NEWS RELEASE

FOR IMMEDIATE RELEASE

October 25, 2018

Contact:

Diana L. Klink
Office: 757.514.4104
Mobile: 757.359.1845

Tim Kelley
Office: 757.514.4103
Mobile: 757.871.3039

POLICE ADVISE TO BE ALERT FOR POSSIBLE CREDIT CARD SKIMMERS

SUFFOLK, VA (October 25, 2018) Suffolk Police would like to alert the public to be aware of possible credit card skimmers which are placed on the outside of ATMs or gas pumps, and their even smaller treacherous cousins, shimmers, which are placed inside machines.

Two such devices were found on gas pumps at the Miller Mart located in the 2800 block of Pruden Boulevard and were installed sometime between October 27th and October 29th. Using these devices, criminals can easily capture your credit and debit card information. It is strongly suggested that if you used your debit or credit card at this business during the noted timeframe, you should check for any possible fraudulent transactions and contact the Suffolk Police Department and your credit card company or bank to report any issues.

To potentially avoid becoming a victim, do the following:

Check for Tampering

When you approach an ATM or gas pump, check for obvious signs of tampering at the top of the ATM, near the speakers, the side of the screen, the card reader itself, and

the keyboard. Consumers should also check the security strip on the pumps for wear or tearing. This is another good indicator for the embedded blue-tooth skimmer.

If something looks different, such as a different color or material, graphics that aren't aligned correctly, or anything else that doesn't look right, don't use that device. The same is true for credit card readers in the checkout line. If you're at the bank, it's a good idea to quickly take a look at the ATM next to yours and compare them both. If there are any obvious differences, don't use either one, and report the suspicious tampering to your bank. For example, if one ATM has a flashing card entry to show where you should insert the ATM card and the other ATM has a plain reader slot, you know something is wrong. Since most skimmers are glued on top of the existing reader, they will obscure the flashing indicator.

If the keyboard doesn't feel right—too thick, perhaps—then there may be a PIN-snatching overlay, so don't use it.

Skimmers read the magnetic stripe as the card is inserted, so give the card a bit of a wiggle as you put it in. The reader needs the stripe to go in a single motion, because if it isn't straight in, it can't read the data correctly. If the ATM is the kind where it takes the card and returns it at the end of the transaction, then the reader is on the inside. Wiggling the card as you enter it in the slot won't interfere with your transaction, but will foil the skimmer.

This tactic won't work on shimmers, and won't work with any ATM that captures and holds your card while your transaction is in process. However, there are still ways to protect yourself when using these machines.

Think Through Your Steps

Whenever you enter your debit card's PIN, assume there is someone looking. Maybe it's over your shoulder or through a hidden camera. Cover the keypad with your hand when you enter your PIN. That's a good policy even if you don't notice anything odd about the ATM. Obtaining the PIN is essential, since the criminals can't use the stolen

magnetic stripe data without it. Of course, that assumes the attacker is using a camera and not an overlay to obtain your PIN.

Criminals frequently install skimmers on ATMs or fuel pumps that aren't located in overly busy locations since they don't want to be observed. The ATMs inside banks and at grocery stores or restaurants are generally safer because of all the cameras than the one that is outside on the sidewalk, however, stop and consider the safety of any device before you use it.

Additional tips to avoid having your credit card information stolen by thieves with a skimmer or shimmer are:

- **Check any payment terminal carefully** as detailed above.
- **Pay attention to your bank accounts**. Check the transactions in your bank or credit card account regularly. Report any suspicious transactions immediately.
- **Cover the keys**. Use your hand to shield your PIN from view. Don’t let the camera, or the person standing behind you, capture the PIN number.
- **Examine the keypad**. Sometimes the thieves add an overlay to the keypad. So if the keypad appears thick or different than usual, don’t use it.
- **Use a credit card at gas stations**. Credit cards have better fraud protections than a debit card. If you use a debit card, run it as a credit card so you don’t use your PIN. If they get your PIN they can get direct access to your bank account. You can also use gas pumps closer to the store. Thieves are less likely to tamper with those because of the chance of getting caught. Or, you can just pay for your gas with cash.

Be alert, be aware, and check your account transactions regularly to avoid losing your hard-earned money to thieves because of credit card skimmers.

###