POLSINELLI

Data Breach & Incident Response

Polsinelli attorneys have a long history of counseling clients impacted by data breaches and other cyber incidents. In fact, one of our shareholders handled one of the first data breach cases shortly after California passed its breach notification law in 2003. Since then, our attorneys collectively have handled thousands of data security incidents and have counseled clients through nearly every conceivable breach, from system-wide ransomware attacks, cyber extortion events, and email system compromises to lost and stolen computer systems, ATM skimming incidents, website compromises, misdirected emails and employee theft.

When an incident occurs, we provide comprehensive assistance, including overseeing forensic investigations and crisis management activities, notifications to affected individuals, regulators and payment card issuers, and responding to federal and state regulatory inquiries and litigation defense. We also assist organizations in preparing for data incidents by developing incident response plans, employee training and board counseling. Our interdisciplinary approach encompasses all data and system security aspects before and after an incident.

Polsinelli's team includes

- Incident response attorneys who are some of the most experienced in the country
- Alumni of enforcement agencies charged with enforcing privacy and security regulations, such as the Department of Health and Human Services – Office for Civil Rights (OCR)
- Attorneys with international backgrounds who are equipped to counsel organizations on evolving international data breach regulations
- Former in-house data privacy attorneys who understand the regulatory landscape and the logistical and business considerations associated with incident response

Polsinelli attorneys have served a broad range of clients in multiple sectors, including

- Banking, credit union and financial services
- Health care providers, suppliers, technology and diagnostic companies
- Life science and pharmaceutical
- Senior housing and long-term care
- Technology
- E-commerce and managed service providers
- For-profit and not-for-profit education
- Tribal and gaming
- Insurance carriers, brokers and agencies
- Federal government contractors
- State and local government
- Manufacturing
- Accounting, legal and other professional services

Regulatory Investigations

Polsinelli is uniquely equipped to represent organizations in investigations brought by industry regulators, State Attorneys General and other enforcement agencies post-breach. Polsinelli attorneys have assisted clients in hundreds of data breach-related regulatory investigations. Team members include alumni of the United States Department of Justice (DOJ) and other enforcement agencies, including the U.S. Department of Health & Human Services – Office for Civil Rights. Having sat on the other side of the table, Polsinelli's attorneys understand the steps organizations need to take to be in the best possible position to respond to an investigation.

Tabletop Breach Exercises

In today's complex risk environment, organizations should assume that it is not a matter of *if* it will suffer a data incident but *when* and prepare accordingly.

Incident response preparedness should not be limited to creating plans or procedures that are then filed away in a policy manual. Rather, organizations should test their preparedness and ensure key stakeholders have thought about how an organization will respond to an incident. Polsinelli's Tabletop Breach Exercises are designed to do just that.

Polsinelli incident response attorneys are some of the most experienced in the country. Our attorneys draw from this practical experience and work with a client's organization to develop a realistic breach scenario. Polsinelli attorneys will then facilitate a mock breach exercise that will require team members to:

- Rapidly assess a stream of incoming information
- Establish response strategies
- Think short-term and long-term about how various actions or inactions could impact the organization's reputation and operations

The exercise can be conducted solely with an organization's incident response team or built into a broader employee training session.

Matters

- Served as breach response and regulatory counsel in connection with hundreds of ransomware and cyber-extortion matters.
- Served as privacy counsel in connection with M&A deals, assisting clients in analyzing the risk associated with purchasing or investing in entities in light of ongoing or recent data security incidents and privacy compliance issues.
- Served as breach response and regulatory counsel for numerous financial institutions investigating and responding to ATM skimmer incidents.
- Served as breach response and investigation counsel for entities investigating and responding to suspected insider threat incidents.
- Served as breach response counsel for numerous e-commerce retailers investigating website and payment card information compromises and responding to inquiries from regulators and payment card brands.
- Served as class action defense counsel for entities involved in litigation arising from data incidents.
- Served as breach response and litigation counsel for financial institution that lost backup tapes containing account information of approximately two million customers.
- 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 response counsel to university following a brute-force password attack, compromising the personal information of over 60,000 students, alumni and employees residing in more than forty states and multiple foreign countries.
- Served as breach response counsel for an e-commerce hosting services provider that sustained a malware attack impacting hundreds of third-party companies that used client's 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 and law enforcement liaison for a national restaurant chain in connection with possible insider theft of payroll records.
- Served as breach response counsel for health care provider, investigating whether patient information was stolen as part of an identity theft ring focused on illegally acquiring prescription medication.
- Advised client regarding internationally discussed device vulnerabilities that led to a security incident, state and federal regulatory investigations, and multiple class action lawsuits. Polsinelli provided counsel regarding all separate matters, including device security, incident response, response to regulator inquiries, and representation in litigation.
- Assisted an art dealer in connection with a wire fraud incident related to the purchase of a multimillion-dollar piece of art.
- Counseled a multinational company notified by a security researcher that credentials to its AWS environment were available on a publicly facing server containing millions of records.

Publications

January 22, 2026
Can State Legislation Help Stem the Onslaught of Data Breach Lawsuits?
Co-Author, 2026 Technology Transactions & Data Privacy Report

January 22, 2026
When Breaches Bring Regulators to Your Door: Preparing for Heightened Scrutiny of Your Security Compliance Program
Co-Author, 2026 Technology Transactions & Data Privacy Report

January 22, 2026
Current Trends in Data Breach Notification Laws: Increased Regulator Scrutiny Leads to Greater Responsibilities for Companies
Co-Author, 2026 Technology Transactions & Data Privacy Report

January 22, 2026
Seven Practical Steps to Data Management: A Guide for Businesses
Co-Author, 2026 Technology Transactions & Data Privacy Report

January 12, 2026
2026 Technology Transactions & Data Privacy Report

October 10, 2025
$19M in Settlements Underscore Cybersecurity Risks for TPAs and Insurers

May 2025
Current Trends in Data Breach Notification Laws: Safe Harbors and Reinforcing the Case for Cybersecurity
Co-Author, Pratt's Privacy and Cybersecurity Journal Vol 11 No 4

February 26, 2025
Current Trends in Data Breach Notification Laws: Safe Harbors and Reinforcing the Case for Cybersecurity

February 6, 2025
2025 Technology Transactions & Data Privacy Report

January 7, 2025
Cybersecurity Compliance in 2025 – Know Your "Technology" Assets

October 28, 2024
Cybersecurity for Critical Infrastructure Update – Incident Response Improves, Industry Standards Evolve

June 2024
Looking Ahead to the Federal Trade Commission's Implementation of the Data Breach Notification Rule for Nonbanking Financial Institutions
Co-Author, The Banking Law Journal Vol 141 No 6

May 2024
Current Issues in Data Breach Class Action Settlements
Co-Author, Pratt's Privacy & Cybersecurity Law Report Vol 10 No 4

April 19, 2024
Critical Infrastructure Cybersecurity – Evolving Incident Response Obligations, Integral to Effective Risk Management

March 27, 2024
Legal Frontiers: Navigating the Rapid Evolution of Privacy Laws and Tech Governance
Featured, The State of Identity Podcast

January 24, 2024
Current Issues in Data Breach Class Action Settlements

January 24, 2024
Arbitration of a Data Breach Lawsuit: Defeating Class Actions with Arbitration Clauses and Class Waivers

January 24, 2024
Cybersecurity Insurance: Practical Steps Your Business Can Take to Become More Insurable

January 24, 2024
Looking Ahead to the FTC's Implementation of the Data Breach Notification Rule for Nonbanking Financial Institutions

January 24, 2024
It's Not Your Fault, but It May Be Your Problem: Increasing Regulatory Scrutiny on Vendor Cybersecurity Risks

January 24, 2024
2024 Tech Transactions & Data Privacy Report

March 7, 2023
FTC Targets Disclosure of Health Data for Web Tracking Again

February 7, 2023
“First-of-Its-Kind” FTC Breach Enforcement Case on Hot-Button Website Tracking Issue

October 27, 2022
FTC Announces Decision “with a 100% chance of far-reaching” Impact for Data Breaches

June 23, 2022
Legal Matters: When The Feds Find Out! Lack Of Data Security Leads To Novel and Hefty Settlements
Co-Author, Houston Medical Times

September 2018
The Alabama Data Breach Notification Act of 2018
Co-Author, The Alabama Lawyer, Vol. 79, No. 5

March 7, 2018
Responding to GDPR pushback: The business case for compliance
Co-Author, IAPP