The Small Business Guide to Mastering EMV

Get Familiar with EMV & Our Plans to Support it

BNG
PAYMENTS

EMV 101

Understanding the Basics of EMV Technology

Get to Know the Chip

What is EMV?

Understanding EMV & the Technology that Powers EMV Cards

EMV, which stands for Europay, MasterCard and Visa, is the technology behind that tiny microchip that's showing up on new credit and debit cards everywhere in the U.S. This tiny little chip has huge benefits when it comes to protecting against fraud for card-present transactions. It offers better data security than magnetic stripe transactions and makes counterfeiting a card next to impossible.

Embedded Microchip

This microprocessor chip is what turns the card into a smart card and enables it to communicate secure EMV transaction data to an EMV terminal.

Embedded Antenna

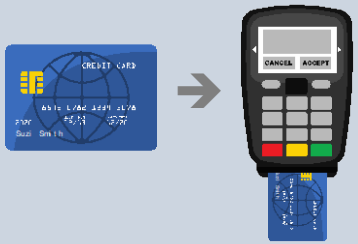
This antenna connects to the embedded microchip and communicates the secure EMV transaction data to a point of sale terminal via NFC technology.

Ways to Accept EMV

Understanding the 3 Ways EMV Payments Can Be Accepted

Contact EMV

Contact EMV payments require a customer to put their EMV card into the slot of an EMV terminal. While the card remains in the terminal, the embedded chip and the terminal communicate to verify the card is real and to validate the cardholder's identity.

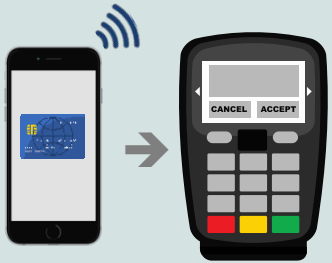


Contactless EMV

Contactless EMV payments allow customers to tap their card against the EMV terminal, enabling the terminal to communicate with the card's embedded antenna via NFC technology while still using the EMV security standards.

Mobile EMV

Mobile EMV payments allow customers to upload their EMV card credentials onto their mobile phone. Then, when it's time for payment, a customer can tap their phone against the terminal, which then communicates with the phone's antenna via NFC technology, while still using the EMV security standards.



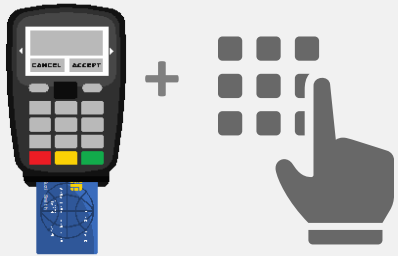
EMV Chip & PIN

Understanding How EMV Authenticates the Cardholder

The EMV card and EMV terminal communicate and work to negotiate the highest level of security available to determine if a PIN or signature will be required for the Contact EMV payment.

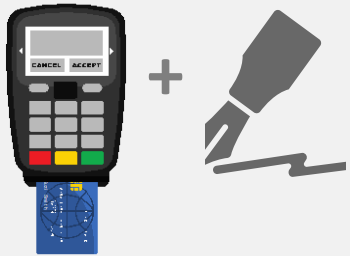
Chip & PIN

The EMV terminal requires the customer to enter their PIN to verify their identity.



Chip & Signature

The EMV terminal prompts and requires the customer to sign for the transaction.



What Happens When an EMV Transaction is Processed?

Understanding the Steps and Key Players Involved in Processing an EMV Credit Transaction

EMV Cardholder

EMV Terminal

EMV-Ready Merchant

EMV Certified Payment Gateway

EMV-Ready Issuing Bank

Key Players in Processing an EMV Transaction

This is Suzi

EMV Cardholder

An EMV cardholder is someone who has obtained an EMV credit or debit card from a card issuing bank and is ready to start using it to make purchases.

EMV Terminal

An EMV terminal is the POS hardware that communicates with the cardholder's EMV card, specifically the embedded chip or antenna on the card.

This is Joe

EMV-Ready Merchant

An EMV-ready merchant has a compatible EMV-enabled terminal in their store and can start accepting EMV payments from their customers (cardholders) for the goods or services they sell.

Joe's EMV Certified Payment Gateway Account

EMV Certified Payment Gateway

The EMV certified payment gateway securely transmits the EMV transaction data and one-time cryptogram to issuing bank.

Suzi's EMV-Ready Issuing Bank

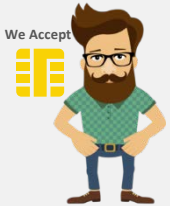
EMV-Ready Issuing Bank (Cardholder Bank)

The EMV-ready issuing bank issues EMV credit cards to consumers like Suzi. They are responsible for decrypting the EMV transaction data and one-time cryptogram, authorizing the transaction and sending back their response via a new one-time cryptogram with the transaction authorization.

Contact EMV Transaction Flow

1. Suzi the EMV Cardholder Purchases a Red Widget

While Suzi is shopping in her town, she spots the perfect red widget while passing by Joe's Widget Shop and decides to stop in and buy it. Suzi is able to make an EMV payment for the widget, since Joe's shop is EMV ready. Suzi makes a contact EMV payment and initiates the transaction by placing her card in the terminal's slot.

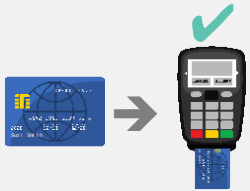


2. The EMV Terminal Verifies the Card's Authenticity

There are a few different ways this can happen, depending on whether it's a contact EMV, contactless EMV or mobile EMV transaction.

For Contact EMV (and in Suzi's Case)

The card is placed into the slot on the terminal and remains there while the terminal verifies the card is real and validates the cardholder identity. The terminal will ask for the cardholder's PIN or signature depending on the issuer's verification method.



For Contactless EMV & Mobile EMV

The user taps the card or mobile phone, and using NFC technology it communicates with the terminal. The same EMV security standards used for contact EMV purchases are employed to verify the card is real and to validate the cardholder identity.

3. EMV Transaction Data is Prepared & One-Time Cryptogram is Created

Once Suzi's card has been verified and her identity has been validated, the terminal and the card work to prepare the EMV transaction data and create a one-time cryptogram that is only valid for this specific transaction.

4. EMV Transaction Data & One-Time Cryptogram are Sent to the Payment Gateway

The gateway receives the EMV transaction data and one-time cryptogram and securely transmits them to Suzi's issuing bank.

Joe's EMV-Ready Payment Gateway Account

Suzi's EMV-Ready Issuing Bank

5. The Issuing Bank Decrypts the EMV Transaction Data & One-Time Cryptogram

After Suzi's issuing bank receives the transaction data, it works to decrypt the EMV transaction data and one-time cryptogram. Now the bank has all the information it needs and can authorize the transaction.

Suzi's EMV Ready Issuing Bank

6. The Issuing Bank Creates a New One-Time Cryptogram to Send Its Response

Suzi's issuing bank now needs to communicate the transaction authorization back to the EMV terminal and creates a new one-time cryptogram to do this.

7. The Issuing Bank Sends the New One-Time Cryptogram to the Payment Gateway

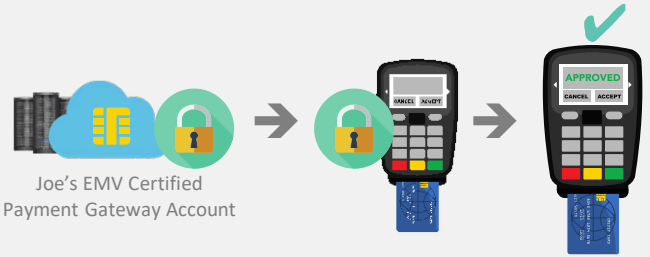
Suzi's issuing bank sends the new one-time cryptogram with the transaction authorization back to the payment gateway.

Suzi's EMV Ready Issuing Bank

Joe's EMV Certified Payment Gateway Account

8. New One-Time Cryptogram with the Issuer's Response is Passed Along to the EMV Terminal

Once the payment gateway receives the new one-time cryptogram, it passes it along to the EMV terminal. From there the EMV terminal decrypts and displays the issuer's response, which in this case is an approval.



Joe's EMV Certified Payment Gateway Account

What Do Merchants Need To Know About the EMV Liability Shift?

Understanding the Liability Shift and the Steps to Take to Avoid Liability

October 1st Deadline

EMV Liability Shift Rules

EMV Adoption

Tips to Avoid Liability

October 1st 2015 Deadline

Understanding How this Deadline Affects the Liability Shift

Liability Shift

After October 1, 2015, if a counterfeit EMV transaction occurs, the liability belongs to whichever party has not yet adopted EMV chip technology. This means that the issuing bank or merchant could end up being financially responsible for the counterfeit EMV transaction if they aren't EMV-ready.

Card Present Transactions Only

The transition toward EMV technology and the liability shift only affects merchants who process card present transactions. Online transactions, on the other hand, are not directly affected by EMV technology or the liability shift.

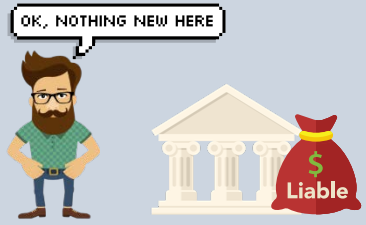
EMV Liability Shift Rules & Scenarios

After October 1, 2015, Who's Liable?[1]

Scenario 1

A traditional magnetic stripe card is swiped by the customer at a magnetic stripe terminal.

In this case, neither the issuing bank nor the merchant is EMV-ready. If the purchase is a fraudulent transaction, the merchant is generally not liable, just like today.



Joe the Merchant

Issuing Bank

Scenario 2

A chip card is used at a traditional magnetic stripe only terminal.

In this case, the issuing bank is EMV-ready but the merchant is not. If the purchase is a counterfeit EMV transaction, the merchant is generally liable, since the issuer has made the investment to upgrade to chip technology and the merchant has not.

Joe the Merchant

EMV Ready Issuing Bank

Scenario 3

A chip card is used at a chip-enabled terminal.

In this case, the issuing bank and the merchant are both EMV-ready. If the purchase is a counterfeit EMV transactions, the issuer will continue to bear the responsibility of the fraudulent activity, as they do currently.

Joe the Merchant is EMV Ready

EMV Ready Issuing Bank

1. "EMV Liability Shift: Why it pays to adopt new technology," *Visa.com*, http://usa.visa.com/merchants/grow-your-business/payment-technologies/credit-card-chip/liability-shift.jsp.

EMV Liability Shift Rules & Scenarios—The Exceptions

Are There Any Types of Transactions Not Included in the October 2015 Liability Shift?[1]

Fuel & ATM Transactions

Liability for automated fuel dispensers and ATM transactions doesn't shift until October 2017.

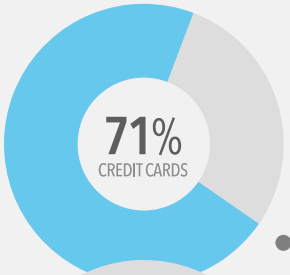
Card-Not-Present Transactions

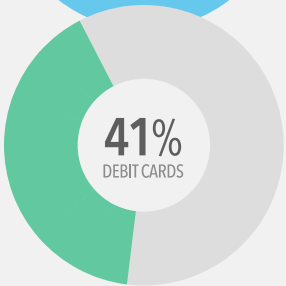
The liability shift doesn't apply to card-not-present transactions. In these cases, the liability remains subject to existing liability and chargeback rules.

1. "EMV Liability Shift: Why it pays to adopt new technology," *Visa.com*, http://usa.visa.com/merchants/grow-your-business/payment-technologies/credit-card-chip/liability-shift.jsp.

EMV Adoption

What is the Expected Adoption Rate of EMV?[1]



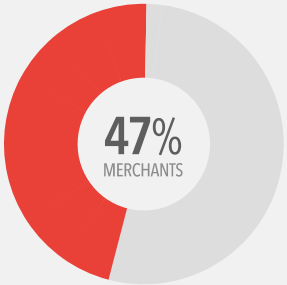


Issuing Banks

By the end of 2015, it's expected that the card issuing banks will be taking the lead when it comes to EMV adoption.

Merchants

By the end of 2015, it's expected that only about half of all US merchants will have upgraded their terminals and will be EMV-ready, leaving a high likelihood that a high percentage of merchants will be financially liable for fraudulent transactions.



1. Shamas, Megan. "With EMV Chip Migration on Track, U.S. Payments Industry Looks Ahead to Mobile, eCommerce and Tokenization at Smart Card Alliance 2015 Payments Summit," *smartcardalliance.org*, http://www.smartcardalliance.org/with-emv-chip-migration-on-track-u-s-payments-industry-looks-ahead-to-mobile-ecommmerce-and-tokenization-at-smart-card-alliance-2015-payments-summit/.

Steps Merchants Can Take to Avoid Liability

Keep Your Merchants on Track to Avoid Liability

Stay One Step Ahead of Card Issuers

Card issuers already plan to have chip cards in consumers' hands by the end of 2015 and once consumers start using those cards, merchants with non-EMV-ready terminals will start taking on the liability.

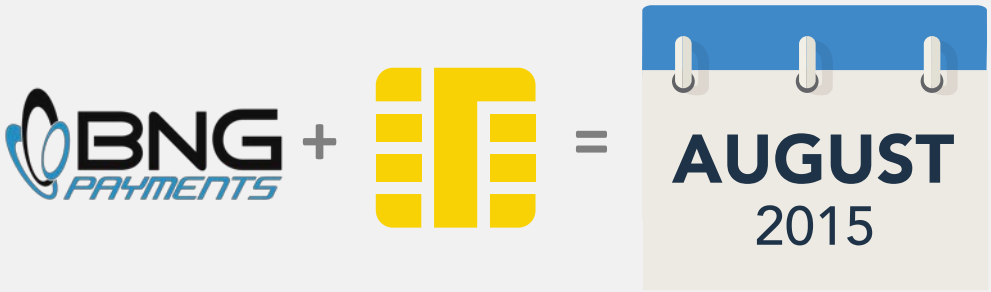
Upgrade & Process Transactions Using an EMV Compatible Device

Having an EMV compatible terminal is just the foundation for EMV; merchants will actually need to process transactions using EMV whenever possible to truly avoid liability.

Mark Your Calendars

EMV is Coming to the Gateway in August

We Will Be “EMV-Ready” in August!



To learn how EMV will affect your business, contact us at
www.bngholdingsinc.com/contact-us/