EMV Technology and the Liability Shift
Additional Protection but No Replacement for Strong Network Security
By Dominic Keller

The introduction of EMV\textsuperscript{1} chip card technology by credit card networks has played an important role in reducing international point of sale (POS) credit card fraud. This technology is being rolled out in the U.S., and card networks have introduced rules that, in some circumstances, shift liability for the costs of fraudulent transactions from issuing banks to merchants. Not surprisingly, this liability shift has gained significant publicity; however, the transactions affected are relatively limited. For example, the liability shift does not apply to costs arising from a network breach, only to the costs of fraudulent transactions involving counterfeit, lost or stolen cards. The cost of investing in EMV compatibility must be weighed against the potential financial burden arising from the liability shift and this assessment will vary greatly among different businesses. Understanding the implications of EMV technology and the effect of the liability shift is critical to any business accepting credit card payments through POS terminals.

Executive Summary

- The liability shift does not apply to costs arising from a network breach, only to the costs of fraudulent transactions involving counterfeit, lost or stolen cards.
- The cost of EMV adoption should be balanced against the increased potential expenses arising from the liability shift and this cost/benefit assessment will vary greatly among different businesses.

EMV technology is an anti-fraud solution, rather than a network security solution and the new rules do not transfer liability for a network breach.
As criminals seek to avoid EMV technology, e-commerce may see an increase of fraudulent transactions.

EMV technology should be viewed as an anti-fraud solution, rather than a network security solution. Maintaining robust network security to manage enterprise risk remains critically important.

**EMV Technology and the Migration to Chip Cards**

Traditionally, credit card transactions have been processed using a magnetic stripe that uses the same data, embedded in the stripe, to authorize each transaction. Instead of a magnetic stripe, EMV chip cards use a microchip that creates a unique digital code for each transaction, and payment is only authorized after the code is accepted by an EMV-compliant POS terminal. If the consumer uses a chip card, and the merchant has compliant POS terminals, it is extremely difficult for criminals to use counterfeit credit cards to monetize stolen credit card data.

The adoption of EMV technology in the United States involves consumers being issued chip-enabled credit cards and significant investment from merchants to purchase chip-enabled POS terminals to update their infrastructure. To encourage merchant adoption, credit card networks introduced a ‘liability shift,’ effective October 1, 2015. The liability shift transfers liability for some fraudulent transactions from issuing banks to acquiring banks that then can pass the costs on to merchants.

**Applying the Liability Shift**

The liability shift has gained significant publicity and many businesses are concerned about additional costs and risks associated with this change. This concern has been amplified by each card network having separate rules outlining the shift and little guidance on how the new rules will be enforced. Despite these uncertainties, the overall purpose of the new rules is relatively clear and provides useful guidance for businesses in assessing the impact of the liability shift on their bottom line.

It is important to note that the liability shift applies to the costs of individual, fraudulent transactions made at a POS terminal using a counterfeit, lost or stolen credit card. It does not apply to the costs or liabilities arising when a merchant’s network is breached and credit card data is stolen. For instance, if a criminal steals credit card data from Merchant A, then uses the data to make a counterfeit card that is successfully used at Merchant B’s point of sale, under the liability shift Merchant B may become responsible for the costs of that transaction. Merchant A’s liability is not affected, even though they were the source of the stolen credit card data. This is a key distinction. EMV technology is an anti-fraud solution, rather than a network security solution and the new rules do not transfer liability for a network breach.

The purpose of the liability shift also provides insight into how the card networks will likely enforce the new rules. While the shift potentially applies to all fraudulent POS transactions, the overall aim is to encourage merchants to adopt EMV technology so that once consumers are issued with chip cards, the full anti-fraud benefits of the technology can be realized. The liability shift therefore aims to shift the costs of fraudulent transactions to merchants where, if the merchant had had EMV technology, the transaction would not have been approved. Card networks are unlikely to use the new rules to penalize merchants who adopt EMV technology or apply it to fraudulent transactions that would have occurred regardless of the merchant’s EMV capability, since this does not further the aim of widespread adoption of EMV technology.

**Considerations For Businesses**

EMV technology requires a significant investment by merchants in new systems and infrastructure. These costs of adoption should be balanced against the increased potential expenses arising from the liability shift. Businesses selling high value, easily re-sellable merchandise, such as jewelry or electronics, may be targeted by criminals and experience increased costs due to the liability shift if EMV technology isn’t adopted. On the other hand, businesses that do not sell goods or services that can be profitably re-sold may find that the potential increased costs from the liability shift are insignificant.

As criminals seek to avoid EMV technology, e-commerce may see an increase of fraudulent transactions. Online credit card fraud has increased dramatically in other countries following the introduction of EMV technology and, while these costs do not implicate the liability shift, they may increase costs for businesses in responding to increased fraudulent online activity.

Importantly, the adoption of EMV technology does not negate the necessity of ensuring robust network security. Cyber-attacks against merchants will continue as long as sensitive data can be monetized and avenues remain for criminals to profit from stolen credit card data. In addition to implementing a
EMV technology is named after the principal global credit card networks: Europay, Mastercard and Visa.

Issuing banks issue credit cards to the consumer. Acquiring banks carry out banking for merchants.

A comprehensive security plan, maintaining appropriate insurance can effectively transfer the risks of a cyber-breach. While EMV compliance may be viewed favorably by underwriters because it is seen as pro-active risk management, there are many other security measures that are critical in managing enterprise risk and preventing cyber-attacks.

The introduction of EMV technology is a significant step in reducing the costs of counterfeit credit card fraud across the United States. This technology should be viewed as an anti-fraud solution, not as a replacement for strong network security. While the liability shift has gained much publicity, the fraudulent transactions for which merchants may become liable are narrow and some merchants may experience little to no additional risk exposure due to the shift. This cost/benefit analysis is just one aspect of a company’s overall risk management, and it remains critically important for merchants to maintain robust systems to protect their data.

---

1 EMV technology is named after the principal global credit card networks: Europay, Mastercard and Visa.

2 Issuing banks issue credit cards to the consumer. Acquiring banks carry out banking for merchants.

---

Contact

Dominic Keller
Assistant Vice President
FINEX North America
Cyber/E&O Practice
D: +1 415 955 0215
T: +1 415 630 0402
dominic.keller@willistowerswatson.com

The observations, comments and suggestions we have made in this publication are advisory and are not intended nor should they be taken as legal advice. Please contact your own legal adviser for an analysis of your specific facts and circumstances.

About Willis Towers Watson

Willis Towers Watson (NASDAQ: WLTW) is a leading global advisory, broking and solutions company that helps clients around the world turn risk into a path for growth. With roots dating to 1828, Willis Towers Watson has 39,000 employees in more than 120 territories. We design and deliver solutions that manage risk, optimize benefits, cultivate talent, and expand the power of capital to protect and strengthen institutions and individuals. Our unique perspective allows us to see the critical intersections between talent, assets and ideas – the dynamic formula that drives business performance. Together, we unlock potential. Learn more at willistowerswatson.com.

Copyright © 2016 Willis Towers Watson. All rights reserved.
WTW-NA-2016-15322
willistowerswatson.com