DORSEY

DORSEY+WHITNEY LLP

New York Department of Financial Services Signals Aggressive Enforcement Stance

State Notifications Deemed to Trigger DFS Reporting of Non-material Breaches

Two successive Consent Orders have demonstrated the seriousness of non-compliance with New York's Department of Financial Services financial regulations. While not surprising given the relatively egregious facts of the two cases, DFS's unprecedented interpretation of the 'other' reporting prong of DFS Part 500.17(a) – any notice to another regulatory authority even if the incident is not material – creates a potential hidden standard for the timing of reporting such incidents.

In March 2021, the New York State Department of Financial Services ("DFS") entered into a consent order with Residential Mortgage Services ("Residential"), a mortgage loan service company based in Maine, which required Residential to pay a $1.5 million penalty for violating DFS's cybersecurity regulation, as well as undertake certain remedial measures.

Residential's cybersecurity event, defined by the regulation as "any act or attempt, successful or unsuccessful, to gain unauthorized access to, disrupt or misuse an Information System", occurred when an employee responded to a phishing email with the false appearance of a signature of a business partner. Although this act compromised the employee's credentials, Residential also required a multi-factor authentication process, which typically acts as a safety net in security protocols. Unfortunately for Residential, the employee then compounded the initial compromise by subsequently successively authenticating four fraudulent multi-factor authentication requests, after business hours, simply by tapping her phone. On the following day, prompted by yet another fraudulent attempted authentication request, the employee notified Residential's IT department of the compromise. In response however, after it determined that the compromise was limited to the employee's email, Residential did not undertake any further investigation, despite the employee's access and use of sensitive personal identifiable financial information of Residential's customers. Further, Residential did not report the compromise to individuals whose personal data was potentially compromised

Related Capabilities

- Banking & Financial Institutions
- Privacy & Social Media
- Financial Services Regulatory

by the hacker's access to the email account.

Months later, Residential Mortgage Services' Chief Information Security Officer ("CISO") certified to DFS that Residential was in compliance with DFS cyber-security regulations. It is not clear whether the CISO was aware of the incident, or conducted any due diligence within Residential before making the certification. As part of a routine audit, DFS discovered certain compliance issues, undertook a more in-depth review of Residential, and ultimately uncovered the incident.

The compliance breakdowns within Residential in connection with the incident were many, presumably leading to the significant penalty to which Residential agreed:

- Inadequate training of employees on standard security protocols;
- Failure to implement an incident response process;
- Failure to investigate the likely compromise of personal financial information;
- Failure to report the likely compromise of personal financial information under state notification statutes;
- Failure to report the incident to NYDFS (which DFS implicitly asserted is required even if the incident was not 'material' under DFS regulations, so long as another supervisory authority was or should have been notified); and
- Failure to undertake appropriate due diligence before certifying compliance with DFS requirements.

Particularly worthy of note is the position by DFS that even if there was no "reasonable likelihood of materially harming any material part of the normal operation(s) of the covered entity" notice to DFS nevertheless was required because notice was required to be given "to any government body, self-regulatory agency or any other supervisory body", specifically via state breach notification laws.

In another Consent Order entered just a few days later involving National Securities Corporation (NSC), DFS imposed a penalty of $3 million, for violations similar to those found in Residential, including improper certification of compliance notwithstanding knowledge of security shortcoming evidenced by breaches, further complicated by NSC's failure even to implement adequate security measures, including full Multi-Factor Authentication (MFA).

As with Residential, DFS asserted that any notifications by NSC that would have been required to state authorities automatically required notifications to DFS, again implying that the materiality standard otherwise required to trigger reporting to DFS is no longer relevant. Particularly noteworthy in the NSC order is the express reference to the 72-hour notification deadline, which DFS seemed to assert was triggered as soon as NSC became aware that state regulatory authorities had to be notified under state breach notification laws, essentially eliminating any requirement of materiality.

The potential consequences of the DFS interpretation could be quite significant for those entities regulated by DFS that experience an incident reportable to any state regulatory authority (which is required by a majority of the state breach notification laws, with varying triggering thresholds), or potentially the FDIC. While virtually no state requires

notification sooner than “reasonably practicable”, and a few states require notification within 30 days (other than Vermont under certain circumstances, which demands 14 days), the interpretation advanced by DFS in the Residential and NSC Consent Orders, if applied in similar circumstances to other DFS-regulated entities experiencing breaches that would not otherwise be characterized as material by DFS, could have the perverse effect of substituting the DFS 72 hour deadline as the *de facto* default standard for all states that require notification to state authorities.[1]

Companies subject to the new DFS regulations or in related industries should pay particular attention to these developments for several reasons. This enforcement was a matter of first impression and demonstrates the potential consequences of overlooking parallel notifications to DFS whenever state regulators are notified, and that incorrect DFS certifications by CISOs will be sanctioned severely. Further, the regulation has served as a model for other regulators who are interested in a more prescriptive approach. Following the enactment of DFS’s regulations, both the U.S. Federal Trade Commission and National Association of Insurance Commissioners have looked to the regulation as model for their own regulations, and that others are likely to follow.

[1] Notice to DFS may be submitted confidentially; under 23 NYCRR 500.18, information provided is subject to exemptions from disclosure under Baking law, insurance law, financial services law, public officers law and other applicable law. Nevertheless, a data controller subject to DFS could find itself in the unenviable position of having to file a protective notice to DFS within 72 hours of discovering a breach that *could be* reportable to *any* state regulatory authority under state law, but before having the opportunity to investigate the incident to assess its full consequences, or perhaps even its ultimate reportability if it is determined that there is no likely risk of harm to the data subject. There are likely to be other significant derivative consequences if such protective notifications are deemed required, that any impacted entity will also have to take into account.