WILMERHALE

Report Highlights Bank Vendor Cybersecurity Vulnerabilities

APRIL 13, 2015

On April 9, the New York State Department of Financial Services (NYDFS) released a report on bank vendor cybersecurity that highlights the risk that hackers will use third-party service providers to gain access to bank data. The report, entitled *Update on Cyber Security in the Banking Sector: Third Party Service Providers*,[1] is based on responses to an October 2014 NYDFS information request to 40 regulated financial institutions and is significant for at least two reasons. First, the report may be useful for benchmarking a company's cybersecurity practices against similarly situated businesses. Second, the report may become the basis for NYDFS to promulgate new cyber regulations for third-party vendors-particularly with regard to the representations and warranties banks receive about cyber protections-in the coming weeks.[2]

The October 2014 NYDFS request had asked that institutions describe steps taken to comply with the third-party stakeholder provisions of the *Framework for Improving Critical Infrastructure Cybersecurity* issued by the US Commerce Department's National Institute of Standards and Technology (NIST).[3] Third-party providers include check and payment processing firms, trading and settlement operations firms, data processing firms and many others, which often have access to banking institutions' information technology systems.

Key findings from the report include:

- Thirty percent of the institutions surveyed do not require third-party vendors to notify them in the event of a data breach;
- Ninety percent have information security requirements for third-party vendors, but fewer than half require any on-site assessments of vendors;
- Twenty-one percent do not require third-party vendors to represent that they have established minimum information security requirements;
- Nearly half do not require a warranty of the integrity of the third-party vendor's data or products;
- Ninety percent utilize encryption for data transmitted to or from third parties, but just over one-third use encryption for data that is not being transmitted or is "at rest"; and
- Sixty-three percent carry insurance that would cover cybersecurity incidents, but fewer than half have insurance that covers information security failures by a third-party vendor.

Attorney Advertising

This new report is an update to a May 2014 NYDFS report on cybersecurity in the banking sector.[4] The report may provide additional impetus for NYDFS to issue new cybersecurity regulations for third-party vendors to the banking industry. It also reflects the growing focus of a variety of state and federal regulatory authorities-including the Securities and Exchange Commission (SEC), the Commodity Futures Trading Commission (CFTC), the Federal Financial Institutions Examination Council (FFIEC) member agencies, and the Financial Industry Regulatory Authority (FINRA)-on scrutinizing the cybersecurity practices of the financial services industry.[5] Regulators have increasingly viewed information security as a critical component of both investor protection and broader market integrity.

---

[1] New York State Department of Financial Services, *Update on Cyber Security in the Banking Sector: Third Party Service Providers*, April 2015, *available at* www.dfs.ny.gov/reportpub/dfs_rpt_tpvendor_042015.pdf.

[2] New York State Department of Financial Services, Press Release, *NYDFS Report Shows Need to Tighten Cyber Security at Banks' Third Party Vendors*, April 9, 2015, *available at* dfs.ny.gov/about/press2015/pr1504091.htm.

[3] National Institute of Standards and Technology, *Framework for Improving Critical Infrastructure Cybersecurity*, February 12, 2014, *available at* www.nist.gov/cyberframework/upload/cybersecurity-framework-021214-final.pdf.

[4] New York State Department of Financial Services, *Report on Cyber Security in the Banking Sector*, May 2014, *available at* www.dfs.ny.gov/about/press2014/pr140505_cyber_security.pdf. NYDFS issued a similar report on the insurance sector. *See* New York State Department of Financial Services, *Report on Cyber Security in the Insurance Sector*, February 2015, *available at* www.dfs.ny.gov/reportpub/dfs_cyber_insurance_report_022015.pdf.

[5] *See* Jonathan G. Cedarbaum, Yoon-Young Lee, Matthew Chambers and Benjamin A. Powell, "The SEC and FINRA Increase Scrutiny of Regulated Firms' Cybersecurity," *The Investment Lawyer*, April 2015, Volume 22, Number 4, pages 26-28; Daniel F. Schubert, Jonathan G. Cedarbaum and Leah Schloss, "The SEC's Two Primary Theories in Cybersecurity Enforcement Actions," *The Cybersecurity Law Report*, April 8, 2015, Volume 1, Number 1; Jonathan G. Cedarbaum, Yoon-Young Lee, Benjamin A. Powell and Matthew A. Chambers, "SEC and FINRA Release Cybersecurity Sweep Reports, Promise Increased Scrutiny of Regulated Firms," *WilmerHale Client Alert*, February 5, 2015, *available at* www.wilmerhale.com/pages/publicationsandnewsdetail.aspx?NewsPubId=17179876235; US Commodity Futures Trading Commission, *CFTC Staff to Hold Roundtable on Cybersecurity and System Safeguards Testing*, March 15, 2015, *available at* www.cftc.gov/PressRoom/Events/opaevent_cftcstaff031815.

Authors

Benjamin A. Powell

PARTNER

Co-Chair, Cybersecurity and Privacy Practice

benjamin.powell@wilmerhale.com

+1 202 663 6770

Jason C. Chipman

PARTNER

jason.chipman@wilmerhale.com

+1 202 663 6195

Marik A. String

SPECIAL COUNSEL

marik.string@wilmerhale.com

+1 202 663 6732

Wilmer Cutler Pickering Hale and Dorr LLP is a Delaware limited liability partnership. WilmerHale principal law offices: 60 State Street, Boston, Massachusetts 02109, +1 617 526 6000; 2100 Pennsylvania Avenue, NW, Washington, DC 20037, +1 202 663 6000. Our United Kingdom office is operated under a separate Delaware limited liability partnership of solicitors and registered foreign lawyers authorized and regulated by the Solicitors Regulation Authority (SRA No. 287488). Our professional rules can be found at www.sra.org.uk/solicitors/code-of-conduct.page. A list of partners and their professional qualifications is available for inspection at our UK office. In Beijing, we are registered to operate as a Foreign Law Firm Representative Office. This material is for general informational purposes only and does not represent our advice as to any particular set of facts; nor does it represent any undertaking to keep recipients advised of all legal developments. Prior results do not guarantee a similar outcome. © 2004-2024 Wilmer Cutler Pickering Hale and Dorr LLP