



# EMV Chip and PIN

## Improving the Security of Federal Financial Transactions

Ian W. Macoy, AAP

August 17, 2015

# Agenda

---

1. Executive Order 13681
2. What Is EMV?
3. Federal Agency Payment Card Acceptance Environment
4. Fiscal Service EMV Terminal Deployment: What Agencies Need to Know
  - Standalone Terminal Migration
  - EMV and Agencies with Third-Party Integrated POS Systems



## Appendix: EMV Resources

# Executive Order 13681




# Executive Order & POS Card Acceptance

---

- Applies to Executive Departments and Agencies
- Point of sale (POS) card acceptance provisions apply to covered agencies directly and to the Treasury through the Fiscal Service's Card Acquiring Service (CAS)
- All new terminals acquired by agencies through Treasury *or through alternative means authorized by Treasury* after December 31, 2014 must include hardware necessary to support EMV chip and pin:
  - “Standalone terminals” acquired through CAS
    - CAS deploying EMV replacement terminals by 9/30/2015, to be in place before 10/1/2015 liability shift in card rules
  - Third-party, integrated agency POS systems
    - Agencies should already be planning and ensuring all new POS card acceptance hardware/software is EMV-compliant
- EMV card issuance provisions of EO are out of scope for CAS

# What is EMV?



# What is EMV?

---

- International standard defining interoperability of secure transactions
  - Introduces **dynamic data** specific to the transaction
  - **Devalues** card data; reducing risk of counterfeit fraud
- World-wide adoption including U.S. neighbors, Canada and Mexico
  - Affecting U.S. multi-national retailers
- Enabler of evolving card payment types
  - Contactless (NFC), Mobile
  - EMV built into devices



# What is EMV?

---

- Chip on card uses cryptography to provide security
- Utilizes 2 forms of cryptography:
  1. Digital signatures – ensures data is **authentic**
  2. Encryption – ensures data remains **confidential**
- Digital signature devalues the data
  - Even if data is intercepted, signature cannot be replicated
- Encryption is only used to protect the PIN
  - EMV does **not** encrypt all transaction data



# Liability Shift

---

- Enforced through card network rules -- **Effective October 1, 2015**
- Counterfeit fraud liability is assigned to least secure party
- Standard rules apply when both are equal
- Inclusion of PIN adds Lost/Stolen shift

**EMV w/PIN > EMV w/Sig > Mag stripe**

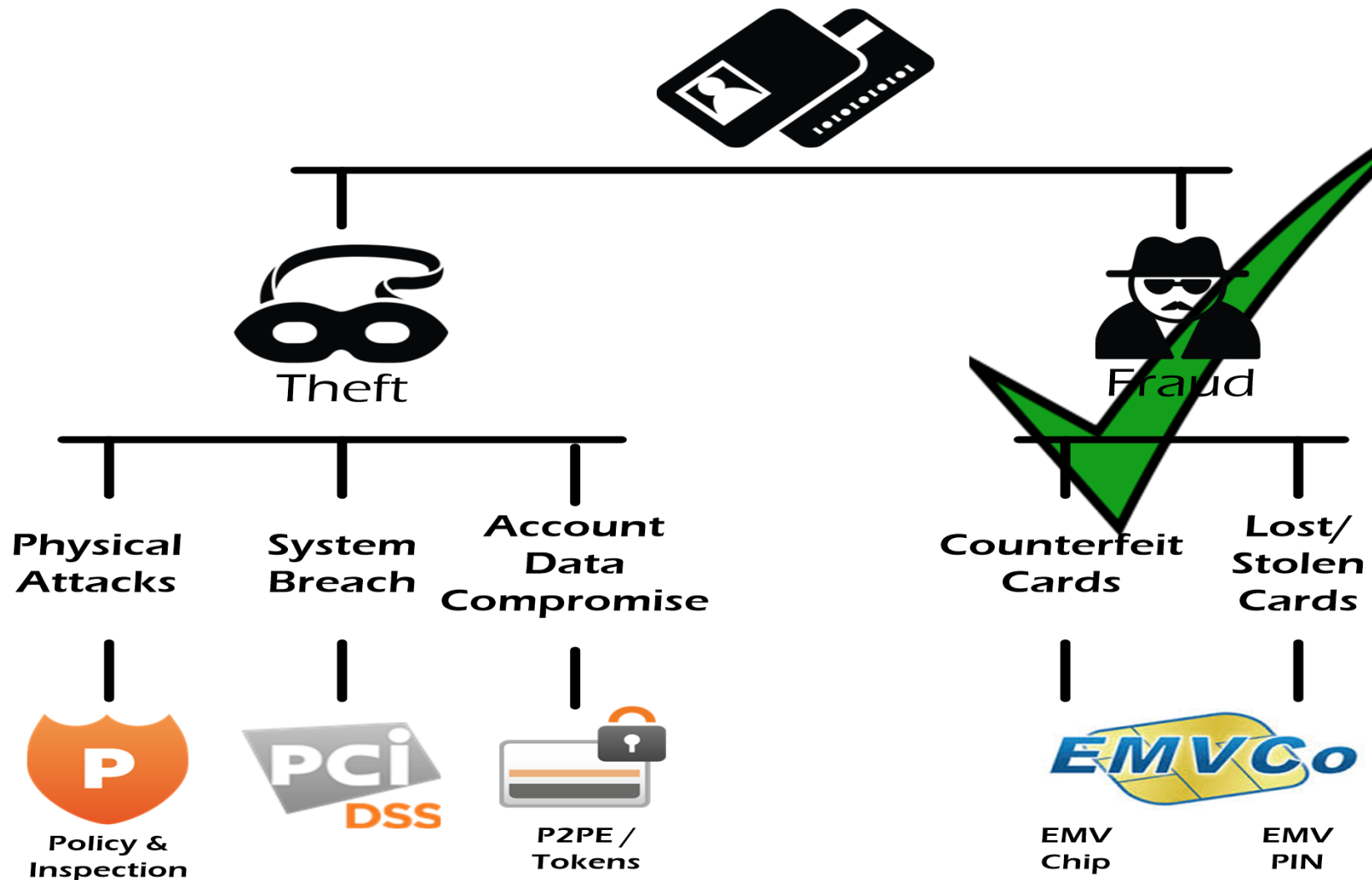


- Visa only states that the party not using EMV technology is liable

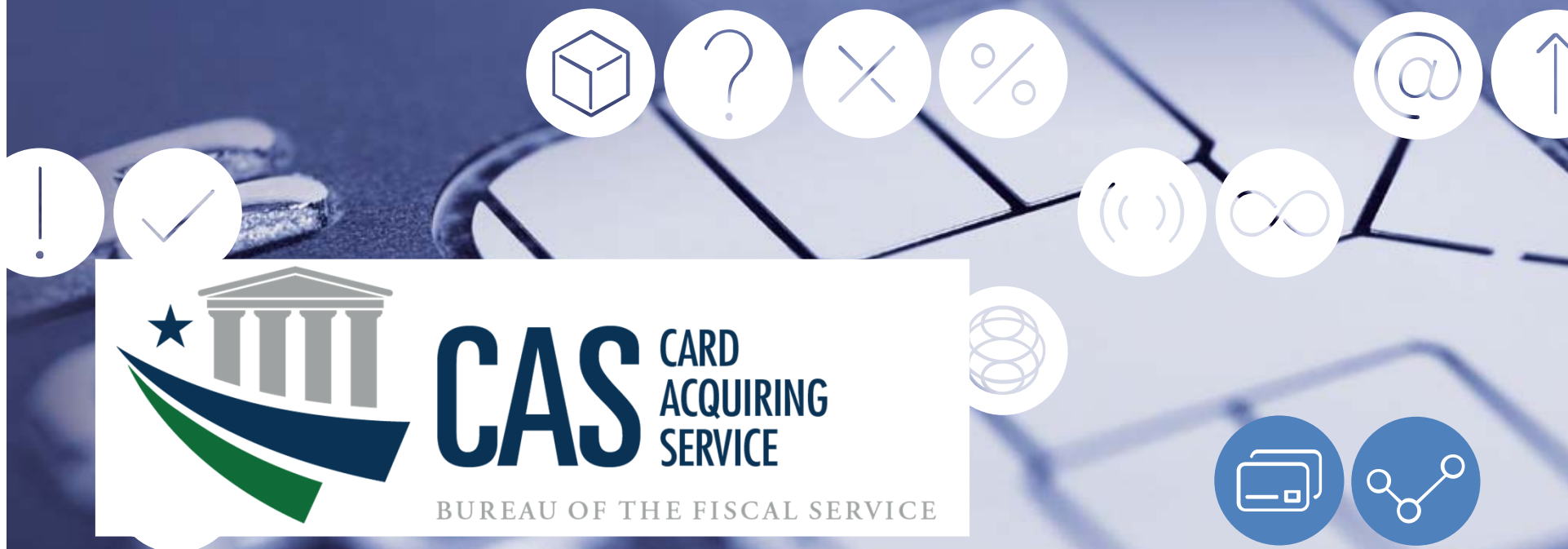




# EMV in the Security Equation



# Federal Agency Payment Card Acceptance Environment



# CARD ACQUIRING SERVICE (CAS)

---

- Processes credit & debit card transactions:
  - VISA, MasterCard, American Express, Discover and PIN debit
- CAS receives and processes card transactions initiated through Pay.gov (“card not present;” some “card present”), and point-of-sale (POS; “card present”) transactions:
  - POS transactions flow from standalone terminals (procured through CAS) and integrated POS systems (ISV/VAR; customized and procured agency-by-agency) directly to our card acquirer
- Program has grown steadily over the past decade with new agencies, agency expansion, and native growth with convenience of cards
- FY14 Volumes: 121 mil. transactions, \$11.5 billion
  - Avg. Transaction: \$95

# CAS Program Metrics\*

## Agency Accounts

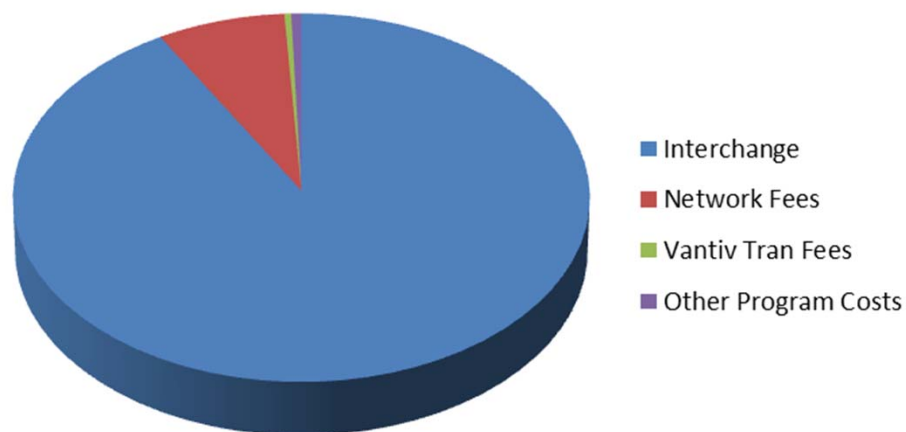
731 agency accounts

6,801 Physical Locations

9,462 Acceptance points

- 38% Standalone terminals
- 40% ISV/VAR
- 21% Pay.gov

## FY 2014 Expense Summary



## How much is collected?

Transaction Volume (dollars):

- Over \$11.5 billion collected on cards in FY2014
  - POS: ISV/VAR/Standalone Terminals collects 49%
  - Pay.gov collects 51%

Transaction Count:

- Over 121 million transactions in FY2014
  - POS: ISV/VAR/Standalone Terminals collects 74%
  - Pay.gov collects 26%

**\*NOTE: As of Fiscal Yearend 2014**



# Replacing Agencies' Standalone Terminals

---

1. Fiscal Service RCM initiates agency contact
  - Configuration summary showing current agency terminal footprint shared for validation/update by agency
    - Agency confirms terminals for replacement and terminals to be deactivated/not replaced
    - Agency confirms location POCs
  - Inter-agency agreement enabling reimbursement of Fiscal Service shared for review/completion by agency
    - Agencies will only pay for actual terminals delivered and related costs, regardless of IAA estimate cost
2. Fiscal Service turns agency over to deployment partner Vantiv with return of validated configuration summary
  - Vantiv ships terminals and contacts agency location POCs to schedule installation and training

# Replacing Agencies' Standalone Terminals

---

## 3. Terminals installed by agency location

- Replacement terminals/PIN pads plugged in
- Terminals requiring just a software upgrade receive download (and PIN pad)
- Agency locations verify with live transactions
  - Troubleshooting with Vantiv if necessary
- Replaced terminals and terminals no longer needed are deactivated

## 4. Agency billing

- With authorization through IAA, and based on actual terminal/PIN pads shipped and locations installed, Fiscal Service initiates IPAC to agency for reimbursement



# Agencies with Integrated POS Systems

---

- Known by several terms: ISVs, VARs, electronic cash registers, integrated card solutions
  - Common denominator: these applications are built and operated by agencies and process through to the CAS program acquirer Vantiv, but these are not supported directly by CAS
- These POS card acceptance points are not subject to the “Treasury Plan” through which CAS is replacing standalone terminals with EMV-compliant terminals
  - CAS still wants to understand agency planning around EMV for these solutions
- Agencies with integrated POS solutions need to be mindful of the following:
  - EO requirement that any card acceptance upgrades post-12/31/2014 must be EMV-compliant
  - 10/1/2015 liability shift under card rules to agency for counterfeit card use if card used at non-EMV-compliant POS
    - Liability realized through chargeback for amount of transaction

# Contacts

---

## CAS Program Contacts

Ian Macoy; Director, Settlement Services Division

(202) 874-6835

[Ian.Macoy@fiscal.treasury.gov](mailto:Ian.Macoy@fiscal.treasury.gov)

Richard Yancy; CAS Program Manager

(202) 874-5217

[Richard.Yancy@fiscal.treasury.gov](mailto:Richard.Yancy@fiscal.treasury.gov)

Lynette Newby; CAS Program Specialist

(202) 874-9208

[Lynette.Newby@fiscal.treasury.gov](mailto:Lynette.Newby@fiscal.treasury.gov)

## Additional Contacts

Card Acquiring Service

[CardAcquiringService@fiscal.treasury.gov](mailto:CardAcquiringService@fiscal.treasury.gov)

Agency Relationship Management

[ARM@fiscal.treasury.gov](mailto:ARM@fiscal.treasury.gov)

Vantiv Customer Support

(866) 914-0558

[rmtreasury@vantiv.com](mailto:rmtreasury@vantiv.com)

## CAS EMV Resources Site:

[https://www.fiscal.treasury.gov/fsservices/gov/rvnColl/crdAcggServ/rvnColl\\_cas\\_emv.htm](https://www.fiscal.treasury.gov/fsservices/gov/rvnColl/crdAcggServ/rvnColl_cas_emv.htm)

- Executive Order 13681
- Links to Fiscal Service webinars
- EMV and deployment FAQs
- Replacement terminal Information
- EMV education resources
- Links to card network rules around EMV liability

# Appendix: EMV Resources



# Additional Resources

---

## Great video resources are available online!

Why EMV is coming and demonstration using an Ingenico Terminal:

<https://player.vimeo.com/video/97432622>

Visa training video on accepting an EMV transaction:

<https://www.youtube.com/watch?v=xA7jt7RFr8Q&feature=youtu.be>

Setting up your VeriFone and Ingenico terminals and adding a PIN pad:

<https://www.youtube.com/watch?v=472XB5-1jQo>

Changing the date and time on your VeriFone and Ingenico terminals:

<https://www.youtube.com/watch?v=MGKu5w6A27E>

Running reports on your VeriFone and Ingenico terminals:

<https://www.youtube.com/watch?v=Wl1RXI77dgQ>

# Ingenico iCT220 Terminal



# Ingenico iPP310 PIN Pad

---

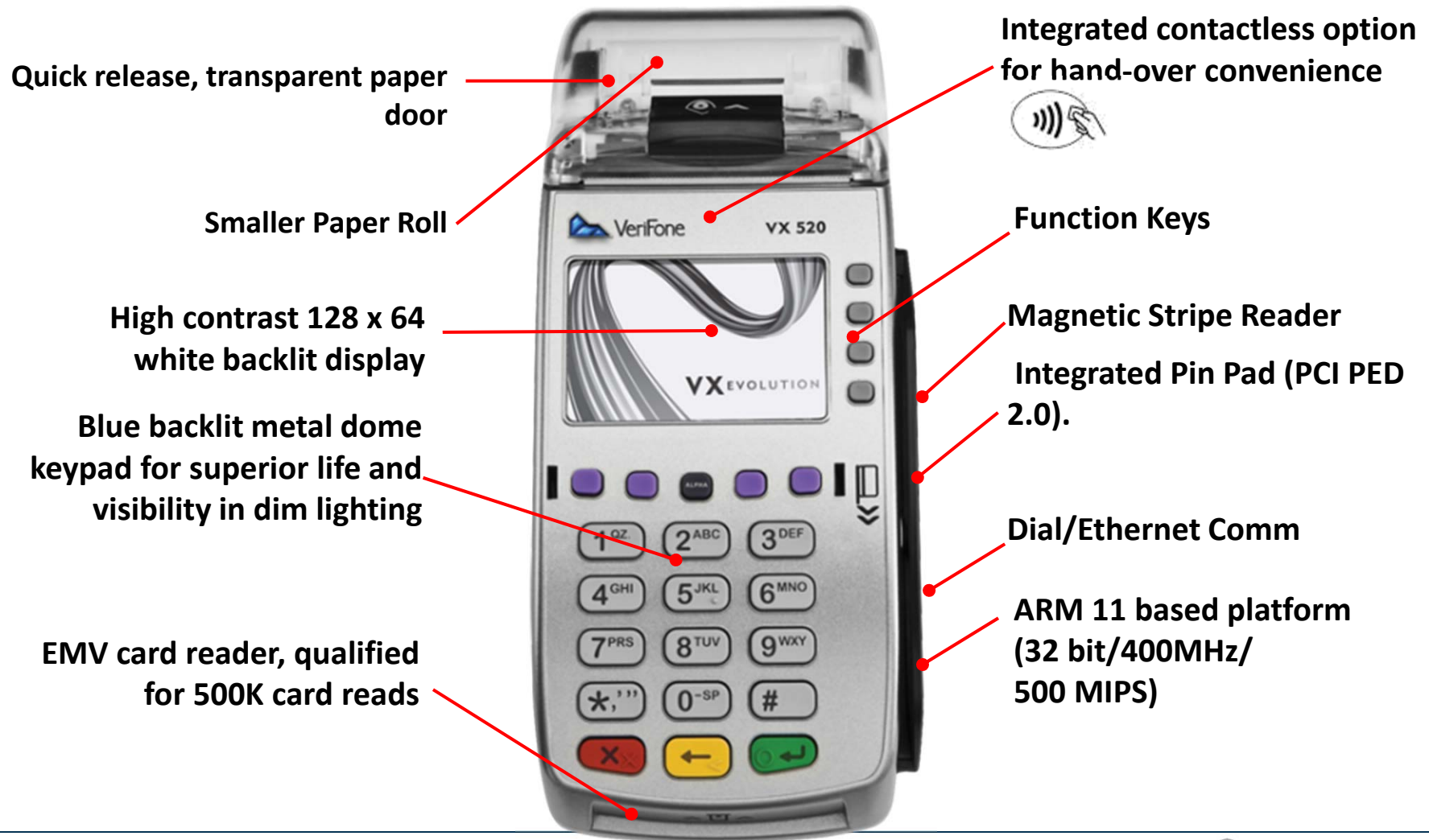
- Built in Swipe for Credit and Debit Transactions
- Built in Contactless/NFC Reader
- Built in EMV Card Reader
- 128 x 64 White Backlit Display
- PCI PED 2.1 / PCI PTS 3.0
- Allows Customers to Swipe/Tap their own card creating faster check out times and improved service.
- Promotes PIN based transactions since the PIN Pad can be utilized for Credit, Debit, and EMV transactions.
- 19 key, Raised, Backlit Key pad





# VeriFone Vx520 – For Existing Agencies

---

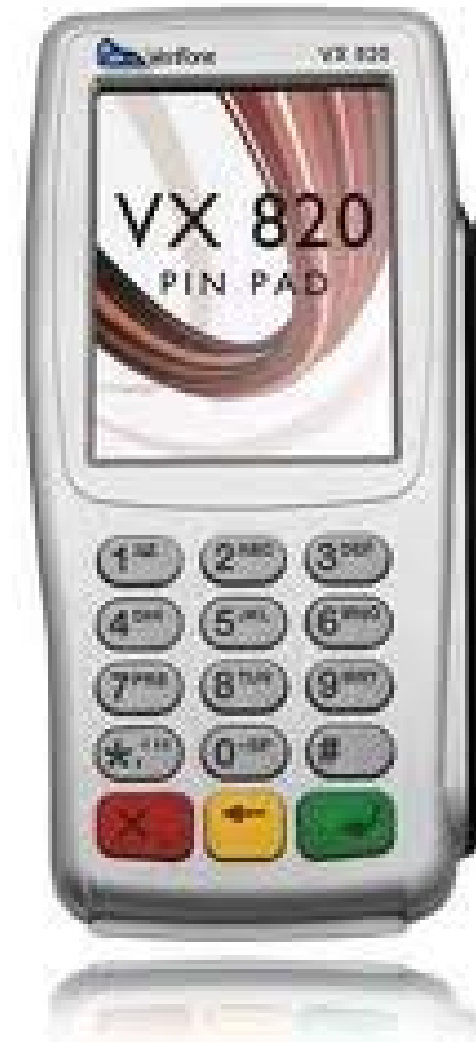




# VeriFone Vx820 PIN Pad

---

- Built in Swipe for Credit, Debit and EBT Transactions
- Built in Contactless/NFC Reader
- Built in Smart Card Reader/EMV
- High Resolution 3.5" Display
- PCI PED 2.0 / PCI PTS 3.0
- Allows Customers to Swipe/Tap their own card creating faster check out times and improved service.
- Promotes PIN based transactions since the PIN pad can be utilized for Credit, Debit, and EMV transactions.



# EMV vs. Mag Stripe

---

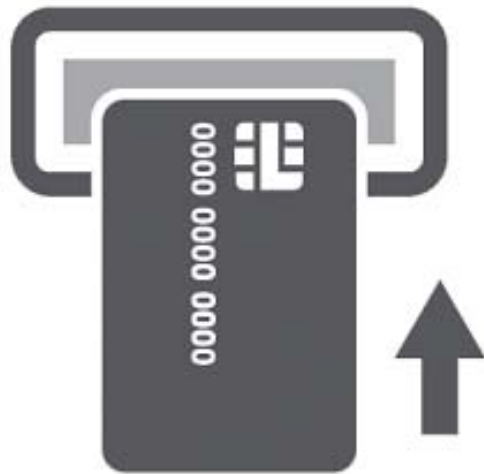
For contact chip cards, your customers must insert the chip card into the payment terminal reader instead of swiping the card as they do with a magnetic stripe card. Also, your customers must leave the chip card in the payment terminal reader until the transaction is authorized.

For contactless cards and mobile devices (NFC), your customers will simply hold the contactless chip card or mobile device up to the payment terminal for a few seconds, until the 4 lights flash and a beep is heard signifying the contactless chip card or mobile device has been successfully read.



# How To Process an EMV Card

---



## Step 1

**Insert your card into the terminal facing up and chip end first**



**Do not remove your card until the transaction is complete. If you remove it too soon, your transaction will be canceled.**

# How To Process an EMV Card

---



## Step 2

**Follow the on-screen prompts.**

# How To Process an EMV Card

---

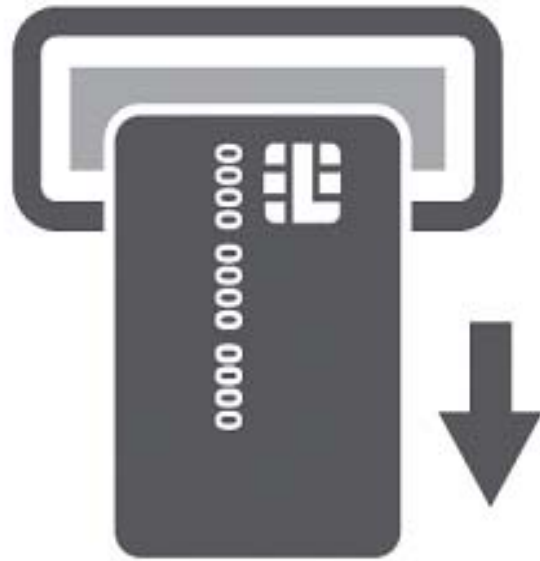


## Step 3

To help ensure only an authorized user has your card, you may be required to enter a PIN or sign the receipt.

# How To Process an EMV Card

---



## Step 4

**Remove your card when prompted.**

# EMV Fallback

---

Fallback allows for mag stripe processing if there is an issue with EMV chip processing.

- Technical Fallback
  - Terminal cannot read chip
  - Terminal prompts cardholder to swipe card
- CVM Fallback
  - PIN Try Counter on card is exceeded
  - PIN Entry Bypass is used
  - Issuer personalizes the card to decide:
    - Decline
    - Fallback to Signature
    - No CVM



# EMV FAQ

---

- What happens if I swipe an EMV card?
  - If your terminal is EMV enabled, you will see a message on the terminal and PIN Pad instructing you or the cardholder to insert the card.
- What happens if a consumer leaves a Chip Card in the terminal?
  - Follow a similar procedure as today - secure the card in a safe location and ensure it is returned to the right person with ID verification if the consumer should return to the store. Otherwise, securely destroy the card.

# EMV FAQ

---

- How can I accept payments?
  - There are 3 ways to pay on the Ingenico iCT220 and iPP310:
    - Swipe the magnetic stripe on a card
    - Insert the EMV chip on a card
    - Tap a NFC device (card, phone, watch, etc...) on the terminal
- What cards types are accepted at my new terminal?
  - **Credit and Debit Cards** – Visa, MasterCard, Discover, Amex, JCB, Diners Club, and China Union Pay.
  - **PIN Debit Cards** – Accel, AFFN, CU24, Jeanie, Maestro, Interlink, NYCE, Pulse, STAR, Shazam, and Networks
  - **NFC Wallets** – Apple Pay and Google Wallet

# EMV FAQ

---

- Will my old paper rolls fit the new terminal?
  - Likely not depending on the model of your old device. The iCT220 uses 2 ¼" x 50' Thermal paper. For your convenience, each terminal arrives with 3 new rolls of terminal paper. Paper can be purchased from a variety of online stores, office supply stores, or by calling Vantiv at 1-866-914-0558.
- What should I do with my old terminals?
  - The old terminals are owned outright by your Agency. Please discuss with your internal staff your policies for disposition of excess equipment or secure destruction for end of life electronic equipment

# Ingenico Help and Troubleshooting

---

- I need to reprint a receipt on my Ingenico terminal.
  - Press Enter button
  - Scroll down to “other” (#9)
  - Choose #3 – “Reprint”
  - Last receipt
- Terminals will settle at 12:01am local time. If you would like a different auto-settlement time\*:
  - Press [.,#\*] key
  - Choose #3 “Setup” menu
  - Choose #5 “Trans options”
  - Choose #4 “Settlement”
  - Choose #6 “Settlement – Set Time” (must be military)

\* it is not recommended to alter the auto-settlement time.

---

# Ingenico Help and Troubleshooting

---

- I need to dial a 9 or other code to get an outside line.
  - Press [.,#\*] key.
  - Enter password: V123456
  - Select “Setup Menu”
  - Select “Communications”
  - Select “Dial”
  - Select “Terminal Setup”
  - Select “Access Code”
  - *Input Access Code* and press Enter
- What if the date and time are not correct on my new terminal?
  - You can reset the date and time by following the instructions provided in this online training video: <https://www.youtube.com/watch?v=MGKu5w6A27E>
  - Call the Federal Agency Support Line at 1-866-914-0558