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

March 16, 2016

To the Non-bank ATM Registrant Addressed:

As a registered ATM provider in the Commonwealth, the Division of Banks is contacting you in an effort to raise awareness about a concerning increase in Automated Teller Machine (ATM) card skimming fraud in the Commonwealth.

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 Non-bank ATM Registrants (Registrant) to take a fresh look at how you are managing this risk. As such, the Division recommends that Registrants, at a minimum:

Monitor your ATMs. Be vigilant of any unusual activity. Assess existing controls to prevent and detect skimming. Consider implementing enhanced procedures for monitoring ATM transaction activity for unusual behavior.

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

Test incident response plans. Make sure the Registrant, merchants and their employees, and third-parties such as transaction data processors understand their respective responsibilities in the event of a skimming attack, including proper notification protocols in accordance with applicable Laws and Regulations, including Massachusetts General Laws chapter 93H, the Office of Consumer Affairs and Business Regulation's Regulation 201 CMR 17.00, and the Division's Regulation 209 CMR 31.06(5)(c).

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

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

Participate in industry information sharing forums. Since threats and tactics change rapidly, participating in organizations such as the ATM Industry Association (ATMIA) and the National ATM Council, Inc. (NAC) can facilitate more efficient information sharing either through industry events and/or publications. The ATMIA and NAC are good sources of information on the methods used to conduct attacks and education on risk mitigation tactics available to minimize their impact.

If you believe your ATM has been subject to a skimming attack, please contact the Division after informing the appropriate law enforcement agency.

Below are additional resources that you may find beneficial. Should you have any questions please contact Chief Director Elizabeth Benotti at (617)956-1500 extension 541 or Elizabeth.Benotti@state.ma.us.

Sincerely,

David J. Cotney
Commissioner of Banks

Additional Resources:

ATM Industry Association https://www.atmia.com/

National ATM Council, Inc. http://natmc.org/

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