Insights: Alerts

New York Department of Financial Services Report Identifies Bank Hackers' "Backdoor Entrance," Stresses Vendor Diligence and Contract Negotiation

April 10, 2015

Written by **Gary R. Bronstein, Christina M. Gattuso** and **Edward G. Olifer**

On April 9, 2015, the New York Department of Financial Services (the "DFS") issued a report titled "Update on Cyber Security in the Banking Sector: Third Party Service Providers" (the "DFS Report"), highlighting significant potential cyber security vulnerabilities with banks' third-party vendors. In the press release announcing the DFS Report, Superintendent Lawsky reiterated his cautionary cyber guidance, "[a] bank's cyber security is often only as good as the cyber security of its vendors. Unfortunately, those third-party firms can provide a backdoor entrance to hackers who are seeking to steal sensitive bank customer data." The DFS Report, which discussed the possibility of new cyber security regulations for banks relating to third-party vendor management, serves as a warning for banks that vendor relationships will receive heightened scrutiny by the DFS, and to evaluate their vendor relationships and renegotiate vendor contracts.

Banks rely on third-party vendors in virtually all business lines of their institution, ranging from data processing to mortgage settlement solutions, and depend on such vendors to maintain the same or similar levels of responsibility and care relating to customer information as does the bank. Many third-party vendors access and use personal customer information on a daily basis, creating increased data breach exposure to the contracting bank. The DFS Report, which surveyed 40 foreign and domestic DFS-regulated financial institutions of all sizes, highlighted the following findings:

- Nearly 1 in 3 banks surveyed do not require their third-party vendors to notify them in the event of an information security breach or other cyber security breach.
- Fewer than half of the banks surveyed conduct on-site assessments of their third-party vendors.
- Approximately 1 in 5 banks surveyed do not require third-party vendors to represent that they have established minimum information security requirements, and only one-third of the banks require those information security requirements to be extended to subcontractors of the third-party vendors.
- Nearly half of the banks surveyed do not require a warranty of the integrity of the third-party vendor's data or products (e.g., that the data and products are free of viruses).
- Nearly 2 in 3 banks surveyed carry insurance that would cover cyber security incidents. However, only 47% of the banks surveyed reported having cyber insurance policies that explicitly cover information security failures by a third-party vendor, and only half of the banking organizations surveyed require indemnification clauses in their agreements with third-party vendors.

The DFS is sending a clear message to regulated financial institutions that third-party vendor relationships will be an area of increased scrutiny, and those institutions should respond accordingly by performing proper diligence on their vendors and by reviewing the contracts that govern their relationships. Specifically, banks should consider drafting and negotiating the representations and warranties of vendor contracts to contain specific requirements, at a minimum requiring vendors to comply with general information security standards. Based on the bank's assessment of the vendor's risk level, the bank should also consider negotiating the agreements to include data encryption, access controls, data classification, indemnification, and business continuity and disaster recovery plans. Finally, as it relates to cyber insurance, and as we discussed in a previous legal alert, it is imperative that financial institutions review their cyber security insurance policies carefully to ensure that the scope of their policies appropriately cover the bank's cyber risk.

If you need assistance in reviewing or negotiating third-party vendor contracts or cyber insurance policies, please contact any member of Kilpatrick Townsend's Financial Institutions team.

To download a printer-friendly copy of this alert, click here.

Related People

Gary R. Bronstein

t 202.508.5893

gbronstein@ktslaw.com

Christina M. Gattuso

t 202.508.5884

cgattuso@ktslaw.com

Edward G. Olifer

t 202.508.5852

eolifer@ktslaw.com