

Client Alert

April 21, 2015

NY Department of Financial Services: Check Your Vendors' Cybersecurity

By Daniel A. Nathan and Kevin J. Matta

According to a recent [report](#) released by the New York Department of Financial Services (NYDFS), the financial industry has a long way to go in overseeing the cybersecurity capabilities of outside vendors who carry out critical banking functions.

The report follows a year of activity on that front. In a May 2014 report, the NYDFS concluded—based on a survey of over 150 banks—that the financial industry's increasing reliance on third-party vendors could create critical cybersecurity risks. Following that report, the NYDFS conducted a second survey of 40 banks concerning how they address cybersecurity with respect to third-party vendors. The second survey resulted in this latest report. As a result of its findings, the NYDFS is considering new regulation that would impact financial institution oversight of third-party vendors.

THE NYDFS REPORT'S FINDINGS REGARDING VENDORS AND CYBERSECURITY

The report on vendors focused on four critical areas:

1. due diligence processes;
2. policies and procedures governing relationships with third-party vendors;
3. protections for safeguarding sensitive data; and
4. protections against loss incurred by third-party failures.

According to the report, almost every institution surveyed conducted risk-based due diligence on vendors, classifying vendors with access to sensitive data as high-risk, and conducting cybersecurity risk assessments on those vendors. In addition, 90 percent of surveyed institutions require vendors to comply with cybersecurity standards. However, fewer than half of the institutions surveyed required on-site due diligence of vendors: only 46 percent required initial on-site due diligence of potential vendors; and even fewer—35 percent—required *periodic* on-site due diligence of even those vendors classified as high-risk.

The report also noted that all surveyed institutions had written vendor-management policies. These policies, however, varied greatly in terms of scope. While 79 percent of surveyed institutions required that vendors maintain information-security requirements, only 36 percent extended that requirement to subcontractors. In addition, 21 percent did not reserve the right to audit their vendors, and 44 percent did not require a warranty of the integrity of the vendor's data or products, leaving them exposed to viruses that could compromise their network's integrity. Most surprisingly, 30 percent of surveyed institutions did not require vendors to notify them in the case of a data breach.

Client Alert

The NYDFS also asked surveyed institutions to describe their methods of safeguarding sensitive data that is sent to, received from, or accessible to vendors. Although 90 percent of surveyed institutions used encryption for data transmitted to or from the vendor, only 38 percent used encryption for data not transferred between the institution and vendor. Further, 70 percent of surveyed institutions used multifactor authentication for at least some vendors to access sensitive information.

The NYDFS also found that only 63 percent of surveyed institutions (78 percent of large institutions) carried cyber insurance, and only 47 percent carried cyber insurance that explicitly covers information-security failures by a vendor. Only half of institutions had vendor contracts that included indemnification clauses.

OTHER REGULATORS' FOCUS ON VENDORS

The NYDFS's report dovetails with recent efforts by other regulators such as the SEC, FINRA, and the CFTC. The [SEC](#) and [FINRA](#) released reports in February that provide guidance to broker-dealers in overseeing outside vendors. The CFTC held a cybersecurity roundtable on March 3 to gather information from industry leaders and regulators that could help in drafting new cybersecurity regulation.

Contact:

Daniel A. Nathan

Washington D.C., (202) 887-1687
New York, (212) 468-8146
dnathan@mofo.com

Kevin J. Matta

(202) 887-6956
kmatta@mofo.com

About Morrison & Foerster:

We are Morrison & Foerster—a global firm of exceptional credentials. Our clients include some of the largest financial institutions, investment banks, Fortune 100, technology and life science companies. We've been included on *The American Lawyer's* A-List for 11 straight years, and *Fortune* named us one of the "100 Best Companies to Work For." Our lawyers are committed to achieving innovative and business-minded results for our clients, while preserving the differences that make us stronger. This is MoFo. Visit us at www.mofo.com.

Because of the generality of this update, the information provided herein may not be applicable in all situations and should not be acted upon without specific legal advice based on particular situations. Prior results do not guarantee a similar outcome.