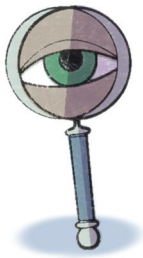
PHILLIPS LYTLE LLP CLIENT ALERT
DATA SECURITY & PRIVACY
MARCH 2017



# *NYS Department of Financial Services Cybersecurity Regulation: Ripple Effects Beyond the Banking, Financial and Insurance Industries*

**On March 1, 2017, the New York State Department of Financial Services ("DFS") Cybersecurity Regulation went into effect. 23 N.Y.C.R.R. 500 (the "Cybersecurity Regulation"). Some portions of the Cybersecurity Regulation must be complied with by the end of the summer – August 28.**

The Cybersecurity Regulation is directed to those operating under, or required to operate under, New York Banking Law, Insurance Law and/or Financial Services Law ("Covered Entities"), but it has ripple effects beyond these businesses.

The goal of the Cybersecurity Regulation is to protect the financial services industry from cybersecurity threats by requiring Covered Entities to have cybersecurity programs in place to protect their information technology systems and various confidential and sensitive information. Specifically, the Cybersecurity Regulation requires a Covered Entity to assess its risk profile and develop certain standards and practices to protect its information technology systems, as well as the non-public information those entities may have, such as business-sensitive information, personal identifiable information of customers and consumers and others, and health condition and services information (collectively, "NPI").

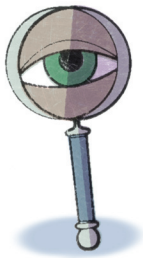
The Cybersecurity Regulation also requires Covered Entities to have a cybersecurity program in place to address the particular risks applicable to a Covered Entity, engage in various risk assessment activities, and evaluate third party providers, which are those who maintain, process or otherwise permit access to NPI through its services to Covered Entities ("Third Party Providers").
By February 15, 2018, Covered Entities will have to certify compliance with the Cybersecurity Regulation, although due to its depth, some portions of the Regulation have grace periods in which Covered Entities have to comply.

**Ripple Effects of the Cybersecurity Regulation**

Although only Covered Entities are subject to the Cybersecurity Regulation, the regulation requires Covered Entities to make inquiries of their Third Party Providers' information security practices. Thus, just as Covered Entities are taking steps to comply with the Cybersecurity Regulation, Third Party Providers with access to a Covered Entity's NPI are preparing themselves for the inquiries that Covered Entities will make to them about their own cybersecurity and information security practices.

**Three Things to Consider Doing Now**

1. **Confirm you have or are in the process of developing a cybersecurity program.** Covered Entities should review existing policies and enhance such policies, if needed, or create new program materials. This review (and potential enhancement) process requires collaboration by a Covered Entity's and Third Party Provider's information technology, management and legal professionals. Covered Entities need to identify a Chief Information Security Officer to oversee the cybersecurity program, which requires



training, risk assessments, multi-factor authentication, data encryption, and other data security measures and practices. A cybersecurity program also requires an incident response plan that the Covered Entity will use to respond to a cybersecurity event. Such response includes notification to the DFS within 72 hours of determination that a cybersecurity event has occurred requiring notice under the law, or has a reasonable likelihood of materially harming any material part of the normal operations. Much of the cybersecurity program must be in effect by August 28, 2017.

2. **Put cybersecurity topics on the board of directors' or other governing body's agenda.** The Cybersecurity Regulation is requiring board and management involvement in discussions about cybersecurity and cybersecurity risk assessments. Leadership should therefore assist in the cybersecurity program development and understand their role in the program.

3. **Review vendor relationships and vendor management programs.** In response to the Cybersecurity Regulation, Covered Entities will be making inquiries of their Third Party Providers' security practices. Covered Entities should discuss the approach and method in doing so with information technology and legal departments. Third Party Providers should consider how they will respond to these inquiries by looking at their own cybersecurity and information security policies and practices.

There are a lot of moving parts with the 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 Cybersecurity Regulation. We have helped evaluate practices and reviewed and enhanced cybersecurity and incident response policies of both Covered Entities and Third Party 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 Cybersecurity Regulation and other regulations and laws to help avoid inquiries or possible enforcement actions.

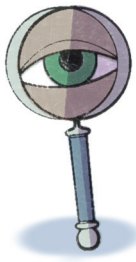
**Additional Assistance**

*For questions regarding the DFS Cybersecurity Regulation, or any other data security and privacy matters, please contact Jennifer A. Beckage at (716) 847-7093, jbeckage@phillipslytle.com, F. Kenneth Graham at (716) 847-7049, fkgraham@phillipslytle.com, or any of the attorneys on our Data Security & Privacy Practice Team.* ■

# PHILLIPS LYTLE LLP CLIENT ALERT

## DATA SECURITY & PRIVACY

MARCH 2017



## Data Security & Privacy Attorneys


Jennifer A. Beckage (716) 847-7093, (212) 759-4888 ext. 7093, (585) 238-2000 ext. 7093 jbeckage@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) 472-1224 ext. 1231 mburgess@phillipslytle.com
Anna Mercado Clark (212) 508-0466 aclark@phillipslytle.com
Jeffrey D. Coren (716) 847-7024 jcoren@phillipslytle.com
John M. Falk (202) 617-2723 jfalk@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
Patrick M. Hanley, Jr. (716) 847- 8306 phanleyjr@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
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 152 The Tannery Kitchener, Ontario N2G 1H6 Canada (519) 570-4800