pennsylvania
DEPARTMENT OF BANKING
AND SECURITIES

September 8, 2015

To: ALL PENNSYLVANIA STATE-CHARTERED, LICENSED, AND REGISTERED FINANCIAL SERVICES INSTITUTIONS AND COMPANIES

As cybersecurity threats to businesses and institutions continue and increase, the need for the financial services industry to implement effective cybersecurity measures is more pressing than ever. The common goals of industry and regulators must be to reduce vulnerability; prevent and defend against cyberattacks; and minimize damage to consumers and investors after a cyberattack. The Department of Banking and Securities (Department) is promoting cybersecurity awareness and working to help those whom it regulates navigate cybersecurity challenges. Furthermore, the Department is working to identify cybersecurity trends and developments, and it will present these and other cybersecurity-related issues in the Department's quarterly e-newsletter (you can subscribe here: www.surveymonkey.com/r/?sm=U9oIup8eTvKnuvQk5tp28A%3d%3d).

Commonwealth Cybersecurity Efforts

The Department's efforts are an extension of the Commonwealth of Pennsylvania's approach to protecting the security of its digital resources. The Commonwealth strives to prevent and defend against cyberattacks, reduce vulnerability, minimize damage and recovery times, and promote awareness and education. The Commonwealth offers online resources aimed at increasing the public's awareness of the importance of cybersecurity. The online resources are available at www.cybersecurity.state.pa.us.

Suggested Cybersecurity Tactics for Regulated Entities

The Department strongly encourages all of its regulated entities to develop cybersecurity attack prevention and mitigation plans. Businesses and institutions should identify and assess their own cybersecurity risks, and evaluate means and methods for protecting their networks and data. Businesses and institutions should run regular vulnerability assessments and penetration tests of their networks, use encryption for customer and investor data, keep their operating systems up-to-date, and employ and frequently update anti-virus and anti-malware software. In addition to implementing technical measures, businesses and institutions should recognize that the weakest links in a secure system may be an employee, a third-party vendor, or even a customer. Businesses and institutions should train and evaluate their staff and vendors, and educate their customers, to

ensure that they understand the risks presented by cybersecurity threats. All parties should be vigilant in protecting their data, and the networks and data of their counterparties.

Available Cybersecurity Resources

The Department believes that it is vital that businesses and institutions implement continuity plans to mitigate disruption and damages should a cyberattack occur.

On June 30, 2015, the Federal Financial Institutions Examination Council (FFIEC) issued a self-assessment tool to guide financial institutions in evaluating their cybersecurity risks. The FFIEC is a formal interagency body comprised of representatives of the Board of Governors of the Federal Reserve System, the Federal Deposit Insurance Corporation, the National Credit Union Administration, the Office of the Comptroller of the Currency, the Consumer Financial Protection Bureau, and a state financial services regulator. A copy of the assessment tool is available at www.ffiec.gov/cybersecurity.htm.

Additionally, in April 2014, the U.S. Securities and Exchange Commission (SEC), Office of Compliance Inspections and Examinations (OCIE) issued a cybersecurity risk alert and conducted a "sweep" of broker-dealers and investment advisers. In this sweep, the OCIE reviewed cybersecurity preparedness. The Department recommends that Pennsylvania-registered broker-dealers and investment advisers utilize the OCIE's sample request for information and documents from this "sweep" to assess their firm's level of cybersecurity preparedness. The sample request is available at http://www.sec.gov/ocie/announcement/Cybersecurity-Risk-Alert--Appendix---4.15.14.pdf. In addition, the SEC's Division of Investment Management released guidance emphasizing best practices and warning compliance officers of the potential securities law violations that could occur due to failure to address deficiencies in cybersecurity programs. A copy is available at www.sec.gov/investment/im-guidance-2015-02.pdf. The Department urges the management of its regulated businesses and institutions to employ these tools in their cybersecurity strategies.

Today, the Department launched a resource page located on its website aimed at offering our regulated entities a variety of resources, such as the ones mentioned in this letter, that may be useful in adopting a more vigilant attitude toward cybersecurity. For more information, visit the Department's website at www.dobs.pa.gov.

Sincerely,

Redacted

/s/

Robin L. Wiessmann
Secretary of Banking and Securities