Featured Articles Software

Credit Card Chips: Industry Grapples with Costly POS Upgrades

March 1, 2017 Phillip M. Perry Dionco Inc., The Strawhecker Group

Consumers love credit cards for quick and easy purchases. Merchants? Not so much. One big problem is fraud: Transactions with bogus plastic can drain significant sums from the bottom line.

In a move to address security concerns, the card industry has introduced plastic with embedded chips highly resistant to counterfeiting. Even so, many businesses are delaying the costly investments required to upgrade their point-of-sale (POS) terminals to read the new technology.

"By late 2016, only 44 percent of U.S. merchants of all kinds had installed chip-reading terminals," says Jared Drieling, Business Intelligence Manager at The Strawhecker Group, an Omaha-based consulting firm specializing in the electronic payments industry (thestrawgroup.com). "And only 29 percent of merchants had activated such terminals to actually accept transactions."
"Businesses are dragging their feet," says Fran Howarth, senior analyst for security at Bloor Research, Amsterdam (bloor.edu).

Stop, thief

So what's the big deal with the new chip cards? Thieves have become skilled at compromising the traditional "stripe and swipe" credit cards so familiar to Americans over the past several decades. That's because the sensitive customer data stored in the magnetic stripe is easily duplicated.

"Crooks have been creating counterfeit cards by copying the magnetic stripe," says James E. Dion, president of Dionco Inc., a Chicago-based consulting firm (www.dionco.com). And the tactic is profitable. "Until the consumer discovers a suspicious transaction on a monthly report, and reports the matter to the bank, the merchant has no way of knowing the card is bad. That's where the danger lies."
The new cards, dubbed "chip and signature," improve matters by storing customer data in a hard-to-duplicate chip instead of a magnetic stripe. New POS terminals read the chip and transmit a one-time-only code to the bank, which approves the transaction and returns an authorization. Because the transmitted data is invalid for any future transaction, criminals gain nothing by stealing it.

That's a big change from the old stripe and swipe cards, where each transaction involved nothing but a straightforward check against a banks' negative database. If no stolen number was discovered, the transaction was accepted. In the meantime, crooks could obtain customer data while it was being transmitted to the card processor or while it was stored on the merchant's computer. Either theft can lead to compromised cards, causing an inconvenienced public to become angry at, and stop patronizing, a resort they no longer trust.

Resort liability
If the new technology sounds like a good way to reduce customer ill will, there's an even bigger motivation for resorts to upgrade: avoiding liability for fraudulent charges. "With the old stripe and swipe cards, merchants were not responsible if someone used a fraudulent card," says Dion. The rules have changed. "Now the merchant without certified and tested chip-reading POS terminals is on the hook." (A merchant's liability for fraudulent transactions made over the Internet remains unchanged.)

Of course, it's difficult to quantify the potential costs of a change in any one resort's risk profile. And against that uncertainty must be weighed what can amount to a significant financial outlay to get new equipment installed. "One terminal might cost you a few hundred dollars," says Paul A. Rianda, an Irvine, Calif.,-based attorney specializing in the bankcard industry (riandalaw.com). "But if you have a whole system that needs to be replaced, you might need to spend tens of thousands of dollars."
To that, add the time required to negotiate with equipment vendors and make sure the new system is working correctly. "Bear in mind that the transition can be complex and time consuming," says Drieling. Merchants must not only arrange to have the equipment installed, but must also have the hardware certified and then tested."

There's one more reason to resist an upgrade: Another costly investment may be required down the road if the card industry opts to switch to a so-called "chip and PIN" system that requires customers to verify themselves with a numerical code rather than a signature.

Used throughout much of the world, chip and PIN has the great advantage of making it much tougher for a crook to use a lost or stolen credit card. A thief would have to know the secret PIN code, rather than scrawl an all-too-common illegible signature to facilitate a fraudulent transaction. "Why we didn't go chip and PIN right away is a real head scratcher," says Dion. "There is only a very slight difference in the hardware. Ultimately the industry will go that direction, because merchants are not trained to be handwriting analysts."

Mobile future

Despite all the controversy, arguments about the new technology may be moot a few years hence. Many merchants have already started to invest in the next level of digital transactions: mobile payments. The move is driven by consumer preference: "Customers have become accustomed to using Google wallet and Apple Pay," says Dion. "Their mobile devices are extensions of their arms."

Many observers expect mobile payments to become the dominant transaction method over the next five to 10 years. "By that time," says Drieling, "merchants might well be asking themselves, 'Do we need a chip terminal at all?'"

In the meantime, though, resorts must continue to grapple with the shift to the latest forms of customer protection and transaction processing. The risk of liability for fraudulent transactions must be balanced against the time and cost required to upgrade equipment and the need to plan for additional improvements down the road.

Even so, the decision to upgrade POS equipment may depend less on these fine points of analysis and more on consumer pressure. "Customers judge merchants partly by their level of technology," says Dion. "Even though customers are not liable for fraudulent transactions, when they see outdated POS equipment they are likely to ask themselves, 'Why is this business not protecting my personal data?'"