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

Consumer Alert: Be Aware of ATM Card Skimming Fraud

What consumers should know about Automated Teller Machine (ATM) card skimming fraud.

What is ATM card skimming?
ATM card skimming is a scam which 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 PIN entered by the customer. Devices vary in design, size, and shape, but look similar to legitimate devices, and continue to evolve to avoid detection.

Where does the information go once a card has been compromised by a skimming device?
The card skimmer reads the magnetic strip or computer chip on your card and transmits your account information to the thieves or saves the information until the skimmer is retrieved. Stolen account information is often 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.

Where are card skimming devices found?
Card skimming devices can be found on debit and credit card readers. Skimming devices are usually found on ATMs or gas station pump point-of-sale (POS) terminals.

What to look for at ATMs or POS terminals to detect a card skimming device?
Before using an ATM, examine nearby objects that might conceal a camera; check the card slot for a plastic sheath before inserting your card. Walk away from an ATM if you notice someone watching you or if you sense something wrong with the machine; immediately report your suspicions to the company operating the machine or a nearby law enforcement officer.

What do I do if I think I have located a skimming device?
Report anything dangerous or suspicious at an ATM or POS terminal to the local police department or to your financial institution. If the machine does not return your card after your transaction is completed, report that immediately to your financial institution.

How to safeguard my accounts against card skimming?
Do not respond to unsolicited requests for your bank account number or PIN for your debit/ATM card. Monitor accounts for unauthorized transactions. If you suspect fraud, immediately contact your financial institution.

Additional Resources

- Massachusetts Office of Consumer Affairs & Business Regulation
- Federal Trade Commission (FTC)
- Federal Deposit Insurance Corporation (FDIC)