

Top 10 Trends in Payments 2018

What You Need to Know



Contents

Introduction	3
Trend 01: Banks becoming platform players to aid collaboration, retain payments' role	5
Trend 02: Infrastructure rationalization is likely as payments intermediaries come together or evolve	7
Trend 03: Payment vendors and banks are expected to consolidate their operations to form larger groups	9
Trend 04: Open APIs enable stakeholder collaboration	11
Trend 05: Alternate payment channels such as contactless and wearables gain acceptance	13
Trend 06: Banks and FinTechs explore distributed ledger technology to transform cross-border payments	15
Trend 07: Instant payments processing likely to become the 'new normal' for corporate treasurers, industry at large	17
Trend 08: As global cyberattacks rise, regulators focus on data-privacy law compliance	19
Trend 09: Robotic process automation, machine learning help payment service providers in fraud detection	21
Trend 10: Payments firms continue to invest in advanced authentication technologies to fight fraud and data breaches	23
References	25
About the Authors	27

Introduction

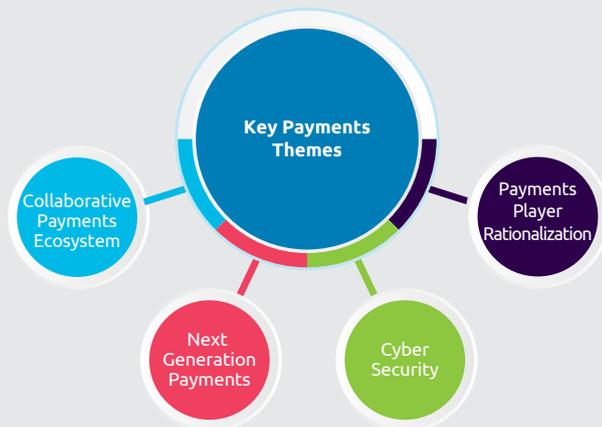


Objective:

This document analyzes the top-10 trends expected to affect payments' industry dynamics as well as stakeholder strategies in the coming year.

Methodology:

We identified trends that significantly impact the payments industry overall, and we took a close look at trends that continued from the previous year. Topics are grouped into four themes: Collaborative Payments Ecosystem, Payments Player Rationalization, Cybersecurity, and Next-Generation Payments.



Summary:

Heightened customer expectation for value-added services, increased competition due to the emergence of FinTechs, new payments-enabling technologies, and an ever-changing regulatory landscape have led to the development of an open and collaborative payments ecosystem. And this new ecosystem is expected to spur collaboration among stakeholders, which may force all players to reassess their roles.

Within this new ecosystem, the traditional payments-processing intermediary function is anticipated to fade, as intermediaries consolidate or collaborate to stay relevant by opening up their systems. Payment vendors also are expanding value-added services through consolidation. Some consolidate to acquire new technology, others to access top talent or new customers.

Payment infrastructure requires next-generation tools to enhance the customer experience. Alternate channels such as contactless and wearables continue to gain traction.

Instant payments are likely to become catalysts for next-generation payments technology offering customers better and faster payments solutions.

Cross-border payments are expected to transform by using blockchain technology to offer efficient, inexpensive, and faster transfers. Technology innovations related to the Internet of Things (IoT) and Distributed Ledger Technology (DLT) are expected to disrupt the payments infrastructure further.

However, an open and collaborative environment introduces vulnerabilities related to cybersecurity and data privacy. To help mitigate exposure, robotic process automation (RPA) and machine learning can monitor for fraud in real time. Regulators and central authorities have increased their focus on stringent regulations related to cybersecurity and data privacy requirements that could impose hefty fines and criminal liability on firms for a data breach.

Authentication is becoming critical. Multifactor validation involving biometrics, secure element, geo-location-based verification, and cryptography keys could be the way forward to alleviate cyber threats and data breaches.

Trend 01: Banks becoming platform players to aid collaboration, retain payments' role

Feedback loops between producers and clients, known as network effects, are central to the success of a bank's collaborative platform model

Background



- Traditionally, banks have provided end-to-end services across the banking and payments value chain
- However, today that position is being challenged because of increased competition from FinTechs and other third-party providers as well as regulations such as Europe's PSD2 that promote open systems
- Banks run the risk of losing market share unless they adapt and change their operating model and become part of the new collaborative payments ecosystem where different industry stakeholders collaborate to provide innovative customer services
- Adjusting to the platform model helps banks to centralize their role in the new ecosystem and own the customer relationship while simultaneously leveraging the innovative capabilities of emerging FinTechs and third-party developers through collaboration:
 - E.g., Industries such as e-commerce have successfully adopted the platform model and reaped benefits

Key Drivers



- Regulatory and industry initiatives, customer demands for personalized services, the evolution of FinTechs, and new technology are leading to increasing openness and collaboration in the payments industry:
 - Customers are demanding real-time, agile, and personalized payment services
 - Banks can enhance the customer experience using technologies and modernization initiatives such as open Application Program Interfaces (API), instant payments, blockchain, and mobile wallets
- As these structural changes impact the payments industry, banking's role as both platform-developer and owner becomes more significant

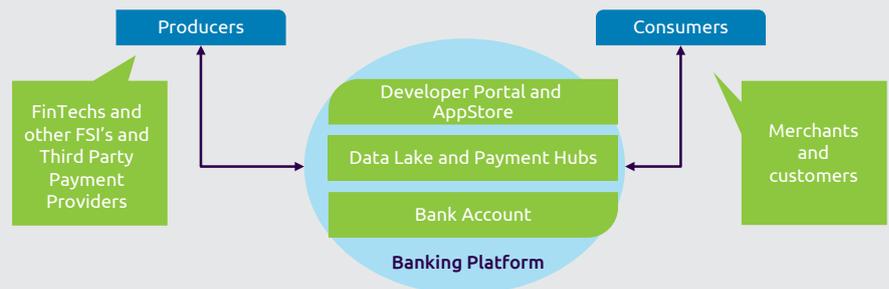
Trend Overview



- Regulatory and industry initiatives such as the Consumer Financial Protection Bureau's (CFPB) push for open data in the United States – combined with advanced payments technologies – are leading to more collaboration between stakeholders
- To connect banking services producers with the right consumers, banks are opening their infrastructures to leverage technology enablers such as open APIs and instant payments

- BBVA, Fidor, Standard Chartered, and Citigroup have led in the adoption of the platform model and are facilitating the exchange of valuable interactions between producers and consumers of banking and payment services:
 - BBVA launched eight APIs in customers, accounts, cards, payments, PayStats, loans, notifications and business accounts to help third parties build innovative, customer-experience enhancing products¹
 - Fidor bank developed the fidorOS platform to securely open their systems to the external world leveraging open APIs²
 - Standard Chartered and Citigroup rolled out open API developer portals to enable third-party developers to create value-added services that can be integrated with bank offerings, including payments³
- In this model, banks own the platform based on their client account relationship, and FinTechs (and other third-party payment providers) produce services on the platform while merchants, corporates, and end-users are the consumers

Exhibit 1: Collaborative Payments Platform



Implications



- The collaborative-platform model helps banks generate new revenue streams by leveraging their customer data and monetizing API-based value-added services
- This model will enable customer centricity by giving more control to customers to choose service providers and products
- FinTechs can achieve scale – with minimal customer-acquisition costs – by accessing the ecosystem’s broad customer base
- Other stakeholders, such as payment processors and network schemes, must also open their systems to competition to maintain interoperability and stay relevant in this ecosystem

1 APIs, BBVA's commitment to the new banking ecosystem", May 31, 2017, accessed October 2017 at <https://www.bbva.com/en/apis-bbvvas-commitment-new-banking-ecosystem/>

2 "What is the fidorOS platform", accessed October 2017 at <https://www.fidor.com/platform>

3 "Standard Chartered Launches Banking API Portal", PYMNTS, February 13, 2017, accessed October 2017 at <https://tinyurl.com/ybkhrum8>

Trend 02: Infrastructure rationalization is likely as payments intermediaries come together or evolve

Globally, payments infrastructure is being transformed to become faster and more inclusive to new players that will launch valuable offerings for retail and businesses

Background



- With the increasing number of regulations focusing on reducing risk along with increasing competition due to opportunity in open banking regulations, payment networks and intermediaries are looking to rationalize⁴ the payment infrastructure
- Emergence of the new payments ecosystem is expected to impact the role of traditional intermediaries in payment processing, and they would have to either consolidate or collaborate by opening their systems to stay relevant in this ecosystem

Key Drivers



- There is an increasing demand for customized offerings, agile solutions, and secure payments from the customers
- Many regulatory and industry initiatives aimed at standardization, competition, and modernization of payment systems are also leading to infrastructure rationalization
- Advancements in technologies such as AI and Blockchain is expected to push further the need to modernize the payments infrastructure

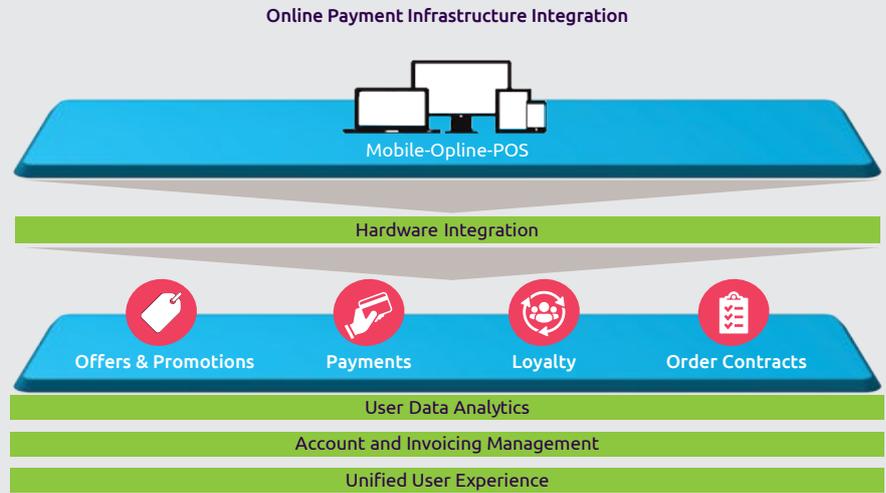
Trend Overview



- Payments infrastructure is expected to converge through mergers and acquisitions to expand the reach of the payments firms, increase their value proposition to meet changing customer expectations, and create customized solutions:
 - VocaLink acquisition enables MasterCard to expand its services in areas of payments initiation, fraud management, and analytics
- Payment schemes and intermediaries are also looking for infrastructure rationalization to be able to provide services in niche and high demand areas of data analytics, cloud, and Digital Customer Experience (DCX)

⁴ Rationalization is the review and reduction, virtualization, or redistribution of technology, software, or infrastructure to ensure maximum operational capability and flexibility at lowest cost.

Exhibit 2: Online Payment Infrastructure Integration



Source: Capgemini Financial Services Analysis, 2017

Implications

- Regulators are working on rationalization of different payments systems – As an example, U.K. Payment System Regulator is working on a proposal to converge three payments systems into one to reduce operational expenses and boost efficiency⁵
- Global initiatives such as Global Payments Innovation (GPI) are expected to lower costs for cross-border transactions where the uniform payments clearing and settlement system would influence the rationalization of the existing systems
- Infrastructure rationalization is expected to help bring more agility and reduce the go-to-market period for bringing the latest offerings to the customers



⁵ New Payment System Operator formed, September, 2017, accessed in November 2017 at, <https://www.psr.org.uk/psr-publications/news-announcements/new-payment-system-operator-formed>

Trend 03: Payment vendors and banks are expected to consolidate their operations to form larger groups

As banks benefit from TPP partnerships, TPPs gain access to seasoned banking expertise and large client bases, which are likely to fuel convergence across all players

Background



- Technology is expected to drive payments evolution in the next decade resulting in the entry of new players in this space:
 - These new players are expected to challenge the existing customer relationships with better and faster interface
- The opening up of the banking platform and the resulting intense competition is expected to drive down the margins in the industry, which will need incumbents to consolidate and form larger groups
- Firms such as PayU snapping up Citrus Pay are examples of consolidation in the payments space

Key Drivers



- TPP activity has catalyzed regulators around the world to improve the collaborative ecosystem
- Regulatory initiatives that promote open banking and data sharing have led to a scenario where TPPs can potentially bypass intermediaries such as merchant acquirer banks and card schemes, forcing these firms to rethink their business models
- Digital payments and e-commerce are attracting more entrants into the payments space, which is increasing competition and forcing payments services vendors to consolidate to capitalize on economies of scale

Trend Overview



- For instance, Fiserv recently acquired Monitise and PCLender to provide a broader range of customer offerings, and banking players Misys and FIS are considering the benefits of integrating operations⁶
- The role of traditional intermediaries in payment processing is diminishing with the emergence of FinTechs and regulatory initiatives such as PSD2:
 - They may consolidate and focus on niche areas of the payments value chain or collaborate by opening up their systems to move up the value chain, to remain relevant in the coming years

⁶ "Fiserv acquires PCLender", August 2017, accessed on November 2017 at <https://www.housingwire.com/articles/40891-fiserv-acquires-pclender>

Exhibit 3: Benefits of Consolidation for Payment Vendors



Source: Capgemini Financial Services Analysis, 2017

Implications

- Payments vendors with advanced digital capabilities could become acquisition targets as incumbents look to scale up operations to make the most of the expanding digital payments market
- As payments processing is becoming commoditized, players are looking to expand their offerings in various value-added services through consolidation
- Most consolidation cases have been to acquire new technology, talent or access to customers, but the key concern has been to minimize costs and to optimize resources
- With image and voice technology expected to drive payments innovation, it is likely that most payments players will ensure their systems remain nimble to adapt to new offerings based on such technologies



Trend 04: Open APIs enable stakeholder collaboration

A major EU regulation, PSD2 fosters partnership opportunities between banks and other industry players with open APIs acting as collaboration-enabling catalysts

Background



- With Europe's second Payment Services Directive (PSD2) coming into force January 13, 2018, FinTechs and other Third-Party Players (TPPs) are expected to leverage open Application Programming Interfaces (APIs) to examine available opportunities
- Key PSD2 provisions include:
 - **Access to Accounts:** The regulation introduces Account Information Service Providers (AISPs) as value-chain stakeholders that leverage APIs to collect information from customer accounts and then develop new customized offerings
 - **Retailer-Consumer Interaction:** EU retailers will now be able to ask customers for permission to use their bank information to initiate payments and will, therefore, assume the role of Payment Initiation Service Providers (PISPs) much in the way as online service providers Amazon and Apple
- By thinking beyond mere PSD2 compliance, banks can tap into monetization avenues and reach customers faster using the open API platform

Key Drivers



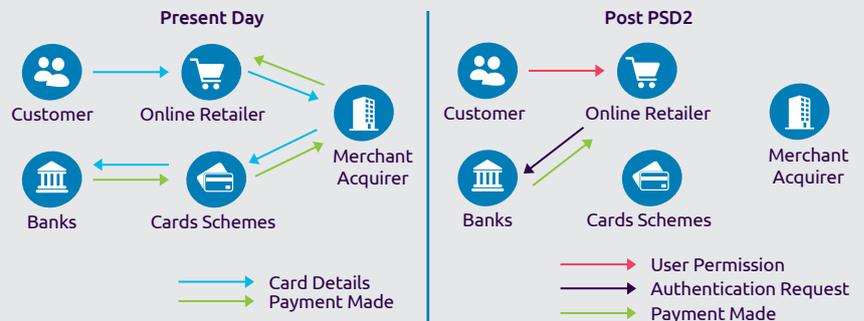
- Regulations such as PSD2 have driven bank/third-party collaboration through adoption of open APIs
- Evolving customer expectations and technology advancements (coupled with the rise of FinTechs in the payments domain) have influenced banks to adopt a collaborative approach in both service and operations

Trend Overview



- Application Programming Interfaces combine functions and procedures to enable two-way data sharing between banks and the third parties in a secure, scalable, and accelerated manner
- APIs are pivotal to collecting information from different banks, which helps in the development of new and improved customized services
- The main benefits from the PSD2 environment are expected to come via the API-based solutions of TPPs, which will deliver incremental value to customers and simplify merchant services:
 - As mandated by PSD2, banks will be obligated to share customer data upon approval from the customer, while maintaining the privacy of the data
 - This data can be accessed by TPPs to develop innovative offerings targeting various customer segments
 - The API-enabled environment has opened doors to stakeholders to play roles such as AISP and PISP and thus improves collaboration between incumbents and new players

Exhibit 4: Payment Initiation Process Pre and Post PSD2



Source: Capgemini Financial Services Analysis, 2017

Implications

- Open APIs are expected to provide opportunities for new payment service providers to tap into the payments sphere:
 - The collaborative ecosystem catalyzed by PSD2 is expected to disrupt the payments industry by bringing in new players and increasing competition
 - In conjunction with a standardized instant-payments architecture, open API-enabled PSD2 is likely to usher in a wave of payments ecosystem offerings
- However, concerns regarding the lack of harmonization due to the absence of a centralized API infrastructure (including common global API standards) may lead to shared API infrastructures developed in silos by banking communities such as Berlin Group – a challenge yet to be addressed:
 - The collaborative ecosystem’s lack of accountability could threaten sensitive customer data, especially with the opening up of banking infrastructure



Trend 05: Alternate payment channels such as contactless and wearables gain acceptance

Alternate payment channels fulfill customer demands for convenience and speed and could soon become mainstream

Background



- With the widespread use of smartphones, mobile banking and payments applications have gone mainstream, and wearables provide convenient access to such applications
- Contactless payments enable consumers to make everyday purchases quickly and safely especially for low-value transactions
- Mobility, Internet of things (IoT), connected homes, entertainment, and media are expected to augment the volumes of non-cash transaction volumes significantly:
 - By 2021, more than 15 billion machine-to-machine (M2M) and consumer electronic devices are likely to be connected⁷
- As merchants start providing Augmented Reality (AR) assisted shopping experiences, they will likely look for an AR-integrated payment gateway that delivers a superior customer experience

Key Drivers



- Increased customer demand for ease of use, along with faster, integrated, and seamless banking experience is driving banks to offer alternate payment channels
- Increasing processing power, smaller devices, and more comprehensive availability of high-speed internet have enabled payments to be integrated with wearables
- With increased focus on IoT-enabled payments (IoP), leading banks such as Bank of America are looking to incorporate IoP into their digital offerings⁸
- Customer confidence in security of contactless payments is increasing with improved device security features such as biometrics and cryptography

Trend Overview



- Alternate payment channels could become more common thanks to benefits such as saving time, frictionless payments, and efficiency with day-to-day tasks
- Driven by the ease-of-use provided by contactless payments, countries such as the U.K., Canada, Singapore, and Australia are experiencing high adoption of contactless cards:

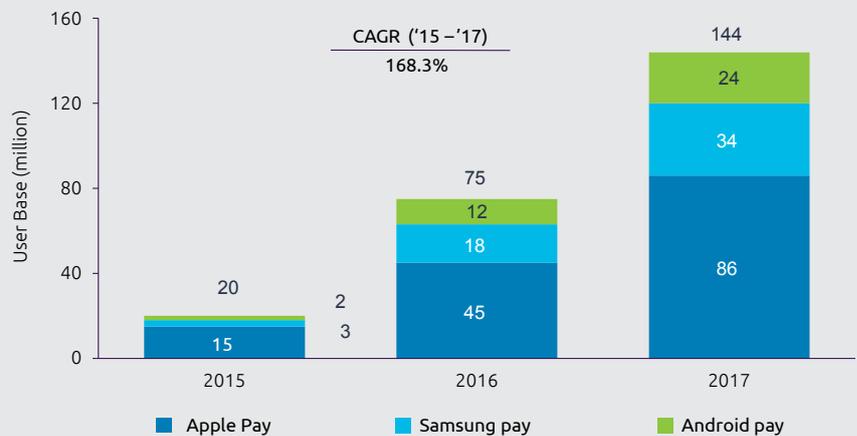
⁷ World Payments Report 2017

⁸ "Bank of America and NXT-ID Subsidiary FitPay Collaborate to Accelerate Wearable and IoT Payment Adoption" accessed October 2017 at <http://goo.gl/4rLfyU>

- For example, in the U.K., the number of contactless transactions grew by 174.1% in 2016 to reach 2.86 billion⁹
- Mobile and wearable contact-less payments are expected to reach \$95 billion annually by 2018¹⁰
- As it expands upon mobile innovation, wearable technology integrates technology even deeper into everyday life, with more than 240 million units of wearables expected to be shipped in 2021¹¹
- Payments via wearables are expected to rise as fitness trackers (expected to constitute about 30% of wearable device market by 2020¹²) partner with MasterCard and Visa to offer contactless payment services

Exhibit 5: Mobile Contactless User Base

Mobile Contactless User Base (million), Apple Wallet, Samsung Pay & Android Pay, 2015-2017



Source: Capgemini Financial Services Analysis, 2017; "More Than 150m People to Use Apple Pay, Samsung Pay and Android Pay by End of 2017" accessed October 2017 at <https://www.nfcworld.com/2017/04/11/351590/150m-people-use-a-ple-pay-samsung-pay-an-droid-pay-end-2017>

Implications



- With expanding acceptance of digital and mobile payments, mobile wallets that offer contactless solutions, easy peer-to-peer transfer and real-time payments are expected to grow steadily
- It is anticipated that payments solutions for wearables will increase as major fitness trackers integrate payments service into their devices
- As the adoption of contactless cards and mobile payments increases, they could challenge traditional magnetic stripe technology and EMV cards

⁹ <http://www.theukcardsassociation.org.uk>, accessed October 2017

¹⁰ "Mobile Wearable Contactless Payments to Approach \$" accessed October 2017 at <https://goo.gl/R5P4iD>

¹¹ "Worldwide Wearables Market to Nearly Double by 2021, According to IDC" June 21, 2017, accessed October 2017 at <https://goo.gl/RRzqpf>

¹² "Cumulative wearable device shipments to surpass 750 million units by 2020" accessed October 2017 at <https://goo.gl/RRzqpf>

Trend 06: Banks and FinTechs explore distributed ledger technology to transform cross-border payments

Banks and FinTechs are exploring blockchain technology for cross-border payments to provide faster, inexpensive, and efficient services

Background



- The current cross-border payments model lacks an international clearinghouse and relies on correspondent banks, which causes inefficiency, slow speed, and high cost
- As a result, corporate customers are demanding transformation
- Distributed ledger technology (DLT) such as blockchain eliminates intermediaries by using algorithms to verify and authorize payment transactions securely
- A distributed ledger-based cross-border payments model is expected to result in improved efficiency, enhanced security, and lower costs

Key Drivers



- The current cross-border payment method (involving correspondent banks) is inefficient and expensive
- There is increasing demand for better cross-border payments regarding speed, cost, and customer visibility
- Increasingly, multinational companies operating across different geographies participate in complex supply chains that require quick settlement of international payments to run efficiently
- Industry stakeholders are looking at DLT as a way to meet these requirements, and many – including banks and FinTechs – have started experimenting with blockchain

Trend Overview



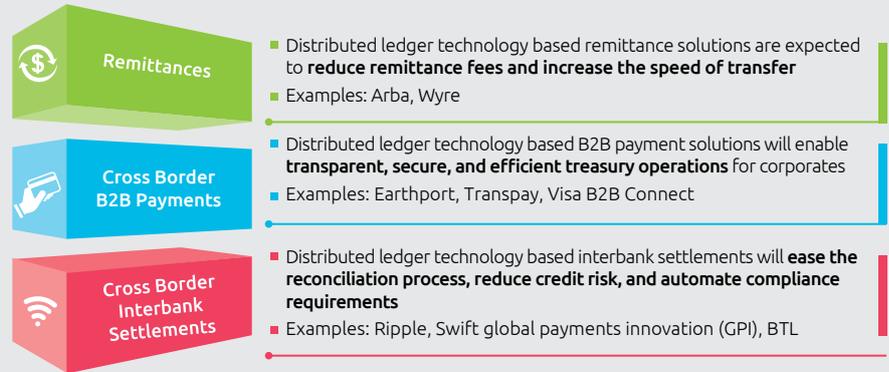
- Banks and FinTechs are looking at distributed ledger technology as the backbone of a new cross-border payments infrastructure to solve traditional cross-border payments inefficiencies (involving correspondent banks) resulting in faster and affordable services:
 - FinTechs such as Ripple¹³, BTL¹⁴, and Wyre¹⁵ have built cross-border payments and settlement infrastructure leveraging distributed ledger technology, and many incumbents are either partnering with these FinTechs or collaborating with players such as SWIFT to experiment with distributed ledger technology for cross-border payments
- Before widespread adoption of DLT, however, challenges related to scalability and lack of standardization must be addressed

¹³“Blockchain and the Ripple effect: did it ripple?”, Carlo R.W. De Meijer, 27 March 2017, accessed October 2017 at <https://www.finextra.com/blogposting/13888/blockchain-and-the-ripple-effect-did-it-ripple>

¹⁴“Blockchain remittance firm BTL working with Visa Europe Collab”, Ian Allison, September 1, 2016, accessed October 2017 at <http://www.ibtimes.co.uk/blockchain-remittance-firm-btl-working-visa-europe-collab-1579121>

¹⁵Wyre launches blockchain-based cross-border payments platform”, Tony Zerucha, December 19, 2016, accessed October 2017 at <https://www.bankless.com/2016/12/19/wyre-launches-blockchain-based-cross-border-payments-platform/>

Exhibit 6: Exploring Blockchain in Cross Border Payments



Source: Capgemini Financial Services Analysis, 2017

Implications



- Distributed ledger based cross-border solutions will benefit banks by reducing their credit risks, managing their costs, improving compliance with regulatory requirements, and enhancing their customers' payments experience
- They can offer more secure, cheaper, and faster services to retail and corporate customers by eliminating intermediaries and making use of robust algorithms
- Professional services firms have an opportunity to develop a distributed ledger based cross-border clearing, and settlement platform may be in partnerships with other stakeholders
- Government and other regulatory bodies must come together to establish standards for increased adoption and efficient functioning of distributed ledger for cross-border payments

Trend 07: Instant payments processing likely to become the 'new normal' for corporate treasurers, industry at large

With wider adoption, instant payments have the potential to emerge as an alternative to checks and cash for retail and corporate customers

Background



- Across the globe, there are major initiatives by central banks and industry associations to implement instant payments infrastructure with an aim to modernize the existing payments processing systems and compete with the non-banks to maintain the existing market share respectively
- The approach for implementation of instant payments is varied as in some countries such as the U.K.; the instant payments system has been developed in parallel to their existing clearing and settlement systems while in countries such as Sweden and Spain instant payments infrastructure is developed by leveraging the countries' existing standards
- Banks are leveraging instant payments platform to connect with third parties to deliver better digital customer experience and provide innovative products and services to both retail and corporate customers

Key Drivers



- Banks are witnessing a demand from retail customers for instant payments solutions as customers witness similar instant solutions in other spheres of their social life
- Corporate customers are also increasingly demanding more agile solutions for payments clearing and settlement that will allow them to track and manage their intra and inter day liquidity
- Most regulators are in favor of instant payments to infuse infrastructure modernization and competition into the industry:
 - New Payments Platform Australia has announced that the country's real-time payments platform, developed to modernize country's infrastructure, will go live on 26th January 2018¹⁶
 - Similarly, in late 2016, Payments Canada has announced that the organization is undertaking a multi-year plan to develop payments infrastructure with real-time processing capabilities¹⁷

¹⁶"Banks to switch to real-time payments from Australia Day", Anne Davies, 3 October 2017, accessed October 2017 at <https://www.theguardian.com/australia-news/2017/oct/03/banks-to-switch-to-real-time-payments-from-australia-day>

¹⁷"Payments Canada announces a multi-year, multi-phase plan to modernize Canada's payment systems", Kashif Zaman, 9 December 2016, accessed October 2017 at <https://www.osler.com/en/blogs/risk/december-2016/payments-canada-announces-a-multi-year-multi-phases>



Trend Overview

- While the instant payments infrastructure is in various stages of implementation across the globe (notably in the U.S. and Australia), the relevant use cases have mostly been witnessed in the retail payments domain only
- Corporate payments domain is slow to adopt the available instant payments solutions due to related challenges of investments in legacy systems and inertia to upgrade the batch-processing systems to real-time processing
 - Initial adoption of the instant payments for corporate could be envisioned in the use cases of Just-in-Time Supplier payments and the short-term loan servicing payments
- With the availability of the instant payments, the adoption of offerings is increasing and it is expected to accelerate further with the implementation of the PSD2 mandate as within PSD2 merchants can become PISPs and thus they can start offering instant payments to the retail and corporate customers

Exhibit 7: Benefits and Challenges of Instant Payments for Stakeholders



Source: Capgemini Financial Services Analysis, 2017

Implications



- With the wider implementation of instant payments, there will be an opportunity for banks to develop value-added services on top of the instant payments infrastructure such as eInvoicing for customers
- Instant payments implementation will also bring banks and FinTechs together to form meaningful collaborations as witnessed in the Netherlands and the U.K.
- While instant payments adoption is expected to increase, the corporate adoption of such services would require further development of the related ecosystem to address AML, Anti-Fraud, and lack of harmonization related challenges

Trend 08: As global cyberattacks rise, regulators focus on data-privacy law compliance

As cyber-attacks and data breaches around the world are rising in terms of both, frequency and intensity, regulators are focusing on compliance with current cybersecurity and data privacy laws

Background



- In H1 2017, 918 publicly reported cybersecurity breaches exposed over 1.9 billion records¹⁸
- Recent attacks, such as the Equifax breach¹⁹ and the WannaCry ransomware attack²⁰ exploited known vulnerabilities in the system, which could have been avoided had the firms been more vigilant:
 - Negligence on the part of firms is forcing regulatory authorities to introduce stronger regulations
- Two new sets of regulations, the European Union's General Data Protection Regulation (EU GDPR) and New York Department of Financial Services' regulation on cybersecurity are already in place, and more regulations from different central authorities are expected with steep penalties for non-compliance
- China's new cybersecurity law includes liabilities such as suspension of business activities and fines up-to 1 million RMB for violation²¹

Key Drivers



- Open banking collaboration between payments stakeholders is affecting banks' data and security, which is increasing cyberattack vulnerability
- Cybersecurity incidents continue to escalate in frequency and impact, as cybercriminals become smarter and employ new technologies and attack methods

Trend Overview



- Cyberattacks can cause personal and commercial data to be lost or compromised causing financial institutions financial and reputational loss:
 - Based on estimates, cyberattacks cost the global economy 1% of annual GDP²²
- Regulators across the world are bringing in new cybersecurity regulations and standards which could impose heavy fines, injunctions, audits, even criminal liability on firms for a data breach

18 "Breach level Index Report" accessed October 2017 at <http://breachlevelindex.com/assets/Breach-Level-Index-Report-H1-2017-Gemalto.pdf>

19 "Equifax Breach Security Hole" accessed October 2017 at <http://money.cnn.com/2017/09/16/technology/equifax-breach-security-hole/index.html>

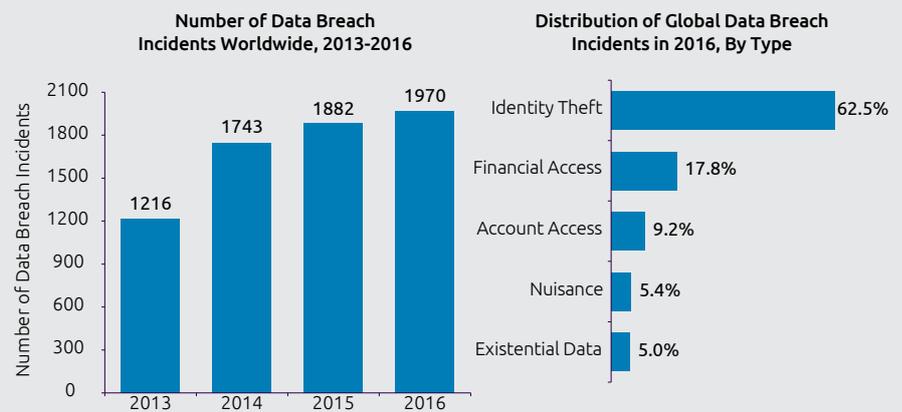
20 "WannaCry Ransomware Attack" accessed October 2017 at https://en.wikipedia.org/wiki/WannaCry_ransomware_attack,

21 "A Primer on China's New Cybersecurity Law: Privacy, Cross-Border Transfer Requirements, and Data Localization" accessed October 2017 at <http://privacylaw.proskauer.com/2017/05/articles/international/a-primer-on-chinas-new-cybersecurity-law-privacy-cross-border-transfer-requirements-and-data-localization/>

22 Symantec Internet Security Threat Report, Volume 21 (April 2016), accessed October 2017 at <https://www.symantec.com/content/dam/symantec/docs/reports/istr-21-2016-en.pdf>

- The cyber insurance industry grew 35% in 2016 to \$1.35 billion²³ in terms of direct written premium, which shows that corporates are looking to protect themselves from liabilities related to cybersecurity laws
- The U.K. announced a data-protection bill²⁴ that gives more control to consumers on their data
- However, lack of harmonization in cybersecurity laws in different countries is posing a challenge for multinational companies operating across the globe

Exhibit 8: Number and Distribution of Data Breach Incidents



Source: Capgemini Financial Services Analysis, 2017; Breach level Index Report H1 2017 accessed October 2017 at <http://breachlevelindex.com/assets/Breach-Level-Index-Report-H1-2017-Gemalto.pdf>; Number of Breach Incidents by Type, accessed October 2017 at <http://www.breachlevelindex.com/>

Implications



- Regulators are bringing in new regulations and standards for ensuring cybersecurity and data privacy, with high penalties for non-compliance
- Payments firms are expected to continue to invest in latest technology measures to ensure that their systems are not prone to fraud and data breaches
- Compliance costs for payment service providers could rise sharply, bringing in new players who could provide innovative and cost-effective solutions

²³ "Cyber Insurance Premium Volume Grew 35% to \$1.3 Billion in 2016" accessed October 2017 at <https://www.insurancejournal.com/news/national/2017/06/23/455508.htm>

²⁴ "UK Government Publishes Draft Data Protection Bill" accessed October 2017 at <https://www.lexology.com/library/detail.aspx?q=6092466a-e167-45de-acb3-41408738dde3>

Trend 09: Robotic process automation, machine learning help payment service providers in fraud detection

Robotic process automation and machine learning are next-generation tools for payment service providers in combating fraud and improving cybersecurity

Background



- With non-cash transactions increasing at the highest growth rate in last decade²⁵ in 2015, and card fraud losses increasing every year, it has become imperative for PSPs to look for better solutions to improve cybersecurity and fraud detection while reducing costs
- Robotic Process Automation (RPA) and machine learning are beginning to play an increasingly important role in the financial services industry by reducing costs and increasing productivity:
 - PSPs can create faster throughput and higher data quality with RPA implementation
- With machine learning, frauds can be identified and analyzed in near real-time with algorithms that mine data from the customers' purchasing history while reviewing patterns of likely fraud for preventing attacks, reducing fraud, and improving risk management
- Machine learning, when combined with RPA, saves PSPs on costs associated with fraudulent transactions and reduces the time and effort required to catch a fraud

Key Drivers



- High losses due to cyberattacks and high costs of existing fraud detection solutions are pushing PSPs to adopt efficient and secure processes
- Increased data availability, faster processing systems, and advancement in machine learning technologies enabled near real-time fraud detection, which could not be done manually

Trend Overview



- With increasing digitalization, banks have become vulnerable to payments fraud and cyberattacks:
 - It is estimated that cards fraud alone resulted in losses of over \$24 million in 2016²⁶ while cyberattacks could cost businesses over \$2 trillion by 2019
- Banks, with the help of RPA and machine learning, can continuously check their processing systems for possible threats, examine previous attacks, monitor

²⁵ World Payments Report, 2017

²⁶ The Nilson Report-2016, accessed October 2017 at https://www.nilsonreport.com/upload/content_promo/The_Nilson_Report_10-17-2016.pdf

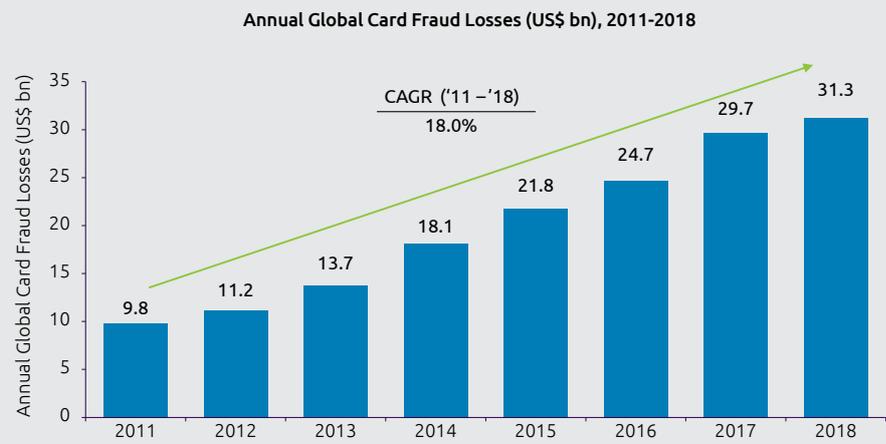
²⁷ "Cybercrime Cost Businesses Over 2trillion" accessed October 2017 at

<https://www.juniperresearch.com/press/press-releases/cybercrime-cost-businesses-over-2trillion>

activities and applications, and establish a payments control center to monitor payments and identify exceptional situations

- In the light of recent data breaches²⁸ including the massive breach at Equifax, fraud rates are expected to rise, and PSPs are turning to machine learning analytics leveraging the vast amount of customer data at their disposal
- Machine learning can also be used in anti-money laundering (AML) to monitor the audit trail of illegal money transfer

Exhibit 9: Annual Global Card Fraud Losses



Source: Capgemini Financial Services Analysis, 2017; The Nilson Report accessed October 2017 at https://www.nilsonreport.com/upload/content_promo/The_Nilson_Report_10-17-2016.pdf

Implications



- It is expected that industry players could place higher focus on RPA to improve security and reliability while driving down costs
- PSPs are expected to use behavior analytics, machine learning and threat matrix to continuously monitor the ecosystem network and fight threats
- Investments in machine learning solutions for fraud detection are expected to rise, with 68% of financial institutions (FIs) citing machine learning analytics as a high priority investment²⁹

²⁸ "2017 Data Breaches" accessed October 2017 at <https://www.identityforce.com/blog/2017-data-breaches>

²⁹ "Innovation Study Finds 68 North American Financial Institutions Plan Invest Machine Learning" accessed October 2017 at <https://goo.gl/f4WcDM>

Trend 10: Payments firms continue to invest in advanced authentication technologies to fight fraud and data breaches

Biometrics, digital identity, secure element, geo-location, and interoperable cryptographic keys are the leading mechanisms being employed by stakeholders to provide robust authentication

Background



- Banks and corporates are witnessing significant losses with an increasing number of cybersecurity-related incidents across the world:
 - SWIFT network was hacked multiple times in different parts of the world leading to losses of several million³⁰
 - WannaCry malware caused a massive ransomware attack affecting more than 150 countries and 200,000 computers³¹
- With the proliferation of technology and increasing collaboration, there will be simultaneous increase in cyber threats and hence banks need to be on constant vigilance and identify ways to do things in a more secure manner
- A paradigm shift is needed by all stakeholders including regulators to take a more proactive approach and take ownership in terms of preventing cyber attacks

Key Drivers



- Cyber threats and frauds are on a rise with increased adoption of mobile payments and wearable devices leading to loss of consumer trust as well as financial losses
- According to Verizon's 2017 DBIR³² report, 81% of hacking-related breaches leveraged weak or stolen passwords last year which calls for more complex user authentication mechanisms without compromising on user convenience

Trend Overview



- The flipside of adoption of advanced technologies (open APIs) and increased collaboration in the industry (due to regulations such as PSD2) could be an increase in cybersecurity vulnerabilities
- Hackers exploit advanced technologies such as brainwave signals to gain access to the confidential data of customers and hence common authentication solutions such as one-time pass codes, or more complex passwords are not enough
- Multi-factor authentication involving requiring multiple layers of defense is the way to go to mitigate the cyber threats from hackers:

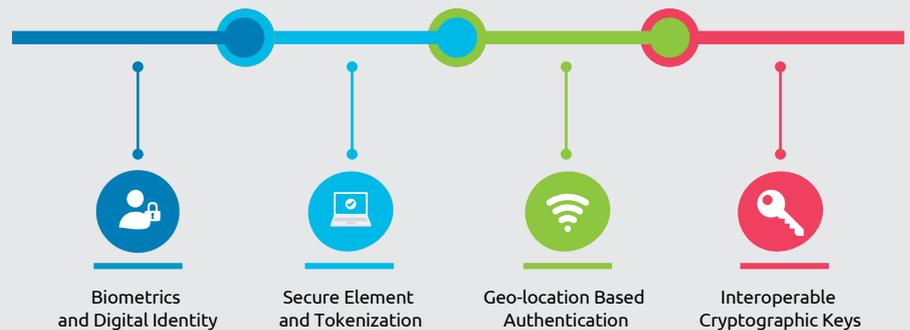
³⁰ "SWIFT Bank Network Hit by Multiple Cyber Fraud Attacks", Reuters, April 25, 2016, accessed October 2017 at <http://fortune.com/2016/04/25/swift-cyber-fraud/>

³¹ "WannaCry ransomware attack," accessed October 2017 at https://en.wikipedia.org/wiki/WannaCry_ransomware_attack

³² Data Breach Investigations Report, Verizon, 2017

- Globally multi-factor authentication services market is expected to grow at a CAGR of close to 23% from 2017– 2021 while the global multi-factor authentication market in banking and financial sector was valued at \$2.4 billion in 2016³³
- Payments firms have to continuously invest in advanced authentication and enabling technologies such as biometrics, secured element, geo-location based authentication and cryptographic keys to stay ahead of the hackers and cybercriminals
- Behavioural analytics in combination with biometrics is expected to witness strong growth by banks to continuously monitor for fraud in the background without impacting the user experience
- Many new authentication technologies such as PIN on glass are being explored by payments firms to improve customer experience but thorough testing needs to be done before introducing them

Exhibit 10: Advanced Authentication Techniques



Source: Capgemini Financial Services Analysis, 2017

Implications

- Stakeholders will collaborate to form interoperable set of standards such as Fast Identity Online (FIDO) for simpler and stronger authentication using biometrics and cryptographic techniques
- Many new players and third-party developers are expected to develop plug and play multi-layered authentication techniques which can be integrated easily with banks' mobile solutions
- Increasing adoption of advanced authentication techniques could be witnessed by banks in the coming years, and there could be more collaboration with FinTechs in this space



³³ "Multi-factor Authentication Market - Top Trends and Forecasts by Technavio", August 2017, accessed October 2017 at <http://www.businesswire.com/news/home/20170807005537/en/Multi-factor-Authentication-Market--Top-Trends-Forecasts>

References

1. *World Payments Report*, Capgemini and BNP Paribas, 2017
2. "The platform is now: Corporate banking and the ecosystems of the future," Falk Rieker and Oliver Bussmann, October 4, 2017, accessed October 2017 at <https://www.bussmannadvisory.com/platform-now-corporate-banking-ecosystems-future/>
3. "Blockchain as an Emerging Cross-Border Payments Infrastructure," IILJ Emerging Scholars Paper 28 (2017), Claire Schupmann, September 27, 2017, accessed October 2017 at <http://www.iilj.org/wp-content/uploads/2017/09/Schupmann-Blockchain-in-Cross-Border-Payment-Infrastructure-IILJ-ESP-28-2017.pdf>
4. *Data Breach Investigations Report*, Verizon, 2017
5. "Next Generation Payment Tablets Launched," Adam Unsworth, August 3, 2016, accessed October 2017 at <http://www.paymentscardsandmobile.com/next-generation-payment-tablets-launched/>
6. "PSD2- The directive that will change banking as we know it". Evry, accessed October 2017 at <https://www.evry.com/en/news/articles/psd2-the-directive-that-will-change-banking-as-we-know-it/>
7. "PSD2- the tip of an Open API iceberg", Banking Tech, October 7, 2017, accessed October 2017 at <http://www.bankingttech.com/1019442/psd2-the-tip-of-an-open-banking-api-iceberg/>
8. "Is mobile and payment industry headed towards consolidation?", The Economic Times, July 15, 2017, accessed October 2017 at <https://economictimes.indiatimes.com/small-biz/money/is-mobile-wallet-and-payment-industry-headed-towards-consolidation/articleshow/59605524.cms>
9. "FinTech players will get a big opportunity," The Hindu, September 30, 2017, accessed October 2017 at <http://www.thehindu.com/business/fintech-players-will-get-a-big-opportunity/article19778288.ece>
10. "How FinTech revolution is breaking down financial exclusion," The Big Issue, October 10, 2017, accessed October 2017 at <https://www.bigissue.com/news/fintech-revolution-breaking-financial-exclusion/>
11. <http://www.theukcardsassociation.org.uk> - accessed October 2017
12. "Worldwide Wearables Market to Nearly Double by 2021, According to IDC" June 21, 2017, accessed October 2017 at <https://www.idc.com/getdoc.jsp?containerId=prUS42818517>
13. "Cumulative Wearable Device Shipments to Surpass 750 Million Units by 2020", June 22, 2015, accessed October 2017 at <http://www.businesswire.com/news/home/20150622005210/en/Cumulative-Wearable-Device-Shipments-Surpass-750-Million>

14. "Real-time payments forcing transaction flow rethink", Kimberley Long, Euromoney, September 14, 2017, accessed October 2017 at <https://www.euromoney.com/article/b14r6x3pgbg5vc/real-time-payments-forcing-transaction-flow-rethink>
15. "Getting real with real-time payments," Daniel Szmukler, EBA Group, September 11, 2017, accessed October 2017 at <https://www.finextra.com/blogposting/14484/getting-real-with-real-time-payments>
16. "For Banking's Future, The Hub's The Rub," PYMNTS, September 21, 2017, accessed October 2017 at <https://www.pymnts.com/news/banking/2017/cgi-on-banking-industry-innovation-via-fintech-payments-competition/>
17. "Risk-Based Security, Data Breach QuickView Report: 2016 Data Breach Trends – Year in Review", accessed October 2017 at <https://pages.riskbasedsecurity.com/2016-ye-breach-quickview>
18. "Mobile & Wearable Contactless Payments to Approach \$100bn by 2018", accessed October 2017 at [https://www.juniperresearch.com/press/press-releases/mobile-wearable-contactless-payments-to-approach-\\$](https://www.juniperresearch.com/press/press-releases/mobile-wearable-contactless-payments-to-approach-$)
19. "How the Equifax data breach happened: What we know now," September 16, 2017, accessed October 2017 at <http://money.cnn.com/2017/09/16/technology/equifax-breach-security-hole/index.html>
20. Symantec Internet Security Threat Report, Volume 21 (April 2016), accessed October 2017 at <https://www.symantec.com/content/dam/symantec/docs/reports/istr21-2016-en.pdf>
21. "The Cybersecurity Regulatory Crackdown" August 25, 2017, accessed October 2017 at <https://www.forbes.com/sites/forbestechcouncil/2017/08/25/the-cybersecurity-regulatory-crackdown/#32d127aa4573>
22. The Nilson Report-2016, accessed October 2017 at https://www.nilsonreport.com/upload/content_promo/The_Nilson_Report_10-17-2016.pdf
23. "UK Government Publishes Draft Data Protection Bill" September 15, 2017, accessed October 2017 at <https://www.lexology.com/library/detail.aspx?g=6092466a-e167-45de-acb3-41408738dde3>
24. "Cybercrime Will Cost Businesses Over \$2 Trillion By 2019", May 2015, accessed October 2017 at <https://www.juniperresearch.com/press/press-releases/cybercrime-cost-businesses-over-2trillion>
25. "2017 Data Breaches-worst So far" October 9, 2017, accessed October 2017 at <https://www.identityforce.com/blog/2017-data-breaches>
26. "Iovation Study Finds 68% of North American Financial Institutions Plan to Invest in Machine Learning to Help Combat Fraud" October 03, 2017, accessed October 2017 at <http://www.marketwired.com/press-release/iovation-study-finds-68-north-american-financial-institutions-plan-invest-machine-learning-2235843.htm>
27. "A Primer on China's New Cybersecurity Law: Privacy, Cross-Border Transfer Requirements, and Data Localization" May 9, 2017 October 2017 at <http://privacylaw.proskauer.com/2017/05/articles/international/a-primer-on-chinas-new-cybersecurity-law-privacy-cross-border-transfer-requirements-and-data-localization/>

About the Authors

Gaurav Garg is a Manager with the Market Intelligence team in Capgemini Financial Services with over eight years of experience specializing in banking and payments.

Ganesh Vudayagiri is a Senior Consultant with the Market Intelligence team in Capgemini Financial Services with over six years of experience specializing in banking and payments.

Sunil Gopinath Pillai is a Senior Consultant with the Market Intelligence team in Capgemini's Financial Services with over seven years of experience specializing in banking and payments.

Rohit Sharma is a Senior Consultant with the Market Intelligence team in Capgemini Financial Services with over two years of experience specializing in banking and payments.

The authors would like to thank these SMEs for their contributions to the paper:

- Jeroen Holscher – Global Payments & Cards Practice Head
- Christophe Vergne – Global Payments Solutions Leader
- William Sullivan – Global Head of Market Intelligence
- David Wilson – Head of Strategic Analysis Group
- Anuj Agarwal – Director, Market Intelligence Group
- Tamara Berry – Editor, Content Manager, Market Intelligence Group



About Capgemini

A global leader in consulting, technology services and digital transformation, Capgemini is at the forefront of innovation to address the entire breadth of clients' opportunities in the evolving world of cloud, digital and platforms.

Building on its strong 50-year heritage and deep industry-specific expertise, Capgemini enables organizations to realize their business ambitions through an array of services from strategy to operations. Capgemini is driven by the conviction that the business value of technology comes from and through people. It is a multicultural company of 200,000 team members in over 40 countries. The Group reported 2016 global revenues of EUR 12.5 billion.

Visit us at

www.capgemini.com

Learn more about us at:

www.capgemini.com/payments or
email: payments@capgemini.com



People matter, results count.

The information contained in this document is proprietary. ©2017 Capgemini.
All rights reserved. Rightshore® is a trademark belonging to Capgemini.