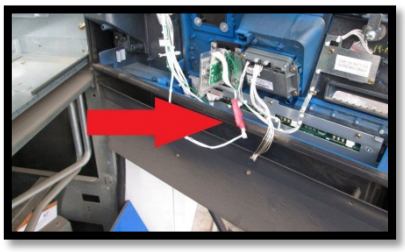

Payment Card "Skimmers"

What to Look For

What are payment card "skimmers" and what do they do?

Payment card skimmers are devices that fraudulently collect payment card (e.g., credit and debit cards) information when the card is used for a purchase. This information is then saved within the skimmer to be retrieved at a later time by the perpetrator or may instantly transmit this information wirelessly to the perpetrator or may transmit the information instantly to anywhere in the world. Payment card skimmers are a major form of theft and are often linked to organized crime.

Where are payment card skimmers located?

Skimmers can be installed anywhere payment cards are used. For example, motor fuel dispensers ("gas pumps"), card readers at stores and restaurants, ATM's, etc. On fuel dispensers, they may be attached externally to the legitimate card reader or they may be installed internally within the dispenser's cabinet.

What do payment card skimmers look like?

In relation to fuel dispensers, there are predominantly two types: internally and externally mounted.

The **externally mounted skimmers** attach directly over top of the legitimate card reader. They appear very similar to the legitimate card reader and they may be very difficult to distinguish.

The **internally mounted skimmers** are installed inside of a dispenser's cabinet among the internal components. They are not detectable from the outside of the dispenser. There are two basic types of these skimmers: ones that attach in-line with the communication wires on the back side of the card readers and ones that are a circuit board that attach directly to the back side of the card reader. The skimmers that are attached in-line are of the same wire design used with the card readers but they have a small digital storage device. The storage device portion is usually wrapped in some fashion to protect it and to make it more difficult to see and identify. The circuit board-types of skimmers attach directly to the back of the legitimate card reader and are very difficult to observe on casual inspection.

To obtain personal identification numbers (PIN), the perpetrators may use very small "pinhole" cameras to observe and record entry of a PIN; they may use a keypad overlay that captures the PINs as they are typed in; or devices installed internally that connect to the keypad itself.

In the cases of internally installed payment card skimmers and keyboard PIN-theft devices, they are invisible to the consumer.

How quickly can payment card skimmers be installed on fuel dispensers?

- It has been reported that payment card skimmers can be attached to fuel dispensers in as little as 7-8 seconds.

What can consumers do?

- Be alert where they are using their payment cards.
- When using payment cards for fuel purchases, consumers should try to select dispensers that are within sight of the cashier.
- Gently attempt to move the card reader on the fuel dispenser. Do not force it. If legitimate, it will not move nor come off.

- Look for broken or missing adhesive security seals on the cabinet of fuel dispensers where the card reader is located. Many businesses are attaching customized adhesive seals to these places to provide evidence that the card reader has been accessed. If a consumer observes the seal broken or missing, they should report it to the business immediately. Be mindful that not all businesses are taking this extra step of precaution.

- Be aware of where purchases are made.
- Change passwords to payment card accounts frequently. Use secure passwords.
- Treat payment cards as cash or any other valuables.
- Check payment card statements frequently, if not daily. Compare payment card receipts to the statements. Look for any suspicious purchases. Communicate with other family members to be alert to where they use their payment cards and any fraudulent charges.

- Ask the card issuing institution if they have purchase monitoring available. There may be a fee associated with this service. These services will detect and report unusual purchase patterns to the customer.

- Another option is to contact credit bureaus and request that they monitor purchasing patterns and report unusual activity to the customer. There is a fee for this service.

- Report suspicious payment card transactions to the card issuing institution immediately. They can "freeze" the card so no additional authorizations can be made.

- Contact the three major credit bureaus: TransUnion, Equifax, and Experian. They can also "freeze" the card to prevent additional authorizations.

- Contact law enforcement immediately. Payment card fraud is theft.

- Perpetrators may not use the payment card for 2 or more months after they have stolen the information. Then they may make a small purchase to just check if thee card is active. Once they are satisfied that the card is active, then they will use it for fraudulent purchases. Consequently, consumers should not assume that their card has not been compromised.