



Stopping Skim Scams

ATM makers are pushing new technologies to thwart skimming devices. Some banks are buying; some are not. BY REBECCA SAUSNER

Most U.S. banks—and their CISOs, for that matter—are loath to say anything publicly about security measures, for fear they become a high-profile target of either criminals or regulators. The story is the same for losses attributed to ATM skimming, and efforts to combat them.

But the problem is much larger and more talked about across the Atlantic. In 2005, UK banks reported 95 million pounds (\$175 million) lost to skimming, according to the Association of Payment and Clearing Services. Tesco Personal Finance is hoping to get out in front of the issue, at the very least from a public-relations perspective, announcing recently that it would spend three million pounds (\$5.5 million), or \$2,900 per ATM, on in-store security, CCTV and internal anti-skimming devices for its 1,900 ATMs.

The investment is necessary because just like every other kind of financial fraud, it seems, ATM-skimming bandits are evolving faster than the security measures intended to inhibit them. It used to be that when ATM owners would find a skimmer, it'd be 90 days or more before an attempt

was made to hack the accounts. These days, banks "see skimmed data in the market within hours," says Rob Evans, director of industry marketing at NCR. And where before skimmers would be left on machines for days or weeks, they're now attached for a few hours and then removed.

Part of NCR's anti-skimming strategy has been "managing the real estate around the card reader," Evans says, with the creation of a fraudulent-device inhibitor kit. The kit, which can be retrofitted onto older ATMs, works by misshaping the area around the card reader in a way that makes it difficult to attach a skimming device. NCR says CIBC, Royal Bank of Canada, and Washington Mutual are beginning deployments.

The other approach is an enhanced card drive that varies the speed at which the card is taken into the reader, causing "jitter" and preventing a skimming device from getting a clean card read.

But, Evans says, NCR's "big gun in the arsenal" is its intelligent fraud-detection tool that will constantly monitor the electrostatic profile of an ATM, looking for the

kinds of changes caused by electrostatic emissions from cameras, recording material or skimming devices. NCR will install the sensors under the fascia on the outer edges of the machine that will do a surface sweep of the device. "We know what electrostatic detail should be coming out of our CRT, from our pin pad, and we can measure and detect them," Evans says. "When the fraud artist puts a skimmer on the machine, he alters that profile."

Any deviation from the norm will prompt an alarm to sound on the machine. And therein lies the danger of false positives. "If Aunt Edna puts her purse down on the machine, we don't want to call the cops even if she has a garage door opener or cellphone in her purse, which also alter the signature," Evans says.

Diebold is also updating its ATM designs to incorporate better anti-skimming technology in its Secure Anti-Fraud Enhanced ATM. Some of the embedded technology includes a sensor in the card-reader light that can detect anything placed in front of it and video technology that can detect changes to the fascia, according to Anna Istnick, senior product marketing manager in Diebold's self-service solutions division. An integrated pin-pad shield is meant to limit the effectiveness of shoulder surfing and spy cameras.

In addition to installing better anti-fraud components to the ATMs, institutions can also work with risk-analytics vendors to predict fraud rates for any given location. CAP Index, a crime and risk forecasting company, can pair their crime statistics and other data with institutional data from other sites to "predict with 80 percent validity" how much fraud an institution can expect at a given location, says Jon Groussman, president and COO of CAP Index. These numbers can help institutions make decisions about how much to invest in anti-fraud technology or personnel at a given site. ATM makers can come up with all the enhancements they want, but institutions and other ATM owners have to spend money to reduce fraud.

This is one area in which the ATM makers have some gripes. "Financial institutions, in the whole ATM lifecycle, are interested in spending two percent on ATM security," says Istnick. "That's \$500 a year."