

Piecing together the global payments puzzle

Towards a more secure, fast, efficient, transparent and global network

#PositiveImpact



Contents

Introduction	3
1. Introducing the global payments puzzle	4
2. Clients need security	5
2.1 Regulators and inter-governmental bodies are striving for a secure financial system	5
Protecting the financial system	5
Payments security initiatives beyond Europe	7
2.2 Industry and market infrastructures are pushing the use of industry utilities and security initiatives	7
2.3 Non-bank competitors are focussing on collaborating with traditional banks	7
2.4 What's next?	8
3. Clients need speed, efficiency and transparency	9
3.1 Regulators striving for competition and Open Banking	9
3.2 Industry and market Infrastructures creating the foundation for industry change, with moves towards real-time payments, modernised high-value payments and improved liquidity management	11
Europe embracing instant payments	11
Modernising high-value payments in Europe	11
Instant payments and modernised high-value payment schemes beyond Europe	12
3.3 Non-bank competitors are either competing or collaborating with traditional banks	14
3.4 What's next?	14
4. Clients need global reach and global networks	15
4.1 Regulators and inter-governmental bodies should remain open for dialogue	15
4.2 Industry and market infrastructures optimising current models and maintaining reach	15
4.3 Non-bank competitors are driving a platform economy	16
4.4 What's next?	17
5. Looking to the future	18

Introduction

By Marc Recker, Global Head of Institutional Market Management, Cash Management, Deutsche Bank



The payments space is evolving rapidly – with new regulations and updated market infrastructures coinciding with new technology and new industry initiatives to drastically reshape the landscape.

With so many new elements to factor in, it's easy to lose track of the big picture and become over-interested in specifics. Indeed, we are now at a stage where evolution has happened so quickly, with much still ongoing, that there is a risk of falling into the trap of innovating for innovation's sake, where individual developments are not fully in harmony with the needs of end users (retail or corporate), or with the overall development of the payments industry.

Market players are looking to spread the benefits of emerging technologies – such as Application Programming Interfaces (APIs), blockchain, Cloud, machine learning or the Internet of Things (IoT) – which have the potential to optimise capacity and processes, glean more insight from data, and help drive increased collaboration. The potential benefits are indisputable: increased connectivity, efficiency, and transparency, leading to enhanced control and oversight.

However, realising this potential requires an understanding of the broader ongoing evolution of the payments landscape in order that payment service providers' solutions are always tied clearly and directly to client needs.

By stepping back and reflecting on the wider picture, we can not only see what industry participants are doing to meet the needs of modern business, but also assess whether they truly meet all of them. With this in mind, we have identified what we see as the three key needs of end users of payments systems:

- Security,
- Speed, efficiency and transparency, and
- Global reach.

Building a future global payments network that is fast, efficient, transparent and secure is the payment industry's key task over the next years, and one that industry players must tackle and solve together – fitting into place the many necessary components like pieces in a giant jigsaw puzzle.

Our objective in this paper is to critically assess how the current pieces stack up against the core needs of end users, exploring what they do, whether they are doing enough, and what further pieces could – or should – be added to complete the picture.

1

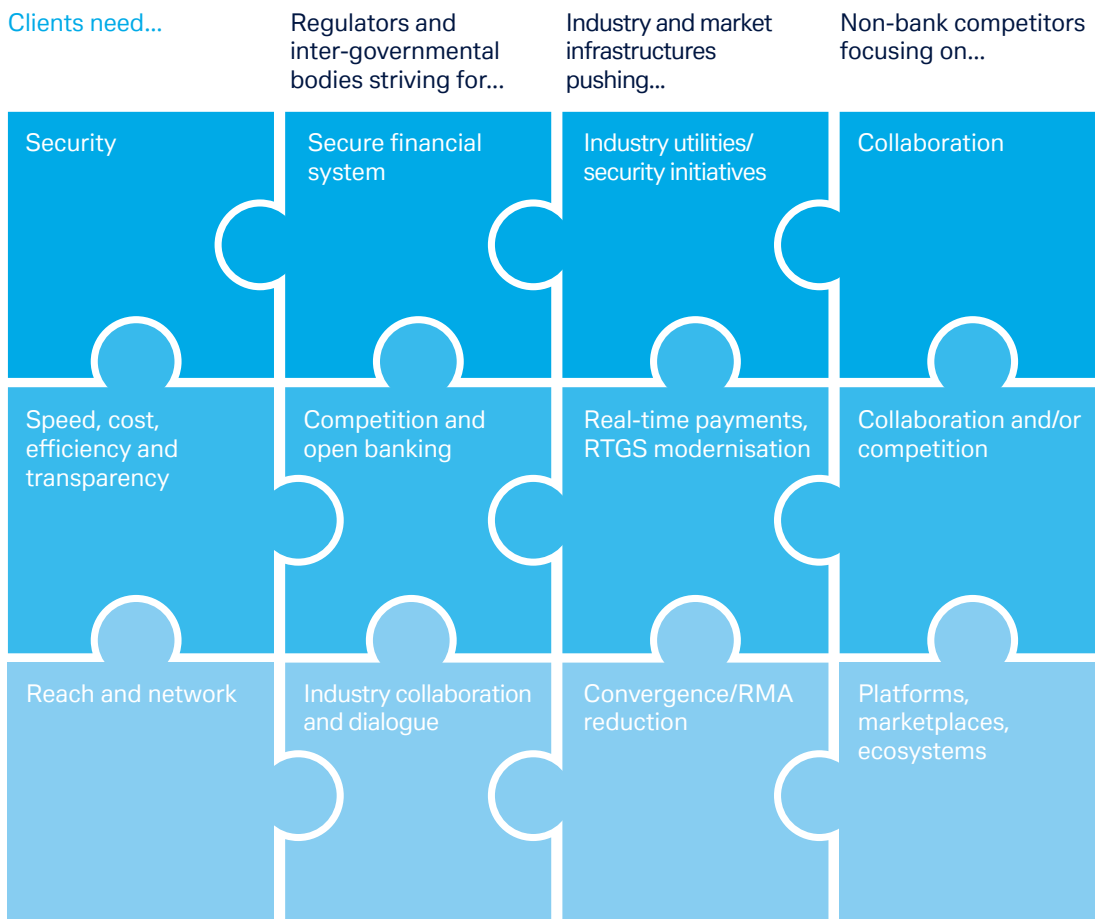
Introducing the global payments puzzle

To better understand ongoing developments, we have mapped out the main payments initiatives currently underway, dividing them according to the end purpose they serve – promoting greater security, speed or reach, for instance – and the industry players behind them

This paper will tackle each of the three key client needs in turn, exploring how regulators and inter-governmental bodies, industry players and market infrastructures, and finally non-bank competitors, are tackling each of them.

As a helpful guide, we've also included a smaller puzzle at the beginning of each section, to illustrate how each section of text corresponds to the graphic below.

Figure 1: The payments markets puzzle: how industry players' initiatives tackle the three key client needs



2

Clients need security

Security has always been a fundamental part of every payments system and can broadly be divided into two parts. On the one hand, it is vital to ensure a stable system, with minimal risk of errors and outages. On the other, there is a growing need to protect against financial crime – particularly as technology continues to fuel rising sophistication among cybercriminals

As focus continues to mount on the latter of these two aspects of payment security, participants from across the industry are rolling out measures to help protect against intrusion from external threats and detect risks as early as possible. In the event that a breach does take place, it is crucial that systems can recover quickly and that accurate, useful reports can be filed, so that similar threats can be countered in future.

2.1 Regulators and inter-governmental bodies are striving for a secure financial system

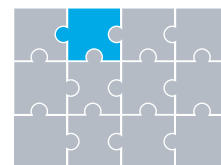
From the perspective of the regulators, they have taken a two-pronged approach to security. First, they have been seeking to improve consumer protection against fraud and liability within the payment ecosystem through regulations, such as the second Payment Services Directive (PSD2) in the EU. PSD2, which took effect on 13 January 2018, incorporates security measures that are likely to have a significant impact on fighting cyber fraud – most notably by introducing a two-factor authentication requirement for electronic payments, online account access and access through remote channels.

Second, they have taken measures to secure the entire financial system against fraud in the form of regulations, such as the Fourth Anti-Money Laundering (AML) Directive and the Funds Transfer Regulation (FTR) 2015.

Protecting the financial system

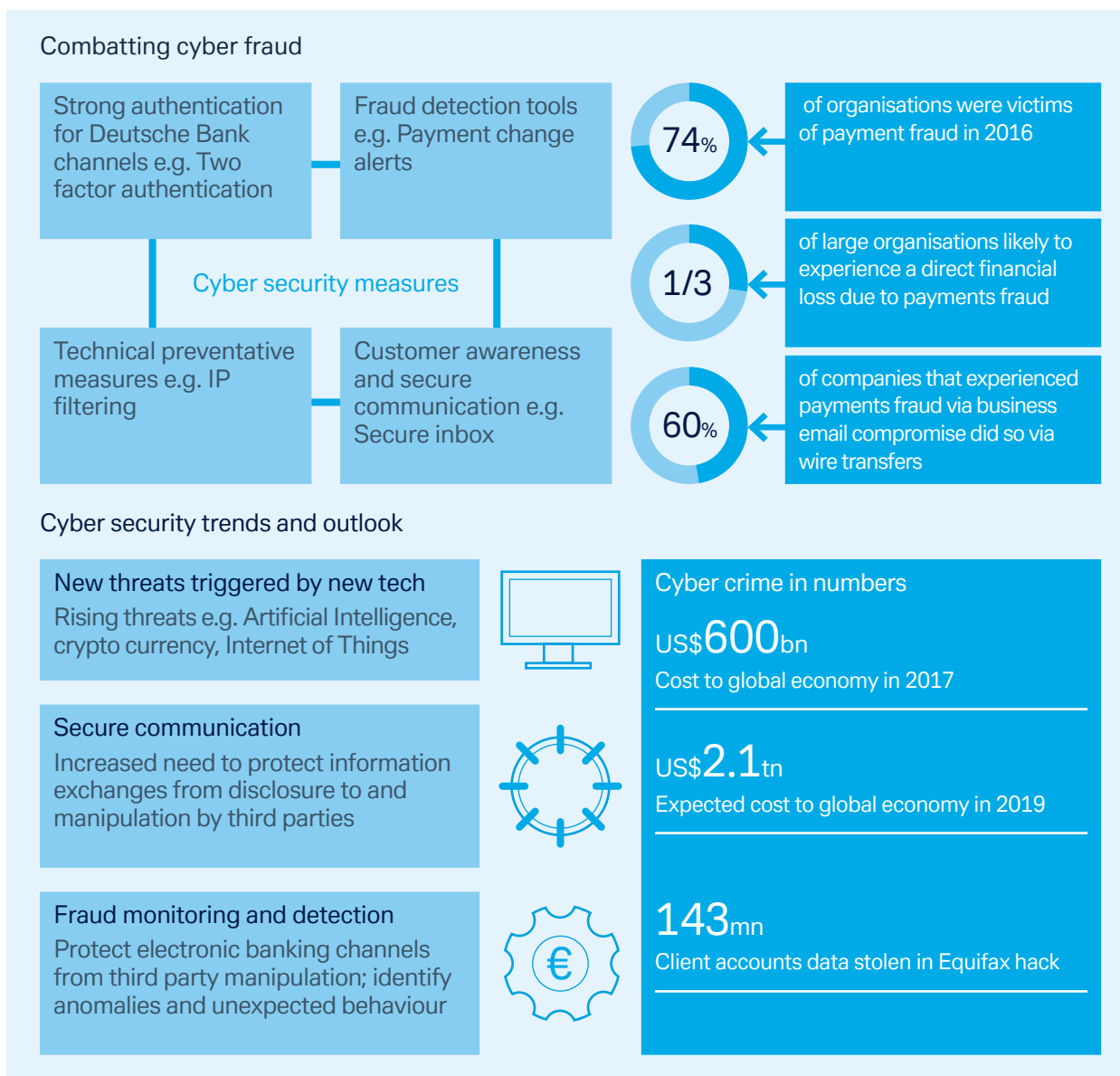
The rise of cybercrime, fraud and money laundering has generated a growing pressure on the payments industry and its market infrastructure to guarantee the security and integrity of payment systems. New threats have arisen as a result of new technologies, such as cryptocurrencies, the IoT and artificial intelligence (AI), and there is also an increased need to protect information exchanges from disclosure to, or manipulation by, third parties (see Figure 2 on page 6 for an overview).

In Europe, regulators have responded to the general level of threat with the EU's Fourth AML Directive, the most sweeping piece of AML legislation Europe has seen in many years. Enacted on 25 June 2015, this came into force on 26 June 2017, requiring banks to practise enhanced client due diligence, and to identify the "ultimate beneficial owners" (UBOs) of their clients – i.e. the legal entity that owns their client or its parent company. Member states must keep registers listing these, for both corporate and other legal entities – and where they cannot be identified, their legal representatives will now be deemed to be their UBOs. The Directive also requires that relationships with parties outside the EU/EEA are categorised as higher risk – and applies not only to correspondent banking relationships, but also to those with non-bank financial institutions, where payments for a third party are being processed.



Aligned to the 4th AML Directive is FTR 2015, which also came into effect on 26 June 2017.¹ It affects payments from an operations, compliance and messaging perspective, and stipulates that payment service providers (PSPs) must ensure that required information on both payer and payee is included in every "transfer of funds" (broadly defined). Moreover, this information must be transmitted in the correct designated fields of the messaging or payment and settlement system used, and – very importantly – must remain with the transfer throughout a transaction chain using one or more intermediary banks. The regulation applies to all transfers of funds sent or received by banks within the EU, including intermediary banks, regardless of currency.

Figure 2: An overview of cyber fraud



Payments security initiatives beyond Europe

Europe is of course not the only region looking to strengthen the security of its payments industry. With a view to meeting the future demands of the payments market, the Monetary Authority of Singapore (MAS) established its Payments Council in August 2017, with the mission to “make e-payments simple, seamless, and secure for all Singaporeans.” The authority has since published a set of guidelines to promote security for end users of e-payments.

The Hong Kong Markets Authority (HKMA), meanwhile, has taken a different approach – outlining a three-pronged strategy for raising the level of cybersecurity among banks in Hong Kong as part of its Cybersecurity Fortification Initiative.² Instead of refreshing infrastructure or regulations, HKMA’s plan involves building a robust assessment framework for determining what level of resilience is necessary, along with training initiatives and a common platform for sharing cyber intelligence and threats among banks.

In the US, meanwhile, the Federal Reserve Bank launched the Secure Payments Task Force in June 2015 to support its strategy for improving the US payment system, focusing on three core objectives – identifying payment security objectives for industry action, advising the Federal Reserve on payment security issues, and co-ordinating with the Faster Payments Task Force to identify approaches to payments that are both fast and secure.

2.2 Industry and market infrastructures are pushing the use of industry utilities and security initiatives

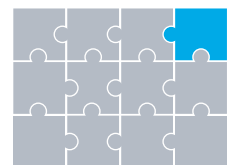
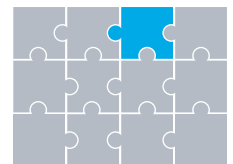
Alongside regulators, market infrastructures have been playing an equally important role in helping to develop a safer payments environment.

In 2016, SWIFT devised its Customer Security Programme (CSP)³, after the infamous Bangladesh heist in which hackers managed to use fraudulent messages to steal US\$81m from Bangladesh Bank’s account at the Federal Reserve Bank of New York.⁴ Although the SWIFT network itself was not compromised, SWIFT introduced a client security control framework consisting of mandatory and advisory security controls for SWIFT users. To ensure adoption of controls, SWIFT has developed an attestation and compliance process which requires users to self-attest compliance against the mandatory and, optionally, the advisory security controls. Going forward, they will regularly review and update the control framework, taking account of the latest cybersecurity practices to address threats arising and thus continuing to raise the security bar.

2.3 Non-bank competitors are focussing on collaborating with traditional banks

FinTechs are also contributing to a more secure payments system by collaborating with traditional banks – often through offering software-as-a-service. Most banks already use software to monitor and analyse client transactions, assessing historical and current client information and interactions to achieve a complete picture of client activity.

However, as financial crime, and the technology used to commit it, grow in sophistication, specialist FinTech companies, known as RegTechs, are providing advanced solutions to safeguard financial institutions against increasingly complex cybercriminal activity, and help them manage their compliance requirements. For instance, some FinTech platforms offer banks an automated embargo filtering service, which instantly blocks any cross-border payments covered by ongoing embargoes. This secures banks against legal infringements and hefty fines. Tasks other RegTechs help clients carry out range from regulatory risk management through reporting, identity management and control to compliance and transaction monitoring.

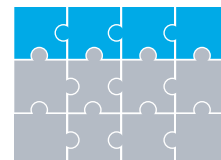


2.4 What's next?

Various regulations set in place over the past few years, together with initiatives such as the CSP, lay a robust foundation for stabilising and safeguarding payments systems. What must now happen is for banks to ensure they comply, and comply effectively.

However, the digital economy is rapidly changing the composition of payment flows, exposing banks to new kinds of fraud and AML risk, resulting in greater need for real-time fraud detection and risk management. Indeed, as the industry increasingly moves to real-time, banks will have to ensure that they have surveillance controls in place that complement yesterday's "ex-post" monitoring with a full "real-time" transaction screening environment. Those that do not, risk losing their licence to operate. In order to stay ahead of the game, banks should also better utilise emerging technologies – AI, for example, can aid fraud detection, identifying high-risk behavioural patterns by scoring them against those detected in large volumes of historical transactions.

Whether banks decide to act alone, or in combination with FinTechs or RegTechs, is down to individual institutions. However, one thing is clear: technology is the key enabler of increasing security and efficiency.



3

Clients need speed, efficiency and transparency

Across the globe, business models are changing – primarily driven by the “anytime, anywhere” demands of new-age consumers and complemented by the availability of mobile devices, next-generation and non-physical interfaces

Client expectations of convenience, immediacy and transparency initially emerged in the retail sector, but have now spilled over into the wholesale arena as well. For example, with more and more real-time payment platforms having emerged across the globe, corporates have for some time now recognised the advantages of instant payments in the domestic space, and are now becoming increasingly expectant of speed and transparency when it comes to cross-border payments.

3.1 Regulators striving for competition and Open Banking

Regulators have so far focussed on creating a level playing field for competition – and, in so doing, promoting speed, efficiency and transparency as requirements for banks and non-bank payment service providers, to benefit end users.

In Europe, it is the EU that champions these objectives, through PSD2. From September 2019, it will require banks to open up their proprietary client data to licensed third-party providers (TPPs), thereby enabling non-bank players to offer supplementary services to bank clients. The growth in numbers and range of activities of these new market participants, together with the API technology that will be used to grant them access to client accounts and data, are expected to spark a wave of innovation throughout the European payments space, generating new business models and creating a wealth of new services for both consumers and corporate clients.⁵

Further still, implementation of PSD2 is expected to pave the way towards Open Banking in Europe. This is the next stage of development for the payments markets, which will put clients in control of sharing their financial assets and personal data with their providers of choice, giving rise to new and more efficient service models. Open access to banks’ client data is the basis and fundamental requirement for all of this to start happening.

From September 2019, banks will be mandated to offer clients access to supplementary services from two types of new providers licensed under PSD2 – Payment Initiation Service Providers (PISPs) and Account Information Service Providers (AISPs). PISPs will be able to initiate direct payments on behalf of a buyer. For instance, in an online purchase, the seller’s bank could act as a PISP, accessing the buyer’s bank account and transferring the agreed amount directly into the seller’s account. AISPs, on the other hand, will provide an aggregated overview of all the accounts a client holds across banks and geographies – giving them a clear view of their overall cash positions, and enabling them to proactively and conveniently manage their own liquidity. Yet this is only the beginning (see Figure 3 on page 10 for more information). It is hoped that first PSD2, then Open Banking will act as catalysts to produce an entire new generation of powerful, innovative and easy-to-use services for clients.

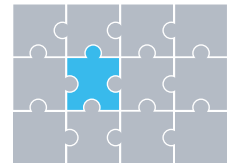
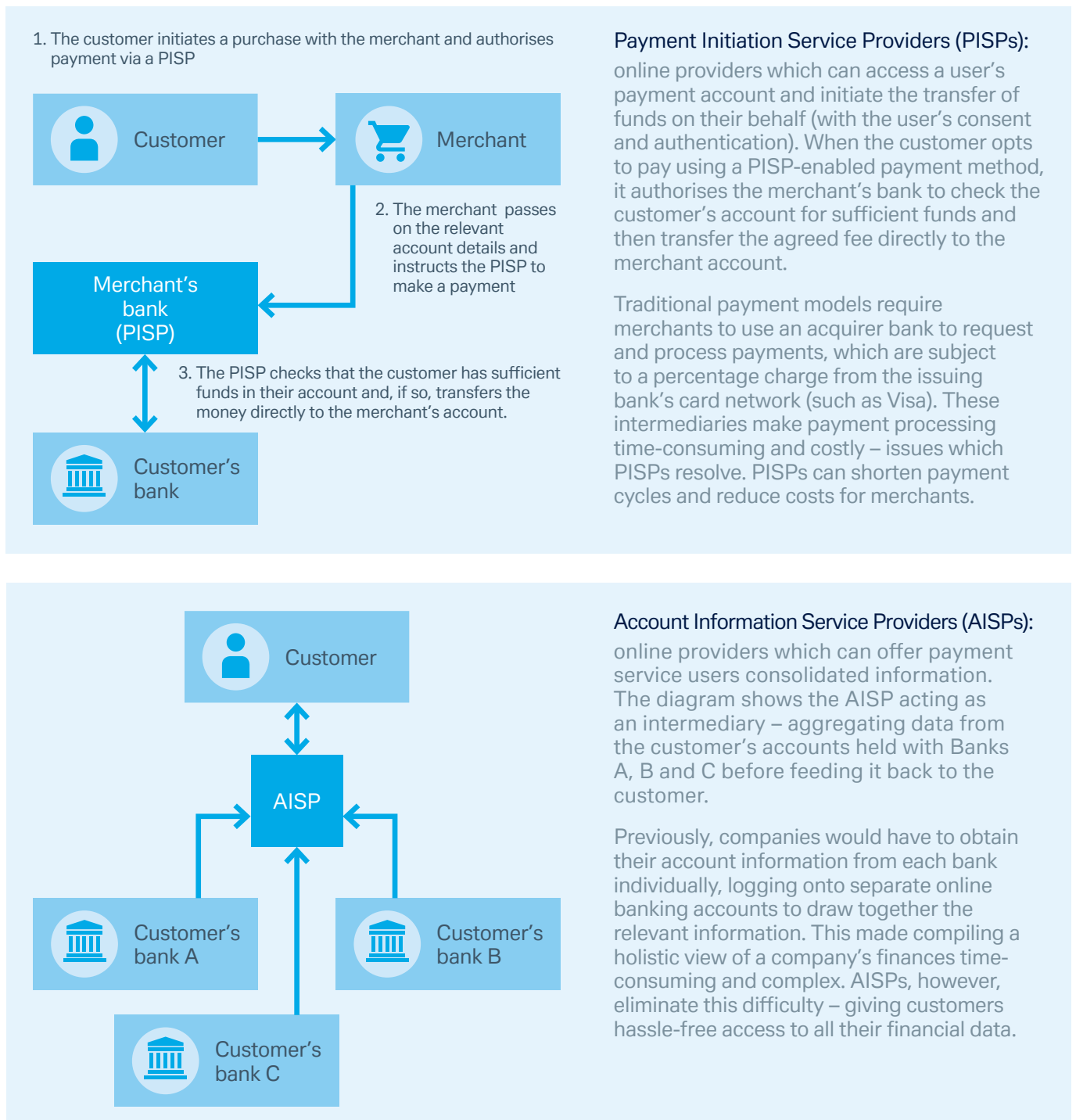
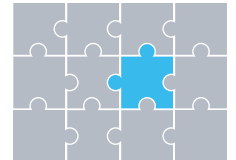


Figure 3: How AISPs and PISPs work



3.2 Industry and market Infrastructures creating the foundation for industry change, with moves towards real-time payments, modernised high-value payments and improved liquidity management



Meanwhile, industry players and market infrastructures in a number of key global locations are adapting to changing client expectations and are looking to increase the speed, resource efficiency and transparency of payments, mainly through two key initiatives: the introduction of real-time payments, and the modernisation of high-value payment systems.

Europe embracing instant payments

Faster, “real-time” or “instant” payment solutions are either being developed, or have been implemented, in many countries across the world, either as central bank-driven or industry-driven initiatives, or as the result of a joint approach.

In Europe, there will soon be two infrastructure solutions supporting faster or instant payments. Launched in November 2017, EBA Clearing’s RT1 scheme processes SEPA instant credit transfers (SCT Inst) at a pan-European level around the clock, any day of the year.⁶ It supports euro transfers between payment accounts in less than 10 seconds end-to-end, with funds available immediately. The scheme can be used for any payment product in euros that is fully compliant with the European Payments Council’s (EPC) SCT Inst Scheme, and is in line with ISO 20022 global messaging standards for real-time payments.

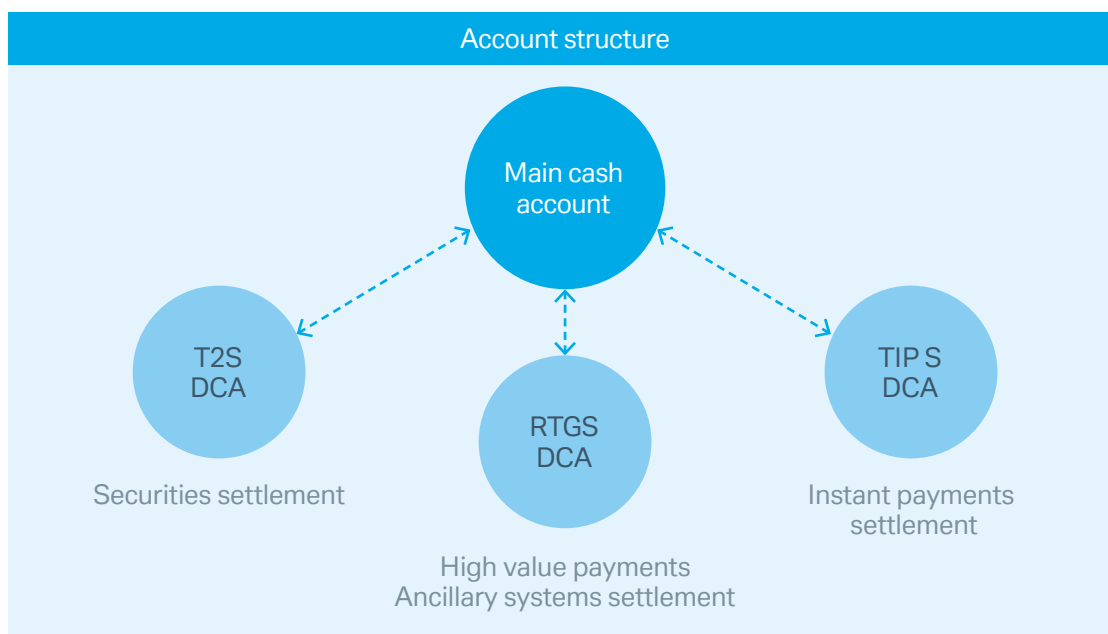
The second is a scheme being set up by the European Central Bank (ECB), running on the Target Instant Payment Settlement (TIPS) platform.⁷ As with RT1, TIPS will offer end-to-end processing within 10 seconds, with 24/7/365 availability. However, this scheme will settle instant payments in central bank money, allowing participating banks to set aside part of their liquidity on a dedicated account opened with their central bank, from which instant payments can be settled around the clock. An added advantage for banks here is that the balance on these accounts will count towards their required minimum reserve. While the scheme will primarily focus on the euro, it will also be able to perform domestic clearing in other European currencies. It is expected to go live in November 2018, with the majority of members joining in 2019.

Modernising high-value payments in Europe

The reorganisation of Europe’s real-time gross settlement (RTGS) system is potentially the greatest change in the European payments market since the introduction of the euro in 1999. The ECB has outlined an ambitious project to upgrade its TARGET RTGS system, creating TARGET2⁸ and TARGET2Securities (T2S).⁹ Together with TIPS, these services will be served from the central bank’s TARGET accounts, with ISO 20022 the sole messaging standard across all services in order to facilitate smooth pan-European payments.

Adapting to these changes will require major migrations in terms of messaging formats, liquidity management and communication methods. There can be no phased implementation for fear of the potential negative impact on liquidity in the market as a whole. Rather, transition to the new system will have to be carefully rehearsed and fully tested a number of times prior to going live, as all participating banks (the euro zone’s current RTGS system, TARGET 2, has over 1,050 direct participants) will have to be ready to migrate at precisely the same time.

Figure 4: How banks interact with TIPS, T2 and T2S through a TARGET account



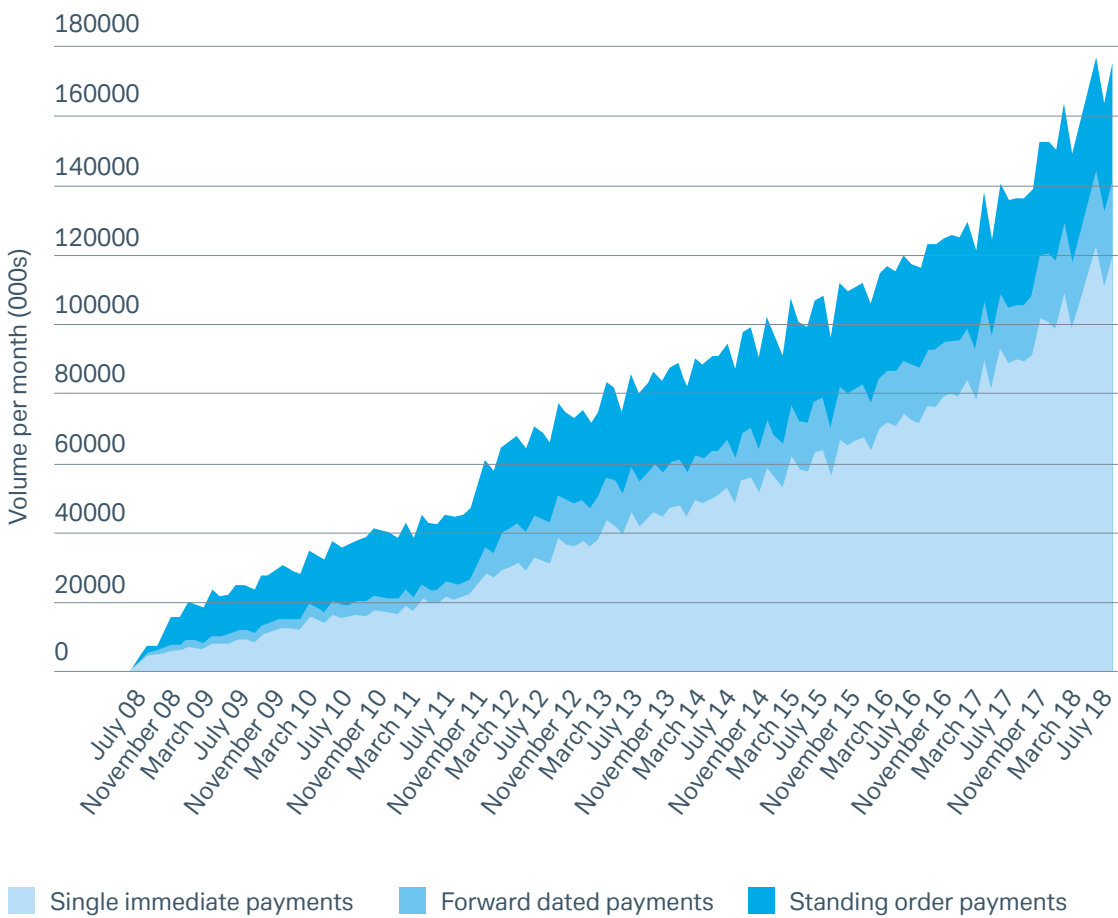
Source: ECB, https://www.ecb.europa.eu/paym/intro/events/shared/pdf/fs06/target2_and_t2s_consolidation_securities_perspective.pdf

Instant payments and modernised high-value payment schemes beyond Europe

There are as many as 45 instant payment schemes live around the world, from Singapore's Fast And Secure Transfers (FAST) to the UK's Faster Payments Scheme (FPS), showing a global appetite for real-time or instant payments driving market infrastructure providers to make faster payments available in many locations. With the exception of the UK and Australia, which both allow "one leg out" transactions to be processed within their schemes, all of these are domestic only, meaning they only support instant payments within a particular country or currency zone.

When the UK's FPS went live in 2008,¹⁰ it was one of the first countries in the world to launch a 24/7 real-time payment scheme (see Figure 5 for volumes of Faster Payments in the UK). However, ten years later, faster payments initiatives are considerably more widespread, and projects are planned or in execution to thoroughly modernise and standardise payment infrastructures in a number of key geographies including Europe, the US and Australia. In response, the UK recently decided to update its payments architecture and to follow the global trend of migrating messaging standards to ISO 20022. It has set itself an ambitious time-table within which to achieve this, with go-live in 2021.

Figure 5: Volumes of Faster Payments since their launch in the UK



Source: Faster Payments <http://www.fasterpayments.org.uk/statistics>

More ambitious still is the US Federal Reserve Banks’ decision to update their payment infrastructure for processing high-value instant Fedwire Funds Transfers and CHIPS payments and migrate the messaging format to ISO 20022. While this will mean significant upheaval for US banks and federal payment infrastructures, it is a far-sighted move – upgrading, standardising and aligning US high-value payments with those of other key geographies. Migration is set to be completed in 2023, in accordance with a three-phase plan, the final phase of which will offer market participants the full range of ISO 20022’s enhancements in transmitting rich and structured data.

SWIFT, as a key market infrastructure provider, together with the largest transaction banks, has also been instrumental in boosting speed, efficiency and transparency by completely transforming the cross-border payments industry through the launch of the global payments innovation (gpi) initiative in February 2017.¹¹ Gpi's tracking capabilities, based on cloud technology, enable clients to see the status of their payments at any time, thereby vastly improving transparency and facilitating end-to-end tracking of payments. The vast majority of cross-border payments are now executed in under 30 minutes (but many within minutes or even seconds). The SWIFT gpi for corporates pilot, launched in July 2018, should take this even further, giving clients the ability to track payments across multiple banks via a single portal.

3.3 Non-bank competitors are either competing or collaborating with traditional banks

Over the past few years, a number of incumbent technology providers, including FinTechs and challenger banks, have entered the payments space with new digital service offerings. As disruptors of the market, a small number have positioned themselves as direct competitors to banks. However, the vast majority see greater potential in collaboration, bringing benefits to both parties. Whereas FinTechs can offer highly innovative, specialised products and services within specific areas of the payments chain, banks can provide the reach, platforms and networks through which these products and services can achieve optimal success and the widest uptake.

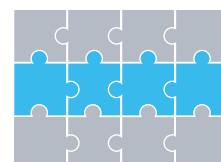
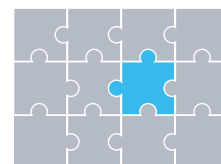
Indeed, when it comes to the trust clients show towards their banking partners, there is evidence to suggest that combining this with FinTechs' expertise is a winning combination – and one that clients feel they can use with confidence. A survey conducted by the Economist Intelligence Unit, in collaboration with Deutsche Bank, of 300 senior corporate treasury executives between April and June 2018 found that 75% of respondents would use fintechs in partnership with banks, and 16% of treasurers would use a bank-fintech combination “unconditionally”, demonstrating that companies view such partnerships as a guarantee that due diligence has been conducted at a level that would satisfy their own processes.

Such collaborations are equally advantageous for banks, more and more of which are considering working closely with FinTechs in order to capitalise on strategic opportunities for growth and value. Deutsche Bank's partnership with US-based mobile payments provider Modo, for example, allows it to extend its digital B2B and B2C payments business to non-bank platforms, facilitating payments beyond traditional banking channels.¹²

3.4 What's next?

The payments industry has already made massive strides in terms of speed, transparency and efficiency. Over the next three to five years, this will be taken to an even higher level, as the key market infrastructures migrate to ISO 20022, real-time payment platforms continue to increase in numbers, and emerging technologies unlock further potential.

The next step is for speed, efficiency and transparency to be firmly rooted in the entire value chain from new client adoption through to reporting and exceptions handling. Banks will have to offer end-to-end services that are fully digitised, including efficient onboarding. This will be coupled with real-time intraday analytics and reporting capabilities, and real-time payment fraud and surveillance controls.



4

Clients need global reach and global networks

While improving the quality of payment services by utilising leading technology is crucial to meet end users' ever-rising expectations, the need for global reach is just as important. Indeed, even the most sophisticated technology is redundant without it

There has always been a need for reach, but supply chains today are becoming increasingly global in nature, and businesses are as likely to have suppliers on the other side of the world as they are to have them in the next city over.

Until now, reach across the globe has been maintained through the correspondent banking model, despite suggestions that this could somehow be replaced by a cheaper, more efficient blockchain-based model. While blockchain will likely play an important role in the future in terms of further process optimisation, there are still a number of significant issues that need to be clarified before it can become more widely spread, especially with respect to governance and the legal framework within which it will operate.

4.1 Regulators and inter-governmental bodies should remain open for dialogue

Despite all the industry efforts with regards to harmonisation, there is no disputing that there has been a recent trend towards nationalism at a national policy level. Yet, it is unlikely that this will significantly impact ever-increasing globalisation. In this respect, it is important however that there remains an open dialogue with regulators to clarify regulatory and supervisory expectations and to avoid any unintended consequences of regulation.

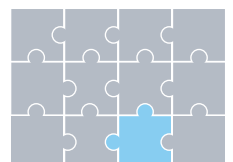
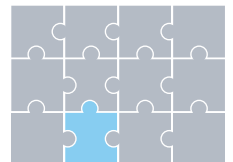
Here, the leading correspondent banking providers can play a pivotal role, providing their expertise to bridge jurisdictions. One such example regards the FTR 2015, which continues to leave room for interpretation at present. Institutions such as Deutsche Bank can help by engaging in discussions with regulators to gain further clarity on its interpretation, thereby creating a level playing field and leveraging the outcome of those discussions to educate their clients.

4.2 Industry and market infrastructures optimising current models and maintaining reach

As mentioned previously, at present the only way to ensure true global reach is through the correspondent banking network. What is currently required is an efficiency drive within that existing network to take correspondent banking to the next level. Here the industry, together with market infrastructures, is playing a prominent role.

The SWIFT gpi initiative is one such example. Indeed, within the space of 18 months, gpi has radically improved the cross-border payments experience, delivering on same-day availability of funds, fee transparency and end-to-end payments tracking (see Figure 6 on page 16 for key stats).. In fact, 90% of gpi payments are credited within a day, and 50% in less than 30 minutes, which has had a dramatic impact on the industry.¹³ Banks can credit payments within minutes or even seconds, while their clients benefit from shorter supply cycles and are able to get to the business of actually shipping goods much more quickly.

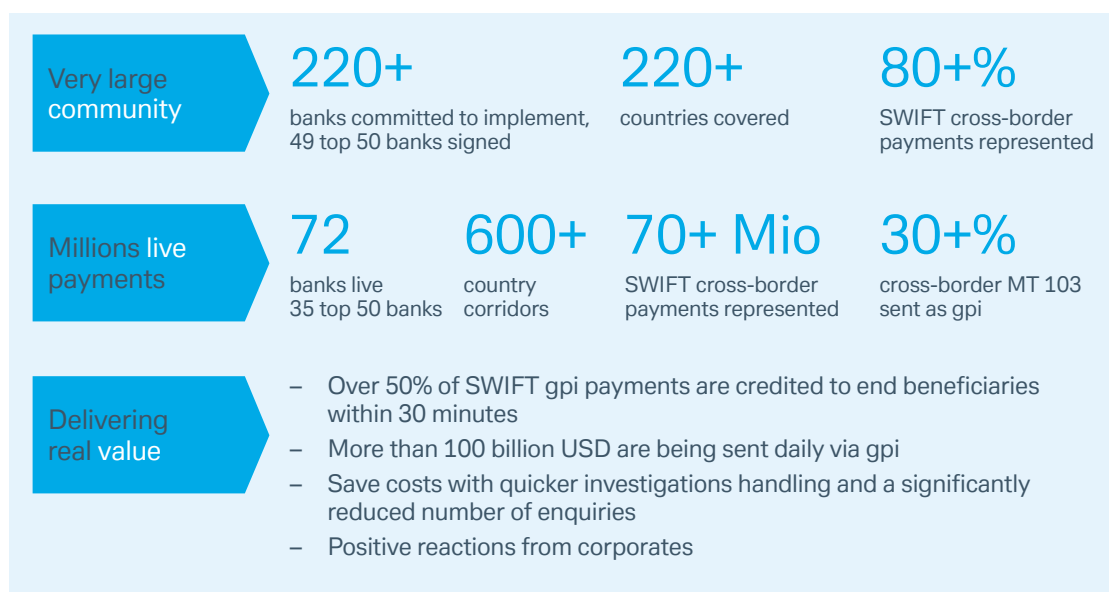
Efficiency and standardisation in correspondent banking has also been significantly improved through the use of KYC (know your customer) registries, providing a simplified way for banks to comply with their KYC obligations, allowing members to share data across a platform.



Indeed, as KYC requirements become stricter (to combat money laundering and terrorist financing), banks must take necessary steps to understand inherent risks in the payment flows not only of their clients, but also their clients' clients.

The SWIFT KYC Registry is one of the best examples in the industry, and has already led to a better level of information standardisation.¹⁴ The SWIFT working group agreed that any bank requesting KYC data from the utility on a correspondent is guaranteed to receive a "baseline" of SWIFT-verified information across five categories: identification of entity; beneficial ownership structure; products and services; AML policies and compliance structures; and tax information.

Figure 6: Current geographical reach of, and industry participation in, SWIFT's global payments innovation initiative (gpi)

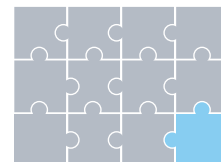


Source: SWIFT

3.3 Non-bank competitors are driving a platform economy

In the past few years, tech giants, such as Google, Amazon, Facebook, Apple and Alibaba, have been hugely successful in carving out entire new areas of engagement and behaviour in consumers' social, commercial and financial lifestyles. However, although they have been touted as potential direct competitors to banks, it should not be forgotten that banking is highly regulated, with complex audit and compliance requirements, subject to strict standards of governance and has need of substantial capital outlays.

These may be some of the reasons why these tech giants have until now hesitated to become banks. However, this could still change if banks fail to deliver on client expectations. The future value of banks in the digital world is not just their balance sheets, but also client relationships, and their ability to build a full business platform model with shared economies.



One key lesson banks can learn from the FinTech giants is that to be truly client-centric and prioritise the client experience, they must look to platforms for their new business models. As client expectations continue to change, and the world becomes increasingly digital, it is therefore vital that banks accept the idea of Open Banking platforms.

4.4 What's next?

In the immediate future, the correspondent banking industry has to leverage its strengths in terms of its high standards of payment security, its global reach and client trust. Any changes to current systems must be impactful, bring greater efficiency and remove points of friction. With regards to gpi, for example, the industry has already come a long way in a short space of time. What we need to strive for now is full adoption of gpi by banks, making this the new standard in the industry, aiming for a 100% gpi ratio for SWIFT payments, and incorporating elements such as pre-validation in the next stage of the evolution.

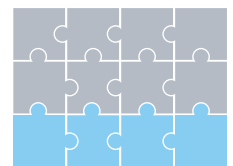
Further efforts also need to be made around KYC. KYC Registry membership is now approaching 5,000 banks in over 200 countries and territories,¹⁵ and a great deal of standardisation has already been achieved. Next steps could be the deployment of API technology to simplify and streamline data gathering and processing for KYC purposes, thereby automating it fully. Now is the right time to do this, given that the “baseline” of what data is required, and in what formats, is now being agreed.

Banks need to look at regulation as a means of providing business opportunities for clients. PSD2, for example, has acted as a catalyst for platform business models, a driver for APIs and shows a need for new interaction models with clients. We are also investing in new payment methods such as push payments. In collaboration with the International Air Transport Association (IATA), Deutsche Bank saw an opportunity to create a new online payment method, as an alternative to credit or debit cards.¹⁶ In this case, the bank acts as a TPP, collecting ‘push’ payments from passengers by means of API connectivity to the passengers’ bank accounts. For merchants, this means cost-savings, enhanced security, reduced risk of fraud, faster and more efficient collections and improved working capital.

To conclude, the future of banking will almost certainly see banks opening up infrastructure to clients, partners and FinTechs, acting as network-agnostic payments providers, offering efficient, highly automatised payments with global reach.

At Deutsche Bank, we are working on all fronts to lay the foundations for an Open Banking platform of tomorrow. We believe that establishing a unified API-ecosystem is key to supporting the Open Banking business models that will in future allow our clients, partners and FinTechs to integrate with us seamlessly and securely. This unified ecosystem will support all relevant payment solutions for our clients, and harness the rich potential of payments data to provide value-added services, including payment (in addition to liquidity and risk) analytics. In short, this is the best way to truly revolutionise client experience 24/7 and in real-time.

To this end, we are expanding our digital capabilities, including in analytics, API connectivity, cloud, and artificial intelligence and robotics, preparing for the coming market infrastructure changes, the migration to ISO 20022, and for shortening our end-to-end processing cycles. We are investing further in cross-border payments, expanding mobile payments, rolling out our real-time payment capabilities, and establishing our role as an aggregator in both the mobile and instant payment segments.



5

Looking to the future

Over the past few years, the payments landscape has undergone a major transformation, driven primarily by advances in technology and ever-increasing client expectations

In the coming years, further changes can be expected as competition increases and emerging technologies become mainstream. Amidst all these changes, however, the key needs for the end users of payments systems will remain unchanged:

- Security,
- Speed, efficiency and transparency,
- Global reach.

How, with whom, and in which form banks fulfil these key needs of clients depends to a certain extent on their preferred business model. For its part, Deutsche Bank sees Open Banking and API technology as an important area of focus – not only to ensure regulatory compliance, but also to explore its business potential to enhance the client experience and enable more flexible integration of banking services. As a bank, we are striving to create a unified API ecosystem which will support Open Banking business models enabling our clients, partners and FinTechs to interface and integrate with us in a seamless and fully secure manner.

On this journey, however, we have to take into consideration the needs of our clients today. With no truly viable alternative to correspondent banking in terms of global reach, we cannot allow it to stagnate: it remains still vitally important to support global trade. It is up to banks to ensure that it remains as efficient and stable as possible, meeting changing client expectations without disrupting them.

We welcome the comments of clients, partners, financial institutions, FinTechs and regulators wishing to join us in the ongoing collective enterprise of envisioning and shaping a payments market fit for a dynamic and digital future.

References

¹See http://cib.db.com/docs_new/DB_FTR2015_Whitepaper_20170519.pdf

²See <https://www.hkma.gov.hk/eng/key-information/press-releases/2016/20160518-5.shtml>

³See <https://www.swift.com/myswift/customer-security-programme-csp>

⁴See <https://www.ft.com/content/39ec1e84-ec45-11e5-bb79-2303682345c8>

⁵See <http://cib.db.com/insights-and-initiatives/white-papers/unlocking-opportunities-in-the-api-economy.htm>

⁶See <https://www.ebaclearing.eu/services/instant-payments/introduction/>

⁷See <https://www.ecb.europa.eu/paym/target/tips/html/index.en.html>

⁸See <https://www.ecb.europa.eu/paym/t2/html/index.en.html>

⁹See <https://www.ecb.europa.eu/paym/t2s/html/index.en.html>

¹⁰See <http://www.fasterpayments.org.uk/celebrating-10-amazing-years-2008>

¹¹See <https://www.swift.com/our-solutions/global-financial-messaging/payments-cash-management/swift-gpi>

¹²See https://www.db.com/newsroom_news/2018/deutsche-bank-takes-stake-in-payments-technology-start-up-modo-en-11663.htm

¹³See https://www.swift.com/news-events/press-releases/swift-gpi-reduces-cross-border-payment-times-to-minutes_even-seconds

¹⁴See <https://www.swift.com/our-solutions/compliance-and-shared-services/financial-crime-compliance/our-kyc-solutions/the-kyc-registry>

¹⁵See https://www.swift.com/news-events/news/bank-of-america-merrill-lynch-sees-significant-kyc-time-savings-using-swift_s-kyc-registry

¹⁶See https://www.db.com/newsroom_news/2018/deutsche-bank-pilots-game-changing-payments-solution-with-iata-en-11574.htm

This document is intended for discussion purposes only. It does not create any legally binding obligations on the part of Deutsche Bank AG and/or its affiliates ("DB"). The information contained in this document is based on material we believe to be reliable; however, we do not represent that it is accurate, current, complete, or error free. Any opinions expressed herein may differ from the opinions expressed by other DB departments. Without limitation, this document does not constitute a DB's view, an offer, an invitation to offer or a recommendation to enter into any transaction. DB is not acting as your financial advisor or in any other fiduciary capacity with respect to this document. The transaction(s) or product(s) mentioned herein may not be appropriate for all users and before entering into any transaction you should take steps to ensure that you fully understand the transaction and have made an independent assessment of the appropriateness of the transaction in the light of your own objectives and circumstances, including the possible risks and benefits of entering into such transaction. You should also consider seeking advice from your own advisers in making this assessment. If you decide to enter into a transaction with DB, you do so in reliance on your own judgment. DB may engage in transactions in a manner inconsistent with the views discussed herein. DB trades or may trade as principal in the instruments (or related derivatives) discussed herein. The distribution of this document and availability of these products and services in certain jurisdictions may be restricted by law. You may not distribute this document, in whole or in part, without our express written permission. **DB SPECIFICALLY DISCLAIMS ALL LIABILITY FOR ANY DIRECT INDIRECT, CONSEQUENTIAL OR OTHER LOSSES OR DAMAGES INCLUDING LOSS OF PROFITS INCURRED BY YOU OR ANY THIRD PARTY THAT MAY ARISE FROM ANY RELIANCE ON THIS DOCUMENT FOR THE RELIABILITY, ACCURACY, COMPLETENESS OR TIMELINESS THEREFORE.** Deutsche Bank AG, including its subsidiaries and affiliates, does not provide legal, tax or accounting advice. The recipient of this communication should seek advice from an independent tax advisor regarding any tax matters addressed herein based on its particular circumstances.

Deutsche Bank AG is authorised under German Banking Law (competent authorities: European Central Bank and German Federal Financial Supervisory Authority (BaFin)) and, in the United Kingdom, by the Prudential Regulation Authority. It is subject to supervision by the European Central Bank and the BaFin, and to limited supervision in the United Kingdom by the Prudential Regulation Authority and the Financial Conduct Authority. Details about the extent of our authorisation and supervision by these authorities are available on request.

Copyright© (October 2018) Deutsche Bank AG.

All right's reserved