COMMONWEALTH OF MASSACHUSETTS
Office of Consumer Affairs and Business Regulation
DIVISION OF BANKS
1000 Washington Street, 10TH Floor, Boston, MA 02118-6200
(617) 956-1500 · Fax (617) 956-1599 · TDD (617) 956-1577
www.Mass.Gov/DOB

CHARLES D. BAKER
GOVERNOR

KARYN E. POLITO
LIEUTENANT GOVERNOR

JAY ASH
SECRETARY OF HOUSING AND ECONOMIC DEVELOPMENT

JOHN C. CHAPMAN
UNDERSECRETARY

TERENCE A. MCGINNIS
COMMISSIONER

May 18, 2017

Guidance on Cyber-Threats and Attacks for Non-Depository Institutions

To the Chief Executive Officer of the Institution Addressed:

As you know from news reports, a global ransomware campaign is affecting over 100,000 (plus) computers in more than 155 countries. The ransomware exploits a vulnerability in Microsoft Windows, **particularly the Windows XP operating system**. The issue primarily relates to "computer hygiene," that is, keeping your computers up-to-date and patched. Specific information about **patching** for this ransomware exploit (Microsoft patch for the MS-17-010 SMB vulnerability dated March 14, 2017) is on the US-CERT website: https://www.us-cert.gov/ncas/alerts/TA17-132A.

Recommended Resources:

- The Division issued an industry letter on cybersecurity self-assessments and the FFIEC's cyber security assessment tool to all licensees on November 30, 2015, which is available on our website: http://www.mass.gov/ocabr/docs/dob/industry-letter-11302015.pdf.
- The Division's information security examination work-program for non-depositories is also available on our website: http://www.mass.gov/ocabr/docs/dob/it-work-program.pdf.
- Additional information on cyber-security and ransomware can also be found on the FBI's website: https://www.fbi.gov/investigate/cyber.

Prevention is the most effective defense against ransomware, and it is critical to take precautionary measures for protection. Most important:

- Never open attachments or follow links included in unsolicited e-mails.
- Back-up your data, particularly sensitive or proprietary data, in a separate secure location.
- Keep your anti-virus software up to date.

Massachusetts General Laws chapter 93H, and Massachusetts regulation 201 CMR 17.00 et seq. establishes guidelines to safeguard the personal information of residents of the Commonwealth. The statute requires any person holding personal information about a resident of the Commonwealth to maintain a Written Information Security Program (WISP) and to report any known breach of security to the Attorney General and the Undersecretary of Consumer Affairs

and Business Regulation as soon as practicable and without unreasonable delay. It is the Division's expectation that a Licensee impacted by the ransomware will also report this to the Division as a data breach / significant event. If you have any questions about the Division's expectations regarding cybersecurity, please contact Chief Director Danielle Sherbertes at danielle.sherbertes@state.ma.us or 617-956-1553. To report a data breach or discuss sensitive information, please use secure email when contacting Ms. Sherbertes.

Sincerely,

Terence A. McGinnis
Commissioner of Banks
Massachusetts Division of Banks