POLSINELLI

Bruce A. Radke

SHAREHOLDER

Chicago, IL | 312.463.6211
bradke@polsinelli.com

Bruce A. Radke is a Shareholder and a member of the Tech Transactions & Data Privacy practice. He has been selected by his peers as a *Leading Lawyer* in Data Privacy and Computer & Technology Law.

Bruce regularly counsels clients on various privacy and data security issues. He has drafted and reviewed data privacy and security policies and procedures to ensure compliance with HIPAA, HITECH, COPPA, GLBA, Payment Card Industry (PCI) Data Security Standards, state breach notification laws, international data security laws, including the GDPR, and other contractual and privacy-related laws and regulations. Additionally, he regularly assists clients with privacy risk assessments and provides board counseling and employee training. Bruce has counseled clients in the development and implementation of data incident response plans.

Bruce has assisted clients through various types of data incidents, from system-wide network intrusions and ransomware attacks to cyber extortion, fraudulent wire transfers, e-mail account compromises, stolen computer hardware and employee misconduct. Bruce has served a broad range of private- and public-sector clients in multiple industry verticals, including banking and financial services, health care, life sciences, not-for-profit and for-profit education, e-commerce, technology, retail, manufacturing, trade associations, state and local government, accounting, legal and other professional services.

Bruce regularly assists companies in investigations opened by enforcement agencies post-breach, including investigations by the U.S. Department of Health and Human Services Office for Civil Rights, U.S. Federal Trade Commission and state attorneys general as well as other state and federal financial, insurance and education enforcement agencies.

Bruce is also member of InfraGard (a partnership between the Federal Bureau of Investigation and the private sector). He has written and spoken extensively on a variety of topics relating to privacy, data security and information management. His articles and comments have been featured in the *Wall Street Journal, Chicago Tribune, Review of Banking & Financial Services* and *Privacy & Data Security Law Journal*.

Capabilities

- Technology Transactions
- Privacy & Cybersecurity
- Commercial Litigation
- Health Care Technology
- Licensing & Transactions
- International
- Biometric Privacy Law
- International Privacy
- Information Security (InfoSec)
- Data Breach & Incident Response
- Privacy & Cybersecurity Counseling
- Financial Institutions Privacy
- Technology
- Litigation

Education

- University of Illinois College of Law (J.D., *magna cum laude*)
- University of Illinois (B.A., *cum laude*)

Bar Admissions

- Illinois, 1993

Court Admissions

- U.S. District Court, Northern District of Illinois
- U.S. District Court, Eastern District of Wisconsin
- U.S. Court of Appeals, Seventh Circuit
- U.S. District Court, Central District of Illinois

Memberships

- Member, InfraGard
- Vice President of the Chicago Bar Association's Cyberlaw and Data Privacy Committee

Recognition

- Named to Cybersecurity Docket's Incident Response Elite, 2026
- Selected for inclusion in *Best Lawyers in America*® for Privacy and Data Security Law, 2026
- *Leading Lawyer*, Commercial Litigation, Computer & Technology Law and Data Privacy, 2017

Matters

- Served as breach counsel for academic health system in connection with an incident arising out of a threat actor's deletion and attempted extortion for the return of the ePHI of approximately 80,000 patients residing across the U.S. and multiple foreign jurisdictions

- Served as breach counsel for financial institution that was the target of ransomware and extortion attack involving the acquisition and posting on various social media sites the sensitive member information and personal information of more than 46,000 of the institution's members and other affected individuals

- Served as breach response counsel for international financial institution whose Office 365 e-mail accounts of users in the United States and the United Kingdom were compromise potentially triggering notification under the New York Department of Financial Services Cybersecurity Requirements for Financial Services Companies and United Kingdom's Data Protection Act of 2018

- Served as breach response counsel for more than one hundred incidents of credit unions across the United States, including ransomware, extortion, fraudulent wire transfers, Office 365 e-mail account compromises, network intrusions and employee

misconduct

- Served as counsel for manufacturer whose production line system was compromised resulting in intentional alteration of specialty product’s alteration and demand by threat actor for payment to cease further product alterations and information on past product alterations
- Served as breach response counsel for health care system that experienced a malware attack potentially impacting approximately four million customers and 40,000 employees
- Served as breach counsel to university following brute-force password attack resulting in the compromise of personally identifiable information (PII) of over 60,000 students, alumni and employees residing in more than 40 states and several foreign countries
- Served as breach response counsel for website/e-commerce hosting services provider that sustained a malware attack impacting hundreds of third-party companies that used clients hosting services as well as thousands of those companies' customers
- Served as breach response counsel for health care system in connection with potential exposure of radiological records of approximately 400,000 patients
- Served as breach response counsel for community bank that sustained malware attack on online banking portal impacting customers across numerous states
- Served as breach response counsel for law firm following theft of the firm's servers containing Pll and protected health information (PHI) of approximately 20,000 clients, adversaries and witnesses located in multiple states
- Assisting major financial institutions to update and improve information security and data privacy practices, including data breach response procedures, and conducting data privacy audits to identify potential privacy and data security issues
- Conducting review of multinational food and beverage company information policies to ensure compliance with data privacy and security best practices
- Conducting privacy and risk management audits for numerous multistate retailers and life science companies
- Developing employee training programs on information security and data privacy compliance for several investment advisers, broker-dealers and other financials service institutions

Publications

January 7, 2025

Cybersecurity Compliance in 2025 – Know Your “Technology” Assets

July 31, 2023
SEC Adopts Cybersecurity Incident and Risk Management Disclosure Rules

February 14, 2023
Cybersecurity To-Dos in 2023

February 2, 2023
Tech Transactions & Data Privacy 2023 Report