TSYS® People-Centered Payments

White Paper

# Cardholder Verification Method (CVM)

## Considerations In A Changing Payments Landscape

We're quickly approaching the liability shift that puts the financial burden resulting from fraudulent use of counterfeit, lost and stolen cards on merchants and acquirers instead of card issuers. This shift will serve as the major impetus for U.S. adoption of the EMV (Europay, MasterCard, and VISA) standard—the globally-accepted approach to payment security based on smart card technology by both issuers and merchants.

With the migration to EMV comes many technology and process-oriented changes to the payment acceptance environment, not the least of which is the preferred cardholder verification method (CVM). Merchants, VARs and integrators play a role in ensuring changes to CVMs are seamless and efficient at the point of sale (POS).

### The CVMs that EMV supports are:

- Online PIN (personal identification number) for credit or debit transactions, in which the PIN is electronically sent to and validated by the card issuer. The potential PIN requirement for credit transactions where a PIN pad is present is new with EMV, and will inevitably require some degree of explanation to the consumer at the POS.
- Offline PIN, whereby instead of sending the PIN to the issuer, the PIN entered by the consumer is matched to that on an application housed on the EMV chip card. This functionality is exclusive to EMV card transactions. The authorization request may still be sent to the issuer.
- Signature, just as it is used today for magnetic-stripe card transactions.
- No CVM in low-dollar transactions, at merchants in low-risk categories, such as fast food, convenience and grocery stores. In this situation, an issuer-set transaction threshold allows the consummation of a sale without cardholder verification. As both card-based contact and contactless payment usage grows for low-dollar transactions, the frequency of no-CVM (i.e., no receipt-based signature required), transactions will increase as well.

The primary benefit of EMV is the near-impossibility of counterfeiting the chip in the EMV card. When the issuer authenticates an EMV card, the likelihood that the card is counterfeit is extremely low. Counterfeiting, however, is not the only means of card fraud. That's where the CVM comes in.

If a stolen chip card is used at a POS terminal that does not require a PIN CVM, the issuer will simply authenticate the card and approve the transaction. The theft victim bears the burden of reporting the stolen card and deeming subsequent transactions fraudulent. The chip card, if used without any CVM, cannot prevent fraud associated with lost or stolen cards.

Of the four general methods previously outlined, offline and online PIN are the most secure. Because the authentic cardholder is presumably the only person who knows the PIN associated with their card, when the chip card is coupled with the PIN CVM, the resulting dual transaction authentication proves a secure approach. In fact, where the chip and PIN transaction process has been widely implemented (i.e., virtually everywhere but in the U.S.), a significant reduction in both lost and stolen and counterfeit card fraud has been seen. That's why card fraud activity has migrated to the U.S. en masse.

In the EMV environment, chip cards are typically personalized with multiple CVMs—depending on the payment brand's guidelines and issuer preferences. This chip-based "CVM list" delineates the issuer's choice of supported CVMs in order of priority. Because different types of terminals support different CVMs, multiple CVMs ensure EMV card acceptance at as many merchant terminals as possible. The card and the terminal simply

use the first matching CVM type to authorize a transaction. For example, if an EMV credit transaction calls for PIN entry but no PIN pad is present, the chip might default to signature CVM instead. The chip-based CVM list also contains logic that enables the issuer's choice to either attempt or deny the next matching CVM type if the first attempt fails.

With that said, the card brands show some variance of opinion on which CVMs—or combination of CVMs—they choose to advocate. While PIN-based CVMs are more secure, they're harder for issuers to implement. Because EMV helps prevent counterfeiting, which Visa sees as the bigger problem, Visa advocates for a combination of chip and signature in an effort to speed the migration to EMV. For its part, MasterCard prefers PIN-based methods because they better mitigate the risks associated with lost or stolen cards. Most security experts agree that it is unrealistic to rely on a store clerk's ability to compare a receipt signature to the signature on a card in order to detect fraud.

Understanding CVM is all about the variables. Varying thresholds for verification requirement, CVM list preferences—and most notably the potential for a cardholder to be prompted for a PIN to conduct a credit transaction—make it incumbent on the merchant to prepare their frontline associates for EMV.

To learn more about EMV and get the facts on what merchants need to know now, download our comprehensive white paper on the topic here.

TO LEARN MORE

contact +1.480.333.7799
or email acq-sales@tsys.com.



© 2013 Total System Services, Inc.® All rights reserved worldwide. Total System Services, Inc., and TSYS® are federally registered service marks of Total System Services, Inc., in the United States. Total System Services, Inc., and its affiliates own a number of service marks that are registered in the United States and in other countries. All other products and company names are trademarks of their respective companies. (07/2013)