



# WARNING

## BIG SIX TOWERS RESIDENTS ARE REPORTING INCIDENTS OF CREDIT CARD FRAUD



"Skimming" is a method by which thieves steal your credit card information, and all it requires is a little illicit technology and a lot of criminal intent by those who handle your credit card.

Skimming occurs most frequently at retail outlets that process credit card payments -- particularly bars, restaurants and gas stations.

### How skimming works

Skimmers are small devices that can scan and store credit card data from the magnetic stripe. Crooks can install skimmers on a gas pump, or corrupt employees can have a skimmer stashed out of sight of customers. Once the card is run through the skimmer, the data is recorded, and the crooks can sell the information through a contact or on the Internet, at which point counterfeit cards are made. The criminals go on a shopping spree with a cloned copy of the credit or debit card, and cardholders are unaware of the fraud until a statement arrives with purchases they did not make.

### How to protect yourself

1. Inspect the card reader and the area near the PIN pad.
2. Look at other nearby card readers to see if they match the one you are using.
3. Trust your instincts. If in doubt, use another machine somewhere else.
4. Avoid using your PIN number when making purchases.
5. Keep an eye on your accounts and look for suspicious authorizations and charges.

If you suspect that you might have had your card skimmed. Keep an eye on your account balance and report any suspicious activity immediately.

***SUSPICIOUS BEHAVIOR SHOULD BE IMMEDIATELY REPORTED TO:  
BST DEPARTMENT OF PUBLIC SAFETY 718.335.8715.***

***ALL CALLS WILL BE HELD IN STRICT CONFIDENCE.***