

# Privacy & Data Security

## **PROTECTING SENSITIVE DATA: AN ESSENTIAL MISSION FOR EVERY BUSINESS IN THE INFORMATION AGE**

The flow of information among businesses, consumers, vendors and investors has become faster and easier than ever before in the 21<sup>st</sup> century. As technology evolves and available communication channels multiply, businesses are presented with new and ever-changing opportunities. At the same time, this progression has dramatically heightened the risks and liabilities that businesses face. In the information age, successful businesses must be well-versed in the handling and protection of both internal and external data. And, the stakes have never been higher.

Business communication is transmitted through many different means, including paper forms and correspondence, phones, e-mail, Web sites, e-commerce, social media, cloud computing and mobile devices. Understanding the different rules and exposures associated with each, developing appropriate policies, and handling data breaches require knowledgeable and responsive legal counsel. We can help you make the most of the many communication channels available, while protecting your business from liability.

Sullivan & Worcester LLP's Privacy & Data Security Group, comprised of experienced attorneys from our Telecommunications, Corporate, Intellectual Property, Tax and Employment & Benefits Law Groups, assists businesses of all sizes and types with:

- Understanding relevant privacy and data security issues
- Developing compliant e-mail, Web site, blog, e-commerce, cloud computing and telemarketing policies
- Appropriately utilizing social media and other Web-and telecommunications-based marketing channels
- Managing customer and investor relationships in the online world
- Addressing privacy and data security obligations and liabilities in contracts with third-party vendors
- Implementing compliant document management and data-retention plans
- Complying with applicable state and federal privacy, data security and breach reporting regulations
- Handling data breaches, privacy complaints and litigation
- Responding to government subpoenas and wiretap requests

- Defending regulatory enforcement actions by the Federal Trade Commission (FTC), Federal Communications Commission (FCC) and state Attorneys General

S&W has particular familiarity with these and related issues through our representation of the telecommunications companies that store and convey business data, host Web sites, and connect companies to the Internet. S&W represents these and other clients before Congress; at the FCC and FTC; before state legislatures and public utility commissions; at the local level; and in litigation.

With the Group's leaders based in our Washington, D.C., office, our proximity to regulatory agencies and Capitol Hill allows us to provide our clients with important contacts and up-to-the-minute insight.

Areas in which S&W provides specific advice include:

## **PRIVACY OF CONSUMER INFORMATION AND COMPLIANT MARKETING PRACTICES**

All businesses must be cognizant of regulations concerning the protection of consumers' personally identifiable information (PII). Those that collect, use and store PII – such as names, addresses, phone numbers, account numbers, credit information and social security numbers – are subject to an increasing number of state and federal laws and regulations that require privacy notices to consumers, patients and employees, and the rigorous protection of PII. Non-compliance with these requirements, as well as data breaches resulting in sensitive information being released to unauthorized persons, can result in substantial fines, penalties and other legal liability.

Businesses also are subject to a bevy of regulations concerning their marketing practices. We regularly counsel our clients on the Can-Spam Act, Do-Not-Call and Telemarketing Sales laws, among others, analyzing whether existing and prospective advertising campaigns and promotions are fully compliant. S&W's attorneys are also experienced with the unique issues presented by new media, such as social networking sites, blogs and mobile advertising, and can guide businesses in protecting themselves while taking best advantage of these powerful communication tools.

## **PRIVACY OF HEALTHCARE INFORMATION**

We counsel clients on healthcare-related privacy regulations, such as those mandated by the Health Insurance Portability and Accountability Act (HIPAA) and the HITECH provisions of the American Reinvestment and Recovery Act of 2009, which extended civil and criminal penalties for mishandling of medical records not only to healthcare providers, but to many of the businesses that support them.

(continued)

SULLIVAN &  
WORCESTER

# Privacy & Data Security

## PRIVACY OF FINANCIAL INFORMATION

S&W counsels clients on dealing with the rapidly evolving body of regulations aimed at protecting financial information. Under FTC regulations adopted pursuant to the Gramm-Leach-Bliley Act, companies that offer financial products or services to individuals, like consumer lending, tax preparation, financial advice or credit counseling, residential real estate settlement and consumer debt collection, must comply with the Financial Privacy Rule, Safeguards Rule and anti-pretexting provisions. The FTC's "Red Flags Rule" requires virtually every business that extends credit to consumers to develop and implement written identity-theft prevention programs. We are experienced in helping businesses to understand their obligations and to develop practical compliance methods.

## WORKPLACE PRIVACY

The Privacy & Data Security Group is experienced in analyzing the internal practices of large and small employers, and the steps they are taking to maintain privacy compliance in the workplace. We advise employers on the development of systematic and consistent data protection policies across various company functions, such as the implementation of effective staff training to increase sensitivity to data privacy concerns, and the maintenance of physical and technological safeguards for sensitive data, such as passwords, encryption and data retention/destruction policies. Equally important, we advise employers regarding workplace monitoring and searches, handling of medical records, employees' personal use of office technology (e-mail, computers, phones) and social media.

## BREACH MANAGEMENT AND LITIGATION

The evolution of privacy regulations has been paralleled by a significant increase in the penalties associated with breaches of privacy. The price of a compromise of confidential information is steep – it can result in fines reaching millions of dollars along with significant public relations and customer service challenges. The lawyers in S&W's Privacy & Data Security Group offer a wealth of experience in guiding clients through such situations, managing them in the most effective way possible to minimize damages and correct mistakes to ensure future compliance.

## REPRESENTATIVE CLIENT WORK

S&W lawyers have advised clients on a wide variety of privacy and data security matters, including the following:

- Prepared privacy policies, Web site terms of use, blog terms of use, and customer terms and conditions for multiple Web site operators
- Advised multiple clients regarding compliance with the FTC's "Red Flags Rule"
- Counseled numerous clients on changes to telemarketing campaigns (telephone and text messaging) to comply with federal telemarketing laws, including the Do Not Call, Telemarketing Sales and "robocalls" rules

- Advised employers with respect to the effect of HIPAA privacy rules on their health plans, including drafting notices, policies, procedures and plan amendments, and reviewing and negotiating business associate contracts
- Drafted employment policies regarding workplace monitoring and searches, medical records, data protection, technology (e-mail, computers, phones) and social media
- Drafted and litigated disputes arising under confidentiality and nondisclosure agreements
- Advised regarding employment-related rights and obligations under the Fair Credit Reporting Act
- Advised multiple Internet service providers regarding behavioral advertising and FTC consumer privacy rules
- Served as regulatory counsel for privacy and data security issues to well-known broadband providers
- Developed and reviewed Customer Proprietary Network Information (CPNI)-compliant privacy policies and procedures for multiple regulated telephone and VoIP providers, including preparing call center scripts, customer notices and annual compliance certifications
- Developed CALEA SSI manuals addressing federal wiretap requests and counseled on subpoena compliance for numerous telecommunications, Internet and VoIP providers
- Advised on federal and state call monitoring/recording requirements for client call centers and telemarketing programs
- Counseled clients on federal and state privacy law compliance in responding to government requests for consumer documents and information
- Defended clients in Do Not Call investigations by state and federal government agencies
- Advised telecommunications companies on use of Automatic Number Identification (ANI), Calling Party Number (CPN), Calling Party Name, and Billing Name and Address (BNA) in compliance with federal regulations

\* \* \* \*

*For further information about our Privacy & Data Security Group, please visit our Web site at [www.sandw.com](http://www.sandw.com) or contact:*

Elise Dieterich at 202 370 3925  
([edieterich@sandw.com](mailto:edieterich@sandw.com))