Global Data Privacy and Security Team

Bryan Cave's Global Data Privacy and Security Team works with data security and risk assessment issues to routinely help clients before a breach happens analyze and improve upon their ability to respond to, and minimize the liability from, a breach if (or when) one occurs.

For more Information Contact:

David A. Zetoony
Partner
david.zetoony@bryancave.com
1155 F Street, N.W.
Washington, D.C. 20004
T: 202 508 6000

One Boulder Plaza
1801 13th Street, Suite 300
Boulder, CO 80302-5386
T: 1 303 444 5955

Courtney Stout
Associate
courtney.stout@bryancave.com
1155 F Street, N.W.
Washington, D.C. 20004
1 202 508 6076

To join Bryan Cave's data privacy and security distribution list visit Bryan Cave Data Matters.

BRYAN CAVE

Enhancing Security at the POS: EMV At A Glance

Over the past several years the credit card industry has been encouraging banks and retailers to migrate to EMV technology, which is sometimes referred to as "chip-and-PIN" or "chip-and-signature."

EMV, which is named after the developers of the technology (Europay, MasterCard, and Visa), is a technical standard that includes a microprocessor physically embedded in a plastic credit card. The microprocessor stores credit card data. When the card is inserted into an EMV enabled card-reading device at a retailer, the device authenticates the card using cryptology. The result is that EMV-enabled cards are harder to skim, or counterfeit.

Each of the major card brands has attempted to encourage retailers to invest in point of sale readers that are capable of reading an EMV chip by announcing changes to their card network rules, that went into effect in October of 2015, that shift more liability for credit card breaches to retailers (and their merchant banks) if the retailer does not have card readers that support EMV technology.

The following provides information relating to EMV technology :

The percentage of transactions in the United States that used EMV in 2014 (before the liability shift went into effect).[1]	The percentage of transactions in Europe that used EMV in 2014.[2]	Percentage of retailers estimated to have EMV in-place as of the October 1, 2015 "deadline."[3]
.12%	**96.6%**	**25%**

Factors retailers should consider to in migrating to EMV:

- ☑ **Fraud Liability Shift:** Beginning October 2015, card network rules shift liability for counterfeit fraud to the party in the payment chain that does not support EMV, or "chip enabled" transactions.
- ☑ **Training:** Are employees at the store level adequately trained on card "dipping", and the increased time required to complete a chip enabled transaction?
- ☑ **Vendor Agreements:** Have your vendors that access PCI data provided you with contractual commitments to meet the EMV standards within a specified time period, and to be responsible for counterfeit fraud liability in the event the vendor causes chip enabled transactions to fail?
- ☑ **EMV Standard:** EMVCo. LLC, with member organizations including American Express, Visa and MasterCard, among others, manages the global chip technology payment standard.

[1] https://www.emvco.com/about_emvco.aspx?id=202 (last viewed Sept. 2015).
[2] *Id.*
[3] Congressional Research Service, The EMV Chip Card Transition: Background, Status, and Issues for Congress (Sept. 8. 2015) at 12 available at https://www.fas.org/sgp/crs/misc/R43925.pdf (last viewed Sept. 2015).