

EMV chip technology and the new liability shift rule: Coming to a retailer near you

[Daniel A. Cotter and Margaret J. Jantzen](#), Butler Rubin Saltarelli & Boyd LLP

If you have walked into any retail shop in recent months, you probably have noticed new credit card readers on display. Many of those readers are already operational but some will "go live" on October 1, 2015. The new credit card readers contain the EuroPay, Mastercard, and Visa ("EMV") chip technology, which has already been implemented in Europe and Asia. In an effort to speed up the adoption of the EMV chip technology by merchants and retailers in the United States, credit card companies have changed the liability rules applicable when fraud is perpetrated using a credit card (the "liability shift rule"). This article summarizes the liability shift rule and raises some questions concerning its implementation.



The new EMV chip technology

Traditionally the credit card issuer assumed all liability for fraudulent transactions. To combat fraud, much of the world outside of the United States switched to EMV chip technology years ago. For a variety of reasons, including its size and complexity, the United States market resisted the new technology. In the wake of the massive theft of credit card information involved in the recent Target and Neiman-Marcus hacks, renewed focus was given to data safety, and the card issuers in the United States began to embrace the EMV chip technology.

The major card issuers strongly encouraged implementation of the new credit card readers at the point-of-sale to enhance the security of a credit or debit card transaction. At the same time, the larger card issuers have sent their credit and debit card holders new cards with the EMV chip technology embedded into the cards. The EMV chip technology provides a more secure payment system than currently exists with magnetic strips. The magnetic strips' data does not change, whereas the EMV chip technology generates a one-time transaction code, making data breaches and credit card information thefts much less valuable.

Most major national retailers have changed their readers to permit the reading of the EMV chip. However, some smaller merchants have not made the change, citing the costs of both the point-of-sale readers and the potential software upgrades necessary to process the new technology. The total costs estimated for the conversion of the entire United States ranges from approximately \$8 billion to more than \$30 billion.

The "liability shift"

To encourage merchants across the board to adopt the new technology and convert their point-of-sale credit card readers, the four major credit card networks in the United States (Visa, MasterCard, American Express and Discover) have implemented a new liability shift rule. Effective October 1, 2015, the liability for fraudulent transactions (and potentially for data breaches) shifts from the credit card issuers, who historically were responsible for all credit card fraud and breaches that occurred, to the retail merchants. The major credit card networks are using this liability shift to encourage and speed up the transition to the new EMV chip technology.

If there is an EMV chip on the card used in a transaction, but the merchant at point-of-sale has not adopted the EMV chip technology, the merchant will be liable for the resulting losses from a fraudulent transaction. If the card used at the point-of-sale contains an EMV chip and the merchant has adopted the EMV-reading capability, the credit card issuer will remain liable. That is, the test for determining liability for a potentially fraudulent transaction focuses on which of the two parties has the least EMV-compliant technology. The party with the lesser technology capabilities will be found liable. In many cases, that liability will rest on the merchant. Not only will the merchant be liable if it has not implemented point-of-sale EMV chip technology, it will remain liable if the transaction was one in which the consumer could have used the EMV chip on their card but instead used the magnetic strip. The idea here is that, where both the issuer and the merchant are equally compliant, the merchant is in the better position to avoid a transaction using the outdated technology. Although a merchant might not flatly refuse a transaction that uses a card's magnetic strip when the EMV technology is otherwise available, the merchant can at least direct the customer to the superior technology and attempt to persuade him or her to make use of it. Each situation will involve a comparison of the relative technologies used in a particular transaction between the credit card issuer and the retail merchant.

Some open questions remain

The liability shift rule will only apply to point-of-sale transactions on and after October 1, 2015. For pay-at-the-pump gas station transactions, the "liability shift" becomes effective on October 1, 2017. The new rule does not apply to "card-not-present transactions" (over the phone, Internet, etc.) or to lost and stolen card fraud. One question that remains open is whether the rules will eventually expand to take into account "card-not-present transactions" as technology evolves and potential large-scale fraud schemes move from point-of-sale transactions to online transactions. (Because the card must be physically present to utilize the existing EMV chip technology, it is unlikely that the liability shift rule can be imposed on "card-not-present transactions," but technology likely will quickly evolve.)

Another question raised by the liability shift rule is the way in which the liability shift will actually take place. Given the vast network of card issuers and merchants, some orderly mechanism for a card issuer to initiate the liability shift and for the merchant to dispute the attempt to place liability on it is warranted. While the card issuers have changed the rules on liability for fraudulent transactions, there does not appear to be any clearinghouse or formal

framework in place to address the numerous disputes likely to arise between the issuers and merchants.

Conclusion

As of October 1, 2015, any merchant who uses in-person credit card readers will be subject to the "liability shift" rule. Some questions remain about the full implementation of the EMV chip technology. Unless and until those questions are resolved, merchants will need to carefully weigh the costs of fully implementing the new EMV chip technology against the substantial exposure they may face by failure to adopt the new technology.

About the Author

Daniel A. Cotter is a Partner at [Butler Rubin Saltarelli & Boyd LLP](#) and Chair of the firm's Insurance Regulatory and Transactions practice. He is a frequent writer on various compliance topics. Margaret J. Jantzen is an Associate at Butler Rubin concentrating her practice in the arbitration and litigation of complex commercial disputes, including cyber security. The views expressed are personal to the authors.