By Patrick T. Zomer

Pat Zomer is a member of our business law and regulated entities practice areas. He helps clients of all sizes navigate business and corporate laws, obtain or facilitate financing, and address data privacy issues. Pat can be reached at 612.877.5278 or ZomerP@moss-barnett.com.

Data Privacy: What's It to You?

Unless you have been the victim of identity theft or have been recently prompted (yet again) to approve Google's or Facebook's newly revised terms of service, you probably spend little time thinking about data privacy. For many, data privacy is a problem for Internet giants (Google or Facebook) or big companies that hold millions or billions of data records (think Sony, TJX, or Global Payments). It is becoming clear, however, that all businesses, regardless of size, face risks associated with data privacy. Failing to adopt appropriate protections can lead not only to significant monetary penalties, but also undermine the trust that serves as the foundation of all commercial interactions.

Data Breach – The Cost of A Breach When You Do Not Have Adequate Protections

The announcement that Global Payments, a third-party processor of Visa and MasterCard transactions, suffered a data breach probably had many of you channeling your inner Yogi Berra, saying, "It's déjà vu all over again." Global Payments is only the latest headline-grabbing data breach, a list that includes Hartland Payment Systems, TJX, Sony, and Epsilon. For each of these companies, direct breach costs likely exceeded $100 million, a number only eclipsed by the indirect damage from diminished reputations, class action lawsuits, and falling stock prices.

While incidents at large companies attract headlines, smaller organizations are more likely to suffer data breaches than industry titans. According to a Verizon study, data breaches primarily occur at organizations with 100 or fewer employees. With direct breach costs of approximately $200 per record, data breaches at these smaller organizations can significantly impact the bottom line, in addition to eroding customer or employee trust.

These trends are magnified by the evolving understanding of what information is private. Modern American privacy law can trace its roots to the seminal 1890 law review article, *The Right to Privacy*, by Samuel Warren and Louis Brandies. Laws requiring the protection of data held by modern business, including Social Security numbers, account or credit card numbers, state identification or driver's license numbers, and Personal Health Information (PHI) can be directly traced to "the right to be let alone," in that each of these items can be used to dramatically intrude upon the data-subject's life. As technology changes the way we interact with the world, however, another principle from *The Right to Privacy* appears to be ascending: the right of an individual to control the extent to which his or her "thoughts, sentiments, and emotions" are communicated to others. The best example of this may be the Epsilon breach mentioned above, where the unauthorized release of names and email addresses was perceived as being as harmful as breaches involving data elements traditionally earmarked for protection. As privacy expectations evolve, more and more information held by businesses, including things as apparently innocuous as contact information, may require protection.

Policies and Codes of Conduct: The First Line of Defense

So what is a business to do? While there is no shortage of splashy new systems, technology, and software that can be directed at the problem, data privacy and security policies and employee training may be your best line of defense. Nearly four in ten data breaches are caused by the actions of negligent individuals inside organizations. Appropriately crafted policies and procedures can help employees

Data Privacy: What's It to You? continues on page 7

avoid the mistakes that can lead to a data breach. Furthermore, with consumers increasingly using privacy as a metric with which to evaluate different companies, data privacy and security policies can become an important means of communicating an organization's values to the broader public.

Luckily, businesses looking to implement data privacy and security policies do not need to start with a clean slate. In 1973, the Department of Health, Education, and Welfare developed a Code of Fair Information Practices designed to protect information held by the federal government. Now commonly referred to as Fair Information Practice Principles (FIPPs), this framework was enacted into law in 1974 and governs the federal government's handling of personal information about individuals. Furthermore, the FIPPs have served as the foundation of several international data privacy frameworks. While expressed slightly differently depending on the context, the FIPPs generally address seven topics: focused collection, respect for context, individual control, transparency, security, access and accuracy, and accountability. Businesses with FIPP-based policies only collect data that is needed to fulfill specifically articulated purposes, restrict employee access to sensitive information based on business need, and make non-disclosure their default position.

Compliance Obligations

In addition to acting as a strong line of defense against potential data breach, policies are increasingly becoming a matter of legal or regulatory compliance. For example, 46 states have adopted data breach notification laws. Implementing data privacy and security policies can help organizations manage the timeline imposed by applicable notice statutes and fulfill their legal obligations to contact affected individuals. There is also a growing list of federal statutes that mandate certain data privacy and security protections, including those implemented through the Gramm-Leach-Bliley Act, the Fair Credit Reporting Act, the Health Insurance Portability and Accountability Act (HIPAA), the Health Information Technology for Economic and Clinical Health (HITECH) Act, and the Sarbanes-Oxley Act. By formalizing policies regarding the collection, use, and disposal of sensitive data, companies can protect themselves against the leading cause of data breach and meet their compliance obligations.

Consumer Privacy Bill of Rights

The Obama Administration recently released a proposal that, if adopted, may begin to harmonize data privacy regulations into a single framework. The so-called "Consumer Privacy Bill of Rights" is designed to supplement existing statutes, including those federal statutes mentioned above, and establish a baseline level of protection that would apply broadly across the economy. The baseline draws heavily from the FIPPs and would govern commercial uses of any data that is linkable to a specific individual. In addition to giving consumers certain rights, including increased control over how their data is collected and used, the Consumer Privacy Bill of Rights includes a national data breach notice standard. It is clear that, if adopted, this proposal could dramatically realign the legal and regulatory protections afforded personal data.

Why Me? Why Now?

Even without a dramatic realignment of public policy triggered by the Consumer Privacy Bill of Rights, there are several reasons why modern businesses should be proactive in addressing issues of data privacy and security. With insider negligence remaining the most common cause of data breach and the universe of data entitled to protection growing, implementing appropriate data privacy and security policies continues to be the first and most effective line of defense against data breach. Furthermore, even in the absence of overarching federal policy, existing laws impose substantial data privacy and security compliance obligations—obligations that apply to more than the Googles and Facebooks of the world. Finally, the Federal Trade Commission continues to bring enforcement actions against companies that do not adhere to their published privacy practices. In the modern economy, businesses that dismiss or ignore issues of data privacy and security do so at their own (and their investors') peril.

Ultimately, data privacy and security is about trust. Customers who cannot trust a business to protect data will not be customers for long. Employers that cannot be trusted to protect data will find it increasingly difficult to process payroll or administer health plans when employees rightfully become squeamish about sharing pertinent information. The exchange of information that acts as the foundation for the modern economy is predicated upon both sides upholding the trust they mutually vest in each other. Proactively managing issues of data privacy and security demonstrates a business that is worthy of that trust and empowers the business to act in ways that reinforce the faith vested in them.

Moss & Barnett can help businesses identify their data privacy needs and find solutions before problems arise.