What is EMV?

EMV is a series of specifications that defines a more secure method of payment. It was developed jointly by Europay, Mastercard, and Visa in the mid-1990s. The goal of EMV is to create a secure transaction between the chip cards and the terminals for both credit and debit transactions. EMV transactions are performed by a “chip” embedded on a card, that contains secure elements and performs cryptographic functions that result in a secure transaction.

When does the liability shift for ATMs?

MasterCard is the first payment brand that has published changes related to ATMs. Beginning on April 19, 2013, a liability shift takes effect to protect inter-regional issuers at U.S. ATMs. As a result, if a chip-enabled card from a non-U.S. region is presented to a non-chip-enabled ATM to perform a Maestro transaction, the Acquirer assumes counterfeit fraud-related liability.

| April 2013 | Processors must support EMV |
| April 2015 | 3rd Party ATM must support EMV |
| October 2015 | Liability shift of counterfeit transactions |
| October 2017 | Liability shift for AFD |

©Copyright 2013 Vantiv, LLC. All rights reserved.
**Are my ATMs EMV capable?**

ATM owners will need to upgrade their ATM fleet to be able to process EMV transactions, in order to avoid liability for transactions conducted by international Maestro cardholders (April 2013 and later) and for transactions conducted by U.S. cardholders (October 2015 and later). To determine specifically what you need to do, you can work with your ATM service provider to do a survey of your current fleet. Upgrades will require a hardware upgrade, in many cases, as well as a software update.

Depending upon the age of the equipment, a complete replacement may be required. Items that may need to be updated by an ATM service provider prior to Vantiv making changes internally to support an EMV download include:

- EMV capable card reader – Motorized or Dip (Swipe is not capable)
- EMV specific certified software versions
- EMV kernel
- Adequate ATM memory

Work with your ATM service provider(s) to identify the necessary upgrades that apply to your fleet. Vantiv has currently completed, or is in process of completing, EMV certifications with the following vendors and associated types of software:

- NCR – Edge Standard
- NCR- Aptra Advance (AANDC)
- Diebold – Agilis

Once all certifications are completed, we will publish the specific software and Kernel versions for your reference. Above certifications are all expected to be completed by May 2013. Once you have a plan in place for your EMV strategy, let your Vantiv Relationship team know that you want to enable your machines for EMV and your expected timeline. Please plan ahead as some of these upgrades / replacements could take some time.

**Will the cardholder see any changes?**

For contact EMV cards, the card will remain in the card reader until the transaction is completed. Motorized card readers will act the same as before and read both the chip and/or magnetic stripe. However, there will be a change in how a dip reader functions. It latches onto the card and reads the chip, retaining the card through the entire transaction. If the card has no chip, the consumer flow asks the cardholder to remove the card and reads the magnetic stripe as the card is removed.

**Is there anything we can do to help mitigate fraud until we upgrade all of our ATMs?**

Yes, as part of our EMV strategy, Vantiv has developed the ability to allow our Financial Institutions to set a ‘maximum withdraw limit’ by terminal, and/or a ‘maximum daily limit’ per Financial Institution to help with mitigating potential counterfeit fraud. The Financial Institution will determine the maximum value(s) to set base off of the following criteria:

- Maximum per-withdrawal limit for not-on-us cardholders
- Maximum per-withdrawal limit for International cardholders, if desired value is different from not-on-us
- Maximum daily limit for not-on-us cardholders (captured across each ACRO)
- Maximum daily limit for International cardholders, if desired value is different from not-on-us

In addition to setting limits, Vantiv has the ability notify when a ‘skimming’ device is detected at your ATMs through our monitoring tool.

Please contact your Vantiv Relationship team if you are interested in these features and determine if your ATMs qualify.