Privacy and Data Security

It starts with an innocent click to open an attachment or to follow a legitimate-looking link in an email. A laptop or smartphone is accidentally left in an airport. A briefcase of paper files is forgotten in a coffee shop.

Each of these simple acts can open the gates to a company's information assets, resulting in the unintentional release of personal information, intellectual property, or other confidential materials. Data breaches have dominated the headlines in recent years, and the trend shows no sign of slowing down.

In this era of the mega breach, businesses face unprecedented challenges in the governance and protection of their information assets and in complying with an ever-changing regulatory landscape. To help our clients meet these challenges, attorneys from Schnader's Privacy and Data Security group advise on information governance issues and help our clients navigate the complex framework of state, federal, and international laws that impact the way they collect, share, and dispose of sensitive personal information. From highly-regulated financial institutions, to unregulated retail companies, from healthcare providers to higher education and other non-profit organizations, we work closely with our clients to ensure they comply with relevant regulations and privacy best practices wherever they operate.

Proactive Approach

Schnader attorneys understand the importance of a proactive approach to privacy and data security issues. We perform privacy impact assessments for clients in order to identify potential privacy issues, and recommend measures to prevent or minimize the risk of a privacy breach. We develop policies and procedures that meet our clients' legal compliance requirements and minimize the possibility of data loss, while honoring their corporate culture, their mission, and their businesses.

In addition to advising our clients on compliance issues, we review and advise on their existing policies and procedures relating to data security, internal security procedures, use of electronic systems, and privacy and data retention. We provide training to our clients' employees to ensure their compliance with these

policies and procedures, and to create an awareness that information assets are valuable and that everyone in the organization has a responsibility to protect them.

We prepare and negotiate vendor contracts involving access to personally identifiable information (PII), personal health information (PHI), and other sensitive information to ensure the appropriate protections are in place. We also evaluate our clients' existing insurance coverage to help them assess first party and third party risk exposure, and we advise on the combination of insurance products to minimize risk and reduce the length of their business interruption.

Breach Response

We work with our clients to assemble breach response teams and to devise and test incident response plans. In the event of a breach, we manage the response team to implement the incident response, guide our clients through the immediate crisis period, and assess and implement notification procedures, including working with the appropriate state regulators. We also provide post-incident counseling to deal with resulting business interruption, fines and costs, and compliance issues. Our litigation and class action attorneys handle any state or federal investigation or private litigation that results from a data breach.

Our experience includes:

- Counseling clients on compliance with U.S. federal statutes addressing privacy issues, such as the Health Insurance Portability and Accountability Act (HIPAA) and the Children's Online Privacy Protection Act (COPPA).
- Counseling clients in a wide range of industries on privacy policies and procedures, bring your own device policies, and social media issues.
- Preparing privacy policies, terms of use, and terms and conditions for our U.S. and European clients.
- Reviewing and negotiating contracts with our clients' vendors with access to client PII, PHI, and other sensitive information, as well as business association agreements under HIPAA.
- Performing data security assessments.
- Advising clients on data protection requirements of the U.S., the European Union, Canada, and Mexico.
- Counseling clients on information governance, records retention, and eDiscovery issues.
- Advising clients on strategies and risk management in connection with the unauthorized access of data by third-parties.
- Counseling clients on data breach response and notification requirements.
- Instituting and implementing a data breach response plan for a HIPAA-regulated entity.
- Working with client's insured to ensure proper reimbursement and coverage of data breach related expenses.
- Identifying, vetting, and securing cyber security forensic team to identify cause of breach of PII data within a nationwide staffing agency.
- Advising client on viability of claim against third party vendor for causing data breach.
- Executing notification to state agencies and individuals following ransomware breach of

international import/export company.

Contacts

Anne E. Kane - Co-Chair
215-751-2397

Stephenie Wingyuen Yeung □□□ - Co-chair; CIPP/US
215-751-2277