The ultimate ATM Security Solution

StopSkimmer

Let's stop ATM skimming

A skimming device placed on an ATM is an unauthorized device equipped with at least one magnetic stripe read head and a data storage facility to collect customer card data. When a customer inserts a bank or credit card into the card reader, the skimming device reads the magnetic stripe and lifts, records and stores customer data. A camera or PIN pad overlay is used to collect PIN data, and criminals can clone the ATM card and steal a customer's money.

Combat skimming with new anti-skimming technology

Skimming remains one of the most popular and well-known ATM frauds. Today, attackers are more sophisticated and are relentless in their efforts to outsmart the ATM security industry.

The SPL StopSkimmer offers a reliable, high-quality and affordable solution against deep insert skimming, digital, analogue and stereo skimming.

Security solutions that protect ATM's from hackers and cybercrime

SPL GROUP

ATM's | PARTS | SERVICE SUPPORT | CASH MANAGEMENT | SECURITY SOLUTIONS

StopSkimmer features

- Patented quasi-harmonic signal.
- The patented signal is proven to have no effect on the normal operation of the ATM.
- Works with DIP and motorized card readers.
- Works with all popular ATM and SST models.
- Dual antenna provides optimal protection against skimming.
- Face plate design is complex to replicate with 3D printers.
- Face plate has a narrow card insert slot for protection against deep insert skimmers.
- If area sensors detect cutting, dismantling of anti-skimmer or panel removal the card reader is powered down.

Add-on protection available

- Integrate with the SPL ATM Access Control Plus System for real-time remote monitoring and ATM device management.
- Capability to add a controller that manages multiple sensors to detect tilting, drilling or torching. Controller can send alarm signal to bank security or ATM monitoring system using a special software agent running on ATM's PC with an independent Ethernet port and IP address.

StopSkimmer protection

Patented quasi-harmonic signal

StopSkimmer combines the patented signal and antennas to prevent data extraction. The StopSkimmer device uses a patented non-repetitive and non-cyclical random signal. The device emits an electromagnetic field that works on frequency, it creates a noise that is both unique and constantly changing, making extraction nearly impossible.

Dual antennas - Protection against stereo, analogue and digital skimming

The antennas are pre-positioned on the device to eliminate the risk of improper installation or movement during maintenance. The antennas are situated at different distances and angles from the skimmer's magnetic head, preventing the recording and processing of stolen data. Both antennas emit a patented algorithm and unique method to create a quasi-harmonic signal modulated by a noise signal. As a result, it is difficult to near impossible to reproduce the field.

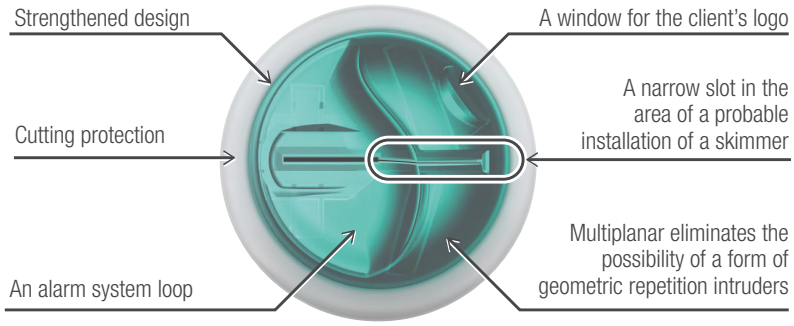
Unique multi-planar shape - Protection against deep insert skimming

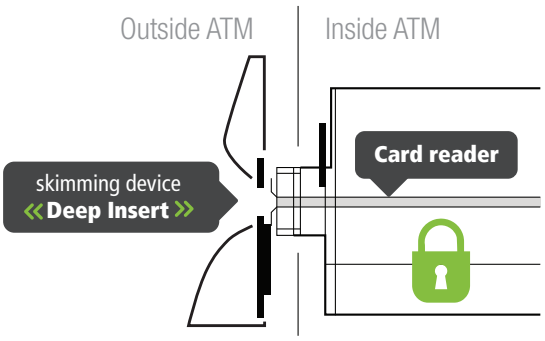
Deep Insert Skimming requires the use of excess space in the card slot to install the deep insert skimmer. The StopSkimmer's face plate card insert slot is narrow, preventing the ability for deep insertion. In addition, the complex shape of the face plate makes it difficult to secure an overlay skimmer. While replication is possible, the complex design deters criminals.

Multi-vendor solution - works with DIP and motorized card readers

The StopSkimmer solution is not card reader specific and works with all popular ATMs and SSTs.

Protection from «Deep Insert» skimming devices





Protection from "Stereo Skimming" devices

Stereo skimming uses two read heads working in tandem to steal card data. One read head records the jammer's noise and the other read head records the card data with the jamming noise. By process of elimination, if the attacker has both pieces of information, they can isolate card data. They isolate the signal from the jamming noise by looking for patterns in the signal. The criminal seeks a pattern it can extract. Extraction is easier with any signal that repeats when being read.

The StopSkimmer prevents the fraudulent card reader to read information by its patented quasi-harmonic signal modulated by a noise signal. The StopSkimmer is equipped with two antennas. Together the signal and the antennas work in tandem to create an electromagnetic field that changes the noise. The noise (wave frequency) is both unique and changes and prevents the fraudulent card reader from extracting card data.

Security Bonuses - Stop attacks in their tracks with self checking methods

1. The StopSkimmer device over a timed cycle monitors the interference between the two antennas. If the antenna interference is not working well, a notification is sent to power off the card reader.
2. An intelligent function calibrates the ATM area sensor frequently, offering additional protection if an attacker powers down the ATM.

Even EMV chip cards require anti-skimming protection

While EMV chip cards cannot be cloned, as long as they contain the magnetic stripe, the customer data can be compromised.

We invite you to attend one of our technical or information sessions by emailing sales@spl.net