What is a skimmer?

- A scanning device or skimming device to access, read, obtain, memorize, or store, temporarily or permanently, information encoded on the computer chip, magnetic strip or stripe, or other storage mechanism of a payment card without the permission of the authorized user of the payment card and with the intent to defraud the authorized user, the issuer of the authorized user’s payment card, or a merchant.

- A person who violates subparagraph 1 a second or subsequent time commits a felony of the second degree.

- It is a felony of the third degree for a person to knowingly possess, sell, or deliver a skimming device. This paragraph does not apply to the following individuals while acting within the scope of their official duties:
BEST PRACTICES
Best Practices:

• Have skimmers been found at the location before? On what pumps?

• Where have skimmers been found? Have there been skimmers found on the same street recently? Look for patterns.

• **Example:** 3 skimmers were found on the same street at different facilities within a week of each other.
Best Practices: Continued. . .

• Look at the pump – is anything different? - check more thoroughly.

• Look for cut, broke, missing, fake security seals, different security seals?

• Are screws missing on credit card reader? Is credit card reader loose?
Best Practices: Continued. . .

• South Florida is densely populated, with cities almost overlapping. It is not uncommon to see one city without skimmers while multiple devices are found in the next.

• Also, we will stop finding them in one city and start finding more in another.

• It should be noted that when that second city starts showing devices again, the first may show none at all.
Best Practices: Continued. . .

• Is one credit card reader in the pumps different from all the others? Is it a different model / new credit card reader?

• Check with station personnel for an explanation. Talk to the attendant, has there been any missing seals lately or anything suspicious?

• Do the locks look like they have been damaged or changed?
Best Practices: Continued. . .

• Pump location no longer matters. Skimmers are found on pumps far away and close to the store entrance.

• Facility locations may be relevant, depending on the situation. Sometimes—in smaller cities—facilities nearer to an interstate or well-traveled highway are more likely to be compromised.

• When a skimmer is found at a facility, our procedure requires we return within 90 days to re-check (re-inspect).
MOST COMMON PUMP MODELS
Wayne Pumps
Gilbarco Pumps
525.07 Powers and duties of department; inspections; unlawful acts.—

• (10)(a) Each person who owns or manages a retail petroleum fuel measuring device shall have affixed to or installed onto the measuring device a security measure to restrict the unauthorized access of customer payment card information. The security measure must include one or more of the following: 1. The placement of pressure-sensitive security tape over the panel opening that leads to the scanning device for the retail petroleum fuel measuring device in a manner that will restrict the unauthorized opening of the panel.

• (e) The department may seize without warrant any skimming device, as defined in s. 817.625, for use as evidence.
Wayne locks Easily Accessible
Wayne Pump W & W/O Security locks
Wayne W/O Security Features
Wayne Pumps With Factory Installed Security Measures.
Standard Keys Online
CREDIT CARD PROTECTED

This dispenser is equipped with the technology that will protect your credit card data from possible theft and illegal use.

Thank you for making Circle K your preferred place to shop.
Secure Card Readers
Amber Light Means There’s A Problem
Additional Secure Card Readers
LOOK AT THE LOCK BOX THEN FOLLOW THE CABLE
SECURITY SEALS
Correct And Incorrect Placement Of Seals
Fake Security Seals
Purchase Security Seals online
APPROVAL FOR ALTERNATIVE SECURITY
CREDIT CARD SKIMMERS
GILBARCO MODEL
THIS CAPTURES PIN ALSO
Inside Card Reader
WHAT INSPECTORS ARE FINDING
Cell Phone Chip In Skimmer
WHAT WAS FOUND IN OUR AREA
We call these ‘Overlays’
Inline Skimmer
Bluetooth Skimmers
Other Styles Of Skimmers
Multiple On The Same Pump
Other Devices
VAMPIRE CLIP
STATE OF FLORIDA RECORD:

8 SKIMMERS !!

1 found in each of the 8 dispensers at this facility.
TYLER, Texas (KLTV) - An Austin man has been sentenced to life in prison for his role in a credit card skimming operation in Tyler.

Felipe Manuel Nieves Perez, 33, pleaded guilty earlier this year to his involvement in the operation, which involved installing card skimmers with blue tooth capability to be accessed by a laptop used in vehicles parked at gas pumps.
SKIMMER COLLECTION
Florida collection law

525.07 Powers and duties of department; inspections; unlawful acts.—

• (10)(e) The department may seize without warrant any skimming device, as defined in s. 817.625, for use as evidence.
Evidence Bags
Starting March 2015 the State of Florida Inspectors collected 169 Skimmers.

Each credit card number stolen is charged on average $750.00

<table>
<thead>
<tr>
<th></th>
<th>Collected</th>
</tr>
</thead>
<tbody>
<tr>
<td>2016</td>
<td>219</td>
</tr>
<tr>
<td>2017</td>
<td>642</td>
</tr>
<tr>
<td>2018</td>
<td>1242</td>
</tr>
<tr>
<td>2019</td>
<td>1100 (to date)</td>
</tr>
</tbody>
</table>

With an average of 100 credit card numbers stolen per skimmer.
SKIMMER CHECKLIST

Florida collection law

525.07 Powers and duties of department; inspections; unlawful acts.—

(e) The department may seize without warrant any skimming device, as defined in s. 817.625, for use as evidence.
How are skimmers used?

• The stolen information is either sold or downloaded then transferred to blank cards and used to make illegal purchases.

• Skimming can take place anytime & anywhere when a credit or debit card is used, including ATM’s, hotels, retail establishments, restaurants, & gas pumps.

• If a crook did their “job” properly these skimmers cannot be detected by consumers.
Examples
Examples
QUESTIONS