

RFID Credit Cards Get Hacked

Researchers have shown that names, credit card numbers and other data can be skimmed off a contactless card with the holder's knowledge.

The New York Times reports that a team of scientists in the [RFID Consortium for Security and Privacy](#) (RFID-CUSP) were able to read the names, credit cards and expiration dates of recently issued credit cards using radio frequency identification transponders to enable customers to pay without swiping their cards (see [Researchers See Privacy Pitfalls in No-Swipe Credit Cards](#)). Is the news a setback for the credit-card industry? For the RFID industry? For both?

The truth is that security is not a one-size-fits-all proposition. If I have \$10,000 in jewelry and cash in my house, it doesn't make sense to spend \$200,000 on a state-of-the-art safe, motion sensors, lasers and other gizmos found in your typical *Mission Impossible* film. Similarly, if I have \$1 million in valuables in my house, it doesn't make sense to spend \$2,000 on a simple burglar alarm.

Banks issuing the RFID-enabled credit cards decide the level of security they need on the card, based on the threat of fraud, the cost of security features on the card and the effect on transaction times. You don't want to use such heavy encryption that a transaction takes too long to make a contactless card worth using.

Credit-card industry executives quoted in the *Times* article point out that there are other security measures, besides those built into the card, in place to prevent fraud, such as software that detects suspicious purchases. They obviously believe these to be adequate, given the potential threat.

The researchers are exposing the vulnerabilities of these cards to raise awareness before people with less altruistic motives abuse them. That's fair. The credit-card industry might not react until there is a problem, but no one can say it wasn't warned.

Richard Smith, an independent security consultant with whom I correspond, points out that a switch on the card would solve the security problem. (The idea has already been [patented](#).) Only when a person turned a card on would the data on it be vulnerable to skimming. That would likely be only when you are making a transaction, and your contactless card would be no more vulnerable than a magstripe card would be when you hand it to a waiter at a restaurant.

I don't think the exposing of potential vulnerabilities of these cards is a huge black eye for the credit-card industry or for the RFID industry. Millions of people won't suddenly have their credit-card numbers exposed to thieves the way they do when someone hacks a bank's database or an employee loses a laptop with the card numbers on it. But it is likely that these vulnerabilities will need to be addressed as the technology becomes more mature and criminals start figuring out ways to abuse it.