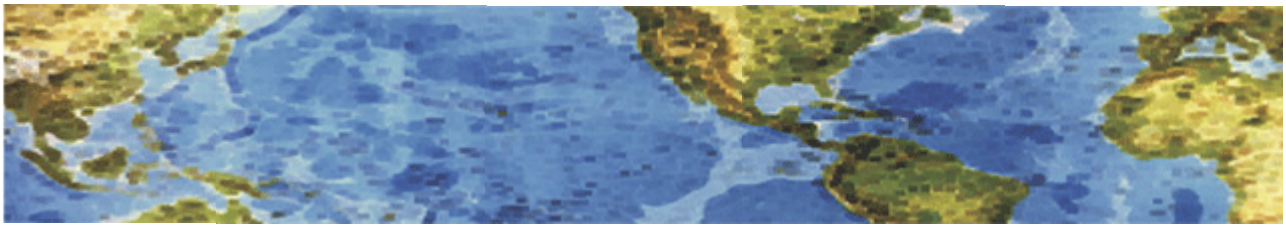
HALL ASSOCIATES



Risk-Based Decision Making Commentary
23 January 2014 Newsletter

Bluetooth Enabled Card Skimmers planted at Gas Stations lead to $2 Million Heist

Cyber Criminals will not let any way out without making Money. Another huge credit card theft and this time they targeted gas stations. 13 men were suspected and charged for stealing banking information, using Bluetooth enabled Credit Card Skimmers planted on the gas stations **throughout the Southern United States** (do you check your accounts for bogus withdrawals regularly?).

They made more than $2 Million by downloading the ATM information, as well as PIN numbers from the gas pumps and then used the data to draw cash from the ATMs in Manhattan. Manhattan District Attorney Cyrus R. Vance explained that the skimming devices were internally installed so was undetectable to the people who paid at the pumps and the devices were Bluetooth enabled, so it did not need any physical access in order to obtain the stolen personal identifying information. Most gas pumps use a default key to open the front covers, so that "protection" is small.

By using skimming devices planted inside gas station pumps, these defendants are accused of fueling **the fastest growing crime in the country**. (Card skimmers – both credit and debit - are showing up in lots of places – ATMs, gas pumps, large and small retail stores and restraints, etc.). Cybercriminals and identity thieves **are not limited to any geographic region**, working throughout the world from behind computers. In this specific case, approximately in between March 2012 to March 2013, the suspects used the forged cards for withdrawing cash from the ATMs, and then deposited that stolen money into bank accounts in New York. The other members of the gang then promptly withdrew that money at banks in California or Nevada.

Each of the defendants' transactions was under $10,000. They were allegedly structured in a manner to avoid any cash transaction reporting requirements imposed by law and to disguise the nature, ownership, and control of the defendants' criminal proceeds. From March 26, 2012, to March 28, 2013, the defendants are accused of laundering approximately $2.1 million. The four top defendants out of 13 – Garegin Spasrtalyan, age 40, Aram Martirosian, age 34, Hayk Dzhandzhapanyan, age 40, and Davit Kudugulyan, age 42 – are considered as the lead defendants and are charged with Money Laundering theft and possession of a forgery device and forgery instruments. The other criminals are charged with two counts of Money Laundering theft.

http://thehackernews.com/2014/01/bluetooth-enabled-credit-card-skimmers.html

HALL ASSOCIATES

4 Strategies for Protecting Your Credit/Debit Card at the Gas Pump

Most skimmers are high-tech and internally placed now. Unfortunately, they're also on the rise. The US Secret Service reported a whopping 3,000 % increase in skimming thefts last year. By practicing a short ritual of security measures before swiping a credit or debit card at the gas pump, you can safeguard your card information.

#1. Look for Tamper-Evident Stickers - Criminals usually infiltrate card mechanisms through the front panel of gas pumps. They implant devices internally, which then capture the card information from within once customers swipe their cards.

What to look for: Survey the gas pump's edges — especially the hatch surrounding the card unit. If it looks battered as if someone tried to pry it open or if the lock itself is broken, it may have been compromised. Some gas stations, like Shell stations, apply a tamper-proof seal across the opening of the card door. When a door is broken into, the sticker is lifted revealing the words "VOID" on the sticker.

What to do: Before using a gas pump, find out whether the pump has a tamper-evident sticker. If it has one that is placed on the unit correctly (i.e. across the opening of the door) and it reads void, move on to the next pump or station. Recommend that you contact local authorities about the situation.

#2. Beware of External Gas Station Card Skimmers - These are external devices thieves attach over a real card slot at a gas station pump. As customers swipe their cards into the skimmer, the device saves and stores card information immediately.

What to look for: If a card slot looks different from the other card readers at the station, it may be a setup for gas station card skimming fraud.

What to do: External Skimming devices are meant to be placed temporarily for a matter of hours or just a day. For that reason, they are usually attached using only double-sided tape, so thieves can easily remove them. Before sliding a credit or debit card through the machine, tug on the reader to ensure it is on securely; skimmers will easily pop off with mild effort. Recommend that you contact the local authorities to file a police report if a card skimmer is found.

#3. Block View of Pinhole Cameras - These inconspicuous cameras are so small that cardholders really have to be paying attention to spot them. They are sometimes used in conjunction with card skimmers to capture footage of customers entering their PIN numbers. With this added information, criminals can withdraw funds directly from bank accounts, as well as make fraudulent credit/debit card purchases.

What to look for: Again, search for anything on the face of the gas pump that looks unique compared to the other pumps. Pinhole cameras are often situated above the keypad area.

What to do: For extra precaution, use two hands when paying for gas at the pump. Use one hand for the transaction, and place the other above the credit card screen to shield the keypad from view of lurking cameras above.

#4. When in Doubt, Use Cash - While credit/debit cards lend convenience, if a situation just doesn't feel right, go with your instincts and just use cash. It saves the hassle of disputing a card charge in the future, and eliminates the risk of putting yourself at risk of long-term credit damage.

If cash isn't a possibility, cardholders also have the option of handling the transaction with the gas station attendant. However, customers still take on a small risk, as there is no guarantee that the employee isn't using a card skimmer behind the counter.