain certain security measures to protect any personal information that they handle.

The Massachusetts data privacy regulations (201 CMR 17.00 et seq.), which apply to any business handling personal information of Massachusetts residents—including those outside Massachusetts—are among the strictest in the country. Among other rquirements, the regulations mandate that such businesses establish a comprehensive written information security program, train employees on data security compliance, update security measures annually, encrypt personal information stored on electronic devices or transmitted wirelessly, and require third-party service providers (e.g., payroll providers, outsourcers, contractors) to implement security measures by contract.

Any business accepting credit or debit cards must also comply with the burdensome Payment Card Industry Data Security Standard (PCI DSS), an information security standard established in 2004 by the major credit card companies that contractually requires merchants accepting such payment cards to protect cardholder data. The PCI DSS establishes a number of requirements, including: maintaining a security network, protecting cardholder data (including by encryption), maintaining a vulnerability management program, regularly monitoring and testing networks, maintaining an information security policy, training employees on data security, developing an incident response plan, and completing an annual "Self-Assessment Questionnaire."

Not surprisingly, a recent report found that data security is now considered the number one legal risk among general counsel and directors of corporations. In light of these growing risks, attorney-directed data risk assessments have become critical in detecting vulnerabilities and ensuring compliance. Although data breaches often result from malicious hacking, they are also commonly caused by internal employee negligence, such as when an employee loses an unencrypted laptop, mobile phone, or other electronic device. Thus, employee training and sound hiring practices are important in reducing the likelihood of a breach. Evaluation of insurance policies, with due consideration to whether cyber liability insurance may be appropriate, is also recommended.

Many companies, particularly small businesses, are not in compliance with applicable data privacy laws and standards, and are at risk of a data breach. In fact, a recent study found that 96% of companies suffering a data breach worldwide have failed to achieve PCI DSS compliance. To mitigate the risk of a data breach and resulting legal liability, it is imperative that restaurants and other businesses maintain adequate data security measures in compliance with their legal obligations, including those imposed under the PCI DSS and state data privacy laws.