Signature Card Services' Sales Agent Newsletter

SigALERT

August 2013

WILL EMV SAVE US FROM FRAUD?

by Cliff Teston
President/CEO, Signature Card Services

Despite the hesitation by US merchants and financial institutions to fully adopt EMV migration, the reality is that by 2015, we will be joining most of the global community with EMV integration. Though you may see this as a cause to worry, it is important to remember that EMV will essentially reduce fraud – and who doesn't want that?

The idea behind the security of EMV cards is that fraudulent purchases are much harder to pull off with the "smart chip" that is nearly impossible to clone. While conventional magnetic stripe technology reveals card information with one quick scan, chip cards require dynamic verification and hold a lot more information within the chip, making life harder for fraudsters.

So, once every U.S. merchant has an EMV terminal and every consumer carries a smart card, will credit card crooks be out of business?

The answer is complex, given the experiences of other countries with EMV conversion.

Two things are certain, however. First, EMV will bring about a reduction in counterfeiting and lost/stolen fraud in the U.S. Second, EMV is coming, and we must be ready and able to pave the way for a smooth transition. It is time for merchants to prepare by re-focusing now the tried-and-true basics of fraud prevention and embracing new methodologies as they become available.

Fraud migration and displacement

EMV has been widely adopted around the world, and now that the U.S. transition is underway, networks are beginning to implement their own EMV migration plans.

While fraud patterns before, during, and after EMV migration have varied from country to country, there are common threads. Typically, fraud has surged in the card-present environment prior to migration deadlines, and then drops dramatically after the EMV cards are introduced. I wish I could tell you that all fraud disappears completely once EMV is in place, but sadly there is no "perfect protection" against crooks. Historically, what has ended up happening is that fraud shifts to overseas and CNP transactions where EMV cards don't offer the same protection as they do in face-to-face encounters. In France, for example, the new standards significantly reduced counterfeit fraud but resulted in a commensurate increase in CNP scams. In the UK, overall fraud for both transaction environments actually increased during the changeover period until additional authentication measures were introduced.

Preparing for what's next

Migration to EMV in the U.S. has been slower than elsewhere, and what the impact will be here is hard to predict. But "watch and wait" may not be the best strategy. Those who are slow to adopt the technology may put themselves at risk, as counterfeiting schemes will naturally surge toward the most vulnerable transactions and merchants.

And for CNP merchants, EMV has a different set of issues. If history is any guide, CNP merchants will likely see fraud increase as face-to-face fraud falls, following the EMV adoption.

Unfortunately for CNP merchants, authentication requirements add friction to the online checkout process. Monitoring and balancing conversion rates of authenticated transactions against overall fraud rates will be a key practice for merchants seeking to maintain revenue while mitigating an increasing amount of fraud. Those merchants may wish to enforce policies in real-time using risk-scoring and categorization (high-value tickets or affiliate-based traffic sources may be good categories) to determine the appropriate situations in which to require authentication, while allowing low-risk carts or customers a more streamlined checkout.

Face-to-face merchants should now bolster their card acceptance protocols in preparation for any surge in counterfeit and lost or stolen card fraud as the deadline approaches. The most low-tech practices like examining signatures and photo IDs – while imperfect – remain simple and effective deterrents to scammers seeking low-hanging fruit.

As for CNP merchants, it is likely wise to prepare now for a wave of threats. Simple and proven protocols like requesting CVV/CID codes should be a given. Gateways should authenticate IP addresses. In France and the UK, the surge in CNP fraud was brought largely under control by moving to 3D Secure practices such as remote PIN entry. 3D Secure (comprising Verified by Visa and MasterCard SecureCode) is a payer authentication protocol that enables cardholders to create a PIN that can be confirmed by the issuing bank during an online transaction.

From biometric fingerprinting tools for home PCs and mobile devices to "social fingerprinting" solutions that authenticate consumers by analyzing their social data from sites like Facebook, new solutions for verifying CNP practices will continue to emerge as online transactions become the preferred target for crooks.

It is likely that some of the fraud experiences of other countries will play out here as the U.S. migrates to EMV technology. It's also likely we'll face some surprises. All of which makes it crucial to shore up the fraud mitigation tools we already have in both CP and CNP environments. We must put tried-and-true protocols in place now and support the innovations of the future.

For agents, the task at hand is to fully educate and support merchants during the transition phase and beyond, ensuring they (and their cashiers) understand and embrace the new processes while adhering to security fundamentals. These new standards will ultimately be a good thing for reducing fraud in the U.S., but there will be bumps in the road. Awareness, education and vigilance will help us all make the transition as smoothly as possible.

Invitation-only Webinar Tuesday August 27th at 10am PDT

- A never-before-seen door opener that wins the account automatically
- A bundling tactic that makes your accounts switch-proof
- Add more revenue to every new account without any work

To RSVP, Contact Christina or Halima
at 888-334-2284
or email marketing@signaturecard.com

Forward your questions or comments regarding this newsletter to marketing@signaturecard.com