PHILLIPS LYTLE LLP CLIENT ALERT
DATA SECURITY & PRIVACY
JANUARY 2018

Additional FAQs Answered by the DFS Concerning the DFS Cybersecurity Regulation

On December 12, 2017, the New York Department of Financial Services ("DFS" or "Department") issued four more answers to frequently asked questions about the DFS Cybersecurity Regulation ("Regulation"). These four are the latest in a series of twenty-six FAQs which, given the young and continually developing nature of cybersecurity law, provide important guidance on the practical impact the Regulation will have on businesses and individuals alike.

The Regulation went into effect March 1, 2017, and introduced a number of compliance milestones. It applies to those operating or required to operate under New York insurance, finance and banking laws ("Covered Entities"), but the Regulation has widespread effect beyond the Covered Entities themselves.

The Regulation requires Covered Entities to perform risk assessments and maintain a cybersecurity program based upon those assessments. Covered Entities were to have a number of cybersecurity and IT policies and procedures in place by August 28, 2017.

On or before February 15, 2018, Covered Entities must certify to the DFS Superintendent compliance thus far with the Regulation. Covered Entities should submit the certification after their legal advisors have evaluated the applicability of the Regulation and the extent to which the entity has complied with it. Going forward, the Regulation requires ongoing cybersecurity activities and other IT controls to be in place by March 1, 2018, and additional and different IT controls in place by September 3, 2018. By March 1, 2019, Covered Entities must establish a comprehensive plan to review Third Party Service Providers who handle Nonpublic Information for the Covered Entity. The complete Regulation can be found at: **http://www.dfs.ny.gov/legal/regulations/adoptions/dfsrf500txt.pdf**.

The DFS' Answers to the Four New FAQs:

1. **Assuming there is no continuous monitoring under 23 NYCRR Section 500.05, does the Department require that a Covered Entity complete a Penetration Test and vulnerability assessments by March 1, 2018?**

   The Regulation requires Covered Entities to have a plan in place that provides for Penetration Testing to be done as appropriate to address the risks of the Covered Entity. Such plan must encompass Penetration Testing at least annually and bi-annual vulnerability assessments, but the first annual Penetration Testing and first vulnerability assessment need not have been concluded before March 1, 2018, under Section 500.05. The Department expects all institutions with no continuous monitoring to complete robust Penetration Testing and vulnerability assessment in a timely manner as they are a crucial component of a cybersecurity program.

2. **If Covered Entity A utilizes Covered Entity B (not related to Covered Entity A) as a Third Party Service Provider, and Covered Entity B provides Covered Entity A with evidence of its Certification of Compliance with NYSDFS Cybersecurity Regulations, could that be considered adequate due diligence under the due diligence process required by Section 500.11(a)(3)?**

No. The Department emphasizes the importance of a thorough due diligence process in evaluating the cybersecurity practices of a Third Party Service Provider. Solely relying on the Certification of Compliance will not be adequate due diligence. Covered Entities must assess the risks each Third Party Service Provider poses to their data and systems and effectively address those risks. The Department has provided a two-year transitional period to address these risks and expects Covered Entities to have completed a thorough due diligence process on all Third Party Service Providers by March 1, 2019.

3. **Does a Covered Entity need to amend its Notice of Exemption in the event of changes after the initial submission (e.g., name changes or changes to the applicable exemption(s))?**

   If there are changes, the Covered Entity should submit a new Notice of Exemption, which would not be considered an amendment to the original submission. For example, if a Covered Entity originally submitted a Notice of Exemption stating that it qualified for exemptions under Sections 500.19(b) and 500.19(a)(1), but it now only qualifies for a Section 500.19(a)(1) exemption, then the Covered Entity must submit a new Notice of Exemption with the correct information.

   The Department also emphasizes that Notices of Exemption should be filed electronically via the DFS Web Portal http://www.dfs.ny.gov/about/cybersecurity.htm. The Covered Entity should utilize the account that they used to file the original Notice of Exemption or create a new account if an individual filing was previously not made. Filings made through the DFS Web Portal are preferred to alternative filing mechanisms because the DFS Web Portal provides a secure reporting tool to facilitate compliance with the filing requirements of 23 NYCRR Part 500.

4. **Should a Covered Entity send supporting documentation along with the Certification of Compliance?**

   The Covered Entity must submit the compliance certification to the Department and is not required to submit explanatory or additional materials with the certification. The certification is intended as a stand-alone document required by the [R]egulation. The Department also expects that the Covered Entity maintain the documents and records necessary that support the certification, should the Department request such information in the future. Likewise, under 23 NYCRR Section 500.17, to the extent a Covered Entity has identified areas, systems, or processes that require material improvement, updating or redesign, the Covered Entity must document such efforts and maintain such schedules and documentation for inspection during the examination process or as otherwise requested by the Department.

The following web address has the complete list of all FAQs issued by the DFS concerning the Regulation: http://www.dfs.ny.gov/about/cybersecurity_faqs.htm.

There are a lot of moving parts with the DFS Cybersecurity Regulation. To determine where to start, contact Phillips Lytle's Data Security & Privacy Practice Team. The team has first-hand experience in assisting Covered Entities and Third Party Providers in responding to the requirements imposed by the Regulation. We have helped evaluate practices and reviewed and enhanced cybersecurity and incident response policies of both Covered Entities and Third Party Service Providers.

Phillips Lytle is uniquely situated to provide legal advice and services in this area because its Data Security & Privacy Practice Team is comprised of former technology

business owners who have hands-on experience dealing with issues and concerns related to cybersecurity matters – from data breach prevention practices to on-the-ground breach response, and then interfacing with the government and responding to litigation in connection with any data breach. The firm also has a long history of being a premier financial services law firm, a reputation built on decades of successful representation of major commercial, savings and foreign banks, trust companies, finance companies, credit unions, and various other types of financial institutions and insurance companies.

Even if you are currently working with consultants to develop a cybersecurity program, the policies and procedures should be reviewed by legal counsel to ensure compliance with the DFS Cybersecurity Regulation and other regulations and laws to help avoid inquiries or possible enforcement actions.

Additional Assistance

For questions about the applicability of and compliance with the Regulation, please contact Jennifer A. Beckage at (716) 847-7093, jbeckage@phillipslytle.com, or any member of the firm's Data Security & Privacy Practice Team. ■

PHILLIPS LYTLE LLP CLIENT ALERT

DATA SECURITY & PRIVACY

JANUARY 2018

Data Security & Privacy Attorneys

Lauren Adornetto (716) 847-7013 ladornetto@phillipslytle.com
Jennifer A. Beckage (716) 847-7093, (212) 759-4888 ext. 7093, (202) 617-2700 ext. 7093 jbeckage@phillipslytle.com
James E.B. Bobseine (716) 504-5794 jbobseine@phillipslytle.com
Edward S. Bloomberg (716) 847-7096, (212) 759-4888 ext. 7096 ebloomberg@phillipslytle.com
Alan J. Bozer (716) 504-5700, (212) 759-4888 ext. 5700 abozer@phillipslytle.com
Mary E. Burgess (518) 618-1221 mburgess@phillipslytle.com
Anna Mercado Clark (212) 508-0466 aclark@phillipslytle.com
Jeffrey D. Coren (716) 847-7024 jcoren@phillipslytle.com
Chad W. Flansburg (585) 238-2009 cflansburg@phillipslytle.com
F. Kenneth Graham (716) 847-7049 fkgraham@phillipslytle.com
Asaf Hahami (212) 508-0432 ahahami@phillipslytle.com
Luke B. Kalamas (585) 238-2035 lkalamas@phillipslytle.com
Timothy P. Kucinski (716) 847-7056 tkucinski@phillipslytle.com
Brendan S. Lillis (716) 847-7058 blillis@phillipslytle.com
Richard J. Marinaccio (716) 504-5760 rmarinaccio@phillipslytle.com
Mark J. Moretti (585) 238-2004, (212) 508-0404 mmoretti@phillipslytle.com
Ian K. Portnoy (202) 617-2713 iportnoy@phillipslytle.com
William V. Rossi (716) 847-7022 wrossi@phillipslytle.com
John G. Schmidt Jr. (716) 847-7095, (212) 508-0426 jschmidt@phillipslytle.com
James Kevin Wholey (202) 617-2714 jwholey@phillipslytle.com

Phillips Lytle LLP

Albany Omni Plaza 30 South Pearl Street Albany, NY 12207-3425 (518) 472-1224
Buffalo One Canalside 125 Main Street Buffalo, NY 14203-2887 (716) 847-8400
Chautauqua 201 West Third Street Suite 205 Jamestown, NY 14701-4907 (716) 664-3906
Garden City 1205 Franklin Avenue Plaza Suite 390 Garden City, NY 11530-1629 (516) 742-5201
New York City 340 Madison Ave 17th Floor New York, NY 10173-1922 (212) 759-4888
Rochester 28 East Main Street Suite 1400 Rochester, NY 14614-1935 (585) 238-2000
Washington, DC 800 17th Street NW Suite 450 Washington, DC 20006-3962 (202) 617-2700
Canada The Communitech Hub 151 Charles Street West Suite 100 The Tannery Kitchener, Ontario N2G 1H6 Canada (519) 570-4800