

# ADT Anti-Skimming Solution Helps Prevent Growing Card Fraud Problem

Card skimming is a high-tech way for savvy criminals to capture personal data from the magnetic stripes on credit, debit or ATM cards and even driver's licenses or passports. The problem has expanded worldwide with reports of skimming across the U.S., Europe, Russia, South Africa and Australia.

Losses from this electronic crime dwarf the losses from a typical bank robbery and are much harder to investigate. The U.S. Secret Service reports \$8.5B in annual U.S. credit card fraud losses, including ATM skimming. In Europe, losses are estimated at more than 350 million euros a year. More than 3 million victims reported an ATM skimming crime, with a cash loss average of \$1000 per incident. Far more than the monetary losses, however, are the reputational damages financial institutions incur with their ATM customers.

It's no surprise that skimming losses are growing, given the world's 1.5 million ATMs and similar numbers of retail Point-of-Sale devices in stores and petrol station pumps. All thieves need is a palm-sized electronic reading device called a "skimmer" that can be bought over the Internet. They then create a housing for the device that installs over the ATM's card reader or the ATM's entire front fascia. When unknowing customers insert their bank cards, the skimmer reads their card information without the cardholders recognizing that their personal financial information has been compromised or stolen.

Illegal skimming devices can capture data on up to 2,000 cards. Criminals often hide tiny wireless video cameras along with the skimmers, so they can also record the customers' personal identification numbers. Once a card is swiped through a skimmer, personal information contained on the magnetic strip is read and stored on the device or transmitted wirelessly to the criminals. With the card data, they can conduct transactional fraud, create new credit cards with the stolen identity and personal information, or sell the cardholder data on the black market.

In 2007 ADT first began to offer anti-skimming technology, known as CPK (Card Protection Kit), for bank ATMs in Europe. In March 2009 ADT will offer a next-generation solution to North American financial institutions to help them protect their sizeable ATM networks.

The [ADT Anti Skim™ ATM Security Solution](#), incorporating proven CPK technology, not only helps prevent skimming attacks from taking place, but also helps detect and alert the presence of skimming devices on ATMs. The solution installs inside an ATM and emits a constant electromagnetic pulse that can prevent card-skimming devices from successfully reading a card's magnetic stripe data.

In case of an attack, ADT Anti Skim™ ATM Security Solution's helps provide added protection by integrating a specific alarm signal and/or video surveillance sequence to invoke a timely response from ADT's or the bank's own monitoring command center.

One advantage of the ADT Anti Skim solution is its universal effectiveness. CPK anti-skim technology functions with all ATM types and any ATM make or model, no software upgrade is needed, and there is no interruption of ATM service. Installation is relatively simple, with no external signs of the solution at work. Most important to the growing retail banking ATM networks, the solution promotes the mitigation of the crime of ATM card skimming, helping safeguard ATMs and especially ATM customers from loss and fraud.

ADT's anti-skimming solution portfolio features a wide range of models, depending on the ATM or sales terminal needing protection. All models are modular and can be upgraded to provide additional levels of protection. [Learn more >>](#)

For more information, contact your ADT representative.