BUCKLEY

Privacy, Cyber Risk & Data Security Practice

Businesses face increasingly complex and difficult challenges associated with collecting, using, disclosing, and securing sensitive and highly regulated data and information. Security breaches and other cyberattacks are a constant risk and have attracted heightened regulatory scrutiny in the U.S. and around the globe. States are responding quickly to consumer concerns, leading to inconsistent and occasionally conflicting expectations and requirements. Buckley provides privacy and cybersecurity legal counsel that safeguards the interests of clients and mitigates future risk.

Our attorneys are well-versed in privacy and data security laws, including the Gramm-Leach-Bliley Act (GLBA) and the Safeguards Rule, the Fair Credit Reporting Act (FCRA), the Electronic Communications Privacy Act (ECPA), the Computer Fraud and Abuse Act (CFAA), the Right to Financial Privacy Act (RFPA), and the CAN-SPAM Act. Additionally, we routinely advise clients on state laws concerning data sharing, information privacy, security breaches, and cybersecurity, including the California Consumer Privacy Act (CCPA), the Illinois Biometric Information Privacy Act (BIPA), the California Financial Information Privacy Act (CFIPA), and the New York Department of Financial Services Cybersecurity Rules (NYDFS Cybersecurity Rules). We also closely track and interpret proposed changes in both federal and state laws with respect to privacy and cybersecurity.

As part of our engagements, we leverage our experience in other regulatory compliance areas to navigate clients through related issues such as the USA Patriot Act and the Office of Foreign Assets Control (OFAC) requirements. We are attuned to the increasingly stringent European Union privacy and security requirements, and those of other nations that have followed the European model, and we advise clients on cross-border information-sharing requirements, including issues arising in criminal and civil investigations. We also routinely advise clients on compliance with foreign privacy frameworks, such as the EU General Data Protection Regulation (GDPR).

Our attorneys perform gap analyses and risk assessments, design comprehensive privacy and security policies, craft privacy notices, and advise on the structure of privacy and security programs, employee education, and training materials. We assist clients with devising solutions to permissibly share information within and outside an enterprise. Our team routinely drafts and revises agreements with third parties to ensure compliance with regulatory requirements. We provide critical assistance in transactional matters by analyzing the privacy and security risks of mergers, acquisitions, spin-offs, restructurings, joint ventures, and significant outsourcing relationships.

We work with our clients on incident response plans and investigations, including customer service and media strategies. Our team negotiates with law enforcement agencies and regulators, and drafts breach notice letters and customer service center call scripts. We have significant experience honed over many years working with federal

and state regulators and attorneys general on inquiries, examinations, and enforcement actions involving privacy and security issues. Our litigators defend individuals and companies charged with data privacy violations.

Our representative experience includes:

- *Privacy and Cybersecurity Law Inventories*. Preparing privacy and cybersecurity law inventories tailored to a company's business models to allow for identification of regulatory requirements in their daily operations

- *Security Incident and Data Breach Response*. Advising many companies in investigating, addressing, and meeting compliance obligations relating to security incidents and breaches. Incidents have ranged from local to global in nature, from targeted attacks to widespread incidents impacting millions, and from inadvertent disclosure to hacking

- *Examination and Investigation Response*. Working with clients in responding to examinations by state regulators and civil investigative demands from federal financial regulators, including the FTC involving privacy and information security practices, particularly for companies in the fintech space

- *Data Sharing*. Advising financial institutions on compliance with the GLBA and state disclosure requirements and restrictions on data sharing, including advising a bank on whether its practices with respect to hashed data triggered Regulation P when shared with third-party joint marketing partners

- *Compliance Advice*. Advising numerous clients on how to comply with the various state and federal laws regarding privacy and cybersecurity, including advising clients on applicable CCPA exemptions, including the exemption available to certain information collected, processed, sold, or disclosed pursuant to the GLBA, and preparing policies and procedures, disclosures, and other relevant materials

- *Vendor Management Compliance*. Conducting enterprise-wide vendor management compliance reviews to ensure compliance with relevant state and federal privacy and cybersecurity laws, including advising one of the largest technology companies in the world on addressing the special requirements that U.S. and foreign financial institutions have for critical third-party vendors