COMMONWEALTH OF MASSACHUSETTS
Office of Consumer Affairs and Business Regulation
DIVISION OF BANKS
1000 Washington Street, 10TH Floor, Boston, MA 02118-6400
(617) 956-1500 · Fax (617) 956-1599 · TDD (617) 956-1577
www.Mass.Gov/DOB

CHARLES D. BAKER
GOVERNOR

KARYN E. POLITO
LIEUTENANT GOVERNOR

MIKE KENNEALY
SECRETARY OF HOUSING AND ECONOMIC DEVELOPMENT

EDWARD A. PALLESCHI
UNDERSECRETARY

MARY L. GALLAGHER
COMMISSIONER

April 16, 2020

Massachusetts Division of Banks - Industry Notice:
Increased Cyber Activity During Times of Crisis

During times of crisis, cybercriminals and nation-state actors often look to exploit financial institutions and their customers for political or financial gain or both. Below are some cybersecurity tips that you and your staff **may** use to improve your institution's readiness to combat these threats.

Evaluating cybersecurity readiness can be accomplished by utilizing the PPT model that considers: **People**, **Processes**, and **Technology**.

I. People

- Continue to remind your employees that human error as a result of social engineering schemes, rather than the use of sophisticated technologies, remains the top method of cyber attacks. Emphasize key training lessons and regularly remind employees to stay vigilant.
- Let remote workers know when online/virtual meeting platform links are expected and legitimate. If something does not look right, employees should contact the meeting organizer.
- Remind customers and staff that while some financial institutions may have adjusted hours or services in compliance with local, state, and Centers for Disease Control (CDC) guidance, customers continue to have access to the various services offered by financial institutions and licensees. Furthermore, consumers should be reminded that banking deposits and shares remain safe and insured by the FDIC or NCUA. In some circumstances, deposits are further insured in full by the Depositors Insurance Fund or the Massachusetts Share Insurance Corporation.
- Inform customers and employees that your institution's brand might be used in a fraudulent email alert to customers. These fraudulent alerts may state that the customer's accounts has been suspended. The victim may receive a link that looks like your institution's login screen, encouraging them to log in with their username and password.

- Communicate to customers that dis-information campaigns are already underway and urge them to rely on government and well-established news sources for credible information. Be wary of unreliable websites and random social media posts.
- Inform customers and staff to expect scams related to COVID-19. They should be extra cautious about clicking links and providing sensitive or confidential information. Be extra vigilant to follow secure cyber practices.
- Remind your staff and customers to be cautious of communications with the following or similar subjects:
    - Obtain U.S. government funding related to Coronavirus relief.
    - Check for an updated Coronavirus map in your city.
    - Coronavirus infection warnings from local school districts/governmental entities.
    - Keep your children safe from Coronavirus.
    - Raise funds for Coronavirus victims – If you wish to donate money, avoid responding directly to email solicitations.

II. Processes

- Anticipate Distributed Denial of Service (DDoS) attacks that are often distractions to carry out wire fraud.
- Exercise special caution when honoring customer requests for special/alternative handling of transactions. Requests for wire transfers or ACH account changes should be verified by contacting the business contact on a known phone number, asking a fellow staff member to review the requests, or calling the customer directly.
- Be vigilant against Business Email Compromise (BEC). Bank policies should be in place to require secondary confirmation of major wires or transactions in-person or by telephone.
- Be on the lookout for Corporate Account Takeover (CATO) attempts. The attacks are usually in the form of emails that ask for your credentials.

III. Technology

- As you utilize alternative systems/equipment in conjunction with your Business Continuity Plan, remember to follow your standard security protocol.
- Maintain secure connections for remote workers.
    - Can you assist staff in securing their home Wi-Fi? Remind staff that public Wi-Fi networks should be avoided.
    - If use of personally owned devices for remote access is allowed, help staff bring these devices up to date with the latest security patches and end-point protection.
    - Implement multi-factor authentication for high-risk remote access.
    - Discuss with your managed service provider (MSP) how they are maintaining security to your network with any of their remote workers.

Other Important Considerations

- **Cyber Insurance**
    - Although optional, if used as a component of your risk management program, know what your policy(s) covers (e.g. forensic remediation, notification expenses, equipment replacement, reputation repair, etc.).
    - Understand your policy's exclusions and how the insurer defines "minimum security standards."
    - Confirm that required security protocols are in place including when employees are working from home.

If you should have any questions, please contact Director of Cybersecurity/IT/FinTech Holly Chase at 617-367-4409 or Holly.Chase@mass.gov.