GAS DISPENSER SKIMMERS

FIGHTING BACK ON ALL FRONTS

By Rich Morahan

Accelerating Attacks on Petroleum Dispensers

America's petroleum dispensers are under nationwide attack, from Washington to Michigan to Florida. A quick trip to Google will demonstrate that, despite the industry's best efforts, gas dispenser skimming devices are being discovered at an ever-increasing rate (at least 15 incidents since November, 2015). It's safe to assume that actual, rather than discovered, insertions are increasing accordingly.

"Skimming Devices Found In 7 Ohio Counties" is a typical headline. Each incident usually references 10 or more additional locations.

Why the Increase?

We may now just be coming better at detection. This level of successful skimming may have been going on for years under everyone's noses. More likely, there is a concerted effort to conquer petroleum dispensers, the last frontier for skimming old style credit card information. The new "chip and pin" card system was implemented for retail businesses in October, 2015, with an exemption for the petroleum industry, which had its deadline extended to October, 2017. Under the new "chip and pin," unless a retailer implements "chip and pin," the retailer, not the card issuer, is responsible for reimbursing the victim. Petroleum operators have pushed back this liability, and the need for serious security, for a year and a half.

Because of this window of opportunity and easy access, gas dispensers remain targets of opportunity for the international identity theft industry.

What is the Petroleum Industry Doing to Prevent Data Skimming?

For a few years, the industry has placed its hopes on security stickers to indicate tampering, a solution based on a lot of hope:

- Will the stickers be applied properly?
- Will they be properly maintained?
- Will low wage employees monitor their condition?
- Will customers even notice that stickers are cut or "voided, " or know what to do?

And if this weren't enough, skimmer gangs have been discovered covering their tracks by installing counterfeit stickers, and probably buying legitimate ones as well.

From CBS Money Watch, November 15, 2015: "Indicted Nov. 13, Floridians Anthony Nunovero and Edelso Sanchez are accused of stealing information from about 2,000 credit and debit cards to create counterfeit versions. The men allegedly attached modified scanners to gas pump readers, with the two even replacing tamper-proof seal stickers on the pumps with phony ones, according to the Federal Bureau of Investigation."

Should we even be surprised that gangs that can insert a small Bluetooth enabled skimming device and auction off credit card numbers can also scan a label and produce a convincing copy on an office printer?

What Are The Implications Of Rampant Skimming?

Whatever the cause, one obvious result is increasing cash loses by the public. Until October, 2017, operators are off the hook. More importantly, victims are open for identity theft. A customer can have his credit card copied, and be reimbursed, but he or she may need months to recover from the fraudulent use of his identity data. The industry is not doing enough to protect its customers. Its solutions are not working.

And there are serious impacts for the industry:

The public may stop using automatic pumps and buy gas only at the counter, increasing labor costs and defeating the whole concept of "Convenience Store" petroleum dispensers..

We have seen increasing attacks on "Mom and Pop" stores, resulting in customers bypassing smaller operations in favor of big well-lighted sites. Large well-lighted operations may necessarily be any safer. For example, a skimming device was discovered in a 24-hour operation outside of Boston at one of two 24-hour stores. The skimming team bypassed five closed stations. Ask yourself, what is the quality of observation at 2:00 in the morning at a gas station?

The Industry Needs to Do More

Does the petroleum industry want to continue to fund criminal enterprises?

The industry needs to actively promote and support a multi-level attack against skimmers, starting not with stickers, but with high security key systems.

Stickers were an attempt to stem the tide, and they surely caught some skimmer devices, after the fact. They didn't catch on universally, and they often weren't employed properly. There are dozens of stories about poorly maintained and improperly applied stickers. You cannot base a security system on the reliability of a minimum wage employee working the night shift.

The proof of the failure of the sticker campaign is in the results. Just Google "gas dispenser or gas pump skimming" as you read this. Quite likely, the incident frequency will probably be even greater than it was in February.

You need more than stickers and an eagle-eyed minimum wage attendant.

You need security locks as a minimum first step.

There are levels of security:

- You could replace your dispensers with a new electronic high security device, or replace your dispensers entirely, but that is probably cost-prohibitive, unless you are opening a new site.
- Only one device stops the skimmer—the lock on the door with a high security key. The other devices, stickers, cameras, alarms, deter, record and announce crime, but they don't stop it.

CONTINUED ON PAGE 22

CONTINUED FROM PAGE 17

GAS DISPENSER SKIMMERS

If you need to maximize your security dollars, invest them in a security lock.

Of course, operators can replace all their dispensers or all their card readers, but that is a major undertaking and a major expense. They can always install more cameras, and spend more time viewing images. Or they can replace their locks with a lock that prevents criminals from opening a dispenser door and installing a skimming device. They need to replace the weak link in gasoline dispenser security, the original equipment key that even a novice thief can easily acquire, duplicate or pick.

You are probably sick of hearing about the "universal master key" in news reports. The stock shipper key is a "universal" key, but is not a master key. A master key is a high security key, virtually pick and tamper-proof, that is part of a master key system. An operator with multiple sites can have a different registered key code for each address, to enhance the security and location accountability, while keeping a registered master key that accesses all of his company's pumps. He can even supply that master key to local fire departments, if they require emergency access to dispensers.

Do You Need to Replace Your Dispensers?

Taking a comprehensive approach, major gas dispenser manufacturers have developed new security measures that defend against skimming at the source: encrypted card readers that retrofit into old dispensers and are available in new dispensers. Data encryption at the reader makes the data unusable for thieves. Additional high level security devices are available built into new dispenser models, including automatic shutdown, and alarms that sound when doors are opened. As an added level of security, European style EMV card readers will eventually become the industry standard. These enhancements combine to combat the current level of attacks. But as we know the battle goes on, and there will likely be more technological challenges, and defenses, to come.

And even with the latest technology, criminal employees with access to a key can bypass most high tech barriers. You cannot secure a lock unless you secure the key.

Install A High Security Key Control System

Obviously, replacing gas dispensers with new models with tamper-proof doors and electronically secure card readers is the optimum response. It is also the most costly. Fortunately, a number of lock manufacturers, among them ComPX, Insta-Key Lock America, PetroDefense and Van Lock have developed "Retrofit Kits" that replace the low security "universal" keys and locks that were shipped with most dispensers. With management controlled key control, registered key codes unique to each customer, and non-duplicatable key blanks, these retrofit kits can protect dispensers against unauthorized access at a fraction of the cost of new equipment.

A high security lock system should have a non-duplicatable key blank, millions of usable key combinations, and a virtually pick and drill-proof mechanism, with its key code registered exclusively to the customer.

Time to Mount A Multi-level Defense Against Skimming.

The plague of skimming costs the public millions, perhaps billions of dollars. It costs petroleum operators and companies millions in downtime, added overhead and a loss of public confidence. A well-maintained sticker program with employee training and buy-in can reassure the public, and deter skimmers, but only a high security key control system can ensure protection against skimming devices.

Rich Morahan frequently writes about security and marketing issues for the petroleum, propane and self-storage industries. Contact him at 617-240-0372, rmwriteg@gmail.com, or go www.rmorahan.com.