KING & SPALDING

Client Alert

Data, Privacy & Security Practice Group

October 15, 2015

Risky Business – Five Facts You Should Know About the EMV Liability Shift

On October 1, 2015 the major payment card companies instituted the EMV Liability Shift in an effort to incentivize card issuers and merchants to migrate to using payment cards with embedded chips ("chip cards") according to the EMV standard. This shift is better characterized as an allocation of liability of counterfeit fraud to whichever party in a transaction has not conformed to the EMV standard. Card issuers can conform by issuing compliant chip cards and merchants can conform by implementing terminals that accept chip cards. Two weeks have passed since the shift was instituted and many companies have not become EMV compliant, meaning they are subject to an immediate increase in risk for fraud liability. Whether you work for a company, are a private equity fund manager assessing risk for your portfolio companies, or are brokering a deal that involves merchants or card issuer companies, these five facts will help you assess the impact of the EMV Liability Shift.

1. Chip Card Migration is Different from Compliance with Payment Card Industry Data Security Specifications (PCI DSS).

As the name suggests, chip cards are payment cards (credit, debit or prepaid cards) that have an embedded microchip. The function of this chip is to make the card more difficult to counterfeit. When a chip card is inserted into a compatible terminal, the terminal uses information contained in the chip to communicate with the transaction processors to verify the transaction. The chip generates dynamic values that are used to authenticate the card as genuine. This is an improvement over magnetic stripe technology, which was static and therefore susceptible to being "skimmed," a process where the information in the magnetic stripe could be copied and then used to create a functional clone of the card. The dynamic nature of chip cards preclude such skimming. Chip card technology could be implemented in any one of a variety of manners but major payment card companies settled on a standard called EMV. The standard is currently maintained by a body called EMVCo, which is comprised of six member organizations—American Express, Discover, JCB, MasterCard, UnionPay and Visa.

Chip card migration refers to the endeavor to migrate all payment card systems to chip card technology through compliance with the EMV standard. It is necessary for all parties including card issuers and merchants

For more information, contact:

Steven T. Snyder
+1 704 503 2630
ssnyder@kslaw.com

King & Spalding
Charlotte
100 N Tryon Street
Suite 3900
Charlotte, NC 28202
Tel: +1 704 503 2600
Fax: +1 704 503 2622

www.kslaw.com

to converge on a single standard for interoperability of cards and equipment. Chip card migration differs from the Payment Card Industry Data Security Specifications (PCI DSS). PCI DSS is a data security standard that governs the security of payment card transactions in a much broader way, applying to not only in-person transactions, but also to online and telephone transactions. The PCI DSS standard is maintained by the PCI Security Standards Council. It is mandatory for U.S. issuers and merchants because the payment card companies will impose fines or fees for non-compliance.

2. Chip Card Migration is not Mandatory in the U.S.

Unlike implementation of PCI DSS, neither issuers or merchants are currently required to implement chip cards and comply with the EMV standard. Instead, the migration is being incentivized by the polices of the individual payment card companies. One of those incentives is the EMV Liability Shift that went into effect on October 1. For example, Visa has implemented a roadmap to facilitate the migration to chip cards and supporting terminals. In 2012, Visa implemented a program that allowed merchants that upgraded their Point of Sale (POS) equipment to forgo certain assessments relating to PCI DSS validation, which results in cost savings. More recently on October 1, they, along with other payment card merchants, implemented the EMV Liability Shift as part of this roadmap.

The EMV Liabilty Shift affects the liability risk for non-migrating issuers and merchants. However, there is no requirement by any of the payment card companies that U.S. issuers or merchants must migrate to chip cards and comply with the EMV Standard at this time, making the EMV Liability Shift an incentive rather than a mandate. A company can assess the costs associated with the migration and weigh them against the increased liability risk to determine the best course of action. However, in doing so, a company should be fully informed in making that decision.

3. EMV Liability Shift Puts Liability for Counterfeit Fraud on Parties That Have Not Migrated.

According to Visa, the EMV Liability Shift means that "the party that is the cause of a chip transaction not occurring (*i.e.*, either the issuer or the merchant's acquirer processor) will be held financially liable for any resulting card present counterfeit fraud losses." In other words, if the merchant has chip card capable terminals, the issuer that issues cards without chips will be liable for any such fraud. If the merchant has not implemented terminals that accept chip cards, the merchant's processor will be liable. That liability will typically be passed by the merchant's processor to the merchant through the merchant agreements between merchants and processors. The EMV Liability Shift is therefore taking a merchant or issuer who was previously covered for fraud of this type and now allocating the risk of that liability to those who have not yet migrated.

4. Stakeholders May Not Be Aware or Understand the Risk of Not Migrating.

There are many stakeholders when it comes to a change in risk for a company. For the EMV Liability Shift in particular, many of those stakeholder may lack understanding or awareness of the issue. As outlined above, any company that is either an issuer or merchant with POS equipment has had some change in its risk profile as of October 1, 2015 if it has not migrated to chip card technology. While that risk can be reasonably quantified, it requires that the relevant stakeholders are aware of the issue and coordination from the appropriate parties to fully understand it. In the third quarter of 2015, Wells Fargo conducted a Gallup poll of Small Business owners which found that 68% of them were not aware of the EMV Liability Shift. While awareness is undoubtedly higher for larger businesses, there are many stakeholders that may not have sufficient awareness or understanding of this issue to properly assess the change in risk to the company.

As an example, to understand this risk for a particular merchant, a number of parties must be informed on this issue and coordinate. One is the party responsible for the technology used for POS transactions. They can assess the costs associated with upgrading the system. These costs not only include the equipment and labor costs, but many variable costs including training and other costs of processes and procedures for new types of transactions. For example, chip card transactions may take longer and when aggregated this may represent a significant cost to certain types of companies that process large amounts of transactions in a short period of time. This analysis may require finance and operations personnel to model the true costs of a system upgrade. Other individuals that should be involved are those responsible for handling the agreements with acquirers and processors, and can inform as to the liability allocation. They can also likely attain information as to current fraud rates. Other stakeholders within the company that should be involved are those in compliance and those responsible for managing reputational aspects of the company. If a company is part of a private equity portfolio or the subject of a deal, the stakeholders outside of the company include those that have an interest in quantifying present and future risk for the company as an asset. It is important that all stakeholders have enough knowledge and information to properly assess the risk associated with the EMV Liabilty Shift.

5. The EMV Liability Shift Creates a Dynamic Risk.

One important aspect of the EMV Liability Shift is that the risk to a company that chooses not to implement chip cards is dynamic and will likely increase over time. Cloned magnetic stripe cards are a very significant problem in the U.S. with losses from that specific type of fraud estimated at $3 Billion in 2014. While there will undoubtedly be some reduction in this fraud as merchants implement chip card terminals, it is also possible that many of these criminals will seek out targets that accept magnetic stripe transactions. While the effect of this is speculative, it could be dramatic for some types of merchants as more and more of their peer companies make the transition. Similarly, the costs associated with making the transition will likely decrease as the technology is refined and there is more competition between providers of the equipment and services. The dynamic nature of the risk and costs suggests that even if a sophisticated cost-benefit analysis is performed and the conclusion is that the company should not migrate to chip cards, this issue should be revisited periodically to make sure the assumptions in the analysis have not materially changed.

Anyone with an interest in a company should understand the EMV Liability Shift to assess whether the risks are being managed appropriately. As discussed herein, this requires coordinating a number of stakeholders to fully understand this issue. Steve Snyder is a Partner in King & Spalding's IP Group and assists clients with complex networking and data security issues. He can be contacted at 704.503.2630 and ssnyder@kslaw.com.