SCHWARTZ & BALLEN LLP
1990 M STREET, N.W. • SUITE 500
WASHINGTON, DC 20036-3465

WWW.SCHWARTZANDBALLEN.COM

TELEPHONE
(202) 776-0700

FACSIMILE
(202) 776-0700

M E M O R A N D U M

October 5, 2016

To Our Clients and Friends

Re: NY DFS Proposes Cybersecurity Requirements for Financial Services Companies

The New York Department of Financial Services (DFS) has proposed a regulation that requires banks, insurance companies and other financial institutions regulated by the DFS to establish and maintain a cybersecurity program designed to protect consumers and ensure the safety and soundness of New York's financial services industry. Public comments on the proposed regulation may be submitted until November 12th. DFS proposes that the regulations become effective January 1, 2017.

The proposed regulation requires covered institutions to maintain a cybersecurity program designed to ensure the confidentiality, integrity and availability of the institution's electronic information systems. The program must identify internal and external cyber risks as follows:

- Identify the nonpublic information stored on the system, the sensitivity of the information and how and by whom it may be accessed
- Use defensive infrastructure and policies and procedures to protect nonpublic information and the information systems from unauthorized access or malicious acts
- Detect cybersecurity events (acts or attempts to gain unauthorized access to nonpublic information and the information systems)
- Respond to cybersecurity events to mitigate any negative effects
- Restore normal operations after a cybersecurity event

A written cybersecurity policy must be reviewed by the institution's board of directors, and approved by a senior officer. The institution must also designate a qualified individual to serve as a Chief Information Security Officer (CISO) who will be responsible for overseeing and implementing the cybersecurity program and enforcing the cybersecurity policy. This requirement can be met by using a third party service provider. Other requirements include conducting penetration testing and risk assessments, maintaining audit trail system, limiting access privileges, and establishing minimum cybersecurity practices required to be met by third parties who have access to the institution's information systems and nonpublic information.

All nonpublic information held or transmitted by the institution must be encrypted. If encryption is currently infeasible, other compensating controls may be used for a specified period of time. Institutions are required to notify the Superintendent of any cybersecurity event. Institutions are required annually to submit a Certificate of Compliance commencing January 15, 2018.

A copy of the DFS's Proposed Cybersecurity Requirements for Financial Services Companies is available on our website at http://www.schwartzandballen.com/news.html

If you have any questions, please call Gilbert Schwartz, Robert Ballen, Tom Fox, or Heidi Wicker at (202) 776-0700.