



Clearwater Police  
Department  
Economic Crimes Unit  
AND  
Public Information

# ATM SKIMMING

Learn to Protect yourself from  
ATM Skimming and PIN Capturing

# WHAT IS...

## SKIMMING AND CAPTURING?

- ◉ ATM Card Skimming is a process where criminals use electronic devices attached to legitimate ATM machines to capture data from the magnetic stripe on the back of unsuspecting customers' ATM cards.
- ◉ PIN Capturing may occur when criminals strategically attach hidden cameras and other imaging devices to ATMs and secretly capture customers' PIN numbers as they are entered on the ATM key pad.



# AREAS TO CHECK ON THE ATM



1. Light diffuser area

2. Speaker area

3. ATM side fascia

4. Card reader entry slot

5. ATM keyboard area



# SKIMMING DEVICES.. WHAT DO THEY LOOK LIKE?



Can you tell if these ATM machines have skimming devices attached?



# TAKE A CLOSER LOOK...



This photo shows the legitimate ATM card slot reader

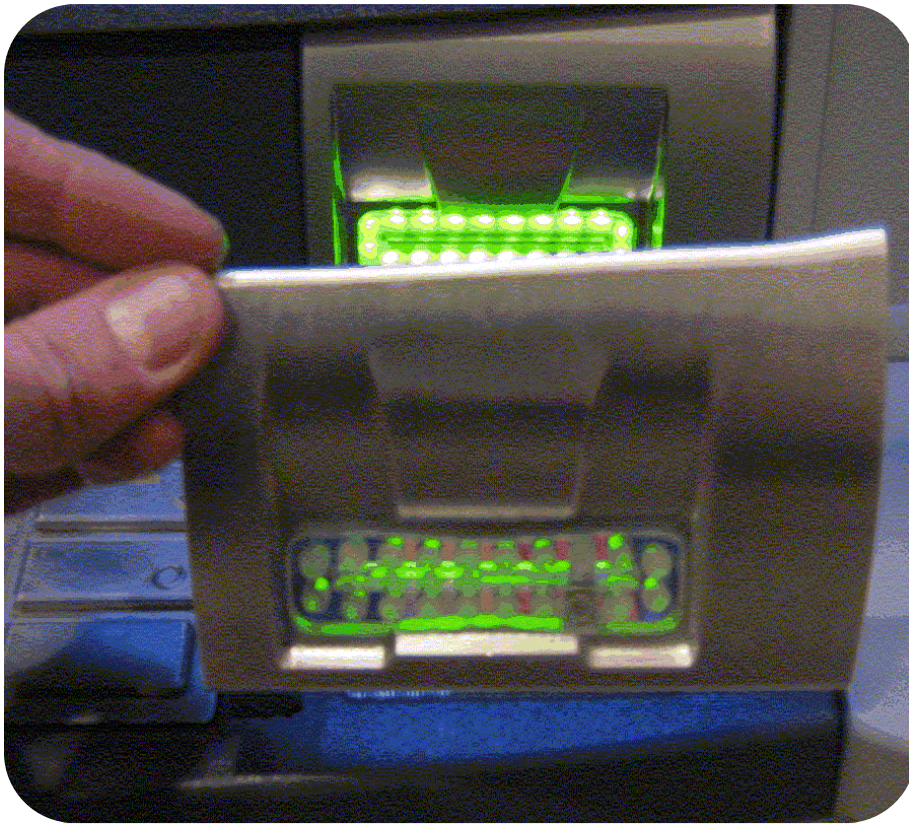


This photo shows the ATM once a skimming device is attached. Notice it hides the flashing card entry area.



# NOT ALL DEVICES ARE ALIKE

Criminals continue to improve their technology...



This device, even when affixed to the card reader, still allows the flashing indicator lights to show.



# ANOTHER SKIMMER EXAMPLE

It can be hard to tell that a device has been attached.

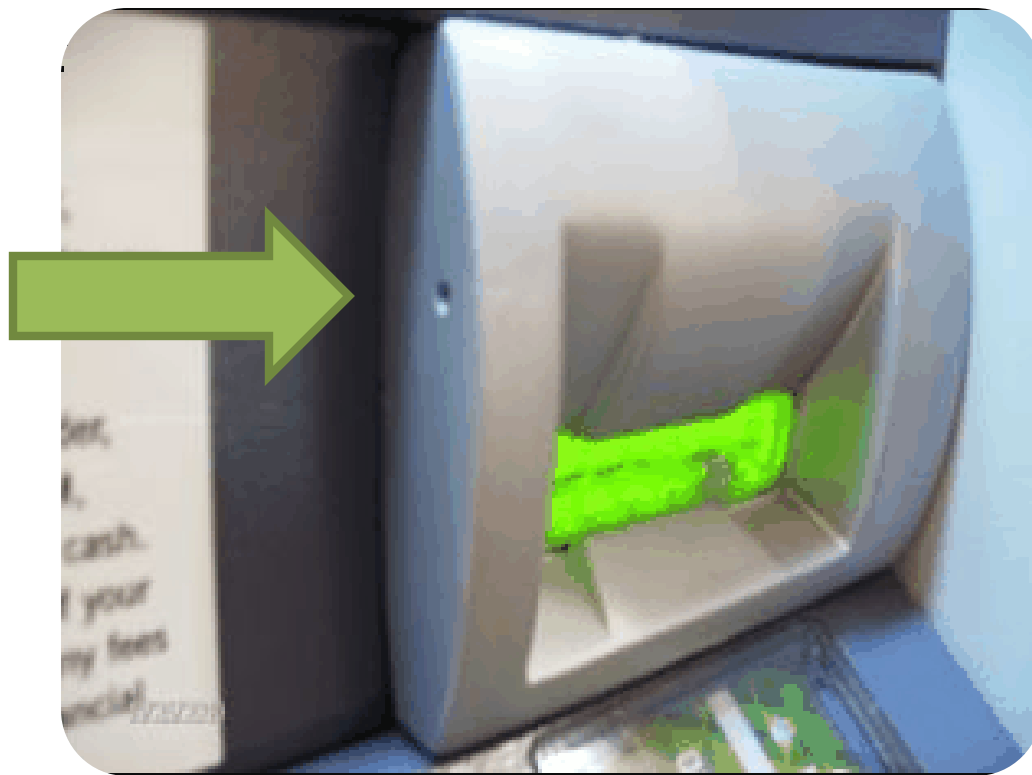


# MANY SHAPES AND SIZES....



Criminals adapt to the specific ATM machine. This device was fitted over the card reader throat.

# PIN CAPTURING DEVICES



Most PIN capturing devices are miniaturized cameras. Here the camera is the small hole, that directly overlooks the keypad.

# PIN CAPTURING DEVICES

This ATM fascia piece , located above the screen, has a hidden PIN capturing device. Hard to see, right?



# TAKE A CLOSER LOOK...



Here you can see  
the electronics and  
pin capturing  
device



# PIN CAPTURING DEVICES



A mobile phone camera is hidden underneath to capture the PIN. The information is then transmitted through a wireless device.



# PIN CAPTURING DEVICES



An extra piece of fascia has been added to this ATM.  
Can you find it?

# PIN CAPTURING DEVICES



As you can see, criminals work hard at producing devices that are difficult to detect.



# PIN CAPTURING DEVICES

Does anything look odd or out of place here?



# PIN CAPTURING DEVICES

Criminals don't lack imagination.....



A pin hole camera was installed on the bottom side of this merchandise unit and aimed at the keypad to capture PINs.

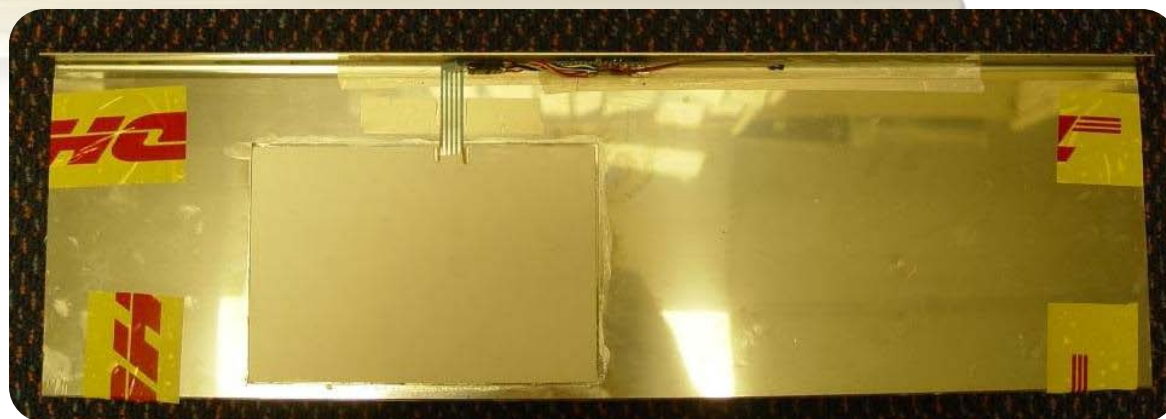
# PIN CAPTURING DEVICES



Keyboards are also a target. Criminals are known to place a skimmer plate on top of existing keyboard.

# MORE PIN CAPTURING DEVICES

This device would capture the customer's PIN when entered on the fake keypad.



# FACTS ON SKIMMING ATTACKS

- ◉ Criminals usually attach skimming devices during the late night hours or early morning. This is usually during low traffic periods.
- ◉ Usually more than one suspect will attach the device. One will alter the ATM, while the other acts as a look out.
- ◉ Remember, according to the type of skimming device, either one or two areas of the ATM might be altered. One to capture ATM magnetic stripe information and one to capture the PIN.
- ◉ The criminals typically attach the devices to the ATM machines for a limited amount of time (hours).
- ◉ Criminals usually remain in the area to monitor the transactions and receive the transmitted information.



# AVOIDING ATM SCAMS



- ◉ **Know your ATM**  
Take time to familiarize yourself with your local ATM. This will help you recognize any suspicious changes or attachments.
- ◉ **Inspect your ATM**  
Look for alterations to the machine. Check for attachments, loose parts, adhesive tape and residue, and keypad changes. Especially pay attention to the ATM fascia, card entry slot, and keypad.



# AVOIDING ATM SCAMS



- Conceal and protect your pin number



- Be aware and look for suspicious people in the area



# REPORT SUSPICIOUS ACTIVITY



When you observe something suspicious, IMMEDIATELY contact your bank AND your local police department.

**Don't be a victim of ATM fraud...STAY ALERT!**