PROTECT YOUR CUSTOMERS AND YOUR BRAND FROM SKIMMING ATTACKS

ACGWORLD.COM

Every day you can read about ATM's being skimmed. The Financial Institutions skimmed are often named and some have even been on the evening news. The losses are not only financial but also negatively affect the Financial Institutions reputation and brand. When a skimming attack is successful there is also a need for investigation and reporting so valuable resources are needlessly utilized.
The two most common forms of skimming attacks are "overlay" and "deep insert".

Overlay on your card reader
The criminals place an overlay on top of your card reader bezel. They also place a tiny camera somewhere on the ATM so they can record the PIN code entered. The bezel and camera are designed so they are very difficult to notice. The overlay skimming bezel is equipped with a battery and all the electronics necessary to copy card data from the magnetic stripe on the card. Once they have the card data combined with the PIN code, counterfeit cards are produced, and you and your customer are vulnerable.

Deep Insert inside your card reader
This method of skimming involves the criminals inserting a very thin skimmer in the throat of the card reader. The skimmer is equipped with battery and electronics to steal the card data from the magnetic stripe. They again install a very small camera somewhere on the ATM so they can record the PIN code entered.

Anti-Skimming solutions will help in preventing the card data from being stolen by the criminals
ACG Anti-Skimming solutions have been installed on thousands of ATMs around the world. ACG Anti-Skimming solutions are endorsed by the CBA and protect many ATM's in Georgia!

To prevent the "Overlay" card data theft method, the Anti-Skimming device detects when the presence of an overlay device has been placed on to your card reader bezel. Once detected, the Anti-Skimming device emits a "jamming signal" so that the card data can not be read. This prevents the criminals from capturing the card data they desire. This does also prevent the ATM card reader from being able to read the magnetic stripe data. However, in an increasing number of situations, the transaction can still occur for your customer if your network uses the chip on the card (instead of the magnetic stripe) for the transaction. The Anti-Skimming solution also sends an alarm signal which can be connected to your alarm system for reporting and proactive removal of the skimming devices (overlay and camera).

ACG's solution utilizes the original ATM manufacturer bezel so there is no "different look" to your customer that might prevent them from inserting their card and completing their transaction.

To help prevent the deep insert data theft method, a physical device has been developed. The device is installed into your card reader and narrows the throat opening dimensions. The concept is if a deep insert skimmer has been inserted into the card reader throat, there is no longer enough clearance for an ATM card to also be inserted, therefore preventing the criminals from capturing the card data they desire.

For more information or an assessment of your current ATM fleet, please contact Tracy Dobson at Tracy.Dobson@acgworld.com.

Tracy Dobson
Account Manager
ACG
A CBA Endorsed Member Company