Chip Payment Acceptance

Putting it Into Perspective for Small-Ticket Unattended Merchants

Whatever the retail merchant size or type of business, EMV chip payment processing can offer greater protection against fraud and increase consumer confidence in the payment system.

As the U.S. migration to EMV® chip continues, merchants who are not yet supporting chip processing are encouraged to carefully assess their point of sale (POS) environment in an effort to weigh the costs and benefits of upgrading/replacing their existing system capabilities.

This is especially important for small-ticket unattended merchants with low-value, low-risk transactions (e.g., parking meters, laundromats, car wash terminals, etc.). Before making any chip terminal hardware or software decisions, merchants in these segments need to clearly understand the what, why, and how behind EMV chip processing to select the right solutions for their business.

As with any large-scale payment infrastructure change, merchants can often receive mixed and sometimes confusing messages from outside sources. With chip payment technology, any kind of misinformation can lead to invalid assumptions and ultimately faulty business decisions.

Myth vs. Reality

The following chart addresses some of the most commonly held myths about EMV chip payment acceptance in the small-ticket unattended merchant environment.

Myth	Reality
All U.S. merchants must be set up to accept chip payments by 1 October 2015.	U.S. merchants are not required to support chip processing. However, **effective 1 October 2015**, the Visa global POS counterfeit fraud liability shift will be instituted in the U.S. With this liability shift, the party that, due to their lack of chip technology, is the cause of a contact EMV chip transaction not occurring (i.e., either the issuer or the merchant's acquirer) will be held financially liable for any resulting card-present counterfeit fraud losses. • Issuers retain counterfeit fraud-related liability if they do not issue chip cards. • Conversely, acquirers assume counterfeit liability if the magnetic-stripe data from a contact chip card is copied and used at a non-contact chip terminal.

*Europay, MasterCard®, and Visa® (EMV)

Myth	Reality
U.S. merchants that choose to upgrade their terminal to support EMV chip payment acceptance must install a PIN pad.	Small-ticket unattended merchants must support the processing of transactions without a Card Verification Method (CVM)*. Unattended merchants are not required to support PIN acceptance. However, if the chip card is presented that supports PIN, and if the unattended terminal has a PIN pad, the transaction must be processed with a PIN, if requested.
All U.S. merchants are going to have to invest in chip technology. The magnetic-stripe is going away.	All Visa-branded chip cards will include a magnetic-stripe on the back. Currently, there are no specific plans in place to eliminate the magnetic-stripe.
Small-ticket unattended merchants that opt to accept EMV chip payments will lose the "No Signature Required" program advantages they have today.	EMV chip payment acceptance does not impact the "No Signature Required" or the Visa Easy Payment Service (VEPS) program. It will continue to operate in the same manner it does today in the magnetic-stripe environment.
Merchants that process EMV chip card transactions do not qualify for the Custom Payment Service (CPS).	EMV chip payment acceptance does not affect small-ticket unattended merchant CPS transaction qualification criteria or interchange rate reduction rules.

Thinking About Implementing Chip?

Where to Start

How and when you proceed has a lot to do with your existing POS system capabilities and whether you own or lease your equipment. Your acquirer has the chip validation tools to assess your EMV chip acceptance options and help you select the terminal hardware and software that are right for your business and meet all EMVCo and Visa standards. Though not required, small-ticket unattended merchants who are thinking about implementing chip technology in their locations should also consider the following key factors.

Dual-interface Terminal Reader Implementation

If you are going to go through the expense of implementing or upgrading your card readers, you should also consider implementing dual-interface terminal readers so that you can support contact and contactless chip acceptance. There are four key reasons why this makes good business sense:

- Generally, there is minimal incremental hardware cost, if any.
- The message formats are the same for contactless quick Visa Smart Debit and Credit (qVSDC) and contact EMV chip.
- The global POS counterfeit liability shift does not apply to contactless transactions. Merchants are protected from counterfeit chargebacks made under the EMV Liability Shift if they have deployed EMV approved contact chip-enabled terminals. An EMV terminal can either be contact-chip only or support both contact and contactless chip interfaces (a.k.a. "dual-interface"). Dual-interface terminals do provide counterfeit liability protection whereas contactless-only terminals (lacking an EMV contact-chip reader) do not.

Dual-interface terminals are able to process chip transactions from various payment products including contact chip cards, Visa payWave (contactless), mobile devices and wallets, and magnetic-stripe cards.

- Issuers are liable for all online authorized fraudulent EMV chip transactions (contact and contactless) that originated at an EMV-capable unattended terminal (excluding ATMs) that supports the processing of transactions without a CVM.

If you are planning to deploy new Visa payWave-accepting contactless readers, you must ensure that your devices comply with the Visa Contactless Payment Specification 2.1 or higher.

For More Information

For more information about EMV chip payment acceptance, please contact your acquirer merchant relations representative.

* All newly deployed chip-enabled (contact and contactless) unattended terminals that are not replacements must be able to process transactions without a Card Verification Method (CVM). **Effective 1 July 2015**, all chip-enabled (contact and contactless) unattended terminals must support the processing of transactions without a CVM.