

# EMV Credit Cards

A WSU Tutorial

April 2017

# What is in my card?

## EMV Terminology to Know

- EMV
  - This is a new chip embedded credit card that limits in-person fraud at the POS (Point Of Sale)
  - Goes by many names, but all are the same product:
    - Chip card, Chip and Pin, Chip and Signature, Smart Card, EMV Card, etc...
  - Stands for “Europay, Mastercard, Visa”; the 3 organizations that developed initial specifications
- Magstripe
  - This is the outdated technology that EMV is replacing.
  - It is a magnetic stripe that holds data and is easily intercepted
  - This is the black bar on the back of the card across the top of most modern USA credit cards
- NFC
  - Stands for Near Field Communication
  - It is a tag or antenna setup within the card itself
    - Allows it to broadcast its info to terminals wirelessly
    - This allows use of “tap and go” style terminals
    - Needs to be within a few inches to work with the card reader
  - Phone payments utilize this technology (i.e. Apple Pay)
  - EMV and NFC are separate products, and not all EMV cards will be NFC capable
    - ***JPMC WSU cards will not and have never had NFC capabilities***
- RFID
  - This is the old technology that NFC is replacing, works very similarly
    - ***JPMC WSU cards will not and have never had RFID capabilities***
  - Stands for Radio-Frequency Identification
  - Can be within few meters and still work with the card reader

# EMV - What is it?

- Typically a chip inset within a credit card
- Chip stores cardholder and application data more securely
- Adds cardholder verification methods
- EMV provides protection against in-person card fraud (not online)



# Who is using EMV?

- Eighty countries globally are in various stages of EMV chip migration, including Canada and countries in Europe, Latin America and Asia. According to EMVCo, as of December 2013:
  - 2.37 billion chip payment cards are in use
  - 99.9% of terminals in Europe are chip-enabled
  - 84.7% of terminals in Canada, Latin America, and the Caribbean are chip-enabled
  - 86.3% of terminals in Africa and the Middle East are chip-enabled
  - 71.7% of terminals in Asia Pacific are chip-enabled
- The United States is one of the last countries to migrate to EMV chip technology.
  - This is why USA fraud rates are going up so dramatically

# Why does it take so long to Implement?

- Merchant Pushback
  - EMV is not a priority for merchants, especially smaller ones.
- Co\$t
  - New hardware is needed to operate EMV readers
  - New processing software must also be put in place
- There are shortages of hardware nationally as most of USA goes to the new technology near the same time
- Many newly installed EMV card readers have yet to be EMV certified, so they are still only using magstripe for transactions. Certification takes longer than the merchants expected it to.

# How Does EMV Work?

- Contact
  - Chip is embedded in a card
  - A contact card is inserted into a smart card reader
  - The contact points on the chip make contact with the card reader
- Contactless
  - Card and Payment station must both be NFC capable to use this
    - NFC may be embedded in cards, key fobs, stickers, mobile phones, etc.
  - A contactless chip requires close proximity to a reader (“tap and go”); both the chip and the reader have an antenna and they use an RF (radio frequency) signal to communicate





Follow terminal prompts throughout the transaction\*

Leave chip card in terminal until prompted to remove



If you swipe your chip card, the terminal will direct you to insert it instead.



Insert card with chip toward terminal, facing up. Do not remove until prompted.



Verify your transaction by signing or entering your PIN. Some transactions may not require either.

**NOTE:** EMV standards support both PIN and signature.



When the terminal says the transaction is complete, remove your card.

# How Does EMV Work? – recap

- Check the card reader to ensure it currently accepts EMV cards
  - If not, you can use the magstripe instead
- Wait for card reader to ask you for your EMV card
- Insert your EMV card into the reader in the front facing slot, chip first and face up, and then leave the card inserted in the machine
  - Wait until the cashier finishes and rings out the transaction to remove your EMV card (the card reader will beep to indicate this)
  - Since the card must be left in the whole time, you may consider not putting your card into the reader until the end of the transaction, so your card is not left out in the open and vulnerable
- The card reader should either finish or prompt you for a signature
  - ***All USA merchants do not require PINs at this time***
- Once the transaction is done, the reader will start loudly beeping, which is your cue to carefully remove your EMV card from the reader
- Ensure to get both your EMV card and the transaction documentation as you exit the store.



# PINs

- PINs are an alternate way to verify who the Cardholder is in-person, as opposed to the signature
  - EMV cards typically require the use of the card’s chip and one additional verification – the cardholder’s signature or a PIN.
  - All USA card companies have decided to go with Chip and Signature for EMV transactions. ***This means no locations in the USA should require a PIN (at this time).***
- Domestic use of your EMV card should not require a PIN
  - No USA readers should ask for a PIN, but if one does tell the merchant you do not have a PIN and want to use a signature instead
  - If the merchant card reader prompts for a PIN code, it may allow you to “Cancel” out of the prompt so you can sign. You may also be able to select “Enter” or “Continue” to bypass the PIN request.
- PINs are used in international locations outside of the USA
  - If traveling outside of the USA, you may need to setup a PIN to use an EMV card
  - If this applies to you, contact the WSU Pcard ADMIN team for assistance to get a PIN before you leave on the international trip
  - NOTE: International merchants may not have magstripe readers on site
  - NOTE: International online transactions are unaffected by this process
- PINs will not be used in online transactions – this is for in-person transactions only.

# What can go wrong at the card reader?

- Card is left unattended
  - The card can be lost or its info can be stolen
  - Be mindful of never putting your card in the reader and walking away from it
    - Always have an eye on your card and your surroundings
- Cardholder leaves the card in the reader and exits the store without it
  - Ensure to always remove the card when done (reader should beep loudly at you to do so)
  - Report the card as Lost if it is left behind anywhere, even if it was for a short period of time
- Transaction declines
  - No transactions should decline due to EMV alone
  - Contact the WSU Pcard ADMIN team to find out why your transaction declined
- Attempting to use the magstripe on a EMV capable reader
  - Most current EMV card readers will beep and produce an error message if you attempt to use the magstripe if you have an EMV card and the reader is working and EMV certified
  - This will cause you to have to use the EMV slot in order to proceed
  - As a rule of thumb, assume the merchant has EMV capabilities until proven otherwise, as opposed to the opposite, or in other words → stop using your magstripe!

# What can go wrong at the card reader?

- Cardholder (or merchant) removes the card before transaction is final
  - This will cause the transaction to fail, and payment will need to be initiated by the merchant again
- Card is bent or broken off at the reader
  - Ensure to remove the card at a straight angle from the reader slot
  - If damaged, let the WSU Pcard ADMIN know so they can replace it for you
- Reader asks for a PIN
  - No USA card readers should ask for a PIN, but if one does tell the merchant you do not have a PIN and want to use a signature instead
  - If traveling internationally, you may need a PIN to use the card outside of the USA

# Fraud Liability

- Merchant
  - As of 10/1/15, all US merchants who do not have working EMV readers as their POS assume fraud liability
    - Excludes automated fuel pumps and ATM's
      - ATM's shifted on 10/1/2016 (MasterCard)
      - Automated Fuel Dispensers (AFD) shift on 10/1/2017
- Issuer
  - If Issuer has not given EMV cards to their users, they retain fraud liability until they do so.
- Cardholder
  - If EMV is available, but you choose to use magstripe anyways, you could assume fraud liability.
    - This is very unlikely to occur though, as newer EMV readers typically do not allow magstripe use if EMV is active.
  - Simply having an EMV card is not enough, you must also use it in the correct manner to get the proper fraud liability protection.
- Not covered: contactless transactions (i.e. NFC), CNP fraud (i.e. online transactions), and Lost/Stolen fraud

# Tokenization

## Combating Online Fraud

- EMV does not secure online payments in any way. To secure online transactions, Tokenization is being implemented nationally in tandem with the EMV rollout.
  - This is a completely separate process and roll-out apart from EMV cards and has nothing to do with in-person transactions.
- Tokenization is the process of replacing the original payment credentials (PAN) with a unique “alternate identifier” which may be used in its stead to initiate payment activity.
  - Replaces a traditional card account number with a unique payment token / digital account number
  - Restricts the use of a payment token by: device, merchant, transaction type or channel
- Payment tokens further enhance security of digital payments and simplify purchase experience when shopping on mobile, computers or other smart devices and help reduce fraudulent activity.
  - Retailers will no longer have access to credit card numbers
  - Data breaches will not be able to get as much info
  - Currently, there is no way to decode the tokens--no mathematical formula that can be reversed to figure out the credit card number (except at the banks of course).

# What makes EMV more secure?

EMV secures the payment transaction with enhanced functionality in three areas:

- **Card authentication**, protecting against counterfeit cards.
  - Chip identifies itself in a very complex algorithm
  - Not economically viable to counterfeit the chip cards
  - EMV transactions also create unique transaction data, so that any captured data cannot be used to execute new transactions.
- **Cardholder verification**, authenticating the cardholder and protecting against lost and stolen cards.
  - Cardholder verification ensures that the person attempting to make the transaction is the person to whom the card belongs.
  - EMV supports four cardholder verification methods (CVM): offline /online PIN (most commonly used), signature, or no CVM.
    - Online Debit will still use a PIN
    - Credit and Signature Debit will still require a signature
  - The issuer prioritizes CVMs based on the associated risk of the transaction (for example, no CVM is used for unattended devices where transaction amounts are typically quite low).

# What makes EMV more secure?

EMV secures the payment transaction with enhanced functionality in three areas:

- **Transaction authorization**, using issuer-defined rules to authorize transactions.
  - The transaction is authorized either online and offline.
    - For an online authorization, transactions proceed as they do today in the U.S. with magnetic stripe cards. The transaction information is sent to the issuer, along with a transaction-specific cryptogram, and the issuer either authorizes or declines the transaction.
    - In an offline EMV transaction, the card and terminal communicate and use issuer-defined risk parameters that are set in the card to determine whether the transaction can be authorized.
      - Offline transactions are used when terminals do not have online connectivity (e.g., at a ticket kiosk) or in countries where telecommunications costs are high.

Unlike a magnetic stripe card, it is virtually impossible to create a counterfeit EMV card that can be used to conduct an EMV payment transaction successfully.

# What is our bank doing?

- WSU Chase cards do not have RFID or NFC capabilities.
  - There is no need to worry about having your card hacked from proximity alone, and there is no need to buy any special merchandise to protect your card (i.e. chip/signal blocking card sleeves)
  - If you want to use a NFC device, you would have to load your card onto a phone and an app that both use NFC (i.e. Android Pay).
    - **At this time we do not recommend using WSU cards with any NFC devices.**
- WSU Chase EMV cards (and most of USA) will retain the magstripe for a few years still
  - Note: Transactions done on magstripe are afforded no EMV protections
- All USA EMV cards do not require a PIN for domestic physical use
  - No WSU Chase cards will be assigned a PIN initially, but a PIN should be setup by the cardholder with JPMC if they are going to travel internationally



# What is our bank doing?

- Replaced WSU EMV cards will have the same card number, but will have a new expiration date (+1 year of current exp. date) and a new CVV number (3 digit code on back of card).
  - You will need to update all websites that have your card info saved on file.
    - This includes sites such as: Amazon, PayPal, Office Depot
    - For Office Depot updates, please contact the front desk of the Purchasing dept.
- EMV cards will not affect your online shopping process in any way

# Next Steps

- Receive your WSU EMV Pcard
  - You will be sent an email when yours is ready, please do not contact us about your new EMV card until then
  - Sign the back of the card once received
- Activate your new card
  - Follow the directions included with the new card to call the bank and activate your new EMV card
    - NOTE: Cardholders will now self-activate their cards through the JPMC hotline instead of sending an email to the Pcard ADMIN team.
  - You can ignore any prompts to setup a PIN as it is not needed.
    - If you do need to setup your PIN for international travel, call the number on the back of your card to do so. This will not need to be done until just before you go on the trip though
    - You can setup PIN if you want to, just know it will likely not be used
- Begin using your new EMV card
  - Destroy your old card at this time
    - Cut it up into pieces or shred it
  - Ensure to update your new card info (i.e. exp. date) with any online merchants you have your card info saved with
    - For Office Depot – send requests to the PURCH Dept. at: [purchasing@wsu.edu](mailto:purchasing@wsu.edu)

The background of the slide features a large, semi-transparent grey shield logo of Western State University. The shield contains a white silhouette of a person with their arms raised in a celebratory gesture.

Thank you for your time and effort in learning about this new card product.

If you have any questions or concerns, please reach out to the WSU Pcard admin team at:  
[purchasing.card@wsu.edu](mailto:purchasing.card@wsu.edu)

**HAVE A GREAT DAY!**