On March 1, 2017, new cybersecurity regulations promulgated by the New York Department of Financial Services (NYDFS) came into effect, requiring banks, insurance companies and other financial services entities to establish and maintain a cybersecurity program designed to protect the confidentiality, integrity and availability of their information systems.

BakerHostetler’s privacy and data protection team has unparalleled expertise when it comes to evaluating and managing cybersecurity risk, having counseled companies on more than 2,000 data security incidents from containment to remediation. We are uniquely well-qualified to assist clients with NYDFS compliance given our experience advising on breach prevention and response for hundreds of financial institutions and insurance companies, coupled with our extensive work directing risk compliance gap assessments and remediation efforts pursuant to federal and state regulatory frameworks, state insurance requirements and industry standards such as the Payment Card Industry Data Security Standard (PCI DSS).

Who’s Affected?
The new regulations affect any financial services provider subject to the jurisdiction of NYDFS, whether or not the entity is headquartered in New York. These include:

- Banks
- Credit unions
- Money transmitters
- Insurers
- Mortgage bankers, brokers, originators and servicers
- Holding companies
- Charitable foundations

Covered entities should act now to verify whether their existing security protocols are compliant with the new regulations and implement any necessary upgrades. The NYDFS regulations are likely to have implications far beyond New York. Given the significant number of financial institutions that will be required to comply, other regulators, clients, customers and counterparties likely will view these requirements as a de facto baseline standard for cybersecurity in the financial industry.

Service Offerings and Experience
In addition to our work counseling NYDFS-regulated entities on the development and implementation of new cybersecurity compliance programs, we also:

- Provide cybersecurity training and counseling to financial services companies regulated by the CFPB, CFTC, FDIC, FinCEN, FINRA, NCUA, OFAC, SEC and various state agencies.
- Conduct service provider and business partner due diligence to assess security posture prior to engagement, and then monitor compliance with contractual obligations on an ongoing basis.
Named to the BTI Client Service 30 for the third year in a row and selected as a BTI Best Value Leader.

109 BakerHostetler attorneys were ranked in the 2016 edition of Chambers USA.

26 BakerHostetler practice areas were also ranked – with five practice areas receiving Band 1 rankings.

Contacts
Ted Kobus  T +1.212.271.1504  tkobus@bakerlaw.com
Jonathan A. Forman  T +1.212.847.2855  jforman@bakerlaw.com
Craig A. Hoffman  T +1.513.929.3491  cahoffman@bakerlaw.com
Randi Gainer  T +1.206.332.1381  rgainer@bakerlaw.com
Melinda L. McLellan  T +1.212.589.4679  mmclellan@bakerlaw.com

Recognized as one of the top firms for client service, BakerHostetler is a leading national law firm that helps clients around the world to address their most complex and critical business and regulatory issues. With five core national practice groups – Business, Employment, Intellectual Property, Litigation and Tax – the firm has more than 940 lawyers located in 14 offices coast to coast. For more information, visit bakerlaw.com.

Model Project Plan

Phase 1 – Scoping and Gap Assessment

- Identify the covered entities within the organization to be included, and assess the complexity and sophistication of relevant information systems.
- Conduct a comparative analysis of the current cybersecurity program against the new requirements, including interviews of security team members and analysis of information security, business continuity and incident response policies, as well as recent risk assessments and vulnerability testing results.
- Confer with key stakeholders regarding the initial compliance assessment to identify requirements to be met during each of the four transitional time periods, potential gaps based on current posture and preliminary goals for remediation.

Phase 2 – Compliance Management Plan Development

- Collaborate on the development of prioritized timelines for completion of the specific tasks necessary to meet the four transitional deadlines.
- Prepare a detailed road map for managing the remediation process to ensure compliance obligations are met in a timely fashion and within budgetary parameters.
- Analyze findings and apply them against the compliance management plan, assess whether enhancements or modifications should be made to the compliance management plan, and develop a triaged approach to address challenges or gaps.

Phase 3 – Risk Assessment

- If a service provider will participate in the risk assessment process, we will engage that third party to assist us in providing legal advice regarding the entity’s compliance posture.

Phase 4 – Execution and Follow-up

- Offer targeted advice and counsel during the execution of the cybersecurity compliance management plan.
- Provide ongoing support relevant to the maintenance, review and improvement of the cybersecurity program over time.

© 2017 BakerHostetler®

Baker & Hostetler LLP publications inform our clients and friends of the firm about recent legal developments. This publication is for informational purposes only and does not constitute an opinion of Baker & Hostetler LLP. Do not rely on this publication without seeking legal counsel.