

Publications

Client Alert: Fallout From The EMV October 2015 Liability Transfer Mandate

Related Professionals

Alycia N. Broz

Kenneth J. Rubin

Related Services

Data Strategy, Privacy and Security

Related Industries

Retail and Consumer Products

CLIENT ALERT | 7.5.2016

EMV, which stands for Europay, MasterCard, and Visa, credit cards allow card users to make purchases using a chip in the card as opposed to a magnetic stripe. The EMV chip communicates directly with the point-of-sale (POS) device when the customer makes a purchase and creates a one-time authentication code for each transaction, which prevents data from being “skimmed” (illegally copied) at the time of use, since the code constantly changes. Countries that have started using EMV technology have seen a reduced amount of card-present fraudulent activity.

The major credit card issuers set an October 1, 2015 deadline for merchants to be EMV chip compliant or there would be a potential shift in liability, meaning that whichever party, the issuer or the merchant, had the least secure technology would be liable for chargebacks and card-present fraud. Traditionally, the card issuer has always been responsible for this type of fraud; that is, fraudulent transactions that occur inside a store when a credit card burned with a stolen number is swiped. To further elaborate, for any merchant accepting credit or debit cards after October 1, 2015, if the card issued to the customer has an EMV chip installed, and the “brick and mortar” merchant has not yet implemented the accompanying chip-capable POS device thereby making use of the EMV chip unavailable, the merchant is responsible for chargebacks and fraudulent card acceptance.

Estimates after the October 1, 2015 mandate indicated that anywhere from 50 to 75 percent of merchants had not upgraded to the new technology or had purchased the technology but were not using it. [1] A survey conducted by the Stawhecker Group reported that only 27 percent of merchants were EMV capable by the time of the liability shift and that merchant adoption rates would not reach 90 percent compliance until 2017. [2]

A recent report from First Annapolis Consulting Inc. indicated that since the October 1, 2015 liability shift, there has been a significant rise in card-present chargebacks. [3] “One acquirer reported that

chargebacks were 3.8 times higher in December, all from non-EMV-enabled merchants. Another reported that EMV-related chargebacks were up 15%.” [4] These chargebacks have become, in some cases, a rather high and unexpected expense for merchants. To further compound the problem, not only do merchants have to incur the cost to upgrade to the new EMV technology, but once the EMV technology is installed, it then also has to be EMV certified. As of March 2016, there was quite a backlog in the certification process, making it even more difficult for merchants to be EMV ready and leading to hardship for merchants and the potential for litigation such as the case discussed below. [5]

A putative class action was filed March 2016 in the United States District Court for the Northern District of California alleging that the credit card networks and issuing banks engaged in anticompetitive conduct against their merchants during the rollout of EMV technology. [6] Namely, two small Florida retailers, in behalf of a putative class, asserted federal and California antitrust claims, as well as unjust enrichment claims against the major credit card networks (Visa, MasterCard, American Express, Discover, JCB and UnionPay), the major issuing banks (Bank of America, Barclays, Capital One, Chase, Citibank, PNC, USAA, US Bank, and Wells Fargo), and EMVCo, the joint entity established by the credit card networks to control EMV technology for credit card transactions.

The complaint states that historically much of the cost of illegitimate charges associated with credit card transactions have been borne by the issuing banks. However, as a condition of the EMV transition, the card networks and issuing banks have colluded to establish unattainable requirements that merchants were required to meet by October 1, 2015. If a merchant failed to meet the newly imposed EMV requirements, the merchant would be liable for illegitimate charges that were not processed using a card’s EMV chip. The complaint alleges that this “liability shift” was imposed despite the defendants’ knowledge that it would be impossible for merchants to meet the EMV compliance standards by the imposed deadline.

In addition to requiring that merchants install new EMV equipment, plaintiffs allege that defendants created a sham “certification” requirement, whereby point-of-sale equipment used for EMV transactions would need to be certified in order to be compliant with EMV standards – a process that plaintiffs allege would take years for merchants to obtain after the October 2015 liability shift. Plaintiffs claim that merchants who processed EMV transactions through the chip technology would nonetheless be subject to the liability shift for EMV-enabled purchases solely on the basis that the required certification has not occurred. The named-plaintiffs allege that they have been subject to a number of chargebacks under the liability shift even though the transactions in question were processed through a credit card’s EMV chip because the point-of-sale equipment had not been certified – a process that the named-plaintiffs claim to have no control over. Plaintiffs argue that small retailers have particularly found it impossible to be EMV compliant by the October 2015 liability shift, and the only means to prevent the imposition of the liability shift would be to stop accepting credit cards.

Based on these allegations, plaintiffs contend that defendants have conspired to shift the cost of chargebacks from the issuing banks to individual merchants through the imposition of the liability shift – namely, by creating requirements and standards that they knew that merchants would be unable to comply with by the set deadline. Plaintiffs filed a motion for preliminary injunction concurrently with the Complaint. The court denied the motion prior to responses being filed, identifying what it considered to be major deficiencies in the motion – the failure to show immediate and irreparable harm – that did not warrant the waste of resources by requiring defendants to respond.

In response to the Complaint, defendants filed a joint motion to dismiss the action in its entirety, alleging that the Complaint fails to allege the existence of a conspiracy between the individual defendants to prevent merchants from being EMV compliant before the liability shift date. The motion to dismiss is currently pending.

Recently, Visa announced new EMV chargeback rules that will remain in effect until April 2018. Effective July 22, 2016, merchants will not be liable for chargebacks under \$25; effective October 2016, issuers will not be able to charge back more than 10 fraudulent transactions per customer account.

--

[1] Taylor Armerding, "Why Have Most Merchants Missed the EMV Deadline?," (2015) *available at* <http://www.csoonline.com/article/2990207/data-protection/why-have-most-merchants-missed-the-emv-deadline.html>

[2] The Strawhecker Group, "EMV How Ready are U.S. Merchants?," (2015) *available at* <http://www.csoonline.com/article/2990207/data-protection/why-have-most-merchants-missed-the-emv-deadline.html>

[3] Jim Daly, "Acquirers Report Varying Levels of Chargebacks in the New EMV Environment," (2016) *available at* <http://www.digitaltransactions.net/news/story/Acquirers-Report-Varying-Levels-of-Chargebacks-in-the-New-EMV-Environment>

[4] *Id.*

[5] Andrew Deichler, "Post-EMV Liability Shift, Chargebacks are a Big Issue," (2016) *available at* http://www.afponline.org/pub/res/news/PostEMV_Liability_Shift,_Chargebacks_are_a_Big_Issue.html

[6] *B&R Supermarket, Inc. v. Visa, Inc.*, 2016 U.S. Dist. LEXIS 57300 (N.D. Cal. 2016).