

Gas Pump Security

12/22/15

You may have heard in the news about debit/credit card skimmers found in gas pumps in the Dayton area, as well as other locations across the country. These devices are small electronic devices that can be illegally installed inside a gas pump to steal card information. When a customer swipes a debit or credit card, the device stores the information contained on the magnetic strip as well as the PIN that the customer types in. The thief who installed it can then retrieve the data via blue tooth without ever returning to the pump itself. The data is used to make duplicate cards which are sold to others who then make fraudulent charges until that card number is disabled.

“It only takes less than a minute for a thief to install a skimmer” says Shelby County Auditor, Amy Berning. “The Auditor’s Office was first alerted about the skimmers by the Chief Deputy State Sealer at the Ohio Department of Agriculture. We are not authorized to monitor anything related to the processing of credit cards, but we are keeping an eye out for potential skimmers as part of the pump inspections. It is the responsibility of our office to verify that the quantity being pumped matches the amount that is actually being dispensed, and that the pump is properly calculating the money due. The Auditor’s round sticker indicates only that our inspection has been performed for the current year. The gas station staff needs to daily monitor the security of their payment equipment.”

“I have put together a packet of information to help gas station staff learn how to make their pumps more secure. Our Inspector, John Turner, and I have hand-delivered the packets and answered questions at all 30 gas stations in Shelby County to alert gas station staff about the importance of being vigilant,” said Berning. “The US Secret Service has been investigating this criminal activity and has made several arrests. They have determined that this is an organized ring headquartered in Cuba, and when one of their thieves gets arrested, they just fly in replacements. This threat has no end in sight.”

Consumers should keep the following in mind in order to protect their funds:

- *Never use a debit card and PIN at the pump, since fraudulent purchases will not be refunded to you with this type of card, and your bank account could be emptied at an ATM.
- *Paying with cash is the best way to protect your card number from being stolen.
- *Monitor the charges on your credit card statement and report any fraudulent charges to the credit card company.
- *Credit cards with the new “chip” technology cannot be duplicated, but the card number could still be used to make online purchases.
- *Report to the station attendant or local law enforcement if you see someone open the face of a pump. They may be installing a skimmer.