

# SKIMMING DEVICES/PIN CAPTURING

A Skimming Device is used to illegally capture a consumer's credit and debit card account information. "Skimming" is one of the newest ways thieves have found to steal your information from credit and debit cards. For as little as one hundred dollars, criminals can purchase card readers to be used as a handheld device or installed into ATM machines to swipe your card -and information, without your knowledge. Rogue employees in restaurants, stores and gas stations can simply slide your card through the handheld device and the information on your card is easily copied. The card is then returned to you, and the stolen information is often sold to identity theft rings who sell the information to various thieves seeking bits of information while visiting underground chat rooms on the web. Skimming Devices seem to be the favorite tool of organized crime rings set out to steal your debit and credit card information. The skimming devices on ATMs are tough to spot. They're nearly exact duplicates of actual card readers- installed right on top of the real one. The devices are attached in a matter of seconds with the help of double-stick tape. Pass your card through, and you're essentially swiping it twice. Then, a hidden camera records your pin code as you punch in the numbers. Thieves are placing them on point of sale debit machines at gas stations and on free standing ATMs. ATM Skimming is a world-wide problem. PIN Capturing refers to a method of strategically attaching cameras and various other imaging devices to ATMs to fraudulently capture PIN numbers. Once captured, the electronic data is encoded onto fraudulent cards and the captured PIN numbers are used to withdraw money from customer's accounts.



## **What you need to know:**

- Skimming devices are normally affixed to ATMs during periods of low traffic (early morning/late evening).
- Length of time skimming devices can be affixed may vary but normally are no more than for 24 hours.
- Successful skimming requires BOTH a card skimmer (card reader) and a camera (PIN capturing device) to be fitted to the ATM in order to steal card data.

## **How you can reduce the risk:**

- Familiarize yourself with the appearance of your ATM
- Inspect the ATM for unusual or non-standard appearance (look and feel)
- Use your hand to shield your PIN when entering it
- Beware of "Out of Service" signs on ATM, which redirect you to the ATM with a skimming device attached.
- Report any unusual appearance to an ATM or if you suspect you card was skimmed by a handheld immediately to the police

Pinecrest Police Department  
12645 Pinecrest Parkway  
Pinecrest, Florida 33156

† 305.234.2100

f 305.234.2132

[www.pinecrest-fl.gov/police](http://www.pinecrest-fl.gov/police)