THE COMMONWEALTH OF MASSACHUSETTS
DIVISION OF BANKS
1000 Washington Street, 10th Floor, Boston, Massachusetts 02118

**CHARLES D. BAKER**
GOVERNOR

**KARYN E. POLITO**
LIEUTENANT GOVERNOR

**JOHN C. CHAPMAN**
UNDERSECRETARY

**DAVID J. COTNEY**
COMMISSIONER OF BANKS

February 26, 2016

To the Financial Institution Addressed:

While the financial services industry in Massachusetts is positioned to thrive in 2016, unfortunately so are criminals intent on targeting institutions and consumers throughout all areas of the Commonwealth. The Division of Banks is issuing this letter to raise awareness about a concerning increase in Automated Teller Machine (ATM) card skimming fraud.

ATM card skimming involves the attachment of electronic devices on or around an ATM to illegally collect data from the magnetic strip of the card, while hidden cameras are also installed to capture the personal identification number (PIN) entered by the customer. Electronic devices used to capture the information vary in design, size, and shape; look similar to legitimate devices; and continue to evolve to avoid detection. In other cases, criminals situate themselves near a compromised ATM and capture card data using a wireless device. A newer method of skimming involves attacks through the use of external devices plugged into the network cables that hijack the ATM's phone or Internet connection. Finally, the stolen account information is encoded onto blank cards which are then used to make withdrawals from customers' accounts. Often the criminals install the device for only a short period of time to avoid detection.

Given the serious harm and inconvenience that results from skimming attacks, the Division encourages institutions to take a fresh look at how you are managing this risk. As such, the Division recommends that financial institutions, at a minimum:

***Include ATM security in your risk assessments.*** Make sure this risk area is captured as you assess the risks facing your institution.

***Monitor your ATMs.*** Be vigilant of any unusual activity. Assess existing controls to prevent and detect skimming, including ATMs located off bank premises such as a convenience or grocery store. Consider implementing enhanced physical security controls such as locks and additional video cameras. Monitor ATM transaction activity for unusual behavior or withdrawal attempts that go beyond normal daily limits.

***Test controls regularly.*** Test the effectiveness of both physical and logical controls periodically to ensure they are functioning as expected.

***Conduct information security awareness and training.*** Include descriptions of various skimming equipment, how frequently employees should check ATMs for skimming devices, and how they can identify and prevent successful card skimming attacks.

***Test incident response plans.*** Make sure employees and third-party processors understand their respective responsibilities in the event of a skimming attack, including proper notification protocols.

***Participate in industry information sharing forums.*** Since threats and tactics change rapidly, participating in organizations such as the Financial Services Information Sharing and Analysis Center (FS-ISAC) can facilitate more efficient information sharing. The FS-ISAC and the United States Computer Emergency Readiness Team (US-CERT) are good sources of information on the methods used to conduct attacks and on risk mitigation tactics available to minimize their impact.

Below are additional resources that you may find beneficial. Should you have any questions please contact Regional Field Manager Holly Chase at (617)956-1500 extension 409 or holly.chase@state.ma.us.

Sincerely,

David J. Cotney
Commissioner of Banks

Additional Resources:
FFIEC Retail Payment Systems Handbook
http://ithandbook.ffiec.gov/ITBooklets/FFIEC_ITBooklet_RetailPaymentSystems.pdf

FFIEC Information Security Handbook
http://ithandbook.ffiec.gov/ITBooklets/FFIEC_ITBooklet_InformationSecurity.pdf

FFIEC Statement on Cyber-attacks on Financial Institutions' ATM and Card Authorization Systems
http://www.ffiec.gov/press/PDF/FFIEC%20ATM%20Cash-Out%20Statement.pdf

United States Computer Emergency Readiness Team - Alert
https://www.us-cert.gov/ncas/alerts/TA14-002A