Client Update
New Cyber Guidance From NY DFS: A Possible Path To "Reasonable Security"

NEW YORK
Jeremy Feigelson
jfeigels@debevoise.com

Eric R. Dinallo
edinallo@debevoise.com

Gregory J. Lyons
gjlyons@debevoise.com

Jim Pastore
jjpastor@debevoise.com

WASHINGTON, D.C.
Satish M. Kini
smkini@debevoise.com

New York State's Department of Financial Services has spelled out a detailed list of issues it will cover in the new cybersecurity portion of its bank examinations. In a world where companies increasingly are said to have an affirmative legal obligation to maintain robust cybersecurity, a major regulator's views on exactly how to discharge that obligation bear close attention – not just by the financial institutions that DFS regulates, but by corporations generally.

The new guidance follows up on DFS's promise, in a report it issued earlier this year, that cybersecurity would become a topic in its bank examinations going forward. The top-level message, DFS says, is that cybersecurity should now be viewed "as an integral aspect of [financial institutions'] overall risk management strategy, rather than solely as a subset of information technology." The more granular mandate is that banks will have to answer questions about these issues, among others:

- corporate governance of cybersecurity, including the CV and job description of the Chief Information Security Officer or other senior responsible person;
- policies and procedures designed to further the goals of confidentiality, integrity and availability, including the integration of data classification (a/k/a, the sorting of data according to its sensitivity and risk level) into such policies and procedures;
- various highly specific security topics, such as the use of multi-factor authentication, patch management, penetration testing, and vendor management (N.B. – it is a matter of public record that criminals' abuse of credentials issued to third-party vendors has been a factor recently in a number of high-profile hacks);
- incident detection and response processes, including monitoring and the organization's written incident response plan;

- cyber insurance coverage; and
- periodic reevaluation of policies and procedures in light of changing risks.

For the banks that will be subject to these DFS examinations, the December 10 memo obviously provides a roadmap of sorts. Strong substantive answers on the enumerated topics, clearly presented, can be expected to generate clean examination reports. Answers that DFS considers highly unsatisfactory, in contrast, could prompt DFS to exercise its authority to pursue civil enforcement measures. DFS's legal authority also includes the capacity to refer matters to criminal prosecution, though that seems unlikely in this context.

(Side note: Banks will want to think about how to present their answers to DFS not just clearly, but confidentially. The examination template calls for a good deal of sensitive information. DFS and its predecessor agencies historically have been generous in allowing regulated entities to claim exemption under New York's Freedom of Information Law for the materials they submit in examinations.)

From a more aerial view, DFS's new guidance might fairly be seen as "regulation by implication." That is - ***simply by requesting detail about the use of particular practices, DFS is sending clear signals as to what it regards as best practices.*** And given that DFS examinations have the potential to trigger enforcement actions, the agency's preference for this or that practice can in substance come to have the force of law.

Take multi-factor authentication as an example. For the uninitiated, this is the practice of requiring a person to enter more than one sort of credential to access a computer system – say, both an alphanumeric password and a code from a token. No state or federal law expressly dictates the use of multi-factor authentication. But by asking companies to describe their practices in this area, DFS is clearly signaling that, going forward, it hopes to see companies adopt policies and procedures favoring multi-factor authentication.

This approach can be seen throughout the DFS guidance: Simply by asking pointed questions – about vendor management, patch management, the use of written incident response plans, and so on – DFS is dropping strong hints as to what it will consider "right" answers in the context of the examinations it will conduct in 2015. For now, the cyber examinations are limited to banks. It is our expectation that DFS will largely if not completely extend them as well to insurance companies, which DFS also regulates.

Corporations in general can take useful guidance from this as well. The DFS memo resonates with a variety of legal authorities that call on companies in all sectors of the economy to maintain so-called "reasonable security" – or face legal consequences for failing to do so. To name just a few examples:

- At the motion to dismiss stage, a Minnesota federal judge this month upheld common-law negligence claims brought against Target by banks affected by the retailer's data breach. The decision recognizes a legal duty of care, while leaving the particulars of what satisfies that duty to be defined down the road. (N.B. – Just yesterday, the same judge also allowed substantial parts of a consumer class action against Target to proceed. The judge dismissed the negligence claims for failure to plead economic harm; the issue of whether Target owed consumers a duty was not before the court.)
- California's Data Safeguard Law, Cal. Civ. Code §§ 1798.81.5, requires companies to maintain "reasonable" data security measures – but does not spell out what those measures must be.
- The Federal Trade Commission is suing a number of prominent hacking victims on the grounds that their cybersecurity allegedly was so poor as to constitute an unfair business practice under Section 5 of the FTC Act, 15 U.S.C. § 45. In court challenges, the FTC thus far has prevailed in its view that substantive data security standards can be established case by case through enforcement actions, and need not be affirmatively stated by the agency.

Corporations of all types thus must consider this potential double whammy: On the one hand, "reasonable security" may be emerging as a legal standard. On the other hand, no court, regulator or legislature has yet laid out an explicit path to satisfying that standard.

In the search for a path, every breadcrumb dropped by a major player like DFS is important. Management and boards throughout corporate America thus would do well to study the DFS guidance, and ask themselves: If a regulator came calling, or we had to defend a post-data-breach negligence action in court, how would we answer the sort of questions that DFS plans to ask the banks?

* * *

Please do not hesitate to contact us with any questions.