

'Massive' switch to new credit cards ahead

Your customers can expect a flurry of thick, credit-card-carrying mail as all banks attempt to get high-tech chip cards into their hands before the end of the year. As a result the way you accept credit and debit card payments is about to change.

There will be a major liability shift to merchants on October 1, 2015: merchants not using EMV (**E**uroPay, **M**asterCard, and **V**isa)-enabled credit card terminals or point of sale (POS) systems will bear the liability for credit cards bearing a computer chip when fraud is involved.

Although EMV compliance is not mandatory, the EMV liability shift is certain. Fraud involving credit card charges could be in the form of fake cards, stolen cards, or cards used without proper authority.

In order to meet EMV compliance requirements, members that accept credit card payments will need to have an EMV-enabled terminal or POS system that allows new credit cards with computer chips to be inserted into the terminal rather than being swiped.

BuisnessInsider.com reports that credit and debit card fraud has caused billions of dollars in losses in the U.S.—\$5.5 billion in 2012 and \$7.1 billion in 2013. In fact, in 2013, 51 percent of global payment card fraud costs were attributable to the U.S. alone. While Europe is already on board and embracing the new technology to reduce fraud, U.S. merchants are lagging behind. In fact, it has been estimated that less than 50 percent of merchants in the U.S. will be in compliance with the EMV guidelines on October 1, 2015.

Who Is Liable?

Members using a terminal that only allows a credit card to be swiped and have a customer who fraudulently uses a credit card with the EMV chip bear the risk of loss for EMV liability. In many other cases, however, issuing banks will be liable.

For instance, an issuing bank will bear the risk of loss if a member still uses a terminal that only allows a credit card to be swiped and has a customer who fraudulently uses a card with no chip, just the magnetic strip on the back of the card.

If a member has an EMV-enabled terminal and a customer fraudulently uses a credit card with the EMV chip, the odds are very strong that the transaction will not go through. Even if it does, the issuing bank will bear the risk of loss because the member was using an EMV-enabled terminal.

Lastly, a member might use an EMV-enabled terminal but have a customer who uses a credit card with no chip, just the magnetic strip on the back of the card. The card is swiped, and the transaction goes through. In the case of a fraudulent transaction, the issuing bank will still bear the risk of loss for the transaction, not the merchant.

To Comply or Not to Comply? That Is the Question.

Although following with the new EMV compliance rules is not mandatory, each member company should consider the risks of noncompliance. For instance, if the merchant sells big-ticket items and has had to deal with instances of credit card fraud in the past, the member will probably not want to risk a large chargeback that would have a noticeable impact on the bottom line.

The chip terminals can be costly, to help defray the costs for our Members-Card Payment Services (CPS) has offered to supply these terminals for no cost for participating members enrolled in their program. Since 2008 CPS has been saving members significant amounts off their credit card processing fees, so not only can they supply our Members with the new technology but also reduce your cost on accepting all credit card and debit card payments. If you would like CPS to review your merchant services program and help make sure you have the proper equipment contact them today by calling Andrew Caine at 888-409-2919, ext. 206 or via email at andrew@cpspayments.com. CPS will also be at our booth during Waste Expo so you can also stop by and learn more about these major changes.