MCDONALD HOPKINS

BREACH RESPONSE | DUAL

Attorney-led cyber incident preparation and response support for ransomware, business email compromise, wire fraud, data theft, vendor incidents, regulatory inquiries, and breach-related disputes.

POST-INCIDENT RESPONSE ACTIVITIES

- **Immediate triage:** Assess whether systems are encrypted, data was accessed or exfiltrated, funds were diverted, or operations are disrupted; preserve evidence and structure privileged communications.
- **Forensic investigation coordination:** Engage and oversee forensic investigators to identify the attack vector, timeline, containment, persistence, impacted systems, and potential data exposure.
- **Legal and regulatory analysis:** Determine whether notice is required to individuals, regulators, attorneys general, consumer reporting agencies, customers, insurers, law enforcement, or business partners.
- **Ransomware and threat actor response:** Advise on extortion strategy, sanctions risk, law enforcement coordination, insurer involvement, data leak sites, and communications with negotiators.
- **Wire fraud and BEC recovery:** Move quickly with banks, law enforcement, insurers, and counterparties to pursue funds recovery and preserve claims.
- **Notice, communications, and defense:** Draft notices, FAQs, call center scripts, public statements, regulator responses, and customer communications while managing litigation and reputational risk.
- **Lessons learned:** Document root causes, remediation, governance improvements, and plan updates to create a defensible record after the incident.

INCIDENT RESPONSE 24/7 HOTLINE

TO REPORT AN INCIDENT:

mh-DUALincident@mcdonaldhopkins.com

OR CALL 833-DUAL007