

Potential Pump Skimming

The purpose of this sheet is to provide information about potential skimming of credit card data from pumps, how it occurs, and what are some of the ways to help prevent it.

The process of skimming (stealing) magnetic card stripe data has been around for a fairly long time. Most cases involve an individual manually swiping the card through a skimmer. This device records (skims) the information from the credit card's magnetic stripe. The customer is not aware that their card data had been stolen. Once the criminal has this information, he/she can create a fraudulent copy of your card, which can then be used to make purchases. There have been a number of prosecutions in the past for these activities.

Several news articles have recently reported that criminals may be installing devices inside gasoline pumps to automatically skim credit card information. To date there has been only one actual instance where we know that a skimming device was used in a dispenser. This happened on the West Coast and was not at an ExxonMobil location.

Recently several companies reported that some of their cardholders may have had their cards skimmed at pumps in Florida. As a result, the Florida Department of Agriculture (responsible for inspecting pumps) issued a press release warning of a growing skimming problem in Florida. The release stated that they are "monitoring the situation and [are] working with credit card companies and other law enforcement agencies to develop leads in an effort to eliminate the scam." They have not actually recovered any pump skimming devices but they are looking.

ExxonMobil security and card fraud personnel have been in contact with Florida law enforcement, FL Department of Agriculture inspectors, the Secret Service, pump manufacturers, and other card fraud experts to assess the situation and to try to develop ways to prevent the possible skimming. Currently the problem is not widespread and is relatively small. However we are working to develop ways to protect against the process. We do recommend some steps that cardholders and retailers should take to help prevent pump skimming and protect themselves.

HOW PUMP SKIMMING WORKS

How do investigators think pump skimming occurs?

- Fraudster chooses a busy station and choose a dispenser that is difficult to see from the store;
- Parks car or truck to block view;
- Uses key or tool to open top of dispenser;
- Installs skimmer on to existing wires;
- Closes dispenser & leaves;
- Returns several hours later and removes skimmer;
- Makes fraudulent card from data.

STORE PRECAUTIONS

- Be alert and look for suspicious activity. Watch for vehicles parked at pumps without making any fuel purchases. If you suspect someone has tampered with a dispenser ask your store manager to look inside the pump for unauthorized connections.
- If you do find something suspicious attached to one of your pumps, notify your Territory Manager immediately. The TM will coordinate necessary contacts. If you are instructed, notify local law enforcement.
- Change the paper in your pumps at different times during the day. Don't keep a regular schedule. Look for unusual things when you change the paper.
- Walk around outside. Random trips outside the store will discourage criminals. When outside for normal duties, be aware of your surroundings and what people may be doing near your pumps.

CARDHOLDER PRECAUTIONS

- Be alert for suspicious activity. If you see anyone tampering with a dispenser or see anything unusual about the dispenser, report it to the store manager.
- Check your monthly statements. Retain your card receipts and carefully reconcile with your statements to make sure you don't have unauthorized charges. If you find unauthorized charges related to gasoline purchases, particularly at pumps, report the incident to your card company immediately AND your local law enforcement. (This will help law enforcement track reported cases.)
- Use pumps which are easily visible, close to the door, or that stay busy. Fraudsters don't want to be seen.
- Consider using Speedpass. This electronic token allows you to purchase gasoline without revealing your card number at the station.

Card fraud is a big business. Anything you can do to help prevent it is good for everyone involved, the cardholder, the retailer, and ExxonMobil. If you have any questions or suggestions send an e-mail note to fraudanalyst@exxonmobil.com.

Potential Pump Skimming - Retailer Q&A's

Q1. What does a skimming device look like?

- A. A skimming device inside a pump could be one of many shapes, but most likely will look like a small box with wires connecting it to the back of the pump's card reader or PIN pad. The box probably will be about the size of a cigarette box but could even be smaller. The wires will probably be a "ribbon" type that matches the wires already in the pump. These wires may run from a connector near the card reader or PIN pad, or may connect to the middle of the existing pump wires.

The device would probably be located near the card reader & PIN pad where it easy to get into and out of the pump. However, it could be "buried" further down inside the pump.

Q2. What should I do if a customer reports a suspicious pump or I suspect a card skimming device is in my pump?

- A. Carefully open the dispenser head and look inside for suspicious wires or devices. If you see something suspicious try not to touch it or remove it. Try to minimize your contact with the dispenser door, lock etc. Do not tamper with or remove any device. Law enforcement officials may want to check for fingerprints or other evidence. If you find a device we suggest you close that fueling position and don't let anyone near the dispenser.

If you find a suspicious device contact your territory manager immediately and follow his or her instructions. Either you or your TM should contact local law enforcement authorities and tell them you suspect there may be a credit card fraud device in one of your pumps.

In Florida several law enforcement agencies are working together to address this problem. If the local law enforcement agency is not familiar with the problem, encourage them to contact the Florida Department of Law Enforcement (FDLE) or the Secret Service.

Q3. What can cardholders do to help protect themselves against pump skimming?

- A. Cardholders can take several precautions. First, always be alert to your surroundings. Do not use a pump that looks suspicious or tampered with. Use pumps that are easier for the cashier to see from inside the store. It would be harder for a potential fraudster to install a skimming device in a pump that is easy to see than one that is far away from the station and hard to view. If you see someone tampering with the inside of a pump or are suspicious of a pump, notify the store manager. Save your receipts and check your card statement promptly each month. Make sure you are not charged for unauthorized purchases. If you find unauthorized charges related to gasoline purchases, particularly at pumps, report the incident to your card company immediately AND your local law enforcement. (This will help law enforcement track reported cases.)

Q4. What is ExxonMobil doing to prevent card fraud?

- A. ExxonMobil is actively working to recognize and prevent all types of card fraud. We are: Involved with industry groups to identify possible skimming devices; Working with various law enforcement agencies, both local and national to follow up on cases; Working with pump manufacturers to encourage development of new pumps with preventative technology, and to develop possible short term improvements; Using our POS computer systems to help identify possible skimming situations; And we are providing communication and information to key impacted groups including cardholders and retailers. ExxonMobil has produced and distributed to all our retailers a fraud video to teach retailers how to recognize card fraud and what steps they can take to help prevent it. ExxonMobil uses sophisticated computer systems to authorize and track card sales. These systems include a number of fraud preventative and detective measures.

Q5. I have Gilbarco dispensers and one key fits all the Gilbarco dispensers everywhere. Does this make it easier for fraudsters?

- A. The locks on dispensers are relatively low tech and are designed to primarily prevent casual entrance to parts of the pump that could cause customers injury or could damage the pump. While keys provide a limited amount of protection, sophisticated fraudsters can get around these types of locks regardless of the key.