TSYS® People-Centered Payments

White Paper

When The Chips Are Down:
Understanding The EMV Safety Net

As U.S. credit card issuers and merchants move closer to the adoption of the EMV (Europay, MasterCard, and VISA) standard—the globally-accepted approach to payment security based on smart card technology—it's important to understand how the payment process will work when and if the new technology fails.

EMV cards look just like the standard magnetic stripe cards we use today. The primary difference is in the interface. EMV card payments are initiated by a chip on the card, which is read by an EMV terminal as opposed to an MSR (magnetic stripe reader). While enclosure of the chip inside an EMV card is designed to prevent damage and tampering, there is the possibility that the chip can break, or that a card could be deployed with a defective chip.

The Magnetic Stripe Isn't Going Away

For the foreseeable future, EMV cards issued in the U.S. will retain their magnetic stripes, and card readers will retain MSRs, for at least a few reasons:

- Despite the liability shift that will place the financial burden resulting from fraudulent use of counterfeit, lost and stolen cards on merchants and acquirers instead of card issuers, not all merchants will adopt EMV terminals. The magnetic stripe will enable backwards compatibility so that consumers can continue to transact in non-EMV environments.
- While the U.S. is the last major country to move to EMV, there are many smaller countries that have yet to adopt the standard. The continued presence of MSRs ensures foreigners who don't carry EMV cards will be able to transact here.
- The magnetic stripe will support technical fallback if the EMV enabled chip is unreadable. Technical fallback is the exception process whereby the magnetic stripe, rather than the chip data, is read by an EMV-capable device.

Fallback Ensures Sales, But Creates Risk

It's critical that merchants understand that in technical fallback situations, the EMV security protocols are bypassed and the security of the transaction is limited to that of a magnetic stripe. For that reason, technical fallback is controlled or may be restricted in markets where EMV has been deployed for some time.

We can expect the same here in the U.S. While technical fallback can indicate a faulty card reader or a malfunctioning chip card, it can also indicate an attempt to circumvent EMV security measures. Merchants should monitor their POS device functionality and promptly address any equipment issues. Merchants should also be aware that criminals may disable the chip in an attempt to bypass the chip-and-PIN security measures. For this reason, unattended payment devices are particularly susceptible to fraudulent attempts to force technical fallback. EMV card transactions conducted via MSR in EMV-capable environments are automatically reported to the payment networks as such. If the percentage of fallback transactions exceeds the expected average rate, the merchant could face financial penalties imposed by the card brands.

Understanding how EMV works is key to enjoying the benefits the technology brings, such as the virtual obsolescence of card counterfeiting and massive reduction in card payment fraud in general. While merchants have some incentives to comply—and incur some level of risk if they don't—the reward is well worth the effort.

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.

GET TO KNOW TSYS

AFRICA	ASIA-PACIFIC	COMMONWEALTH OF INDEPENDENT STATES	EUROPE	INDIA & SOUTH ASIA	JAPAN	MIDDLE EAST	NORTH & CENTRAL AMERICA, MEXICO & THE CARIBBEAN	SOUTH AMERICA
+27 21 5566392	+603 2173 6800	+7 495 287 3800	+44 (0) 1904 562000	+911204191000	+81 3 6418 3420	+971 (4) 391 2823	+1.706.649.2307	+55.11.3504 6600