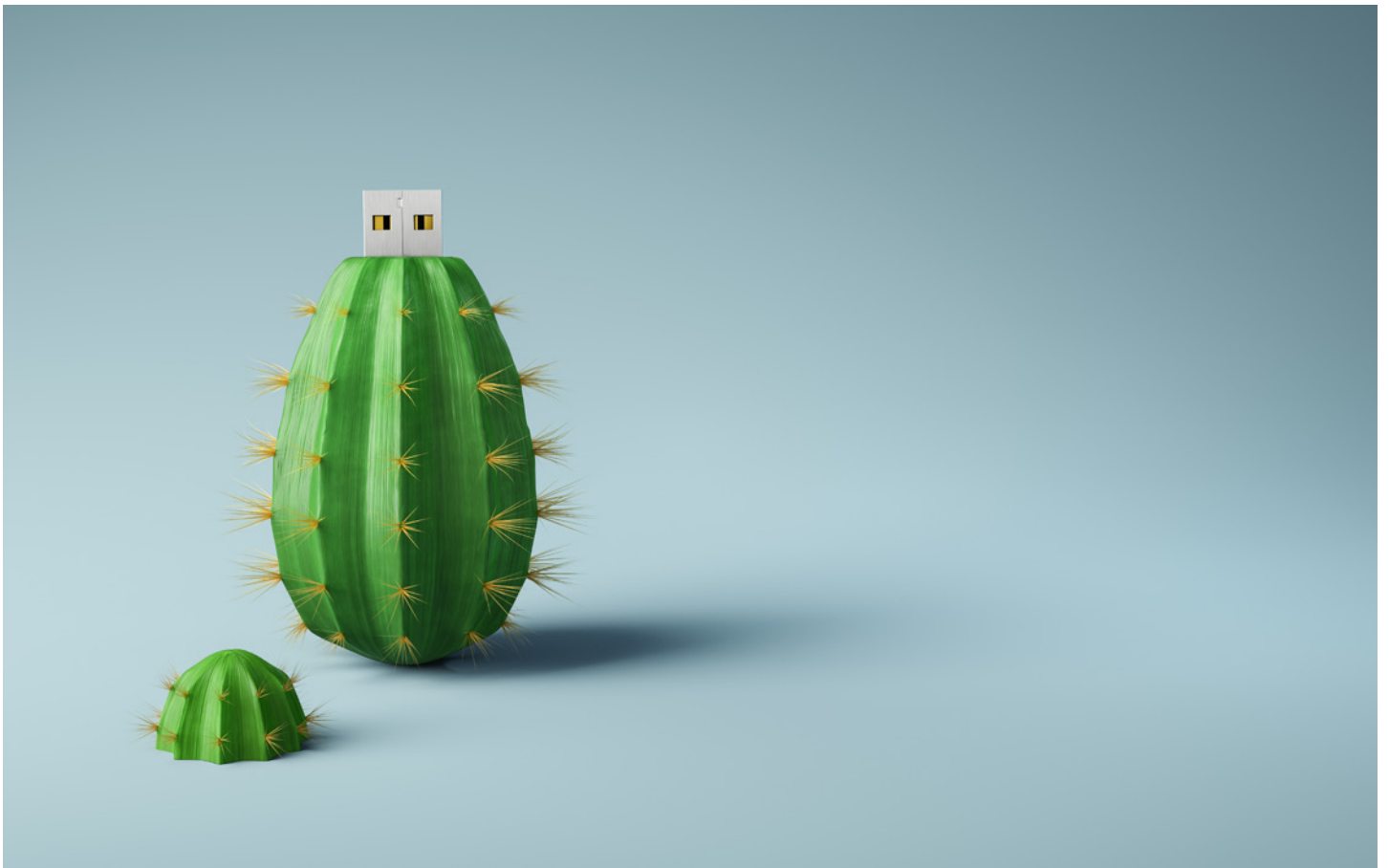




■ **INDEPTH FEATURE** Reprint August 2021

DATA PROTECTION & PRIVACY LAWS

Financier Worldwide canvasses the opinions of leading professionals around the world on the latest trends in Data Protection & Privacy Laws.





UNITED STATES

Proskauer Rose LLP

Respondents



MARGARET A. DALE

**Partner and Vice Chair, Litigation Department
Proskauer Rose LLP
+1 (212) 969 3315
mdale@proskauer.com**

Margaret Dale is a trial lawyer and first-chair litigator handling complex business disputes. As head of the data privacy and cyber security litigation group, her practice covers the spectrum of privacy and data security matters, including regulatory investigations and class action lawsuits stemming from data breaches. Since 2017, she has been honoured by Benchmark Litigation as one of the Top 250 women in litigation and recognised since 2019 as a litigation star in New York. Ms Dale is a frequent writer and authored and annually updates the 'Data Breach Litigation' chapter in PLI's Proskauer on Privacy treatise.



RYAN BLANEY

**Partner and Head, Privacy & Cybersecurity
Practice
Proskauer Rose LLP
+1 (202) 416 6815
rblaney@proskauer.com**

Ryan Blaney is the global head of the privacy and cyber security group. His practice focuses on regulatory, enforcement, litigation and transactions in data privacy and cyber security. He advises clients on compliance, cyber security incidents and government investigations, including acting as lead counsel in defending clients in regulatory investigations by the DOJ, FTC, FCC and state attorneys general. He also counsels clients on federal, state and international privacy and security laws including CCPA and GDPR. He represents investors and lenders in privacy and security due diligence and transactions and negotiations. He is the editor of PLI's Proskauer on Privacy treatise.

Proskauer Rose LLP

Q. Based on your experience, do companies in the US properly understand their data protection duties? To what extent are you seeing rising awareness?

A. In the US, there is no single comprehensive law or regulatory agency addressing cyber security, data protection or privacy. Instead, companies must navigate a patchwork of federal, state, local and sector-specific privacy and data protection laws, regulations and guidance, and engage with regulators from various federal agencies and state attorneys general. The combination of the passage of state privacy laws in California, Virginia and Colorado and the recent highly sophisticated cyber security attacks impacting companies has increased companies' awareness and focus of their privacy and data protection responsibilities. Today, companies in the US are more focused on implementing publicly facing privacy policies, scrutinising third-party vendors and conducting cyber security risk assessments to identify and remediate vulnerabilities. We anticipate that companies' awareness will only increase as more privacy laws

are proposed and passed in the US and internationally.

Q. When companies undertake data processing activities – including handling, storage and transfer – what regulatory, financial and reputational risks do they need to manage?

A. Any missteps by companies in undertaking data processing activities can result in significant regulatory, financial and reputational harm. In the US, the risks are particularly great since all 50 states have data breach notification requirements and some states make their notifications public. The US also has an active plaintiffs' bar that monitors the data processing activities of companies and files public lawsuits in federal and state courts. These lawsuits are often brought as class actions and result in significant costs, expenses and reputational harm to the companies. Companies may also need to manage parallel investigations by state attorneys general, sometimes in the form of multistate investigations, and federal regulatory bodies such as the Federal Trade Commission (FTC) or the Department of Health and Human Services Office of

Proskauer Rose LLP

Civil Rights (HHS-OCR). Regulators often scrutinise whether the company failed to implement reasonable data security measures, made material inaccurate privacy and security representations and violated consumer privacy rights.

Q. What penalties might arise for a company that breaches or violates data or privacy laws in the US?

A. Because there is no overarching federal data or privacy law in the US, a company may face monetary and other penalties for violations of any of the data or privacy laws of any of the over 50 states and territories. Additionally, a company may also be subject to monetary penalties from sector-specific federal data protection legislation, such as the Health Insurance Portability and Accountability Act of 1996 (HIPAA), the Fair Credit Reporting Act (FCRA) and the Gramm Leach Bliley Act (GLBA). Sector-specific federal privacy laws are often enforced by specific regulators, like the Consumer Financial Protection Bureau (CFPB), the Securities and Exchange Commission (SEC), the Federal Communications Commission

(FCC), and the Department of Health and Human Services (HHS).

Q. What insights can we draw from recent data breach cases? What impact have these events had on the data protection landscape?

A. Recent decisions have impacted the requirements for litigants to gain access to the courts. In the US, to have standing to sue in federal court a plaintiff must show, among other things, that the plaintiff suffered a concrete injury in fact. Over the past decade, decisions in the federal courts have been mixed as to whether the heightened risk of future identity theft from a data breach is sufficient to demonstrate injury in fact. In June, the Supreme Court found that, in a suit for money damages, the risk of future harm is not sufficient, by itself, to constitute injury in fact. Litigants will continue to test the boundaries in court to determine rights for compensation and other relief related to perceived data breach violations.

Q. In your experience, what steps should a company take to prepare for a potential data breach, such as developing response



Proskauer Rose LLP

plans and understanding notification requirements?

A. Preparation is essential. Companies cannot wait for a breach to create an incident response plan or identify the regulatory authorities and third parties that they need to be notified. In advance of any breach, companies must understand what types of personal information they have, the location of the personal information and the purpose for which the company is keeping the personal information. To mitigate risk, companies should implement written internal privacy and cyber security policies that include designated employees and senior management responsible for managing the breach and a detailed incident response plan. Companies should also conduct regular internal training to practice responding to a data breach.


Q. What can companies do to manage internal risks and threats, such as rogue employees?

A. There are many steps companies can and should take to manage internal risks and threats. Among them, companies can impose access controls, ensuring



Proskauer Rose LLP

that highly sensitive material is only accessible to personnel with a need to know the information. Companies can also include data privacy policies in employee handbooks and impose sanctions, up to and including termination, for violations of the policies. Companies may also consider providing employees mandatory data protection training, to educate them on avoiding inadvertent disclosures and security threats such as phishing attempts. Companies can also impose comprehensive procedures for collecting sensitive material from employees who have been terminated or are otherwise leaving the company, to lessen the risk of data disclosures by former employees.

constantly changing. Companies must also align their cyber security controls and risk management processes to respond and mitigate against evolving threats, such as ransomware. 

Q. Going forward, how important will it be for companies to remain focused on data protection efforts, continually enhancing their controls and risk management processes?

A. Companies collecting personal information from clients, consumers, employees and third parties in the US need to continually monitor the federal, state, local and sector-specific laws and regulations. The legislative landscape is



Proskauer Rose LLP

www.proskauer.com

PROSKAUER is a recognised leader in privacy and cyber security law. The firm's practice leaders have specialised in this area for more than 20 years. The firm assists clients in all industries around the world with the 'A to Z' of privacy and data security-related legal services. The firm's practice is one of the few that offers the deep data protection expertise of highly specialised lawyers in corporate transactions, compliance, litigation defence and labour and employment. The firm's leadership and reputation for providing pragmatic, business-oriented advice make it the ideal choice to assist businesses with legal needs in this area.

MARGARET A. DALE Partner and Vice Chair, Litigation Department
+1 (212) 969 3315
mdale@proskauer.com

RYAN BLANEY Partner and Head, Privacy & Cybersecurity Practice
+1 (202) 416 6815
rblaney@proskauer.com

NOLAN M. GOLDBERG Senior Counsel
+1 (212) 969 3472
ngoldberg@proskauer.com

Proskauer >>