CARTER/LEDYARD

cybersecurity and data privacy

practice chair

Matthew D. Dunn / Partner

Guy Ben-Ami / Partner
John M. Griem, Jr. / Partner
Jonathan Trafimow / Partner
Claudia Carbone / Associate
Jennifer "Jenny" Frank / Associate
Jodutt Marwan Basrawi / Associate
Sarah H. Ganley / Associate

As companies manage or store increasing amounts of data, cybersecurity and data privacy issues and obligations transcend geographies to become huge assets or liabilities. The costs associated with a data breach or other cybersecurity event can be devastating, and thus protecting organizations from a breach has become the responsibility of senior executives and directors. Every company must implement appropriate safeguards and best practices to protect data, comply with the many regulations and statutes, and minimize risks. The failure to follow proper cybersecurity and data privacy protocols can expose an organization to significant liability.

Carter Ledyard's Cybersecurity and Data Privacy Group helps clients to better understand the ever-changing landscape of cybersecurity and data protection threats and how to best address those threats. We counsel clients on a wide variety of cybersecurity and data privacy issues, including:

- Development of cybersecurity, data protection, and privacy policies
- Compliance counseling
- Corporate governance
- Data protection and breach prevention
- Risk assessment and management, and mitigation strategies
- Incident response planning and execution, and related investigations
- Incident reporting and disclosure in accordance with regulatory requirements
- Third-party vendor assessment and management
- Cybersecurity insurance assessment
- Litigation
- Mergers and Acquisitions due diligence

Data Privacy Legal Services

Our Cybersecurity and Data Privacy team collaborates across numerous practice areas, including litigation, intellectual property, corporate transactions, employment and financial services regulations. This diversity of experience enables the Cybersecurity and Data Privacy Group to provide clients with well-rounded advice on developing, strengthening, testing, and enforcing their information protection policies and procedures. The Group has advised for-profit and not-for-profit clients of various sizes, from small firms and start-ups with limited resources to middle market firms and large, public companies, helping clients navigate the myriad of state,

federal and international cybersecurity and data protection regulations and guidelines.

EXPERIENCE

Our attorneys have helped clients develop cybersecurity and data privacy programs and manage related challenges, including:

- Assisted non-profit client with fraud scheme involving a threat actor impersonating a vendor to obtain payment from client. Spearheaded incident response, including investigation and reporting, which resulted in successful recovery of funds by client's bank.
- Advised an international technology company in connection with a cyber ransomware attack and associated disclosure obligations.
- Prepared and updated privacy policies, terms of use, cookie policies, and notices of consumer rights under the European Union's General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA) for many clients, including for-profit and nonprofit entities across many industries, such as textiles, cosmetics, cannabis, and e-commerce.
- Reviewed privacy policies, terms of use, and other privacy documents of target companies in connection with due diligence efforts for M&A transactions.
- Provided advice to foreign clients on cyber risk disclosures in publicly filed documents, including those filed with the SEC.
- Advised a non-profit in connection with a data breach resulting in the disclosure of personal data, which involved incident response and an assessment of regulatory reporting obligations.
- Responded to a regulatory inquiry on behalf of a broker-dealer in connection with a cyber attack, and advised on the client's cybersecurity policies, procedures, and incident response plan.
- Conducted a cybersecurity assessment and developed cybersecurity policies and procedures, an incident response plan, and vendor due diligence protocol for a FinTech company
- Advised international organizations on GDPR compliance
- Advised an industrial conglomerate in connection with a data breach resulting in the theft of a domain name and website, which involved a forensic investigation, litigation, and related strategies to recover the domain name
- Analyzed conflicting U.S. and foreign regulations regarding data and employee privacy for a global financial firm engaged in private banking, asset management, and investment banking
- Drafted a GDPR-compliant privacy policy and terms of use for a not-for-profit membership corporation with members in the U.S. and abroad
- Assisted a not-for-profit organization in developing a standard certification of cybersecurity best practices to be included in its third-party contracts
- Responded to a regulatory inquiry on behalf of a broker-dealer in connection with a cyber attack, and advised on the client's cybersecurity policies, procedures, and incident response plan

---

Introduction to Cybersecurity Enforcement and the NY SHIELD Act – A Video Series