MARCH 6, 2019

For more information, contact:

Phyllis Sumner
+1 404 572 4799
psumner@kslaw.com

Scott Ferber
+1 202 626 8974
sferber@kslaw.com

Ehren Halse
+1 415 318 1216
ehalse@kslaw.com

John Horn
+1 404 572 2816
jhorn@kslaw.com

William Johnson
+1 212 556 2125
wjohnson@kslaw.com

King & Spalding

New York
1185 Avenue of the Americas
New York, New York 10036-4003
Tel: +1 212 556 2100

Atlanta
1180 Peachtree Street, NE
Atlanta, Georgia 30309-3521
Tel: +1 404 572 4600

NY DFS Cybersecurity Regulation, Two Years In - What Comes Next?

This past Friday, March 1, 2019, marked the second anniversary and final effective date of the New York Department of Financial Services (DFS)'s cybersecurity regulation.[1] Since its enactment, regulated institutions,[2] subject to limited exemptions,[3] have had to implement and maintain "robust" cybersecurity programs and file annual certifications with DFS attesting to their compliance. As set forth in more detail below, the mandated programs must contain core policies and procedures governing cybersecurity, involve risk assessments, and ensure oversight for company operations, employees, and third-party service providers. The cybersecurity regulation also requires regulated institutions to report qualifying cybersecurity events within 72 hours.

As of December 2018, DFS has received approximately 1,000 notices of cybersecurity events, with a "significant number" involving breaches stemming from credential-stealing email schemes. As a result of this activity, in a memorandum to the CEOs of regulated institutions, DFS has emphasized that institutions "make sure all persons who can access a company's systems have the proper protections and are using the appropriate protections," have "strong access controls and training," and "embrace opportunities to improve and advance their cybersecurity readiness and systems."[4] DFS has further underscored "the importance of full compliance" with multi-factor authentication, "strong access controls and encryption for data in transit and at rest," and "ongoing training."[5]

DFS CYBERSECURITY REGULATION REQUIREMENTS

Regulated institutions, subject to limited exemptions, must implement, maintain, and annually certify to DFS that they have "robust" cybersecurity programs protecting the confidentiality, integrity, and availability of their information systems, including:

- a written **policy**, approved by the board of directors or a senior officer, setting forth the policies and procedures for protecting information systems and stored nonpublic information;
- a written **incident response plan** designed to promptly respond to, and recover from, a cybersecurity event;
- periodic, documented **risk assessments** of information systems, in accordance with written policies and procedures, updated as reasonably necessary to address changes to information systems, nonpublic information, or business operations;
- continuous **monitoring** or annual penetration testing and bi-annual vulnerability assessments;
- a qualified **Chief Information Security Officer** responsible for overseeing and implementing the cybersecurity program and enforcing cybersecurity, who submits written reports, at least annually, to the board of directors or a senior officer;
- secure systems that can sufficiently **reconstruct material financial transactions** (to the extent applicable and based on the institution's risk assessment);
- secure systems that generate **audit trails** designed to detect and respond to cybersecurity events (to the extent applicable and based on the institution's risk assessment);
- data retention and secure destruction policies and procedures, in accordance with defined **recordkeeping** timetables;
- limited **user access privileges** to information systems that provide access to nonpublic information, with periodic review of those access privileges (based on the institution's risk assessment);
- written **procedures, guidelines, and standards** governing internally and externally developed **applications**, which are to be periodically reviewed;
- written policies and procedures governing information systems and nonpublic information accessed or held by **third-party service providers** (based on the institution's risk assessment);
- qualified cybersecurity **personnel** and intelligence;
- ongoing **training and monitoring** for all authorized users; and
- **effective controls**, which may include multi-factor authentication, risk-based authentication, encryption, and effective alternative compensating controls (based on the institution's risk assessment).[6]

WHAT COMES NEXT?

What can DFS-regulated institutions expect going forward? Now that the cybersecurity regulation is effective, and DFS has in its hands two years' worth of incident notices and certification information, regulated institutions can reasonably expect continuing, rigorous oversight and enforcement of non-compliance. DFS will likely use all of its powers of supervision (including yearly provision of licenses to operate in New York) and/or examination of regulated institutions to ensure compliance with the cybersecurity regulation. The fact that regulated institutions have fully complied to date does not keep them in safe waters in perpetuity. As the regulations and DFS's own public statements reinforce, institutions must be continually vigilant in assessing their cybersecurity risk and maintaining (and documenting) appropriate programs and steps to address that risk in a "robust fashion."[7] Concerning consequences for non-compliance, the text of the cybersecurity regulation does not detail how penalties and fines may be calculated or assessed. During the public comment period, DFS responded to requests for additional details as to such enforcement mechanisms by saying only that the existing language was "sufficient." Enforcement actions under the cybersecurity regulation could stem from the general authority of DFS under the New York Banking Law, which allows for penalties for violations as high as $2,500

per day during which a violation continues, $15,000 per day in the event of any reckless or unsound practice or pattern of misconduct, and $75,000 per day in the event of a knowing and willful violation.[8] Given DFS's clearly expressed intent to move regulated institutions to compliance, and the potentially significant penalties at DFS's disposal, regulated institutions should make every effort to ensure compliance with the cybersecurity regulation's numerous obligations.

[1] *See* 23 NYCRR 500, available at https://www.dfs.ny.gov/docs/legal/regulations/adoptions/dfsrf500txt.pdf.

[2] 23 NYCRR § 500.01(c) (defining a "covered entity" as "any person operating under or required to operate under a license, registration, charter, certificate, permit, accreditation or similar authorization under the Banking Law, the Insurance Law or the Financial Services Law").

[3] 23 NYCRR § 500.19 (exempting: (a) a covered entity (1) with fewer than 10 employees, including any independent contractors, of the covered entity or its affiliates located in New York or responsible for business of the covered entity, (2) with less than $5,000,000 in gross annual revenue in each of the last three fiscal years from New York business operations of the covered entity and its affiliates, (3) with less than $10,000,000 in year-end total assets, calculated in accordance with generally accepted accounting principles, including assets of all affiliates; (b) an employee, agent, representative, or designee of a covered entity, who is itself a covered entity, to the extent that they are covered by the cybersecurity program of the covered entity; (c) a covered entity that does not directly or indirectly operate, maintain, utilize, or control any information systems, and that does not, and is not required to, directly or indirectly control, own, access, generate, receive or possess nonpublic information, from the requirements of sections 500.02, 500.03, 500.04, 500.05, 500.06, 500.07, 500.08, 500.10, 500.12, 500.14, 500.15, and 500.16; or (d) a covered entity under Article 70 of the Insurance Law that does not and is not required to directly or indirectly control, own, access, generate, receive or possess nonpublic information other than information relating to its corporate parent company (or affiliates) from the requirements of sections 500.02, 500.03, 500.04, 500.05, 500.06, 500.07, 500.08, 500.10, 500.12, 500.14, 500.15, and 500.16. Notably, a covered entity that qualifies for an exemption must file a notice of exemption within 30 days of determining exemption applicability. See 23 NYCRR § 500.19(e). In addition, a covered entity that ceases to qualify for an exemption has 180 days from the end of the fiscal year to comply with all applicable requirements. *See* 23 NYCRR § 500.19(g).

[4] https://www.dfs.ny.gov/system/files/documents/2019/01/cyber_memo_12212018.pdf.

[5] *Id*.

[6] 23 NYCRR §§ 500.00, et seq.

[7] *See, e.g.,* 23 NYCRR § 500.00 ("This regulation requires each company to assess its specific risk profile and design a program that addresses its risks in a robust fashion."); https://www.dfs.ny.gov/system/files/documents/2019/01/cyber_memo_12212018.pdf ("Accordingly, by March 1, 2019, all banks, insurance companies, and other financial services institutions and licensees regulated by DFS will be required to have a robust cybersecurity program in place that is designed to protect consumers' private data").

[8] *See* NYBNK § 44.