MILLER CANFIELD

Cybersecurity and Data Privacy

While the news headlines are dominated by large-scale security incidents at giant corporations and various branches of state and federal governments, data security issues are pervasive in nearly every business in every industry, large and small.

Cybercriminals abound, and the data that banks, broker-dealers, retailers, governmental bodies, health care practices, employers, manufacturers, and legal and accounting firms collect and store in the ordinary course of their operations is highly sought-after.

State and federal regulations, professional ethics rules and practical considerations of preserving customer/patient/client privacy and goodwill require the security of that data remain a top priority for every entity.

Our cross-disciplinary team has expertise to help our clients take the steps they need to secure their data, including:

Data Collection, Storage and Use

- Advising clients on applicable statutory and regulatory obligations for collection, storage and use of personal data
- Preparation and implementation of appropriate privacy policies
- Compliance with industry standards, including behavioral advertising principles, credit-card data standards, and mobile advertising guidelines
- Advising on issues regarding data sharing and access within and outside of companies, including issues with the international transfer of data, and preparation and advising on appropriate data-sharing agreements
- Advising on available insurance coverage for breaches and tailoring policies to fit client needs

Data Security

- Assessing data security structure and preparedness, and recommending changes, if necessary
- Assistance with bring-your-own-device policies
- Developing incident response plans
- Providing training to boards, shareholders, employees and other affiliates about best practices for preventing infection of computers, other electronic devices and networks
- Advising on specialized statutory and regulatory guidelines for companies collecting particularly sensitive data, such as financial data

Incident Response

- Working with clients on implementation of incident response plans
- Identifying vendors to provide technical assistance in isolating and mitigating damage from the breach
- Working with law enforcement and other governmental agencies while the breach is active and in any subsequent investigations/audits
- Developing appropriate notice to individuals affected by the breach

Continued

- Defending post-breach litigation and regulatory enforcement