

Global Trends in the Payment Card Industry: Acquirers

Key trends faced by card acquirers and their
implications for the payment card industry

Contents

1. Highlights	3
<hr/>	
2. Introduction	4
2.1. Global Payment Card Industry Performance	4
2.2. Key Payment Card Industry Participants	5
<hr/>	
3. Emerging Trends in the Payment Cards Industry: Acquirers	7
<hr/>	
4. Trend 1: Emphasis on Compliance to Security Standards and Increased Enforcement by Card Networks	8
<hr/>	
5. Trend 2: Increased Use of End-To-End Encryption to Prevent Security Breaches	10
<hr/>	
6. Trend 3: Focus on Innovative Technologies to Cater to the Low-Value Transaction Market	12
<hr/>	
References	15

1 Highlights

The payment card industry was relatively resilient to the global economic slowdown, with cards transaction volumes up by 8.4% in 2009¹. This growth was primarily driven by stronger growth in the developing markets of Asia and Latin America. Transaction volumes are expected to continue to have grown in 2010 with developing countries such as China and Brazil as the growth engines. The average global value of card purchases however has been slowly declining as consumers in developed nations cut down on their big ticket purchases.

The key payment card industry stakeholders of card acquirers², card processors³, and card issuers⁴ are all witnessing shifting trends. This paper identifies the key emerging trends pertaining to the acquiring side of the payment card industry.

The recent rise in data breaches specifically targeted to the financial services industry has led to a greater focus on more stringent compliance from card industry associations. The card acquiring side of the business has shown a greater emphasis on compliance due to a regulatory push, as well as the need to avoid reputational risks associated with data breaches.

The sophistication of breach attacks has been increasing both in terms of quality and quantity. As a result, acquirers are increasingly deploying end-to-end technology to protect themselves. Deployment of end-to-end encryption for magnetic stripe card technology has the potential to drastically reduce any future data breaches, though this technology may not make magnetic stripe cards (such as those still found in the U.S.) as secure as EMV-enabled cards.

While the payment card industry has evolved over the years to become one of the most important payment modes, there still remain many untapped areas such as the low-value transactions market. Card acquirers have largely ignored small businesses, which generally resort to small value but large volume transactions. Emerging alternative technologies such as Square[®] and PayPal's virtual terminal network are now tapping this market. Acquirers need to constantly monitor such emerging disruptive technologies, which have the potential to change the competitive landscape.

¹ *World Payments Report 2011*, Capgemini

² Acquirer refers to the merchant's bank

³ Processor refers to a third party organization that aids in the card authorization and settlement process. Sometimes acquirers perform this task themselves

⁴ Issuer is the cardholder's bank and issues a credit/debit/prepaid card and maintains the customers' accounts

2 Introduction

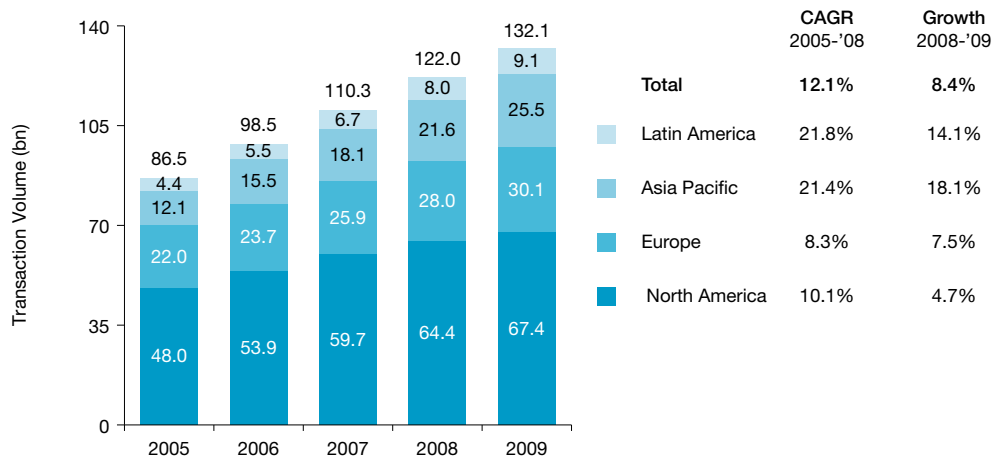
Developing nations in Asia-Pacific and Latin America are increasingly replacing their cash transactions with debit and credit cards, which is driving the card industry growth in the region.

2.1. Global Payment Card Industry Performance

The global payment card industry was relatively resilient to the financial crisis of 2008-09, as evidenced by the 8.4% growth in card transactions volume which increased to 132.1 billion transactions in 2009 (as compared to 122.0 billion transactions in 2008 as shown in the exhibit below). Cards represent one of the most preferred non-cash payment instruments, with an estimated 40% of the global non-cash payments being routed through cards⁵.

Based on a regional comparison, Asia-Pacific has been one of the fastest growing regions in terms of card usage. Cards transaction volumes grew by 18.1% during 2008-09 within Asia-Pacific, compared to North America and Europe which grew 4.7% and 7.3% respectively for the same period.

Exhibit 1: Global Card Transactions by Volume (bn), 2005-2009



Source: Capgemini Analysis, 2011; ECB; Red Book 2010; World Payments Report, Capgemini 2011

⁵ World Payments Report, 2011 (Cards represent just debit and credit card transaction across the globe)

In 2008 and 2009, the payment card industry represented the two-speed nature of global economic growth, with developed nations slowing down and the developing nations growing strongly. For instance, the transaction volume growth in developed countries was modest, with the U.S. growing by 4.7% and the Eurozone growing by 6.8%. This was slower than their historic 2005-08 compound annual growth rates of 10.6% and 7.6% respectively. On the other hand, developing nations witnessed higher card usage, with China growing by 32%, Russia by 30.9%, and Brazil by 10.1% annually in 2009.

This two-speed growth is expected to continue in the near-future. The still-low absolute usage levels of cards as a payment channel in developing nations, coupled with the potential for faster economic growth, augurs well for the payment card industry in these regions. However, card industry growth measured by transaction value is expected to be subdued in the near future as weaker consumer confidence in most developed nations is likely to manifest itself through a lower amount of high value purchases as already witnessed in 2009 in the U.S. and peripheral Europe.

The slow growth in transaction values, increasing regulations designed to favor and protect card users (in terms of fees charged), and competition from other payment sources is expected to put pressure on margins for payment card industry participants. Various stakeholders therefore need to better utilize technology to deal with compliance issues, and stay ahead of the competition within the industry as well as external competition such as mobile payments.

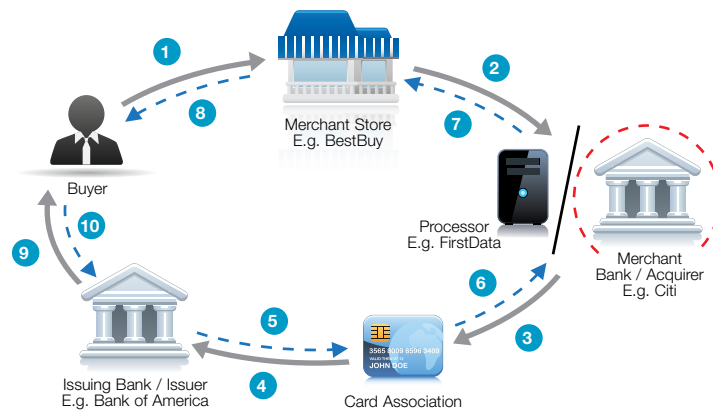
2.2. Key Payment Card Industry Participants

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

- **Card acquirers:** the merchant's bank.
- **Card processors:** third party organization that aids in card authorization and settlement process.
- **Card issuers:** the cardholder's bank who issues the card and maintains the customers' accounts.

Additionally, card association network providers (typically MasterCard® or Visa®) play an essential role in completing the card authorization and settlement cycle, as illustrated in the following exhibit.

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, 2011, "Transaction Flow", Serve First Solutions, Inc., <http://www.serve-first.com/resources/sfs-university/42-transaction-flow>

This paper focuses on the key trends that card acquirers have been experiencing and how the industry is responding.

3 Emerging Trends in the Payment Cards Industry: Acquirers

Card/Merchant acquirers perform a vital role in a typical card payment transaction. They provide a wide array of services including the setting up of new merchant accounts with a point of sale terminal or providing online payment modes, authorizing and settling merchant transactions, providing fraud control and data security services, and offering loyalty schemes to merchants.

The card acquiring business has gradually evolved over the years by providing retailers and merchants a platform to efficiently process card payment transactions with relative ease and greater speed. However, the overall card industry operating landscape is currently changing due to regulations mandating more stringent fraud control and security. Moreover, acquirers need to be more watchful about the emerging technologies that are providing alternative acquiring platforms to merchant organizations and changing the competitive landscape of the industry.

Increasing competition in the acquiring industry has led to declining margins for acquirers, which has forced them to focus on offering various value-added services to merchants, rather than competing solely on price. Acquirers are expected to continue to focus on compliance due to the Payment Card Industry Data Security Standard version 2.0 that was released in October 2010. Additionally, high profile data breach events that have been making news headlines and emerging technologies such as the Square app for mobile devices are expected to have major implications for the industry.

The changing operating environment, data security, compliance issues, and emerging alternative technologies have led to three major trends for merchant acquirers:

1. Emphasis on compliance to security standards and increased enforcement by card networks.
2. Increased use of end-to-end encryption to prevent security breaches.
3. More focus on innovative technologies to cater to the low-value transaction market.

4 Trend 1: Emphasis on Compliance to Security Standards and Increased Enforcement by Card Networks

The Payment Card Industry Data Security Council released Version 2.0 of Payment Card Industry Data Security Standard in October 2010, which needs to be followed by card industry stakeholders by January 1, 2012.

4.1. Background and Key Drivers

The payment card industry has witnessed various high profile card network breaches, especially in the recent past. These high profile data breaches have compromised the personal information of a large number of cardholders and thus exposed them to possible fraud. Personal financial data is one of the most lucrative targets for online criminals.

Globally, an increasingly large proportion of customers are moving to internet- or phone-based purchasing, largely helped by the proliferation of internet usage and the focus of various companies on this growing sales channel. Such card-not-present transactions (where the cardholder does not present the card in physical form to the merchant) create a higher risk for card frauds.

The key drivers for a stronger compliance to security standards by acquiring banks are:

- Increasingly sophisticated skimming⁷ methods used by fraudsters to steal data from traditional channels such as point of sale (POS) and ATMs.
- An increasing proportion of card-not-present transactions, which generally put the merchants at risk if the payments are under dispute and are being charged back (especially when the merchant does not follow certain rules for processing such transactions set by the acquiring bank).
- Payment Card Industry Data Security Standard version 2.0 released in October 2010, which needs to be followed by all payment card industry stakeholders by January 1, 2012.
- Increased media attention on data breaches leading to reputational risks to financial services institutions.

4.2. Analysis

Data breach events affecting card users have hit news headlines at several points in the past couple of years. In a recent data breach, Michael's, a nation-wide craft retailer in the U.S., experienced tampering with point of sales (POS) terminals. This was a classic case of the growing skimming trend. In May 2011, Michael's reported that around 90 of its stores' POS terminals were being swapped with tampered ones by the attackers, resulting in customer data being compromised through these terminals. Such advanced fraudulent methods highlight the need for better coordination between merchants and acquiring banks to combat any future data breaches.

The Payment Card Industry Data Security Standard Council announced their revised version 2.0 in October 2010, with most changes being aimed at enhanced clarifications. All organizations which store, process, or transmit credit card data in electronic form need to comply with the Payment Card Industry Data Security Standard. Card networks have put in place stringent processes to ensure the

⁶ Theft of credit card information, typically by insiders or employees of a merchant organization

compliance of all stakeholders. Generally, large card processors are subject to periodic external audits and certifications, while smaller merchants on the other hand are exempt from mandatory external audits but are subject to self certification with a possibility of audit.

The lack of compliance on the part of merchant organizations generally leads to fines being charged by the acquiring bank, and in the worst case, even possible suspension of the merchants. However, non-compliance remains a large issue across all stakeholders with just 21% of organizations being fully compliant during the time of the initial report of compliance⁷ in 2010.

Recent studies have highlighted the strong relationship between Payment Card Industry Data Security Standard compliance and data breach prevention⁸. Around 64% of compliant organizations globally had no history of credit card data breaches over the two year period (2009-10). In contrast, only 38% of non-compliant organizations had reported that they suffered no data breaches involving credit card data during the same period.

4.3. Implications

The growing threat of data breaches and the consequential revised standards require card acquirers to educate merchants regarding the security norms of card networks as well as the benefits of compliance with evolving regulatory standards. In the case of merchants using card-not-present transactions, acquirers may need to provide specific monitoring and underwriting norms that are to be followed by these merchants⁹.

On the other hand, merchant acquirers need to update their network infrastructure in order to ensure compliance with the network security norms. Overall, the focus of the acquirers needs to be on enhanced data security through process and organizational transformation.

⁷ "2011 payment card industry compliance report", Verizon

⁸ "2010 PCI DSS Compliance Trends Study", Ponemon Institute study conducted for Imperva

⁹ "The Visa Global Acquirer Risk Standards Guide", Visa Inc., 2011

5 Trend 2: Increased Use of End-To-End Encryption to Prevent Security Breaches

End-to-end encryption for the payment card industry can be defined as encryption of cardholder data from the point the card is swiped at the point-of-sale terminal to the point data reaches issuers for authorization.

5.1. Background and Key Drivers

The recent rise in high profile data breaches and related media attention has led to the payment card industry becoming increasingly focused on high levels of data privacy. The acquiring side of the payment card industry (acquirers and merchants) has been increasingly supportive of end-to-end encryption and tokenization as measures to prevent and minimize high profile data breaches and the related reputational risk to firms and the industry. From the acquiring side of the business, the point-of-sale terminal manufacturers, third party processors, and acquirers all play a crucial role in the encryption of a merchant transaction through the time it is authorized.

End-to-end encryption is most common in countries where magnetic stripe cards are widely used, such as the U.S. Additionally, the tokenization of a portion of the permanent account number of cardholders is also one of the most widely used techniques to secure data on the acquiring side.

The key drivers for increased adoption of end-to-end encryption by card acquirers include:

- Ever-increasing sophistication of attacks on corporate networks.
- Anonymous online criminal markets for services such as phishing, email spam, and virus kits.
- New guidelines regarding securing data with end-to-end encryption along with virtualization and tokenization as outlined in the new Payment Card Industry Data Security Standards.

5.2. Analysis

Since magnetic stripe cards are more vulnerable to fraud, end-to-end encryption is expected to secure them right from the point of a card swipe. End-to-end encryption for the payment card industry can be defined as encrypting cardholder data from the point it is acquired at the magnetic stripe reader (point-of-sale terminal), until the data reaches the issuers for authorization. This process significantly reduces the retailer liability as all cardholder data would be rendered unusable until it reaches issuers. However, in practice end-to-end encryption is mostly lacking since current deployments start at the point of sale and end at the point of interface with the acquirer, rather than encrypting sensitive customer until the time the transaction reaches the issuer¹⁰.

¹⁰ Master Card Acquiring News <http://www.mastercardacquirenews.com/pdfs/encryptionAnalysis.PDF>, 2009

The idea behind end-to-end encryption is to address data security issues at the network and storage levels to ensure a secure and trusted network. However, a key requirement for building an effective system is the adequate evolution of standards to prevent encryption and decryption cycles¹¹, which can create a weakness exploitable by criminals. However, such a process involves significant costs for all stakeholders including retailers, acquirers, processors, and issuers.

End-to-end encryption technology has certain inherent advantages as it offers a relatively simple solution to secure the complex enterprise software systems of online and offline retailers, especially for merchants with point-of-sale terminals supporting magnetic stripe cards. Encryption and strong identity management are expected to enable organizations to mitigate data breaches to a great extent and detect such events at a much earlier stage.

However, some believe that end-to-end encryption may not be the best available technology to fight fraud for the payment card industry. Although it addresses data security issues it does not address the weaknesses of format in which magnetic stripe data is stored compared to other chip-based Europay, MasterCard and VISA (EMV) cards. So end-to-end encryption as a technology only complements the magnetic stripe cards that are prevalent in U.S. and may not be applicable in other regions where chip-based cards are prevalent.

5.3. Implications

The replacement of hardware such as point-of-sale devices is expected to add to the capital cost component for card acquirers. Additionally, card acquirers will likely have to invest in strengthening and increasing the capacity of their infrastructure since fully-encrypted connections demand greater resources.

Overall compliance maintenance costs would fall for merchants since the burden of complying with certain PCI standards would be transferred from the merchant to the end-to-end encryption service provider, which could be third party processors.

¹¹ The act of converting data or information into code and decoding it back

6 Trend 3: Focus on Innovative Technologies to Cater to the Low-Value Transaction Market

6.1. Background and Key Drivers

The payment card industry has witnessed tremendous growth over the past few years to become one of the most prominent non-cash payment channels across the globe. However, there still remains a large untapped market in the form of low-value transactions (micropayments) which are predominantly cash-based. Taxi bills, household repairs, and purchases from smaller vendors operating over the internet are just a few examples of micropayments market. Card acquirers in general have found this market relatively unprofitable and have largely chosen to ignore it rather than trying to identify solutions to address the problems and profit from these important niche markets.

Square™, a startup by one of the co-founders of Twitter, has built itself into an alternative to traditional card processing services for low-value transactions through its Square card reader. Square has built a market for itself in certain areas where cash has traditionally been the only payment mode, such as small vendors or street-side coffee shops.

The virtual terminal network from PayPal® also offers a solution for merchants dealing in lower transaction costs by allowing their customers to place orders over phone, fax, and mail. The lower-transaction cost feature of PayPal's virtual terminal gives it an upper hand over traditional card payment modes and thus has helped it to tap the low-value transactions market.

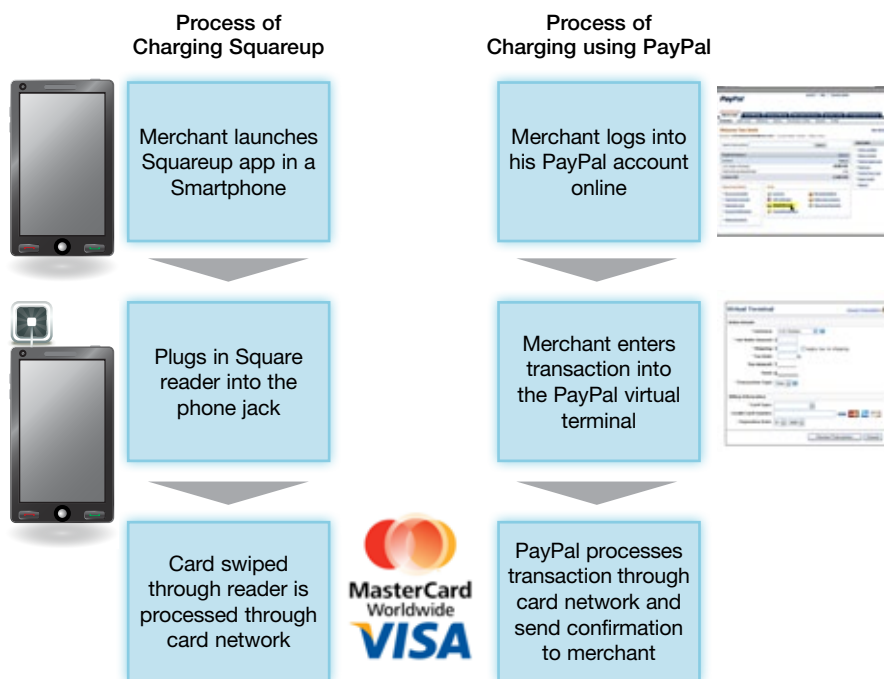
The key drivers of the emergence and increased acceptance of alternative payment processors include:

- The prohibitive high cost per transaction for merchants. Small merchants often choose not to route low-denomination transactions through the traditional card network.
- Identity validation to access card network. This is an onerous task and most small business owners find this to be the biggest barrier to access a card network.

6.2. Analysis

Disruptive technologies in the form of Square and PayPal have built innovative systems that simplify the process of accepting cards. The key reason for Square and PayPal to have established a disruptive presence in the card acquiring market is their highly differentiated positioning, which targets an often ignored market.

Exhibit 3: Accepting Cards Simplified by Innovative Systems in the form of Squareup and PayPal's Virtual Terminal Network



Source: Capgemini analysis, 2011, Square Inc. and PayPal

Square had around 500,000 merchants signed up by the end of June 2011, driven by its positioning, which is targeted towards the untapped low-value transactions market.

The demand from the untapped low-value transactions market can be gauged by the growing popularity of Square, which had an estimated 500,000 merchants signed up by the end of June 2011¹², and is believed to add approximately 30,000 to 40,000 customers on average every month.

Along with Square and PayPal's virtual terminal there are several platforms including VeriFone™ and ROAMpay™ that are competing for a piece of the low-value transaction market that has been largely ignored by the large acquirers.

6.3. Implications

Innovative services such as Square and PayPal's virtual terminal network do not just have the potential to tap the niche markets (low-value transactions), but may also compete with the existing processors as they gain greater acceptance.

Card acquirers have to be responsive to evolving customer needs and expectations, especially due to the emergence of numerous alternative acquiring platforms apart from Square and PayPal, such as VeriFone and ROAMpay.

¹² "Square gets \$1bn valuation with \$100m investment", The Register, http://www.theregister.co.uk/2011/06/29/square_money/, June 29th 2011

References

1. *World Payments Report 2011*, Capgemini
2. *The Visa Global Acquirer Risk Standards Guide*, VISA Inc., 2011
3. *2010 PCI DSS Compliance Trends Study*, Ponemon Institute study conducted for Imperva
4. Square Inc. <https://squareup.com>, accessed on 29th September 2011
5. “*Transaction Flow*” *Serve First Solutions*, <http://www.serve-first.com/resources/sfs-university/42-transaction-flow>, accessed on 28th September 2011
6. “*VeriFone, Square and the market*”, *The Green Sheet*, http://www.greensheet.com/emagazine.php?story_id=2372, 28th March 2011
7. PCI Security Standards Council, <http://www.pcisecuritystandards.org>, accessed on 28th September 2011
8. “*Tokenization vs. end-to-end encryption*”, PCI Knowledge Base http://www.computerworld.com/s/article/9136680/Tokenization_vs._end_to_end_encryption, August 14th, 2009
9. “*Square gets \$1bn valuation with \$100m investment*”, *The Register*, http://www.theregister.co.uk/2011/06/29/square_money/, June 29th 2011
10. “*An Analysis of End-to-end Encryption as a Viable Solution for Securing Payment Card Data*”, *Master Card*, <http://www.mastercardacquirenews.com/pdfs/encryptionAnalysis.PDF>, 2009

About the Author

Santosh Ejanthkar is a Lead Consultant in Capgemini's Strategic Analysis Group within the Global Financial Services Market Intelligence team. He has over seven years of experience in research and strategy consulting for investment banking, asset management, private banking, and wealth management businesses.

The author would like to thank **Prasanth Perumparambil**, **Venugopal PSV**, **William Sullivan**, and **David Wilson** for their contributions to this publication.

For more information, visit www.capgemini.com/cards or e-mail cards@capgemini.com.

All products or company names mentioned in this document are trademarks or registered trademarks of their respective owners.

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 witnessed by three major participants of the payment card industry: merchant acquirers, card processors, and Card Issuers. The papers include information on the current situation, drivers, analysis, and implications. The latest publications in this series are available at www.capgemini.com/cards.



About Capgemini and the Collaborative Business Experience

Capgemini, one of the world's foremost providers of consulting, technology and outsourcing services, enables its clients to transform and perform through technologies.

Capgemini provides its clients with insights and capabilities that boost their freedom to achieve superior results through a unique way of working, the Collaborative Business Experience™.

The Group relies on its global delivery model called Rightshore®, which aims to get the right balance of the best talent from multiple locations, working as one team to create and deliver the optimum solution for clients.

Present in 40 countries, Capgemini reported 2010 global revenues of EUR 8.7 billion and employs around 112,000 people worldwide.

Capgemini's Global Financial Services Business Unit brings deep industry experience, innovative service offerings and next generation global delivery to serve the financial services industry.

With a network of 21,000 professionals serving over 900 clients worldwide, Capgemini collaborates with leading banks, insurers and capital market companies to deliver business and IT solutions and thought leadership which create tangible value.

For more information please visit www.capgemini.com/financialservices