

A close-up photograph of a hand holding a silver credit card over a payment terminal keypad. The keypad has various colored buttons: red, yellow, green, and grey. The background is dark and out of focus.

Everything You Wanted to Know About Payment Processing But Were Afraid to Ask

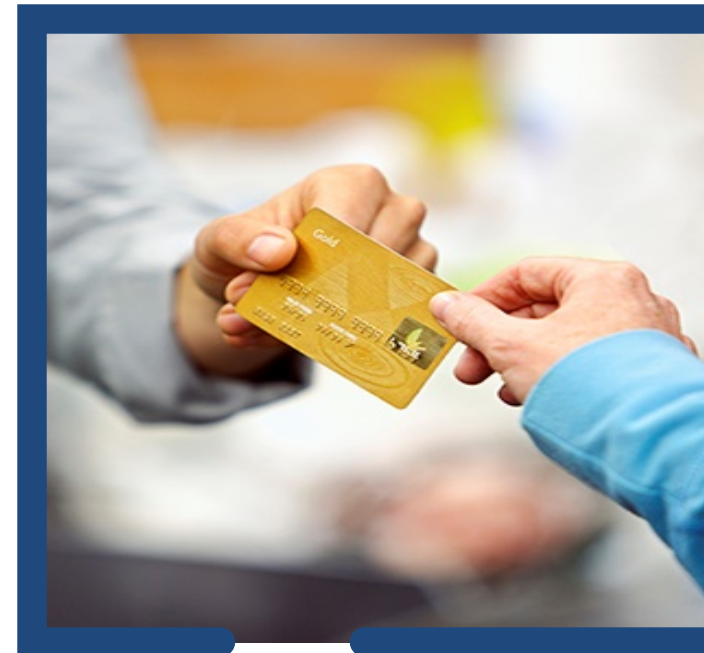
Payment Procession 101

Kathleen Ervin & Carrie Daniels, TSYS



QUESTIONS FOR YOUR PROCESSOR

- How are you taking payments today?
- How would you like to take payments?
- What products and services are best for your type of business?
- What questions do you have?



TODAY'S AGENDA

- The basics of merchant processing
- The Golden Rule of taking credit cards
- Interchange
- EMV® and retail
- What is PCI Compliance and why it's important?
- Q&A



WHAT IS MERCHANT PROCESSING?

A **payment processor** is a company appointed by a **merchant** to handle transactions from various channels such as credit cards and debit cards for **merchant** acquiring banks.



WHAT IS MERCHANT PROCESSING? (CONT'D)

- Credit and debit cards payment processing
- Point-of-sale (POS)
- B2B Level II, Level III
- Recurring billing payments
- Web or E-Commerce
- Mobile
- Apple Pay®
- ACH or Automated Clearing House check drafting and payment services
- Check guarantee and check conversion services
- Gift card and loyalty programs

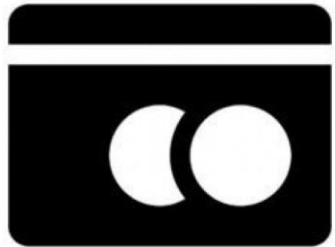


DIFFERENCE BETWEEN DEBIT & CREDIT CARDS



DEBIT/CHECK CARDS

- Draws money from a bank account. Debit requires a PIN.
- Check cards use the Visa[®] /MasterCard[®] interchange.



CREDIT CARDS

- Draws money against a credit limit.
- Over 250 types of credit cards including bank-issued cards, rewards, corporate and gift cards.

THE GOLDEN RULE OF ACCEPTING CREDIT CARDS



Handle your customer's credit card data the way you want your own credit card data to be handled.

- How you and your staff accept cards
- How you store card data

WHAT IS INTERCHANGE?

Interchange describes the fee paid for the acceptance of card-based transactions.

Interchange fees can be based on:

- Card brand (V, MC, A or D)
- Type of credit or debit card
- Type and size of the accepting merchant
- Type of transaction
(e.g. online, in-store, phone order, whether the card is present for the transaction, etc.)



WHAT IS YOUR RATE?

- **Interchange**

Percentage of the dollar amount of transaction plus a per item transaction fee

- **Assessments**

Percentage of the dollar amount of the transaction

- **Discount Authorization**

Cents per item



WHAT IS YOUR PRICING MODEL?

- **Buckets:** Qualified, Mid-Qualified and Non-Qualified
- **B2B pricing:** Level II, Level III
- **Bundled** with a Base Rate and Surcharges
- **Pass-through**
- **Flat rate** eg. Square™ or PayPal™



EMV® and Other Security Considerations



WHAT IS EMV®



WHAT IS EMV

- An acronym for Europay®, MasterCard® and Visa®
- Global standard for the implementation of microchip cards for the purpose of facilitating a more secure electronic payment transaction
- A security framework that defines the payment interaction at the physical, electrical, digital, data and application levels between chip cards and payment devices

EMV is also known as “chip-and-PIN” in the U.K.; domestically, EMV may be implemented as chip-and-PIN, chip-and-signature or other variations.



INDUSTRY TRENDS

Highlights

- October 2015 Liability Shift: The party responsible for a chip transaction not occurring will be financially liable for any card-present counterfeit fraud losses.
- As of 2015, 1.5 billion+ cards that are in use in the U.S., only 394 million are EMV capable.¹
- As of 2015, issuers have distributed 166 million EMV credit cards and 105 million EMV debit/prepaid cards, which account for just 29% and 17% of the total cards in circulation by the card brands.²
- Estimated 4.5 million chip-capable terminals to be installed in the market.³
- **Estimates are that counterfeit card present fraud will fall 51% due to EMV chips.**⁴
- However, online and card-not-present fraud is estimated to increase 106%, from \$3.3 billion to \$6.4 billion.⁴

Industry Response

- Product and Technology
 - EMV terminals are made available for card present environment
 - EMV compatible mobile solutions become available
 - POS application certification
 - Semi-integrated processing in process

¹ Source: www.businessinsider.com 2016 article "US EMV is still slow-going"

² Source: Javelin Strategy & Research: 2014 Press Release "Javelin Forecasts U.S. to Reach Global Parity in EMV by 2018"

³ Source: www.emv-connection.com 2014 "U.S. Migration to Chip Payments Accelerates as EMV Migration Forum"

⁴ Source: www.banktech.com 2014 article "Chip and Quill: How EMV Will Increase Card Fraud in the U.S."

DEFINITIONS



- **EMV:** Europay, MasterCard and Visa — The global standard for the implementation of chip cards for the purpose of facilitating a more secure electronic payment transaction. EMV can help protect against card counterfeit and fraud.
- **Tokenization:** Different from encryption. Instead of scrambling the card data with a key that allows decryption at an end point, it substitutes the card number and related information with a single token that can be used to process a financial transaction with no correlation to the actual card number.
- **P2PE/Point-to-Point Encryption:** Encrypts card data from the point of card swipe, card dip, or manual entry so the card data is never captured by, or exposed to, the POS operating system and merchant network. The card data is decrypted at the point it reaches the payment gateway/processor.
- **NFC:** Near Field Communication is a technology that leverages short-range wireless/radio communication to initiate a connection between devices such as a smartphone and POS device to pass data. This is the technology leveraged to support secure “contactless” payment processing such as Apple Pay™ and Google Wallet™.

HOW DOES EMV AND/OR CONTACTLESS BENEFIT MERCHANT?

Liability Shift October 2015: The party that is the cause of a contact chip transaction not occurring will be financially liable for any resulting card present counterfeit fraud losses.

Visa®

- EMV must be enabled

Mastercard®

- EMV must be enabled
- Must support both contact and contactless interfaces

American Express®

- EMV must be enabled

Discover®

- EMV must be enabled
- Must support both contact and contactless interfaces

The Liability Shift encompasses **all face-to-face transactions**, including cash advance. It does **NOT** cover contactless/mag stripe cards, card-not-present transactions, lost cards, stolen cards or fraud.

EMV TERMINALS



VeriFone VX520

EMV and Contactless capable
released 6/28/2013 – PCI PED v3



Ingenico ICT220CL

EMV and Contactless capable



Ingenico ICT250

EMV and Contactless capable
released 3/28/2014 – PCI PED v3

CORE WIRELESS TERMINAL DEVICE STATUS



VeriFone VX680
EMV and Contactless capable
released 12/5/2013 – PCI PED v2



Ingenico IWL252 and IWL255
EMV and Contactless capable
released 3/28/2014 – PCI PED v2 –
3G SIM Card GPRS and Bluetooth



PCI COMPLIANCE

Keeping Cardholder Data Safe



WHAT IS PCI COMPLIANCE?

Payment Card Industry Security Standards Council

- Global Forum of Industry Leaders
- Launched in 2006
- Development of Industry Security Standards
 - Data Security Standards (PCI-DSS)
 - Payment Application Data Security Standards (PA-DSS)
 - PIN Transaction Security Requirements (PTS / PCI-PED)
- Primary Goal is to Protect Cardholder Data



WHY PCI?

90% of all breaches occur at small businesses.¹



Merchants are at the center of payment card transactions.



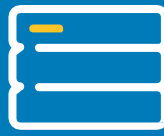
Merchant-based vulnerabilities can occur almost anywhere in the card-processing environment.



Point-of-sale
devices



Personal
computers



Servers



Wireless
hotspots



Web shopping
applications

¹ Source: National Small Business Association Small Business Congress white paper "Small Business ID Theft and Data Breach, 2015"

WHY DO I NEED TO BE PCI COMPLIANT?

"I'm only a small business. Why do I need to be compliant?"

- 90% of all breaches occur at small businesses.¹ That's why the card companies mandated that all businesses, regardless of size, must become compliant.

"My business is low-risk; I'm not concerned about compliance."

- Even the lowest-risk business is vulnerable to a security breach. And expenses from a breach can be financially devastating, even as high as \$500,000. Compliance greatly reduces the risk.

"Will compliance guarantee that I won't have breach expenses?"

- While it certainly reduces the risk, there are no guarantees against a security breach.

¹ Source: National Small Business Association Small Business Congress white paper "Small Business ID Theft and Data Breach, 2015"

HOW PCI AFFECTS MERCHANTS

All merchants are required to comply with the PCI Data Security Standard

- Industrywide requirement
- Ensures that cardholder data is handled properly
- Minimizes the risk of a breach by following industry best practices
- PCI Compliance is an annual requirement



GUIDING MERCHANTS TOWARD COMPLIANCE

What to expect from the validation process

PCI Compliance programs offers services that help merchants become and stay compliant as requirements change. To get started, merchants should visit www.compliance101.com/PCI.

Self Assessment Questionnaire (SAQ)

- Intuitive, easy-to-use tool, even for online/computer novices
- Picture-driven qualification helps merchants easily determine their validation type
- Expert help text and real-life examples

Offers personalized services to each merchant

- Network vulnerability scans for merchants that have external-facing IP addresses
- Web application scans to find holes in web-based applications
- Easy-to-understand reports that detail the scan results and prioritize vulnerabilities by severity
- Hands-on assistance to provide remediation guidance

Q&A

TSYS is a long-standing NFIB Member Benefit provider.

To learn more about TSYS' products and services, please contact us at (800)619-5301

Visit [NFIB.com](https://www.nfib.com) to learn more about the NFIB Member Benefit programs.



©2018 Total System Services, Inc.® TSYS® is a federally registered service mark of Total System Services, Inc. EMV is a registered trademark or trademark of EMVCo LLC in the United States and other countries. Apple Pay is a registered trademark of Apple Inc. Google Wallet is a trademark of Google Inc. All trademarks contained herein are the sole and exclusive property of their respective owners. Any such use of those marks without the express written permission of their owner is prohibited. TSYS Merchant Solutions is a registered ISO of Wells Fargo Bank, N.A., Concord, CA; Synovus Bank, Columbus, GA, and First National Bank of Omaha, NE. TSYS Business Solutions LLC is a registered ISO of Wells Fargo Bank, N.A., Concord, CA; Synovus Bank, Columbus, GA; and Deutsche Bank, New York, NY for Visa and Mastercard transactions only.

Kathleen Ervin
Director, NFIB Relationship Management

615-593-5327

KErvin@tsys.com

TSYS.com

