Capgemini
CONSULTING.TECHNOLOGY.OUTSOURCING

WHAT YOU NEED TO KNOW
CARDS

Global Trends in the Payment Card Industry 2013: Processors

Key challenges faced by card processors and implications for the payment card industry

People matter, results count.

Table of Contents

1. Highlights

As payment card usage continues a steady increase worldwide, fraud is not far behind relentlessly nipping at the heels of the industry's security measures. According to the figures released in 2012 by ECB Statistical Data Warehouse, cards have remained the most preferred non-cash payment instrument globally, with 58.8% of global non-cash payments originated via cards versus other non-cash payments, such as direct debit, credit transfers, and checks.

As fast as payment card processors implement consumer security measures, fraudsters and cyber criminals adapt to them and continue to hack into consumer card data.

As this game of one up-man-ship continues, today's need for higher security measures has led to two primary trends for card processors.

PCI DSS Standards

The payment card industry has developed a code of best practices designed to prevent hackers from obtaining consumer card details – Payment Card Industry Data Security Standards, or PCI DSS, for short. These best practices have been evolving over the past decade, the newest set of which was released November, 2013. Additionally, in an effort to tackle e-commerce fraud, payment processors are implementing a combination of authorization levels ranging from address verification, payer authentication program, real time authorization, calling the card issuing bank, and card verification methods, such as a one-time password.

Increasing Technological Innovation in Payments Processing

Over the past few years, payment card players have been cultivating new and innovative payment functions, such as near field communication (NFC), quick response code (QR code) and biometric identification, each of which has an increasingly important role in the payment card ecosystem.

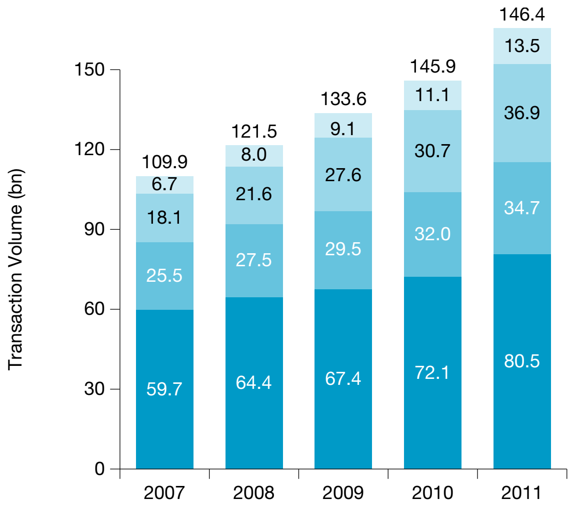
2. Introduction

2.1. Global Performance: Payment Card Industry Performance

Card usage across the globe has been growing since the financial crisis hit the world in 2008–2009. During 2011, the transaction volume for cards grew by 13.5%, which is considerably more than the growth rate of 9.2% seen during 2010 largely due to increasing debit card usage globally. The percentage share of cards in the mix of non-cash payments has been consistently growing and was 55.8% in 2010. In 2011, cards also remained the most preferred non-cash payment instrument globally, with 58.8% of the global non-cash payments originated via cards. The growing share of cards in the non-cash payment mix indicates an increasing preference for cards compared to other non-cash payment instruments, such as direct debit, credit transfers, and checks.

In developed countries, card transaction volume is very high, as consumers prefer to use cards even for low-value transactions. However, the developed countries have not been able to match up to the growth showcased by the emerging world. The growth in transaction volume of cards in Europe was in single digits at 8.6% in 2011 and in the U.S. it was 11.7%. This growth is hardly comparable to growth rates exhibited by Latin America, which saw a growth rate of 21.0% and Asia-Pacific, with a growth rate of 20% in 2011. Both Latin America and Asia Pacific have been showcasing enormous growth for the past few years.

Exhibit 1: Global Card Transaction Volume (bn) by Region, 2007–11



		CAGR 2007-'10	Growth 2010-'11
	Total	**9.9%**	**13.5%**
■	Latin America	18.6%	21.0%
■	Asia-Pacific	19.3%	20.0%
■	Europe	7.8%	8.6%
■	North America	6.5%	11.7%

Source: Capgemini Analysis, 2013; ECB Statistical Data Warehouse, 2011 figures released September 2012; Bank for International Settlements Red Book, 2011 figures released January 2013, Country' Central Bank Annual Reports, 2011

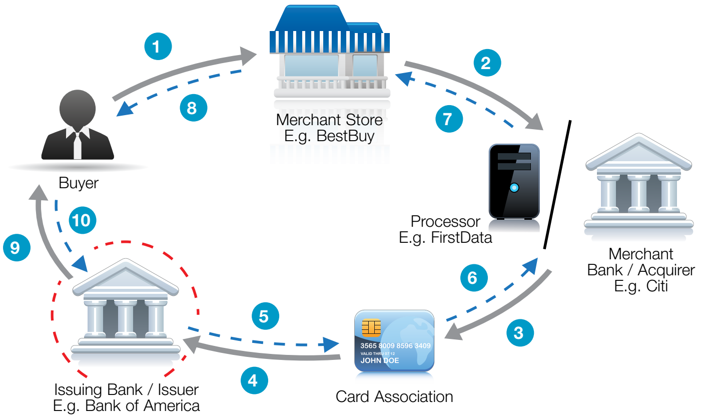
In terms of number of card transactions per inhabitant, North America emerged as the market leader with an average number of transactions per inhabitant of 232.6 in 2011. This is significantly high when compared to Latin America (22.6 transactions per inhabitant) and Asia Pacific (13.1 transactions per inhabitant) in 2011. This trend is due to the high penetration of cards in North America. However, emerging countries have a high growth potential and card usage is likely to grow in the coming years as consumer preference shifts from cash to plastic. The growing acceptance of cards at various point-of-sale (POS) units is also likely to drive increased adoption and usage of cards in most emerging countries.

2.2. Key Payment Card Industry Participants

A simple card transaction between a cardholder and a merchant involves several players:

- **Card acquirers:** the merchants' banks
- **Card processors:** third-party organizations that aid in card authorization and settlement processes
- **Card issuers:** the cardholders' banks that issue the cards and maintains customers' accounts
- **Card association network providers:** typically MasterCard® or Visa®—play an essential role in completing the card authorization and settlement cycle, as illustrated below

Exhibit 2: Typical Card Transaction Flow Structure



1 Cardholder uses a credit card to pay for a purchase transaction

2 Merchant sends transaction information to the acquirer by swiping or manually feeding card information at the POS terminal

3 The acquirer or third-party processor on acquirer's behalf sends the transaction information to the card association

4 The card association sends the transaction information to the issuer for authorization

5 Issuing bank pays the card association network once it validates the transaction (after deducting their charge)

6 Card association pays the acquirer processors on acquirer's behalf (after deducting their charge)

7 Merchants account is credited for the transaction amount by the processor (after deducting their charge)

8 Purchase transaction is completed

9 Issuer bills the buyer for the transaction based on the billing cycle

10 Buyer settles the bill

Source: Capgemini Analysis, 2013; http://www.yahoofinance.com, August, 2012

This paper focuses on key trends card processors are experiencing and industry response to these trends.

3. An Overview of Trends in the Payment Card Industry: Processors

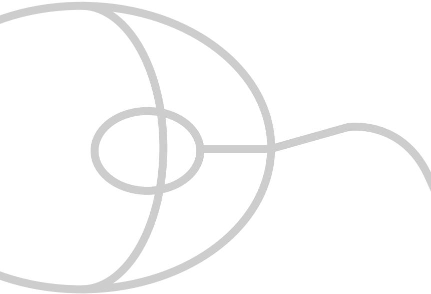
Credit card transactions are not processed by the merchant, but by a payment processor, instead—typically a third-party firm. Through secure internet connections, the processing firm processes, verifies, and accepts or declines credit card transactions on behalf of the merchant.

During this function, payment processors interact with numerous players, such as consumers, merchants, acquirers, card networks, and issuing banks. As cardholder data flows from one entity to another, and card information is aggregated at various collection points, it becomes vulnerable to exposure, loss, and theft. With increased card usage by end consumers, hackers have more chances than ever before, to breach security and obtain card information.

As such, there is greater demand for higher security measures from merchants and consumers, which has led to the following trends for card processors:

1. Evolution of PCI DSS standards
2. Increasing technological innovation in payments processing

While trends covered in the 2012 *Global Trends in the Payment Card Industry* series continue to be relevant, they are not discussed in detail in this paper.



Capgemini
CONSULTING.TECHNOLOGY.OUTSOURCING
WHAT YOU NEED TO KNOW
CARDS
Global Trends in the Payment Card Industry 2012: Acquirers
Key challenges faced by card acquirers and their implications for the payment card industry
People matter, results count.

Global Trends in the Payment Card Industry: Acquirers

Capgemini
CONSULTING.TECHNOLOGY.OUTSOURCING
WHAT YOU NEED TO KNOW
CARDS
Global Trends in the Payment Card Industry 2012: Processors
Key challenges faced by card processors and their implications for the payment card industry
People matter, results count.

Global Trends in the Payment Card Industry: Processors

Capgemini
CONSULTING.TECHNOLOGY.OUTSOURCING
WHAT YOU NEED TO KNOW
CARDS
Global Trends in the Payment Card Industry 2012: Issuers
Key challenges faced by card issuers and their implications for the payment card industry
People matter, results count.

Global Trends in the Payment Card Industry: Issuers

4. Trend 1: Evolution of PCI DSS Standards

4.1. Background and Key Drivers

It is of utmost importance that processors and other card industry participants upgrade their infrastructure to comply with stringent security standards, such as those outlined by the Payment Card Industry Data Security Standard (PCI DSS).

PCI DSS was created by the PCI Security Standards Council, in collaboration with leading card networks, including Visa, MasterCard, American Express, Discover, and JCB, International. Until November, 2013 PCI DSS 2.0, was the most recent version. Its primary contributions were to enhance clarity, improve flexibility, and address evolving threats. With the introduction in November 2013 of PCI DSS 3.0, this newest set of updated global standards will be enforced industry-wide in 2015.

4.2. Analysis

PCI DSS is a widely accepted set of policies and procedures formed to provide a high level of security to card transactions and protection to cardholders against misuse of their personal information for fraudulent purposes. The initial PCI DSS was focused on six major objectives.

1. Maintain firewalls and a secure network in which transactions could be conducted
2. Protect cardholder information and encryption of cardholder data when transmitted through public networks
3. Protect systems against activities of malicious hackers by using frequently updated antivirus software, anti-spyware programs, and other anti-malware solutions
4. Ensure restricted access to system information and operation by assigning a unique and confidential identification name or number to every person who accesses the system
5. Consistently monitor and regularly test the networks to ensure all security measures and processes are in place, functioning properly, and up-do-date
6. Ensure that a formal information security policy is defined, maintained, and followed at all times and by all participating entities, and enforce audits and penalties for non-compliance

PCI DSS Version 2.0

Released in 2010, PCI DSS 2.0 was a set of 12 of security controls that businesses are required to implement to help protect credit card data.

Any organization that handles payment card, including debit and credit cards, must meet the 12 requirements directly or through a compensating control. Compensating controls, however, are not always allowed and must be approved on a case-by-case basis by a PCI QSA[1]. Failure to meet PCI DSS requirements may result in fines or termination of credit card processing privileges.

[1] Payment Card Industry Qualified Security Assessor (PCI QSA) is a designation conferred by the PCI Security Standards Council to individuals it deems qualified to perform PCI assessments and consulting services

Twelve Requirements

1. Install and maintain a firewall configuration to protect cardholder data
2. Do not use vendor-supplied defaults for system passwords and other security parameters
3. Protect stored cardholder data
4. Encrypt transmission of cardholder data across open public networks
5. Use and regularly update antivirus software
6. Develop and maintain secure systems and applications
7. Restrict access to cardholder data to a business need-to-know basis
8. Assign a unique ID to each person with computer access
9. Restrict physical access to cardholder data
10. Track and monitor all access to network resources and cardholder data
11. Regularly test security systems and processes
12. Maintain a policy that addresses information security

The new set of PCI DSS 3.0 standards will be enforced in 2015. To develop the standards, PCI SSC obtained inputs on the standards from its global stakeholders through a variety of avenues, which included a formal feedback period. This feedback process provided an opportunity for more than 700 participating organizations including merchants, banks, and processors to play an active role in improving global payment security. According to PCI SSC, version 3.0 will introduce more changes than version 2.0. While the 12 core security areas will remain the same, the updates will include several new sub-requirements, which did not exist in version 2.0. In an effort to allow organizations more flexibility in planning for and adapting to these changes, these sub-requirements will be best practices until July 1, 2015. On that date compliance enforcement begins in earnest. With that said, however, these organizations are being encouraged to begin implementation of version 3.0 as soon as possible.

The updated standards seek to add more flexibility for integrating card security into the payments business-as-usual activities. Simultaneously, the changes will look to provide increased stringency for validating proper implementation. Additionally, the changes are expected to outline more rigorous and specific testing procedures that will seek to clarify the level of validation the assessor is expected to perform.

PCI DSS Version 3.0

In addition to the original 12 requirements of version 2, PCI DSS version 3.0 will additionally:

- Provide stronger focus on some of the greater risk areas in the threat environment
- Build greater understanding of the intent of the requirements and outline how to apply them
- Improve flexibility for all entities implementing, assessing, and building to the standards
- Drive more consistency among assessors
- Help manage evolving risks/threats
- Align with changes in industry best practices
- Clarify scoping and reporting
- Eliminate redundant sub-requirements and consolidate documentation

4.3. Implications

To ensure stakeholder compliance with these standards, stringent processes have been implemented.

- Large card processors are subject to periodic external audits and certification
- While smaller merchants are exempt from mandatory external audits, they are subject to self-certification with a possibility of audit
- Failure to meet standards is punishable by levying fines

Considering the need for compliance and standards updates, which must be met by 2015, 2014 could be a year that might offer opportunities to professional services firms to develop solutions for the same. As it is an industry practice to comply with PCI DSS standards, many processing firms are likely to try and meet the new set of requirements as soon as possible. Once the new requirements are released, professional services firms should jump in head first to develop their customary solutions for the same as it is likely to throw open a market in 2014 and 2015.

2ABC
3DEF
5JKL
6MNO
8TUV
9WXY
#
0
CORR
OK
CANC
ANNUL

5. Trend 2: Technological Innovations in Payments Processing

5.1. Background and Key Drivers

Consumers continually demand newer, personalized, and secure transaction technologies. To that end, they expect better security and convenience for these transactions. With the growing market of smartphones, the global population is becoming more technologically savvy and, naturally, wants access to on-the-go payments.

The payments industry has been under pressure to cater to these demands. Processors are responding by adopting newer technologies and capabilities.

To a large extent, processors have kept pace with technology by developing payment solutions, based on technologies that have made their presence felt or are likely to overtake the market.

Over the last few years, for example, major technologies that have emerged into the payments ecosystem include near field communication, quick response code, and biometric payment.

5.2. Analysis

Payment processors have built the infrastructure to process payments through the use of newer technologies for payment transactions, which many consumers have been using for other purposes:

- NFC to exchange data among themselves
- QR codes for quick access to certain links
- Biometric details for identification purposes, such as during immigration checks

Near Field Communication

Through NFC technology, two similar devices can establish a radio communication with each other when brought together in close proximity. This technology has been adapted to the payments market and is being increasingly implemented on a global scale. In order to make a transaction, a consumer simply needs to bring an NFC-enabled smartphone in close proximity to the NFC payment device at the point of sale terminal, and then key in the authentication pin into the phone. To conduct NFC payments, the user simply needs to link bank account or credit/debit card with NFC-supporting applications, such as Visa Contactless Payments. The application will automatically detect the need to make a payment upon close proximity to another NFC device that is structured to receive payments.

It is estimated that 140 million NFC handsets were sold in 2012 and that 170 million units are in use worldwide. The number of units will rise rapidly through 2017 when 2.1 billion NFC handsets are anticipated to be in use. There has been a similar growth in NFC terminals. It is estimated that 3.9 million NFC-ready POS terminals were shipped in 2012, which was double the 2011 total. By 2017, 44.6 million NFC-ready POS terminals will be shipped annually[2].

[2] The installed base of NFC-enabled handsets to reach 2.1 billion units by the end of 2017, http://www.thepaypers.com, June 5, 2013

Although the NFC infrastructure is increasing at a rapid pace, NFC payments have only a minute share in the total volume of mobile payments. By the time 2013 statistics are available, it is estimated that 245.2 million people will have made a mobile payment worth $235.4 billion (USD) with 2% of those transactions having gone through NFC. By 2017, 450 million users globally are likely to make mobile payments of $721 billion (USD), with 5% of that total expected to be NFC growth[3].

“

We see the use of QR Codes as a means to reduce data quality issues, decrease costs, improve efficiencies, and enhance the customer experience. It’s a win-win for consumers and billers, alike, and the industry evaluation will help to develop a marketplace of users.”

Rich Langan
Senior Product Manager, DST Output

Quick Response Code

The quick response code or QR code, for short, was first used by the automotive industry in Japan. Today it has been successfully implemented in the global payments industry, as well. It works like this: The consumer links his bank account or debit/credit card details with an online payment processor equipped to carry out QR code transactions. On scanning the QR code through a phone or tablet, the user’s bank information is unlocked and transactions can be completed after proper authorizations. Because it is easy to generate a QR code, the system offers convenience to businesses and consumers, alike. It can be printed on business cards, points of sale, and product labels which customers can simply scan to pay for a product or service.

The focus of the industry on QR payments seems to be growing. PayPal made an announcement at the Money2020 trade show in Las Vegas in October, 2013, that it intends to introduce an app which will enable QR payments in 2014. In December 2012, the Electronic Payments Association’s Council for Electronic Billing and Payment (CEBP) collaborated with its members to develop recommendations on ways to approach consumer bill payments through QR Codes.

These guidelines contain recommendations regarding QR code size, the data to be included, and layout of the data represented in the QR code, among others.

NACHA, the U.S.-based electronic payments body, is currently investigating a December, 2012, proposal of *QR Encoding for Consumer Bill Payment Guidelines*. More than 20 companies have signed on to evaluate the guidelines, with US Bank and Verizon among them. The purpose is to evaluate factors that may arise from paying bills via QR codes and to identify an open standard for using QR codes in various billing and payment models.

[3] Gartner, Inc: Forecast: Mobile Payment, Worldwide, Sandy Shen, May 15, 2013

Biometric Payments

Since, ideally, biometric payments require a thumb or fingerprint to authorize a transaction once a card is swiped, it is perceived as very secure. PayTouch, headquartered in Spain, has gone a step further by linking credit or debit cards to two fingers of the user on its PayTouch server. To make a payment, the user simply presses two fingers on a PayTouch pad. When Saral Money was recently launched in India, for example, it began using the Adhaar database, which includes biometric information of the Indian population, along with TSYS's technology to authenticate the user by confirming fingerprints collected at POS. There is scope in this technology to even incorporate other biometric features, such as retina scans and voice recognition.

5.3. Implications

These newer mobile payment technologies offer better convenience and security to consumers. With a growing number of smartphones, particularly those with NFC capability, more consumers are likely to want to pay using these newer technologies. Since merchants need proper technological infrastructure to accept payments through these technologies, they are likely to seek out professional services firms to develop it for them.

Starbucks saw close to four million mobile payment transactions in 2013, nearly double the two million transactions of 2012. Additionally, mobile payments now account for approximately 10% of the total U.S. revenue of Starbucks[4].

Considering the growing presence of these payment methods, more processors are likely to offer these types of payment services. It would be well worth the time and effort for payment processors to keep tabs on the market and remain ever-diligent in seeking new and emerging technologies which could have the potential for development of a payment function.

[4] http://www.mobilecommercedaily.com/starbucks-generates-10pc-of-u-s-revenue-from-mobile, April 29, 2013

References

1. *Bank of America tests QR code mobile-payment service*, Marguerite Reardon, http://www.cnet.com, September 27, 2012
2. *Billing scheme may provide consumers with QR code payment model*, Zen Terrelonge, http://www.mobile-ent.biz, April 19, 2013
3. *Biometric Payment*, http://www.morpho.com
4. BIS Red Book 2011, ECB, other central banks
5. Gartner, Inc., *Forecast: Mobile Payment, Worldwide*, Sandy Shen, May 15, 2013
6. *History of QR code*, http://www.qrcode.com
7. *One in three smartphones now comes with NFC*, Rian Boden, http://www.nfcworld.com, August 1, 2013
8. *PayTouch lets you pay for purchases using your fingerprints*, Ben Coxworth, http://www.gizmag.com, May 1, 2013
9. PCI Security Standards website, http://www.pcisecuritystandards.org
10. *QR Bill: QR Codes for Consumer Bill Payment Guideline*, http://www.qrstuff.com
11. *QR Payments*, http://www.businesscardsqrcode.com
12. *Samsung Galaxy S3 contactless NFC payment tested in UK shops*, Rich Trenholm, http://www.cnet.com, June 28, 2012
13. *Starbucks generates 10pc of US revenue from mobile*, Chantal Tode, http://www.mobilecommercedaily.com, April 29, 2013
14. *The installed base of NFC-enabled handsets to reach 2.1 billion units by the end of 2017*, http://www.thepaypers.com, June 5, 2013
15. *The new PayPal app that lets you pay with QR Codes*, http://www.fespa.com, October 10, 2013
16. *TSYS Technology to Help Achieve Financial Inclusion in India*, http://www.tsys.com, January 15, 2013
17. *World Payments Report*, 2012 and 2013, Capgemini, RBS, and Efma

Capgemini

CONSULTING.TECHNOLOGY.OUTSOURCING

WHAT YOU NEED TO KNOW

CARDS

The *What You Need to Know* series from Capgemini Financial Services is written by our Strategic Analysis Group and provides trends, research, and analysis on key topics for financial services firms.

What You Need to Know: Cards looks at emerging trends in the card payments industry for three key participants: merchant acquirers, card issuers, and card processors. The papers include analysis of key market trends, business and technology implications of these trends, and leading practices in the industry. The latest publications in this series are available at www.capgemini.com/cards.

About the Authors

Saurabh Gupta is a Senior Consultant in Capgemini's Strategic Analysis Group within the Global Financial Services Market Intelligence team. He has over two years of experience in the financial services industry with a focus on the banking domain.

Smita Roy is an Associate Analyst in Capgemini's Strategic Analysis Group within the Global Financial Services Market Intelligence team. She has three years of experience in the financial services industry with expertise in research & analysis, and strategic consulting with a prior focus on insurance and banking domain.

The authors would like to thank **David Wilson, Prasanth Perumparambil, Deborah Baxley, Venugopal PSV, Christophe Vergne, William Sullivan,** and **Amit Jain,** for their contributions to this publication.

About Capgemini

With 130,000 people in 44 countries, Capgemini is one of the world's foremost providers of consulting, technology and outsourcing services. The Group reported 2012 global revenues of EUR 10.3 billion.

Together with its clients, Capgemini creates and delivers business and technology solutions that fit their needs and drive the results they want.

A deeply multicultural organization, Capgemini has developed its own way of working, the Collaborative Business Experience™, and draws on Rightshore®, its worldwide delivery model.

Learn more about us at

www.capgemini.com

For more information, contact us at: **cards@capgemini.com**
or visit: **www.capgemini.com/cards**

People matter, results count.