Why EMV-Compliant ATMs Need Anti-Skimming Technology

Although the chip on an EMV card can't be cloned, EMV cards will remain vulnerable to skimming so long as they contain magnetic stripes. As part of the migration to EMV, ATM deployers should think about installing EMV-compliant card readers that contain anti- skimming technology.

Globally, skimming costs the card industry around $2 billion a year, according to an atmAToM.com blog published by Long Beach, Mississippi-based ATM manufacturer Triton Systems. The U.S. Secret Service estimates that the cost of an ATM skimming incident in the U.S. has risen to $50,000 on average, up from $30,000 a few years ago.

The U.S.

Criminals have been ramping up skimming attacks at ATMs in the U.S. before the U.S. cards industry updates its card base to EMV and the ATM industry completes its EMV migration.

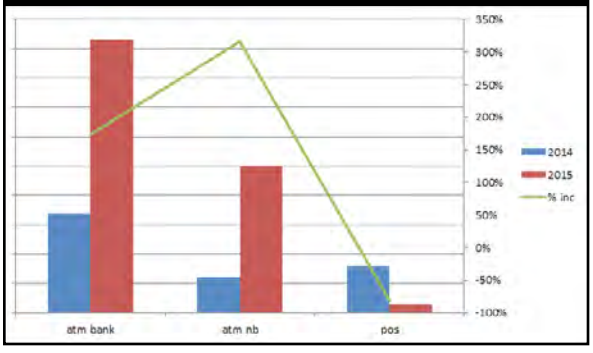
MasterCard and Visa have respectively set October 2016 and October 2017 as the deadlines after which counterfeit card fraud liability will shift to ATM acquirers that don't accept MasterCard- and Visa-branded EMV cards at U.S. ATMs. Once these deadlines have passed, if an EMV card is used fraudulently at an ATM that doesn't support EMV, the acquirer will

Once these deadlines have passed, if an EMV card is used fraudulently at an ATM that doesn't support EMV, the acquirer will be liable for the issuer's fraud losses.

U.S. merchants were required to upgrade their POS devices to EMV by October 2015 or risk becoming liable for fraud involving EMV cards.

In May 2015, U.S.-based credit-scoring and fraud analytics firm FICO warned that cardholder data theft at U.S. ATMs had reached its highest peak in over 20 years. According to a FICO report, between Jan. 1 and April 9, 2015, debit card data theft rose by 174 percent at bank-owned ATMs compared to the year-earlier same period and by 317 percent at non-bank ATMs. However, during the same period, card data theft at POS terminals in merchant locations dramatically declined by 81 percent.

CARD & PIN POINTS OF COMPROMISE CASES



Cardholder data theft at bank-owned ATMs in the U.S. and at non-bank U.S. ATMs rose by 174 percent and 317 percent respectively between Jan. 1 and April 9, 2015, compared to the year-earlier same period.

Source: 2015 FICO® Card Alert Service

In July 2015, NCR issued a security alert about the risk of skimming at ATMs in the U.S. and Mexico.

ATM users are most concerned with the threat of skimming at ATMs in the U.S., according to a recent survey by Synergistics Research, "Expanding the Role of ATMs." When ATM users were asked to identify their concerns regarding usage of ATMs, illegal devices put on ATMs to steal personal information and PINs elicited the widest response, with over eight in ten expressing concern, Norcross, Ga.-based Synergistics says.

ATM PIN capture overlay device pulled back to reveal the legitimate PIN entry pad.

Vulnerability

"The U.S. will remain vulnerable even after EMV is mandatory because mag-stripes will remain present for the first few years of EMV card-issuance," says Mark Smith, southeastern region sales manager at Marietta, Ge-based Sharenet ATM. "Until all terminals of all types are upgraded to EMV, the mag-stripe will remain as a fallback on cards. But mag-stripes can be copied and compromised."

Smith recommends ATM deployers invest in anti-skimming devices. "Even when EMV is deployed, the anti-skimming device will stop mag-stripes from being compromised," he says. "Skimming occurs heavily at gas pumps in U.S. fuel stations."

Under the card schemes' EMV migration mandates, gas stations will have until October 2017 to migrate their pumps to EMV. "Once a cardholder's card and PIN have been skimmed at a gas station, a counterfeit card can be used at an ATM to drain their account," says Smith.

PCI

The PCI Security Standards Council recommends that ATM deployers install anti-skimming technology as part of their fraud prevention practices, along with PCI PTS (PIN Transaction Security) approved components.

FICO Recommendations

- **Increased security around all ATMs**
- **Consult your local law enforcement** to coordinate police involvement for increased patrols & surveillance.
- Make an extra effort to **examine the front of every ATM** for unusual attachments that may be disguised as native equipment. Loose ceiling tiles could house hidden cameras.
- **Examine the façade of ATMs** for sticky tape or Velcro residue. The presence of similar "sticky" adhesives may indicate an ATM parasite was attached.
- It may be helpful to **photograph ATMs** to aid in physical security inspections.
- Card skimming time ranges are largely authenticated through video surveillance. **Test all equipment to ensure it is in working order and properly archived.**
- **Contact law enforcement and FICO® Card Alert Service** if you suspect your ATM has been tampered with.

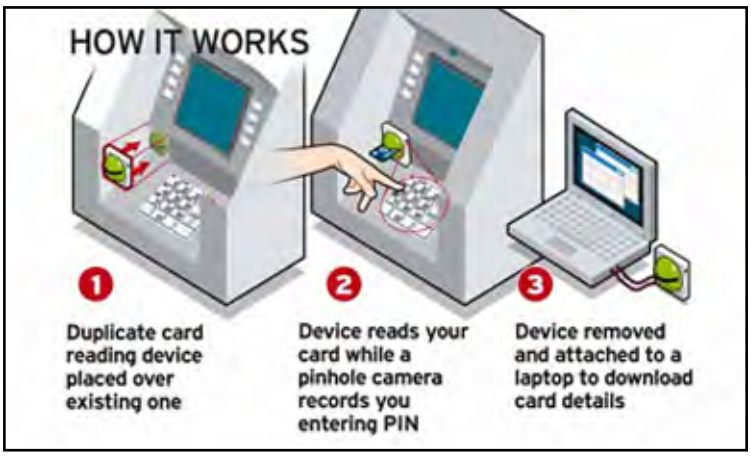
Source: FICO® Card Alert Service

In its Information Supplement: ATM Security Guidelines, the PCI SSC says: “An ATM should be equipped with an anti-skimming device according to at least one of the following anti-skimming methods:

- The device is able to prevent attachment or placement inside a card reader of a skimming device or a partly or completely fake ATM front on a card reader. Such an anti-skimming device should be equipped with active removal and modification detection functionality to shut down the ATM when activated;
- The device is able to detect attachment of a skimming device or a partly or complete fake ATM front on a card-reader. Such an anti-skimming device should be equipped with a detection functionality to shut down the ATM when activated;
- The device is able to disturb the reading of the magnetic stripe by attached devices whenever a card is entered into the card reader;
- The device is able to detect or prevent the placement of a skimming device in between the fascia and the reader (e.g., with internal/motorized readers).”

Types of Skimming Attacks

There are three types of ATM skimming attack: externally-mounted digital or analog attacks, and eavesdropping attacks inside an ATM.



“In a digital skimming attack, criminals place a device on an ATM’s card reader which looks like a card reader and copies the data when the card is passed through the device,” Triton says in an atmAToM.com blog. “The data is stored in the skimmer’s memory and is downloaded to a PC where it can be read and used to make fake cards. In an analog skimming attack, criminals record the sound of the card’s data signal during the transaction. The data is retrieved from the recording and used for fraudulent purposes.”

It is conceivable that a fraudster could disable an ATM’s EMV card reader so that it defaults to reading mag-stripes, and then attach a skimming device.

Douglas Russell, director of U.K.-based DFR Risk Management, as saying that anti-skimming devices have been extremely successful in distorting card data, making it more difficult for criminals to extract card data. Russell says ATM skimming devices which use a form of electromagnetic signals to distort or jam the data are a very good defense against digital and analog skimmers.

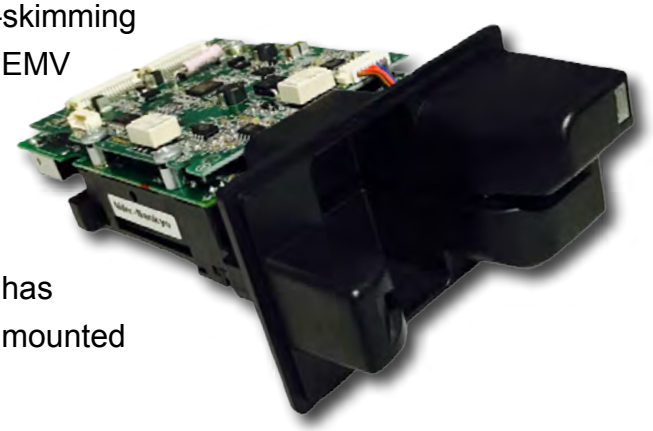
As an alternative to external skimming devices, fraudsters may place internal eavesdropping devices to collect cardholder data from inside the ATM.

ATM skimming devices which use a form of electromagnetic signals to distort or jam the data are a very good defense against digital and analog skimmers.

– Douglas Russell
DFR Risk Management

Anti-Skimming EMV Card Reader

Triton is offering its customers an upgrade to its new anti-skimming EMV card reader. Customers that have a Triton-supplied EMV card reader in working order, can return it for a credit towards the new anti-skimming EMV card reader.



The dip-style anti-skimming EMV card reader offers detection, jamming signal interference and encryption. It has the ability to detect a parasite device such as a skimmer mounted on top of the card reader.

If such device is detected, the ATM will go out of service, and report the incident to its remote monitoring system. Along with detection, when a card is inserted into the card reader, jamming signals interfere with the ability of the skimmer to read the mag-stripe. Moreover, the card reader encrypts the mag-stripe data to defeat an eavesdropping attack inside the ATM.

“Although the EMV mandate took place in October 2015, skimming is still a major issue in the ATM industry as the use of mag-stripe/chip cards is still prominent within the U.S. and will continue to be prominent for years to come,” Triton says. “It’s important for the technologies to remain one step ahead of the criminals in fighting the war against skimming.”

“Through the years of studies, tests and an ever-changing world, eliminating skimming attacks will remain a constant battle,” Triton says. “With the help from partners and advanced technology, we will continue to provide better solutions that are safe and bring a peace of mind to the client and ultimately the end user.”

Need More Info?

Triton Customer Service
1 (888) 728-4866
sales@triton.com
www.TritonATM.com