

Jan 13, 2012

AS U.S. CHIP ADOPTION ADVANCES, VISA PROVIDES GUIDANCE

We've received a lot of positive feedback since [Visa announced a roadmap](#) for the U.S. adoption of EMV chip cards and NFC-enabled mobile payment devices. There's growing consensus in the industry that it makes a lot of sense to encourage investments in chip technology. That's because it adds a layer of safety to transactions, through the use of dynamic authentication, as well as enhances international card acceptance. And it helps to build an acceptance infrastructure to support mobile payments.



Along with this support, we've also received a lot of questions from people in our industry on how best to implement these technologies. We've pulled together a set of [recommended practices](#) customized for the U.S. to answer them, drawing on our many years of experience deploying chip technology in other parts of the world.

One thing that's clear from the questions is that there's a lot of confusion around the myth that EMV means "chip-and-PIN." It doesn't in many countries, including the U.S. That's because, in the U.S., we can rely on online processing where transactions are transmitted in real-time to the issuer for approval. With that in place, there's no need for the offline authentication that was the genesis of chip-and-PIN.

Here's what Mercator Advisory Group analyst George Peabody [recently wrote](#) about this: "In the United States, in our 100 percent online environment, there is no business case or requirement for offline PIN transaction support." We agree. In fact, as a late adopter of EMV, there's a great upside for the industry in the U.S., because we can avoid much of the cost and complexity involved in deploying older-generation chip cards, while still reaping all of the benefits of reduced counterfeit fraud.

The key is to implement a streamlined, online-only version of EMV chip. At the time EMV was created, the cost and complexity of connecting a merchant POS device to some telecommunication networks was prohibitive. The way around that was to introduce "floor limits" and create a magnetic stripe alternative – EMV chip-and-PIN – as a counter to potential fraud.

Of course, we all know how much telecommunications has changed since EMV was conceived in 1994. Online authorization is now practical in much of the world (less than 7% of transactions in Europe today rely on offline authorization). And in the U.S., our telecommunications system means we can rely on online processing that is fast, and where transactions are routinely analyzed with our real-time fraud scoring system prior to issuer review. By adding the dynamic cryptogram of the EMV chip to online authorization, we'll increase transaction safety even more, yet without the more complex and expensive cards, terminals and processing capabilities that are needed to support offline authorization.

Visa will continue to support a range of cardholder verification methods (CVMs) with EMV chip, including signature, online PIN and no-signature for low-value, low-risk transactions. In the longer term, we expect the industry will reduce or even eliminate its use of static verification methods, such as signature and PIN in favor of new and dynamic forms of cardholder verification.

For those who choose to deploy online PIN, it's important to remember that newly deployed PIN entry devices must comply with [industry standards](#) to ensure the security of sensitive PIN data. Merchants and acquirers should follow security practices to prevent payment device tampering and data compromises that may put valuable cardholder data, especially PINs, at risk.

As the U.S. payments industry takes initial steps to adopt chip technologies, we hope our recommended practices will help financial institutions and merchants make informed decisions as they plan their implementations and evaluate competitive vendor offerings.

More information on Visa's U.S. EMV chip roadmap is available at www.visa.com/cisp.