CentralPayment®

Top Merchant Questions on EMV

1. **What is EMV?**
    a. EMV is a metallic microprocessor chip on credit cards. Lots of cards today have both a magnetic strip and a chip, but only the chip is EMV. To use the chip, the card is inserted into a slot on the terminal, rather than swiped.
2. **Why would I want to use EMV?**
    a. EMV transactions are more secure and fraudulent transactions are virtually impossible. As a customer, you should use EMV in order to protect your private and sensitive information (such as credit card number and billing information). As a merchant, you should process EMV transactions to protect your business from becoming liable for fraudulent transactions.
3. **Why is this changing? Why are you doing this to me?**
    a. Cybercrime is at an all-time high and the United States has been a target for fraudulent activity. This has motivated card issuer companies (such as Europay, MasterCard and Visa–EMV) to develop a more secure payment method. In order to encourage everyone to use the most secure technology available, liability for fraudulent transactions will land on the party who uses the less secure technology.
4. **Can I still use regular cards with no chip?**
    a. Yes, if the card does not have a chip, it is perfectly safe for you to run the transaction with the magnetic strip. In such a case, you will not be held liable for processing a fraudulent card. You are only in danger of becoming liable when you process a card with the magnetic strip when the EMV chip was an available option.
5. **What are my options?**
    a. The Vx520 is the best option; it is affordable and easy. We also offer a wireless Vx680, and a Vx805 pinpad that can process EMV transactions. MOTO and keyed transactions are also except from the EMV liability shift.
6. **I have a Vx520; am I ready to accept EMV transactions?**
    a. There are a few considerations here. First, the way your terminal connects to the internet is very important: we highly recommend using a high speed internet (IP) connection as opposed to dial or phone line connection. EMV transactions take around 7 seconds to process over an IP connection, and up to 30 seconds over a dial connection. The next consideration is if your terminal has had the required software update. This may have been done automatically, or feel free to call our tech support team to expedite the download. You'll know if your terminal is EMV-ready by swiping an EMV credit card: if your terminal prompts you to insert the card, then you're EMV-ready!
7. **What about restaurants without counter service?**
    a. EMV "best practice" advises customers to keep possession of their card at all times. That means, it is not recommended for servers to take a credit card away from the table to process it at a payment location. Furthermore, certain cards will require a PIN authorization, which will need to be entered by the card holder. Our best product for this situation is our wireless Vx680, which accepts EMV and NFC payments.
8. **What about PINS & Signatures: How do those work and who determines if cards will be authorized by PIN or signature?**
    a. EMV cards are authorized either with a PIN or signature. The card issuer (such as Visa or MasterCard) determine which cards will have PIN and which will have signatures (though it is expected that most cards will need signature authorization). For PIN transactions, customers will need access to a pin pad; signature transactions work just the same as they do now.
9. **Does C-cap cover this?**
    a. The card compromise assist plan covers expenses resulting in a suspected or actual breach of credit card data from a payment device. For example, c-cap comes into play if a hacker is able to extract card data from your terminal. On the other hand, EMV prevents cards from being illegally duplicated; illegally duplicated cards are *not* covered under c-cap. In short, if you are not processing EMV transactions, ccap **will** cover data breaches, and **will not** cover transactions processed with an illegally duplicated card.
10. **Who is going to charge me the chargeback fines related to the EMV liability shift?**
    a. A chargeback resulting from fraud will be administrated by Central Payment the same way a chargeback is done today. These are charges applied by Central Payment, however, they are not mandated by Central Payment.