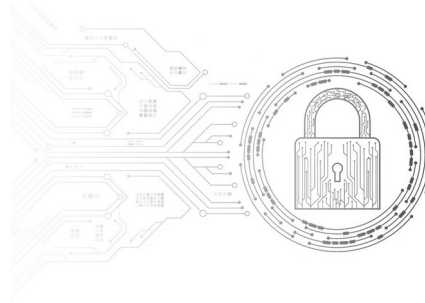


Cybersecurity & Data Breach Response

Ready to respond if a data breach occurs



Your company's data is one of its most important assets. In the event of a security incident or breach, our team responds immediately:

- Coaching you through the incident
- Advising on each step of the process
- Mitigating the damage and operational disruptions
- Navigating the numerous consumer protection and industry specific notification laws

Streamlined process developed from years of experience managing hundreds of security incidents and breaches, including business email compromises, system intrusions, and ransomware attacks.

We help clients

- Comply with data breach notification requirements by industry and jurisdiction
- Engage forensic experts for assessment, mitigation, and ongoing fortification of information technology systems
- Communicate with affected parties, employees, the public, law enforcement, and regulators
- Conduct internal investigations and respond to government investigations
- Defend related private and class action lawsuits

Data breaches can impact any business.

We've represented hundreds of clients across industry sectors, including:

- Automotive
- Banking & Financial Services
- Consumer Products & Retail
- Education
- Energy & Utilities
- Healthcare

Related Practice Areas

[Blockchain & Digital Currency](#)

[Class Action & Multi-Claim Litigation](#)

[Cybersecurity & Data Privacy](#)

[E-Discovery - Encompass](#)

[E-Discovery & Information Governance](#)

[Global Privacy & Security](#)

[Litigation](#)

[Payments & Digital Commerce](#)

[Records & Information Governance](#)

[White Collar Defense & Government Investigations](#)

Related Industries

[Banking & Financial Services](#)

[Consumer Products & Retail](#)

[Insurance](#)

[Life Sciences, Pharmaceuticals & Medical Devices](#)

[Manufacturing](#)

[Technology and Commercial Transactions](#)

- Hospitality, Leisure & Travel
- Manufacturing
- Real Estate
- Technology
- Transportation

How we work

- Our team provides individual client attention and 24/7 service
- Our team customizes our approach to meet the needs of individual clients and move efficiently through the life cycle of an incident
- Our team stays ahead of the curve and up to speed as technology and legal requirements change rapidly
- Our team stays focused on swift recovery and damage control aggressively working the case from the first date of discovery to reduce the risk of media, regulatory, and litigation fallout

Why Nelson Mullins?

- Highly experienced team
- Available 24 hours a day, every day to respond to a data breach
- Track record of success
- Efficient and organized approach
- Practical solutions when it matters most

Experience

The following is a small sampling of the hundreds of data security incident matters our experienced team has handled over the years and is provided for informational purposes only.

- Counseled financial institutions and payment processing vendors through all stages of data security incidents involving the loss of sensitive customer data, including incident analysis and breach containment, incident disclosure (i.e., notification in compliance with all regulatory requirements), loss mitigation, and remediation customized to meet each client's specific business and industry requirements.
- Counseled numerous clients (including financial institutions, payors, and payees) through wire transfer fraud incidents – including notification to federal authorities to recover funds.
- Counseled major national retailer through a security incident investigation involving the discovery of malware potentially compromising all credit card processing of the company, regulatory compliance, risk assessment, and remediation.
- Counseled international companies through breach investigations, response and notification involving the theft of

employee W-2 tax information obtained as the result of a phishing schemes.

- Counseled the domestic subsidiary of a major international company through a security incident investigation involving employee theft and misappropriation of customer credit card information.
- Counseled member organization providing conference services in over 250 countries through a global data security incident.
- Counseled accounting and outside law firm clients through data breach investigations involving the release of sensitive client information to unauthorized recipients and customer notification.
- Counseled numerous manufacturing companies through ransomware attacks involving extensive interruption of business operations in the U.S. and abroad.
- Counseled large health systems and educational universities through multi-service provider data security breaches and ransomware attacks.
- Counseled numerous school systems and municipalities through direct and vendor related ransomware attacks and e-discovery of data to provide notification as needed under the applicable law.
- Counseled health systems, academic medical centers and major universities through data security incidents (including ransomware attacks) involving millions of consumers, patients, employees, and students.
- Counseled numerous clients of all sizes from all industry sectors in business email compromises resulting from phishing scams.
- Counseled numerous clients in data privacy matters – such as the theft / loss of millions of consumers personally identifiable information (PII) resulting from improper data retention / destruction practices.
- Counseled numerous clients in data mapping and risk management strategies for compliance purposes and to prevent catastrophic loss of data and reputation in the event of a data breach.
- Counseled hundreds of HIPAA covered entities and HIPAA business associates through data security incidents and breach reporting and complaint investigations (including multiple right of access claims) with the Office for Civil Rights with a 100% success rate to date and no fines or penalties assessed.
- Assisted multiple clients with international presences develop and implement privacy compliance programs including assessing and mapping company-held personal information, developing policies and procedures, drafting and refining workflows and language for data subject requests, and negotiating vendor agreements with data processors and service providers pursuant to standards laid out in privacy laws.
- Conducted data breach simulation tabletops across the country for middle-market to Fortune 500 companies with domestic and global operations.
- Counseled numerous clients from small businesses to Fortune 500 companies on incident response plans, emergency preparedness and disaster recovery planning.
- Drafted millions of breach notification letters for clients nationwide and with operations across the globe.