

>> WHOSE CUSTOMER ARE YOU? THE REALITY OF DIGITAL BANKING //

Sponsored by



TEMENOS
The banking software company

CONTENTS

- 2 About this report**
- 3 Executive summary**
- 5 Section I: Evolving trends: The digital future is here**
- 9 Section II: New business models: What do banks want to be?**
- 10 Monzo: Aiming for seamless growth**
- 15 Europe: Wide open**
- 16 Section III: Digital transformation: Move fast but don't break anything**
- 17 A digital Greater China**
- 20 Pepper: Starting from scratch**
- 21 Section IV: Artificial Intelligence is watching and learning**
- 24 Section V: Security: An increasingly global concern**
- 25 If the face fits**
- 27 USA: You're next**
- 28 Customer due diligence: Who are you?**
- 29 Conclusion: Play to your advantages**

ABOUT THIS REPORT

In February-March 2018 The Economist Intelligence Unit, on behalf of Temenos, surveyed 400 global banking executives about the challenges retail banks expect to face between now and 2020, and the strategies they are deploying in response.

The survey respondents were geographically diverse: 25% were drawn from Europe, 25% from the Asia-Pacific region and almost 18% were from North America. This year's survey had our highest ever representation from emerging markets, with approximately 16% of respondents from Latin America and 16% from Africa and the Middle East.

By size of their employer, the respondent base is evenly split. Half work for parent groups with assets over US\$10bn, the other half work for smaller organisations, including co-operatives and community banks. In terms of seniority, 51% are at C-suite level and 10% are board members.

A fifth (20%) of respondents work in finance roles, over 10% work in general management roles and 9% work in IT. Marketing, sales and customer service constitute 16% of the base. A further 6% of respondents work in information and research and 5% in research and development.

In addition, in-depth interviews were conducted with 20 senior executives and experts from banks, fintech companies and security advisers. Our sincerest thanks are due to the following for their time and insight.

Neil Aitken	Head of communications, UK Payments Administration
Tom Blomfield	Chief executive officer, Monzo
Josh Bottomley	Global head of digital, HSBC
Ray Brash	Chief executive officer, PrePay Solutions
Ilan Buganim	Chief technology officer, Bank Leumi
Hector Cardenas	Co-founder/CEO, Conekta
Tamara Cook	Head of digital innovations, FSD Kenya
Stefan Erne	Chief digital officer, Handelsbanken
Hakan Eroglu	Executive, Digitisation in payments & banking, Accenture
Andres Fontao	Managing director, Finnovista
Carol Hung	Chief information officer, Standard Chartered Hong Kong
Francisco Illescas	Co-founder, Tesseract
Jane Jee	Chief executive officer, Kompli-Global
Michel Léger	Executive vice president, Innovation, Ingenico
Katie Mark	Senior communication manager, Competition and Markets Authority
Eduardo Morelos	Programme director, Startupbootcamp FinTech, Mexico City
Robert Prigge	Chief revenue officer, Jumio
Carlos Orta Tejada	Vice president, Regulatory Policy, Comisión Nacional Bancaria y de Valores
Hans Tesselaar	Executive director, Banking Industry Architecture Network
Edoardo Totolo	Research Economist, FSD Kenya
Roberto Valerio	Chief executive officer, RISK IDENT

The report was written by Paul Burgin and edited by Renée Friedman of The Economist Intelligence Unit.

EXECUTIVE SUMMARY

The future of banking is digital, but the human touch will remain essential in attracting new customers for loans and complex investment products. Stakeholders must co-operate like never before to deliver the user experience customers want while keeping their money and data safe.

This report, the fifth in The Economist Intelligence Unit's series on the future of retail banking, marks a significant shift in the strategic concerns of banking executives worldwide. Previous reports tracked the shift in customer expectations and its likely impact on distribution and product design. Now the focus is firmly on implementing open banking and dealing with its consequences.

- **Technology and digital are now bigger—and more important—trends than regulation.** Changing client demand, the rise of the smartphone and the introduction of new digital technologies have replaced post-financial crisis regulation as the drivers of strategic thinking at banks around the world. Integrating open banking that allows apps to initiate payments and other financial transactions is core to adapting to the digital banking age.
- **No single digital strategy suits every bank in every market.** Respondents say their banks are adopting different strategies. While 61% want to develop niche propositions, others are, to varying degrees, opening up and giving access to new third parties. Some banks will view regulatory and technological change as opportunities to recreate themselves and build new ecosystems, while others may simply comply with emerging norms and regulations by granting access to customer data and payments via competitors' smartphone apps. Going with the easiest options may leave banks, and their products, at risk of being assimilated, aggregated and unbundled by agile competitors, leading to a loss of brand and product visibility.
- **Banks must become more agile.** The development of agile products requires improved organisational agility as well. According to 52% of survey respondents, product agility is now their top strategic priority. New payment players and the likes of Google, Apple, Facebook and Amazon, collectively known as GAFAM, know what their clients want and are able to adapt quickly. Banks have to keep up, restructuring their business models to ensure that new products and features can be integrated quickly across physical and digital channels.
- **The impact of open banking and tighter security and data rules—and the conflicts between them—do not appear to be fully understood.** While 71% of respondents are focusing their digital investment on cyber security, only 17% are concerned about a third-party relationship vulnerability being exploited as a result of open banking. The biggest danger to a sustainable banking model is the loss of valuable data on customers' lifestyles and needs. Without that insight, all banks will struggle to upsell more profitable loan, investment and retirement products.
- **Customer and regulator concerns about data security may limit some of the big banks' ambitions.** The larger banks can take the fintechs on by building all-encompassing platforms that offer a seamless interaction with other products, services and comparison tools. Offering greater functionality means banks can learn more about customer needs and tailor new products to match.

- **Artificial intelligence and chatbots have a role in customer services, authentication and fraud, but banks are taking a cautious line as they do not want to lose their customers' trust.**

Just over 20% of respondents think artificial intelligence (AI) will improve the user experience. However, banks need to appease customers' uncertainty about the security of their personal information and how these data about them may be used. They will need to do this while maintaining a frictionless user experience that still takes into account individuals' needs.

SECTION I: EVOLVING TRENDS: THE DIGITAL FUTURE IS HERE

“In many ways we are already a digital bank.” Josh Bottomley, global head of digital, HSBC

Smartphones, e-wallets and contactless technology are already displacing the branch, ATM, online PC banking portal and call centre. The challenges—and the opportunities—differ from continent to continent.

In the UK, its largest market, 90% of HSBC’s transactions are already digital. More importantly for the bank’s shareholders, roughly 50% of all revenue-generating transactions have shifted online too.

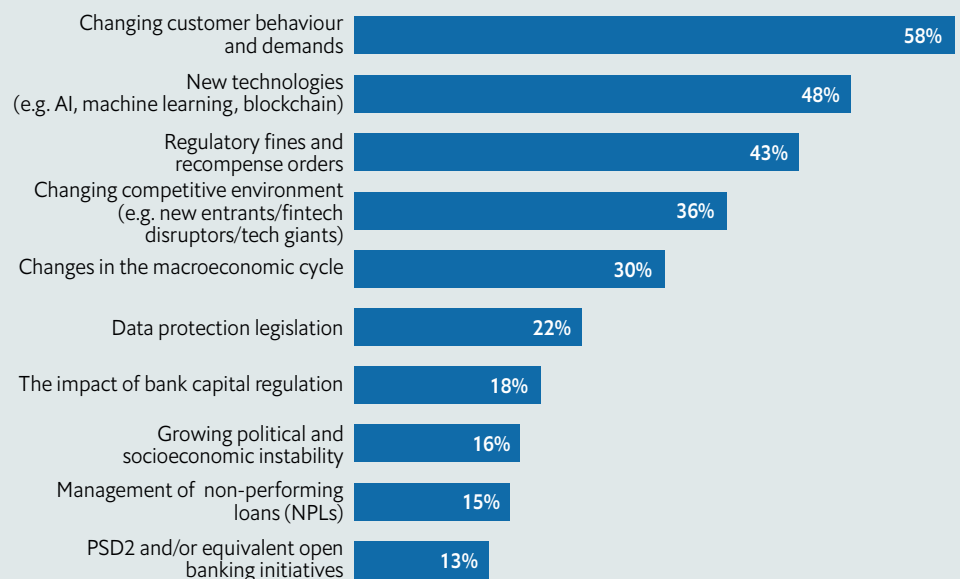
In the branch and back office new technology is also stripping costs, increasing productivity and boosting fraud and compliance capabilities.

As a result, and for the first time in its five-year history, the annual Economist Intelligence Unit survey on the future of retail banking shows that bank executives are now more concerned with technology-driven trends than they are by regulation.

Chart 1

Which trends will have the biggest impact on retail banks in the years to 2020?

(% of respondents)



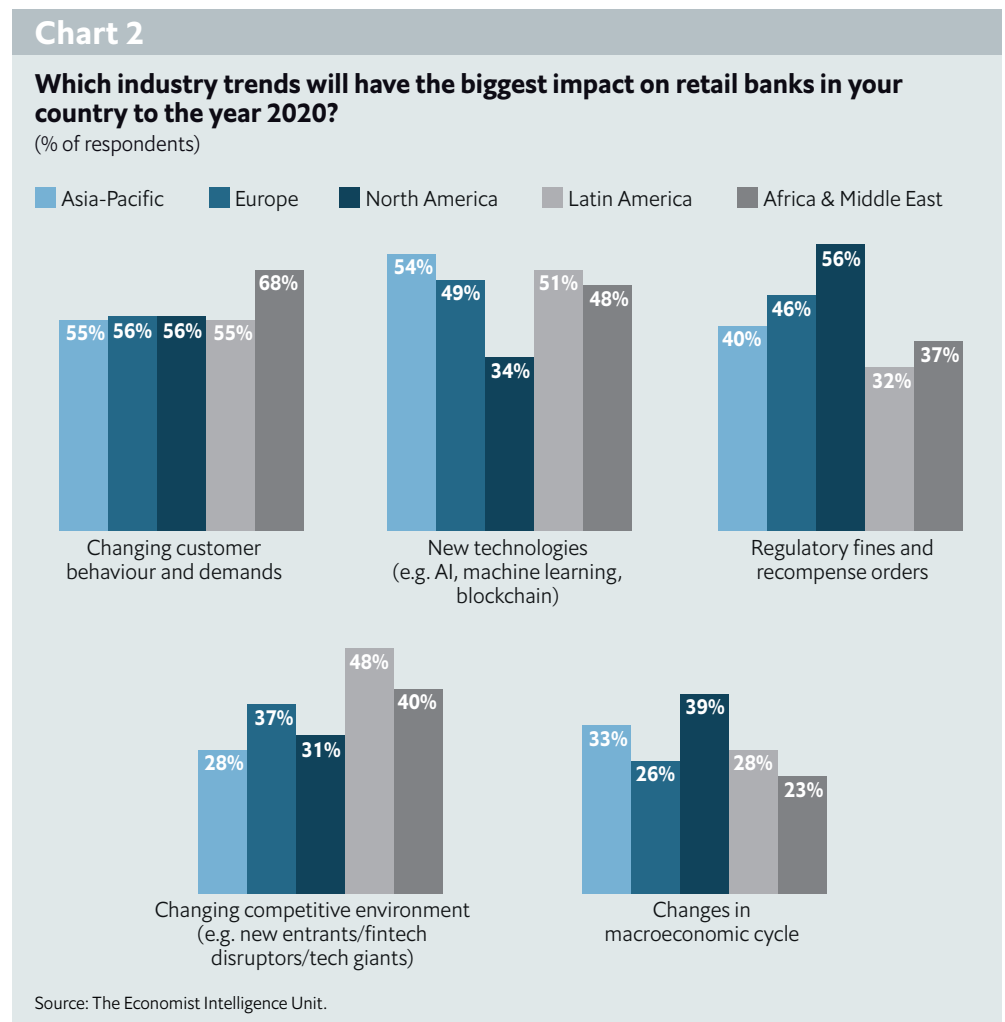
Source: The Economist Intelligence Unit.

The regulatory backlash to the global financial crisis continued to sap banks' strategic planning resources until last year. There are still outstanding regulatory issues, particularly around consumer protection, but they are no longer the priority.

Different drivers, same devices

As can be seen in Chart 1, responding to changing customer behaviour and demands will be the key trend in all regions in the years up to 2020 and beyond. However, as shown in Chart 2, there are geographical differences regarding the trends that will have the biggest impact.

The changing demands of customers are more keenly felt in some regions than others. The shift in customer expectations is most urgent in the Middle East and Africa, where Mobile Money Operator (MMO) phone-based payment platforms control the majority of the transaction market across the Sub-Saharan region.¹



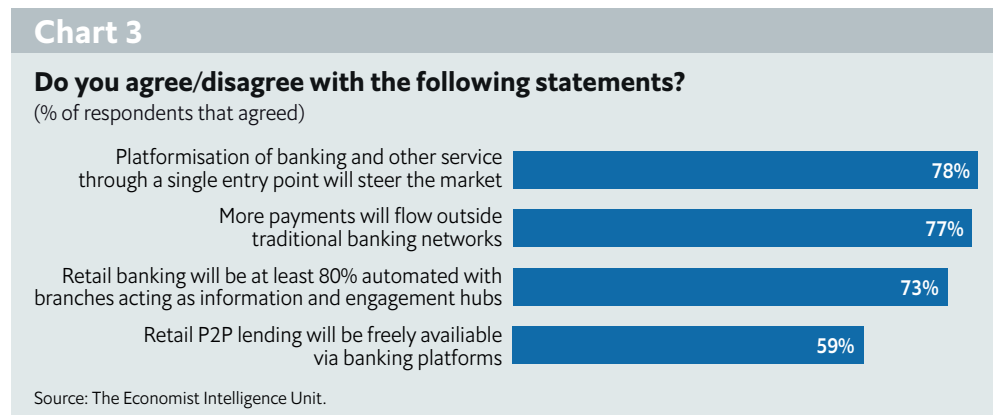
¹ GSMA, *State of the Industry Report on Mobile Money*, 2017. http://www.gsma.com/mobilefordevelopment/wp-content/uploads/2017/03/GSMA_State-of-the-Industry-Report-on-Mobile-Money_2016.pdf

In North America, regulatory fines are expected to have a bigger impact than anywhere else. Federal and state regulators are acutely aware that consumer protection needs tightening in the wake of recent scandals, including the opening of as many as 3.5m bogus customer accounts by financial services company Wells Fargo. In Asia, the lack of top-down regulation may explain why open banking barely seems to be a concern.

Established players in Latin America say that new entrants are more of a threat than anywhere else in the world. According to the World Bank, the continent is underbanked.² This may make it easier for new non-bank competitors to enter the market with smartphone and cloud technology as e-commerce takes off.

“Fixing payments from scratch is about social impact. We have customers thanking us for our role in developing the digital economy. It is a big responsibility,” says Hector Cardenas of Conekta, a Mexican fintech start-up bridging the gap between unbanked and digital payments.

The Latin American story also underlines an established trend seen elsewhere. Payments, as agreed by 49% of survey respondents, are always where new entrants try to enter the market.



In fact, that particular battle has already been lost in much of the world. Globally, 77% of respondents say that by 2020 the majority of payments will flow outside traditional banking networks, with bankers in Asia-Pacific the most likely to agree.

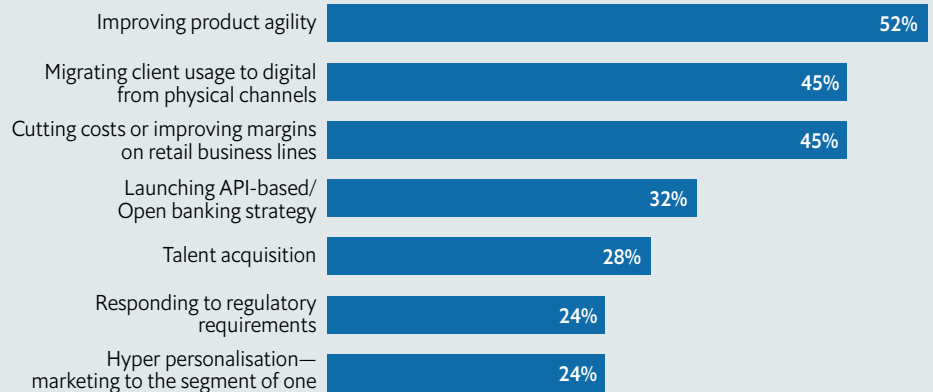
Product agility has also come to the forefront as a strategic priority for banks, with 52% of respondents considering it to be their top priority. As banking products and services must now be more agile to meet changing customer needs, this requires an almost simultaneous improvement to organisational agility. The pace of technology change is forcing banks to restructure how their business units operate. They no longer have the luxury of time, or the comfort of rigid business unit silos.

² World Bank, Global Findex Data. <http://datatopics.worldbank.org/financialinclusion/region/latin-america-and-caribbean>

Understanding and implementing new technology and procedures can be costly. As shown in Chart 4, customer services bosses are still under pressure to slash costs and improve product margins if banks are to head off the low-cost start-ups. However, there is one area where regulation needs to

Chart 4

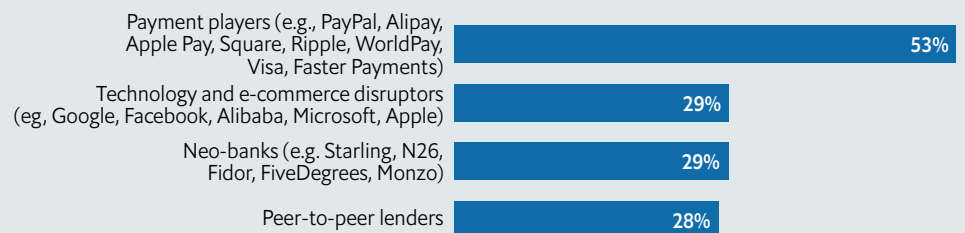
What are the top strategic priorities of your company in the years to 2020?
(% of respondents)



Source: The Economist Intelligence Unit.

Chart 5

Which non-traditional entrants to the retail banking industry will be your company's biggest competition in the years to 2020?
(% of respondents)



Source: The Economist Intelligence Unit.

be watched, interviewees report. Supervisors are increasingly concerned about the systemic and personal-data risks posed by digital payments and services.

Surprisingly, survey respondents appear to be more concerned about losing business to new payment players, including the threat posed by Google, Apple, Facebook and Amazon (collectively known as GAFA), than they are about ensuring that new payment frameworks are secure. As Chart 1 illustrates, 22% of respondents believe that data protection legislation will have the biggest impact on retail banks in the years to 2020, while 13% expect it will be the Revised Payment Services Directive (PSD2) and/or equivalent open banking initiatives.

As we explore in the following chapters, those priorities may need to be reversed—and quickly—to ensure that banks retain their role of trusted custodian of customer money and data.

SECTION II: NEW BUSINESS MODELS: WHAT DO BANKS WANT TO BE?

“If I were a banker right now, I would be justifiably worried.” Ray Brash, CEO, Prepay Solutions.

New entrants, new technologies and changing customer demands are forcing banks to rethink, adapt or completely change their business models, including their digital strategies. As interviewees for this report point out: “If you don’t have a digital strategy, your bank is already dead.” But what kind of bank do bankers envision will be the most sustainable and profitable model by 2020?

There appear to be two main options: the first is specialisation by market or product, the second is to play the fintechs at their own game.

Specialisation by market

When it comes to how banks see their current business model evolving, 61% of global survey respondents believe the best strategy is to develop a niche that will retain customer loyalty. An example of this “niche” approach is the “local digital strategy” being followed by Swedish bank Handelsbanken. This strategy is heavily based on face-to-face and personal contact. Although the bank is using new technologies, it operates a decentralised banking service based on local managers and staff with real decision-making powers.

Chief digital officer Stefan Erne says his bank is always looking to improve customer touch points, whether in a branch or during customer meetings, online or via a call centre, and is not focused on cutting costs internally.

Handelsbanken is rolling out a new personal finance management tool across Sweden, its biggest market. Country-specific versions operating to local needs will also be rolled out in other Nordic countries, the Netherlands and the UK. However, Mr Erne calculates that around 85% of the Swedish app’s features are reusable in other territories.

Handelsbanken’s view on customer data is also unconventional. While many banks are focusing on customer data analysis to increase cross-selling rates, Mr Erne has no such intention.

“Branches have the freedom and responsibility to take decisions based on individual customer needs. We don’t have a centralised segmentation model and we are not pushing products. And we take security and integrity very seriously and will not monetise the data if customers do not want us to,” he explains.

Yet all these data do not go to waste. The bank is investing heavily in customer-relationship management tools. Branch and call-centre staff now know whether a customer tried to sign up for a

new product online and then abandoned the process. Next time they meet, in a branch or by phone, they can offer some friendly assistance.

Specialisation by product

A more radical approach to a niche strategy may be to focus on specific products or features that can be unbundled from standard banking, savings or loan offerings.

For example, the UK's Competition and Markets Authority (CMA) now insists that customers are alerted when they are about to run an overdraft. That could lead to a market for cheaper unbundled short-term loan providers under open banking. But that market is only viable if costs are low, volumes high and on-boarding of customers made easy.

MONZO: AIMING FOR SEAMLESS GROWTH

The UK challenger bank Monzo received its banking licence one year ago, allowing it to begin the process of upgrading from offering prepaid credit cards to a full current-account service.

The upgrade was important for both the business and the customer base. The prepaid arrangement was loss-making, says CEO Tom Blomfield. He calculates that Monzo was losing around £65 (US\$91) per year per customer, mostly owing to the card processing fees that applied when customers loaded their cards with funds.

"Now we have a settlement account with the Bank of England and are a member of Faster Payments, we can run a current account for about £20 per year," says Mr Blomfield.

With 500,000 cardholders, Monzo was careful to test that the transfer was as seamless as possible. Since the prepaid scheme was shut down in April 2018, Mr Blomfield says 94% of active users upgraded. Customer numbers are

now close to 650,000.

Offering a full banking service will also assist the development of new products and services, according to Mr Blomfield. Lending is the priority. Monzo has introduced a new overdraft facility that allows customers to set their own overdraft limit, with a simple, single daily fee for using the service.

The average bank makes £60 on overdrafts, half from interest and half from charges. We only need around £20 to be profitable," says Mr Blomfield.

Giving customers control and transparency is vital to building the brand and customer loyalty.

"It is not rocket science. We are not ten times better than the banks, more like one-and-a-half times better. Spending notification, identifying retailers by their logo and budgeting tools are the little things that add up," suggests Mr Blomfield.

The founding team at Monzo, a UK challenger bank, developed such an “underdraft” concept more than two years ago. CEO Tom Blomfield says that current technology is not up to the job of creating a smooth pathway between current account, overdraft and back again.

“The pinch point is always whether you can make it seamless enough. It is tricky to do that right now,” he says.

Prepaid card providers are already adding new features that allow them to mimic bank accounts. They are adding a functionality that can easily turn their mobile apps into a full suite of services that appeal to immigrants, students and those with poor credit histories. As customers become more financially stable and their needs more sophisticated, then loans, mortgages and investment products can be layered on.

Ray Brash, CEO of PrePay Solutions, a UK-based one-stop-shop for prepaid programmes, says this is already happening in the Middle East, where governments, in a crack-down on employment abuses, now insist that people are paid electronically. As most migrant workers do not have sufficient credit histories to obtain traditional bank accounts, prepaid card providers have jumped in. Salaries are loaded onto payment cards, which are then used for transactions. Prepay apps are also used for remittance payments.

However, many of these workers still prefer cash for day-to-day use. Every payday, therefore, mobile ATMs are regularly driven across the desert to these migrant-manned oil rigs, says Mr Brash.

Africa offers a vision of how this unbundling can evolve. Over 40% of all adults in Gabon, Ghana, Kenya, Namibia, Tanzania, Uganda and Zimbabwe regularly use mobile-based money transfer services. There are now more MMO accounts in Sub-Saharan Africa than traditional bank accounts.

This has completely upended bank-product distribution and design. Banks now have to adapt their products to the MMO platforms, not the other way round. Every bank in Kenya now offers QR-code access to the M-Pesa mobile phone-based money transfer and financing service that reaches 70% of the population.

M-Pesa’s control over payments has forced ever greater numbers of banks to rethink how they reach their customers. The banks are belatedly devising new automated, digital lending products that pay directly into M-Pesa accounts.

Those that do not follow suit may find themselves without a viable survival strategy. Those that do will have to ensure that their service is better than M-Shwari, M-Pesa’s own micro-loan service that has already been tried by one in four Kenyans.

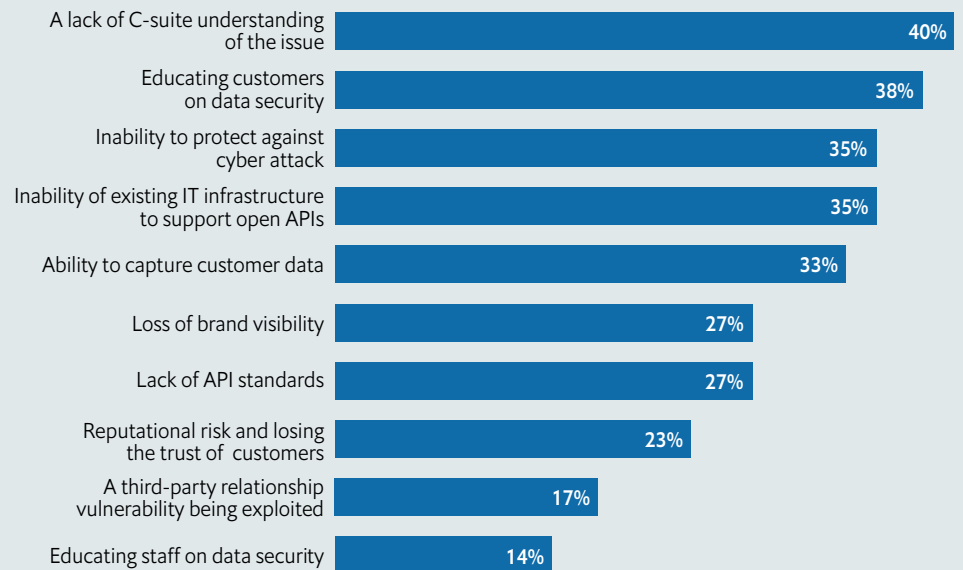
Ownership and distribution: taking on the apps

The second strategy is to fight the start-ups head-on. Open banking based on API, or application programming interface—a technology protocol that allows diverse software components to

Chart 6

What are your main concerns in relation to API based Open banking?

(% of respondents)

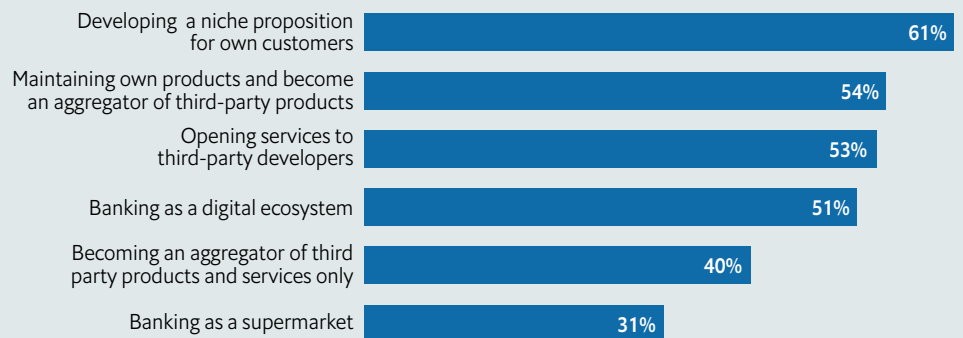


Source: The Economist Intelligence Unit.

Chart 7

How do you see your current business model evolving?

(% of respondents)



Source: The Economist Intelligence Unit.

communicate—threatens laggards if they only do the minimum in opening up to third-party payment apps. Their largely indistinguishable products would be reduced to small on-screen icons on aggregator apps that consolidate financial data from different accounts.

Worse still, banks themselves risk losing highly valuable customer lifestyle data. That's why the majority want to be aggregators, not aggregated. The big question is, exactly what type of aggregators do the

banks want to become? Their answers suggest that respondents are not entirely certain.

Should banks focus on their own products first, linking their customers to accounts they may hold with other institutions, or should they integrate more aggressively by offering personal finance management tools?

Big challenges need big solutions, particularly as 31% of respondents want to become a banking supermarket. They want to offer product comparisons and switching to own and third-party products. This is especially the case in Europe, where 37% of respondents want to leverage the trust customers place in them to become a personal provider of choice. As noted in Chart 3, 78% of respondents believe that “platformisation” of banking and other services through a single-entry point will steer the market.

China’s Alipay and WeChat Pay are already there in many respects. Mobile payments topped Rmb81trn (US\$12.8trn)³ in China over the first ten months of 2017, the absolute majority via Alipay and WeChat Pay. But their rapid ascent highlights four further issues as incumbents and newcomers battle to become the platform of choice.

First, regulators are assessing the systemic risks that new technologies present. In China, tech giants such as Alipay and WeChat must start clearing their payments through a new national clearing centre later this year, allowing regulators greater oversight and competitors more access to payment-flow data.

Next, the China experience cannot easily be replicated in other markets. The two Chinese giants grew in an unregulated space, where incumbents were not necessarily motivated to spot emerging mobile-payment trends.

Third, customers in other markets who are already well served by existing infrastructure and banking apps may not be as willing to switch to new platforms. Research by consultancy firm Accenture, conducted in the run-up to the entry into force of the Revised Payment Services Directive in January 2018, found that 85% of UK consumers were worried about sharing data via open banking.⁴ As security concerns grow, the grand ambitions of incumbents, social media giants and fintechs in developed markets may fall short.

Lastly, banks and their competitors must ensure that platforms, APIs and infrastructure work together. Strangely, bankers believe that new API-using apps and services will be more robust than their own systems and procedures: 35% of respondents say they are concerned about the inability of existing IT infrastructure to support open APIs. And only 17% are concerned about a third-party relationship vulnerability being exploited as a result of open banking.

Could banks really win the platform wars?

There is some scepticism whether conventional banks stand a chance of becoming the digital platforms of tomorrow when faced with emerging fintechs or GAFAs giants. But in the maelstrom of

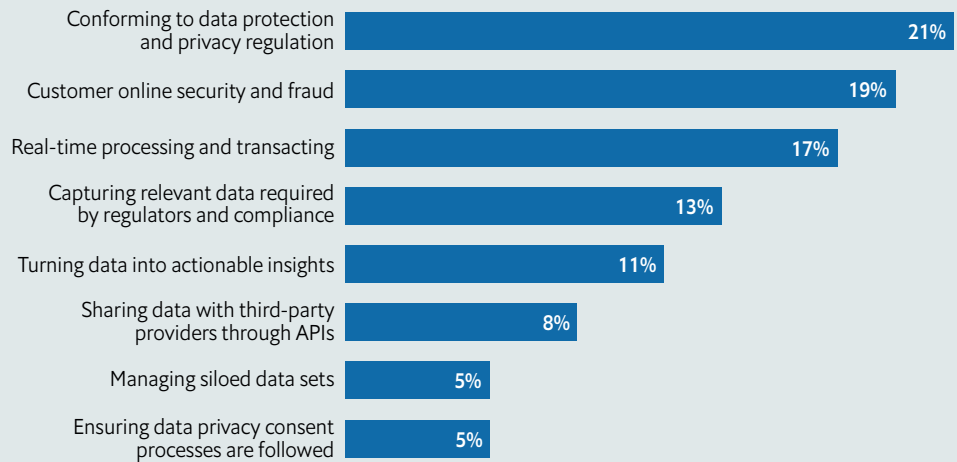
³ Straits Times, February 19th 2018. <http://www.straitstimes.com/asia/east-asia/chinas-mobile-payment-volume-is-worlds-largest-at-s167-trillion>

⁴ Accenture, October 2nd 2017. <https://newsroom.accenture.com/news/accenture-research-finds-lack-of-trust-in-third-party-providers-creates-major-opportunity-for-banks-as-open-banking-set-to-roll-out-across-europe.htm>

Chart 8

What is the biggest challenge your company faces concerning data and third-party access?

(% of respondents)



Source: The Economist Intelligence Unit.

change it is easy to forget three simple truths, the first one being that to a large degree such banks already have the trust, the data and the connections that the fintech newcomers need.

More than 60% of the world's population over the age of 15 already have relationships with a bank, credit union or co-operative, far more than have accounts with an MMO or non-bank.⁵ This is important, as there is an element of trust and familiarity embedded in deciding where best to place your cash.

Second, when a bank has the primary current-account or payment-card relationship, it should already have a good picture of a customer's life. If it can use transaction data to spot suspicious activity, it should be able to turn the same information into actionable selling opportunities.

Although these data are often spread across multiple systems, as noted in Chart 4, only 24% of respondents list hyper-personalisation as a top strategic priority. It appears that banks think they can do better at guessing what customers want, as only 11% see turning data into actionable insights as their biggest challenge (see Chart 8).

Third, banks should not overlook the network effect. Global, regional and domestic infrastructure connects everything, from the point-of-sale transaction in the coffee bar to the central bank.

These systems are extremely robust. The UK's Faster Payments, a real-time payment system, reports 100% uptime since it was introduced in 2008. Retail and business users do not need to know how it works, but they had sufficient trust in it to send £123bn (US\$171bn) through the system in February 2018 alone, a 23% increase on 2017.⁶ In much of the world, fintechs may find it hard to replicate what already works and ensure that their new models are financially viable.

⁵ Global Findex Database, 2014. <http://documents.worldbank.org/curated/en/187761468179367706/pdf/WPS7255.pdf#page=3>

⁶ Faster Payments: Total payments between launch on May 27th 2008 and February 28th 2018 were 8.8bn, worth £6,7218 bn. February 2018, volume 148.6mn (+23% year on year).

EUROPE: WIDE OPEN

Open banking, which requires banks to share customer data and allows third parties to initiate transactions, is becoming a reality from Asia to Latin America. But when asked which trends will have the biggest impact on retail banks in their country in the years to 2020, only 13% of global respondents cite the challenges and threats posed by open banking. Even more concerning is the finding that less than 6% of risk personnel see the riskiness.

Interviewees warn that the industry is seriously ignoring the impact, particularly in Europe, where the new Payment Services Directive (known as PSD2) came into force in January 2018. When asked about their main concerns in relation to API-based open banking, 40% of survey respondents say that C-suite understanding of what is at stake is the biggest impediment to open banking being taken seriously by incumbent banks.

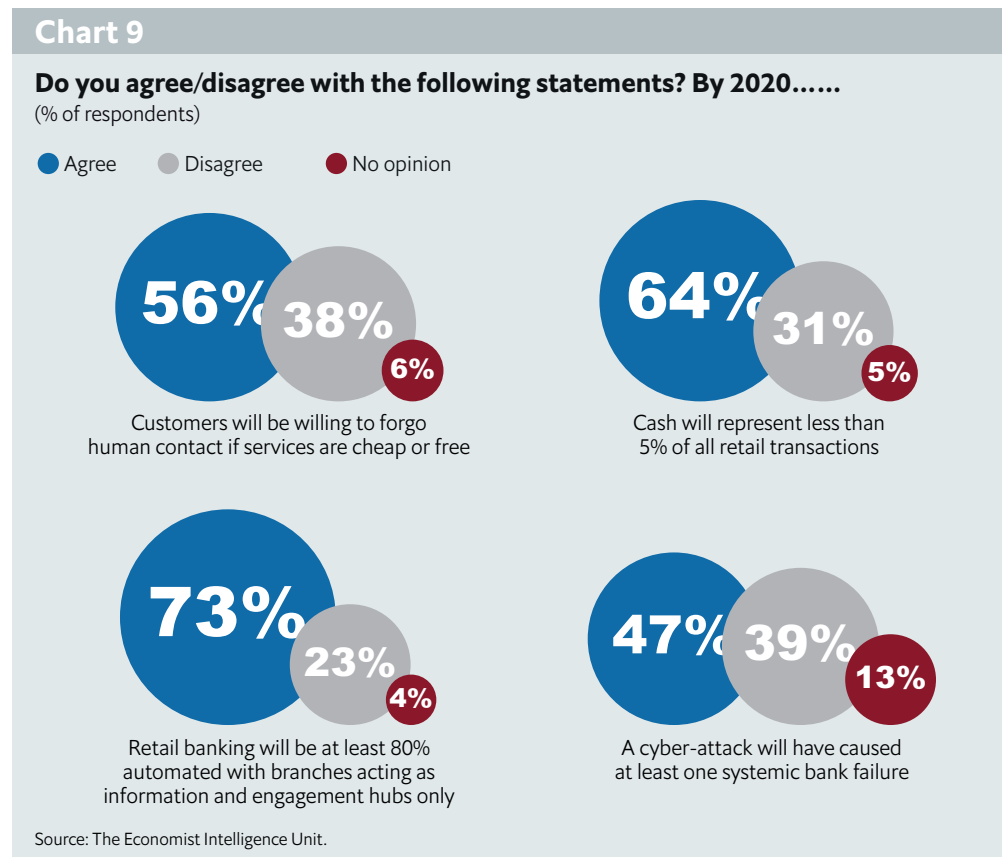
Would a big cyber-attack from a third party to which their bank has opened its data galvanise management into action? Perhaps not: only 22% of respondent identify data protection as a strategic priority. North American respondents are the most attuned to data concerns, with 30% citing it as a priority, but given the real threat posed by cyber criminals, this is surprisingly low.

The fact that only 24% European respondents consider data protection to be one of the trends that will have the greatest effect is also worrying. According to security experts, this figure should be far higher. The EU's new General Data Protection Regulation (GDPR), due to come into force in May 2018, will test all companies in every sector, but given the amount of personal data they hold and must now share, banks are particularly vulnerable.

SECTION III: DIGITAL TRANSFORMATION: MOVE FAST BUT DON'T BREAK ANYTHING

Established banks have many advantages in the platform wars, but there is no question that winning them would require substantial transformation.

The scale of the transformation ahead is evident from the survey. Nearly three-quarters of survey respondents think retail banking could be largely automated by 2020, over half (56%) believe customers will forgo human contact if services are free or cheap, while 64% say that fewer than 5% of retail transactions will be in cash in three years' time. A disturbing 47% believe that a cyber-attack will have caused at least one systemic bank failure.



In undertaking this transformation, banks are often at a disadvantage. Unlike Facebook with its old mantra of “Move fast and break things”, banks must move fast, but they cannot sacrifice security or trust while doing so.

Banks must therefore find ways to undergo a rapid organisational and business-model transformation while preserving the qualities that customers know and respect. That means updating the branch, transforming the IT infrastructure and collaborating with the ecosystem of fintechs even as they present competitive challenges.

The future of the branch

Branches are disappearing quickly as customer behaviour changes. The ratio of branches per 100,000 of the population fell by 44% in Norway and by nearly 65% in Finland between 2010 and 2016 as payment apps have led to less reliance on cash.⁷

The volume of Swedish currency in circulation has halved over the last decade, with the fall accelerating in the last two years.⁸ The banking industry's Swish app is now so ubiquitous that many shops and bank branches no longer accept notes and coins. This has politicians and Stefan Ingves, the governor of Sveriges Riksbank, the central bank of Sweden, worried. When economic activity flows through apps run by commercial banks, the central bank has less power over monetary policy as it cannot remove notes from circulation. Those app operators also control access for shoppers, potentially impacting the elderly and marginal members of society who may not have smartphones.

Will payment apps kill off the branch entirely? Respondents and interviewees think not. Over 61% of respondents still see a place for the traditional transaction-based branch model, nearly twice as many as those who think it will be dead by 2020.

The number of branches and call centres that remain will depend on changing customer demand. But the technology underpinning physical and online channels is developing rapidly.

A DIGITAL GREATER CHINA

Asian banks are racing to digitalise their entire suite of financial products. However, as Standard Chartered Hong Kong found out, usage patterns vary across the Greater China region.

The bank recently surveyed online and mobile banking habits in Hong Kong, Shanghai and Taiwan. Shanghai has a significant lead in terms of mobile-payment users. It also has a higher adoption rate for person-to-person payments.

"Hong Kong and Taiwan have also demonstrated great appetite for other fintech solutions, such as online stocks or foreign-exchange trading, while people in Shanghai tend to use more real-time online support, live chat and video banking," says Carol Hung, the bank's chief information officer.

But wherever they are, customers are wary about their security. In Hong Kong, 31% of survey respondents say that security and data leakage are key concerns that hinders them from using fintech.

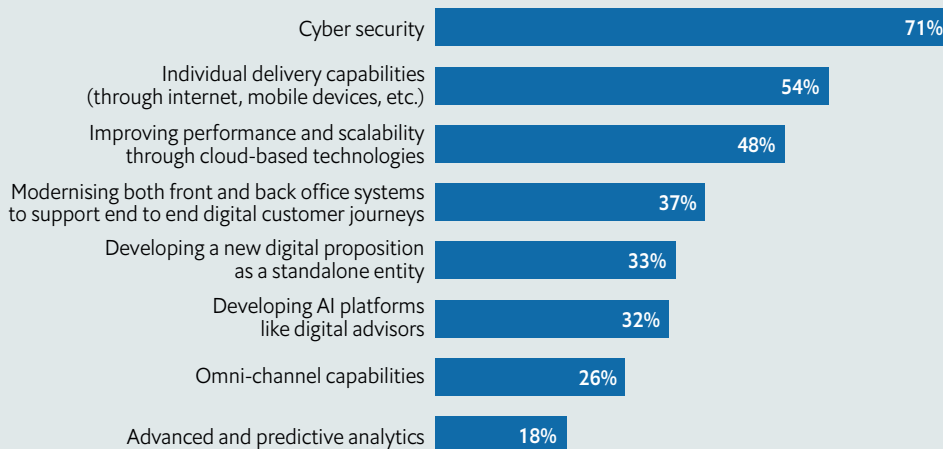
⁷ International Monetary Fund, Financial Access Survey. <http://data.imf.org/?sk=E5DCAB7E-A5CA-4892-A6EA-598B5463A34C>

⁸ Sveriges Riksbank, Statistics on notes and coins. <https://www.riksbank.se/en-gb/statistics/payments-notes-and-coins/notes-and-coins/>

Chart 10

Where is your company focussing its digital investment?

(% of respondents)



Source: The Economist Intelligence Unit.

Redirecting digital investment

By now most banks have either fully or partially completed standardising the look and feel of their services across different platforms; it is no longer the most important aspect of their digital investment.

Technology budgets are now being directed to mobile and other internet-connected channels, with mobile being the focus of 54% of respondents. Banks are investing heavily in cloud-based technology, with 48% of investment focused there, and also in modernising front- and back-end systems to ensure that processes run more smoothly and economically (cited by 37% of respondents).

According to Hans Tesselaar, executive director of the Banking Industry Architecture Network (BIAN), an international association of banks, software vendors and service providers, open banking will lead to a rethink of how banks structure their IT and digital investment. He believes that as APIs become more complex in their functionality, banks will need to rationalise their IT infrastructure.

“Fintechs are focused on the simplest utility apps that ask a question and the bank gives an answer,” he explains. “Initiating a loan through an API will be much harder.”

Dancing with fintechs

Most banks have long since recognised that if they are to keep pace with innovation in the sector, they must work with the fintechs, even if some pose competitive challenges. Many have invested in fintech start-ups directly or bought them outright. Others are forging partnerships, in some cases under agreements that prevent the fintechs from sharing ideas with competitors.

GLOBAL RETAIL BANKING REPORT

WHOSE CUSTOMER ARE YOU? THE REALITY OF DIGITAL BANKING

Tie-ups vary in size, focus and structure. In Australia, Westpac recently bought an equity stake in flexible payments platform Assembly Payments so that it can integrate payment terminals and retailer point-of-sale software.⁹ Singapore's OCBC Bank has set up an artificial intelligence (AI) laboratory after collaborating on suspicious transactions with ThetaRay, a cyber security and data analytics company, and a chatbot for loan queries developed by fintech start-up CogniCor.¹⁰ Innovative banks are even setting up new entities to sell their fintech expertise to others. LHV of Estonia already works with remittance giant Transferwise and cryptocurrency exchange Coinbase. The bank is now opening a UK branch to attract more partners.¹¹

The aim of forging closer ties with emerging fintechs is not necessarily to be first to market with a killer app: education and exposure to the digital way of working are just as important.

Startupbootcamp Fintech Mexico City is a programme that aims to put 11 hopeful fintechs on the road to success by providing access to resources and banking expertise. It is funded by established companies including HSBC, Visa and small business lender BanRegio, and according to the programme's director, Eduardo Morelos, and Andres Fontao, managing director at Finnovista, a Mexico-based impact platform improving access to digital finance, bank bosses are eager to attend sessions with software developers.

"Our sponsor firms have gained valuable insights into artificial intelligence and big data," says Mr Morelos. "A number of their chief executives have had hands-on experience at the fintech frontline."

⁹ Financial Review, April 3rd 2018. <http://www.afr.com/business/banking-and-finance/financial-services/westpac-strikes-deal-with-assembly-payments-20180329-hoy4gh>

¹⁰ Enterprise Innovation, April 4th 2018. <https://www.enterpriseinnovation.net/article/ocbc-banking-ai-future-revenue-streams-1961029509>

¹¹ Finextra, March 14th 2018. <https://www.finextra.com/newsarticle/31806/estonias-lhv-to-open-uk-bank-to-serve-fintech-industry/wholesale>

PEPPER: STARTING FROM SCRATCH

Buying, attracting or nurturing new innovation hubs and centres seem to be the easier options for an established bank. However, only 22% of survey respondents agree that if your existing banking and IT structure is holding you back, just build a new one.

Israel's Bank Leumi thinks otherwise. It has big plans for Pepper, its stand-alone mobile-only bank launched in 2018. It has also launched Pepper Pay, a person-to-person payment app that is open to everyone, including customers who bank with competitors.

Pepper Pay has proven to be remarkably popular, with hundreds of thousands of customers already signed up. Although Pepper bank's customer base is smaller, over 1,000 new account holders are joining each week.

Ilan Buganim, Bank Leumi's chief technology officer, has been surprised by exactly who is signing up. Although Pepper firmly targets millennials, 40% of the banking app's clients are over the age of 30.

Speedy development and personalisation count. Accounts can be opened in less than eight minutes, says Mr Buganim. New services

have gone down well too, especially when targeted at lifestyle and behaviour.

A new group payment function makes paying the bill easier when friends regularly meet for dinner. And a new promotion on tuition fees has pleased universities and students. Applying is quick, and universities receive the money directly as soon as each tuition-fee loan is approved.

Pepper's success validates the decision to launch a stand-alone venture, says Mr Buganim. One day Pepper could even swallow its parent. Rather than rebuild Leumi's existing traditional banking operations, customers could be migrated across.

"We would not be able to run so fast on the old infrastructure," admits Mr Buganim. "That's why we built Pepper on a new and separate platform."

International expansion could also be on the cards. However, according to Mr Buganim, Europe's mobile market is already saturated. Developing markets and the US offer far more interesting greenfield opportunities.

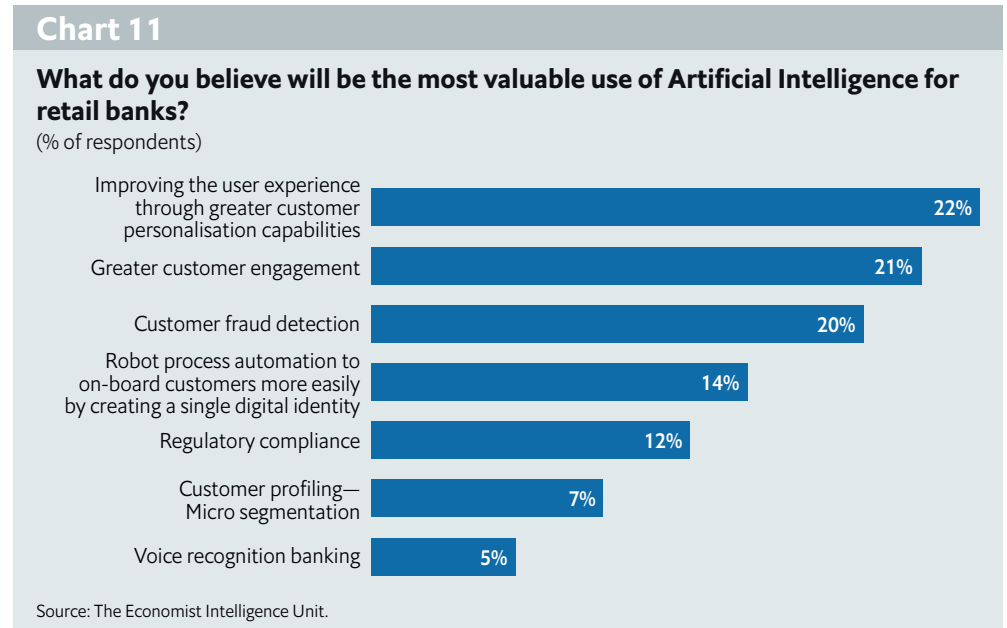
SECTION IV: ARTIFICIAL INTELLIGENCE IS WATCHING AND LEARNING

Automation looms large on the horizon for retail banks: as previously discussed, nearly three-quarters of survey respondents think that retail banking could be mostly automated by 2020.

The increasing volume of online and mobile transactions, new account sign-ups and the growing realisation that these data can be profitably used means that banks need to continually increase investment into newer technologies to make these channels safer as well as seamless.

Artificial intelligence: coming to the forefront of the banking experience

Artificial intelligence is becoming a key part of the new technology mix. It is emerging at all levels of banking, from the customer front-end to the behind-the-scene processes and compliance procedures. Done well, customers should not notice they are talking to a machine—or that a machine is watching and learning from their actions. Whether customers should be informed of who, or rather what, they are interacting with is still debatable.



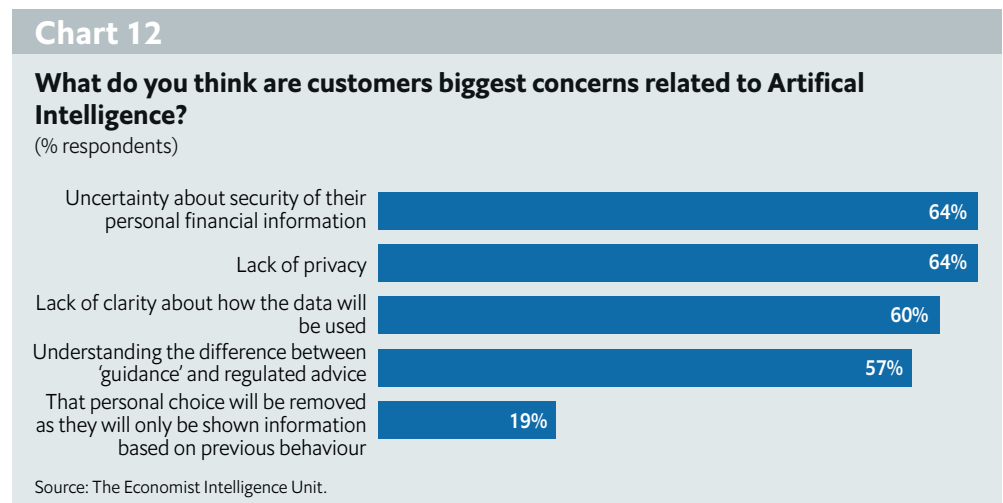
Survey respondents see most AI benefits concentrated on the existing customer, with more than one in five saying that personalising the user experience and boosting customer engagement will be the most valuable use of AI for retail banks.

Of the respondents to chart 11, it was private banks that are particularly keen on developing AI-based robo advice capabilities. This is not surprising, considering that relationship managers comprise a significant portion of their cost base. These high staff costs often keep minimum investment criteria beyond the reach of the fast-growing affluent mass markets in Latin America, Africa, the Middle East and Asia.

According to the survey, IT executives are the most likely to believe that the most valuable use of AI will be for on-boarding customers (cited by 28%, twice the overall average). Their colleagues in risk and customer services are less enthusiastic, with only 12% happy to employ AI to facilitate product sales. Even fewer see opportunities for AI to assist in micro-targeting.

Artificial intelligence: should customers be worried?

Although the banks think that AI holds significant potential for easing processes safely and effectively, it is clear that they believe customers still have some doubts.



AI raises significant issues about customer data, particularly in relation to privacy, personal information, and how these data are used.

Whether used for verification and fraud detection, transactions or product sales, banks will have to justify how AI and automated systems make a decision, according to our interviewees.

“You have to be transparent on how you process, store and use data. If you do something wrong, you will be caught,” says Roberto Valerio, chief executive officer at RISK IDENT, a fraud-prevention software provider. From a compliance point of view, understanding the difference between “guidance” and “regulated advice” can be a fine line. Our survey indicates that North American banks are the most likely to fear fines for getting it wrong, with 56% of respondents indicating that it will have the biggest impact on retail banks.

The advice to apply caution when using these terms is appropriate: banks continue to pay out billions in recompense for mis-sold investment, savings and mortgage products. Nobody wants more multimillion-pound fines if AI proves defective too.

However, these compliance challenges could actually be to the advantage of the banks. They have decades more experience than the fintechs. The gap may become even more apparent as new players move on from relatively simple transactions, prepaid cards and displaying aggregated spending data. For them, the regulatory challenge of providing full-service banking will be complex and expensive.

A bank is far better equipped to spread the cost of compliance over a large customer base. Having lived through—and dealt with—new technologies in the past, it also has more experience in problem-solving.

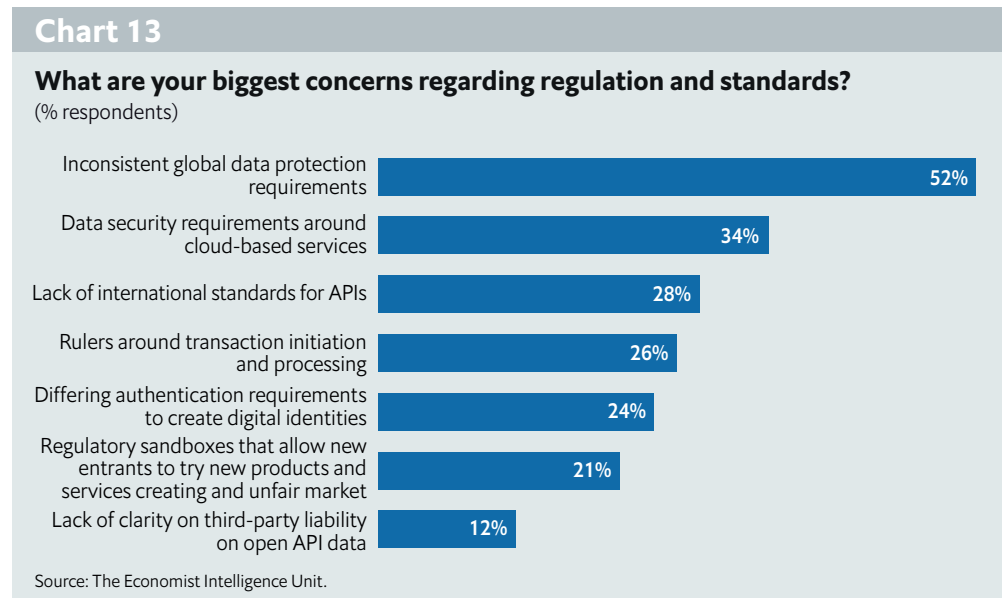
“It plays to our advantage as time goes on. As the start-up companies try to add incremental services, do more international transfers or loans on the back of a credit card, you will have more and more of these challenges that have higher fixed costs,” says HSBC’s Mr Bottomley.

SECTION V: SECURITY: AN INCREASINGLY GLOBAL CONCERN

Security now has to be considered from many different angles. It is no longer just an internal issue for banks. The need to protect customers and their data is becoming increasingly complicated as services as well as customers become ever more globalised. New regulations are not only changing the banking infrastructure—they are changing who banks actually serve and how they can serve them.

Regulation: security or simplicity?

Open banking will change the nature of who can initiate payments that connect to these networks, and how. But unless new market entrants apply for full banking licences and, in some cases, a clearing account with their central bank, they will have to rely on existing participants for access.



European regulators are clear that banks will be held responsible for incorrect payments, even when initiated by a third party. Opening up to competitors is important, but so is security. For many banks the challenge may be to tackle these simultaneously.

Broadly, banks are more concerned about protecting customer data than about opening up to APIs, the building blocks that allow apps to talk to banks to get the information they need.

Interviewees suggest that most banks are also clear on focusing on security first. If customers lose trust or money, they will take their business elsewhere. However, as seen in the US, regulators are likely to fine the banks in question, even when they are not entirely to blame for mistakes. It is clear that North American bankers are worried more about regulatory action (31%) than by angry customers (13%).

There are genuine concerns about the real cost of innovation at a global level. More than half (52%) of survey respondents believe that global data protection standards are inconsistent.

Because the overwhelming bulk of retail bank transactions remain domestic, the absence of international API standards is raised as a concern by only 28% of respondents. But even in Europe that may increase as aggregators (and the aggregated) spread their business.

It is highly likely that open banking will eventually expose system weaknesses. Uncertainty about third-party security as well as the ongoing need to educate customers and staff on data security will help to ensure that banks will continue to focus on beefing up their defences. According to 71% of survey respondents, cyber security already accounts for the biggest chunk of their digital investment spends.

Deploying that investment wisely depends on where banks believe the weaknesses lie.

For 38% of survey respondents, customers are the weakest link and therefore need to be educated on how to bank safely. Thankfully, bank staff is more aware of data security, with only 14% of respondents citing it as a key concern.

IF THE FACE FITS

A look or swipe is all you need to access your banking app. However, few users know just how complex biometric security could be. New Android devices and iPhones are shipped with embedded fingerprint and face-recognition technology. When users register their unique physical features, images are encrypted and held locally on their devices. At present, many bank apps, in effect, hand their login security to the giants of Silicon Valley.

Hakan Eroglu, executive, digitisation in payments and banking at consultancy firm Accenture, thinks that may not be enough. Banks will need tougher authentication systems, especially when forthcoming European Regulatory Technical Standards (RTS) on Strong Customer Authentication (SCA) and Secure Open Standards of Communication (CSC) under PSD2 come into force in September 2019.

According to the RTS, banks will be allowed to provide authentication methods based on biometrics as well,

on top of “knowledge” (eg, password) or “possession” (eg, smartphone, token), and will need to comply with stricter security requirements.

Mr Eroglu believes banks, not the device manufacturer, should have control over the creation of biometric security credentials, collection and validation of biometric data.

Banks also should combine multiple biometrics characteristics and not rely on a single biometric feature only. A copied fingerprint in a fingerprint-only solution could lead to your account being emptied. Adding behavioral data such as keystrokes or finger pressure on the screen is key for a more secure and convenient solution, he suggests. But banks should not store any biometric raw data directly on their systems. Instead, they should build templates to match data from the device for a good fit. Security and convenience need to be kept in balance. “Frictionless customer experience in secure payments is key,” says Mr Eroglu.

Regulatory security: the rise of regtech

Less dramatic but costly nonetheless, day-to-day security issues are rising up the agenda too. This will be tested with the introduction of new anti-money-laundering requirements, such as the EU's Fourth Anti-Money Laundering Directive, known colloquially as 4MLD, which may force banks to rethink their approach to know your customer (KYC), anti-money-laundering (AML) and counter-terrorist financing (CTF) rules.

The 4MLD replaces a tick-box approach to checking new customers and monitoring existing ones for connections to corruption and bribery, politically exposed persons (PEPs) and money-laundering. Under a new risk-based approach, banks and other entities will need to apply enhanced checks on everything from identity to beneficial ownership if they think a customer is a greater risk.

This could mean that current procedures, usually involving on-boarding checks by external agencies such as LexisNexis, Thomson Reuters or Experian, will no longer be sufficient. Banks will have to demonstrate that they are searching deeper and wider for information from multiple sources, and across the globe. They will also have to prove that every subsidiary or branch in every jurisdiction is taking the same tough line.

"Larger banks have big barriers to adopting digital regulatory technology [regtech]. They have to re-engineer their current systems and processes, but are afraid this would then leave them open to regulatory sanction," says Jane Jee, CEO of UK-based regtech firm Kompli-Global. However, this is where AI can help to automate processes.

Ms Jee calls it "Google for AML". Her firm is applying a multi-language system that can assess the trustworthiness of sources of news, allegations or convictions against an individual. A national news outlet would rank more highly than a blog, but a persistent story or rumour from a "lesser" source would also be given prominence.

"We do not replace human judgement; we enhance it. We sift huge amounts of data, identify relevant information and reduce false positives. Real-time, thorough searches for adverse information mean a faster and better basis for the human analysts to make a more accurate risk assessment," explains Ms Jee.

Europe is tightening AML rules further. A fifth directive has been adopted by the European Council and European Parliament and could be in place by early 2020. The US is introducing tougher rules on ultimate beneficial ownership (UBO). And from May 2018 all financial institutions will have to track the entire relationship from customer to UBO and every corporate vehicle in between.

USA: YOU'RE NEXT

The huge data breach at credit bureau Equifax and the fake-account scandal at financial services company Wells Fargo may nudge the US to follow Europe's lead on data protection.

The General Data Protection Regulation (GDPR) comes into force in May 2018 across the European Union. It will oblige all companies, including banks and fintechs, to have controls and systems in place relating to how they obtain customer data, how they store it and for how long, and how they may reuse it.

Fines for mishandling data will rise substantially. Today's fines of €50,000 to €300,000 (US\$61,000 to US\$370,000) are often just seen as a cost of doing business, not a deterrent to poor practices. This will change when companies face fines of up to 4% of gross turnover.

Germany and France already have strict data laws in place, says Roberto Valerio of online fraud-prevention firm RISK IDENT. His company is based in Germany, working for Otto, the second-largest online retailer in Europe after Amazon, as well as a number of telecoms companies.

European data laws mean that his company cannot pool information from different corporate clients to assess whether a shopper or customer is who they say they are.

"In the US you have more freedom to combine information from different sources. If you see fraud from a certain person or email address,

that can be used when they apply online elsewhere," notes Mr Valerio.

How the GDPR will work in practice is still unclear, but Mr Valerio is pleased to see that the regulation gives customers more rights over their data, such as being able to have it deleted. Others welcome new consumer powers too.

"If a verification decision has an impact on someone, the bank has to know the reason why and how," says Robert Prigge of global ID and verification service provider Jumio.

Mr Prigge's firm has an army of humans who intervene if documents and selfies do not match, or if bad lighting renders a photo unreadable by a machine. Competitors who rely solely on artificial intelligence and machine learning may struggle if questioned by their customers.

"If you rely 100% on machine learning, the machine cannot explain its decision to you," says Mr Prigge.

There are still many unknowns about the GDPR. Nobody quite knows whether a European citizen temporarily living in New York is covered by the regulation or not. The courts will probably have to decide.

But the US is likely to follow Europe as public anger against intrusion and data mishandling increases. Money-laundering and terrorism financing may also force American politicians to take data protection more seriously.

CUSTOMER DUE DILIGENCE: WHO ARE YOU?

The EU's Fourth Anti-Money Laundering Directive (4MLD) imposes strict compliance standards on financial institutions, intermediaries, lawyers, accountants and even estate agents whose clients may pose a money-laundering risk. According to Jane Jee, CEO of Kompl-Global, a UK-based regulatory technology (regtech) firm, banks will have to collate and sift far more information about their customers.

"We live in a sea of data. Until now, banks relied on trusted partners for checking customers. Now, no single source is seen by regulators as sufficient," Ms Jee notes.

Here is one of many new regtech firms that are developing technology to automate processes and cap the cost of compliance. Instead of relying on existing databases and adding new information to them, the Kompl-Global team takes a customer's details and then deploys artificial intelligence (AI) to trawl through published data sources around the world. This approach is more thorough because it analyses both structured and unstructured data, including audio, video and social media.

However, an opinion issued on January 23rd 2018 by the European Banking Authority, the European Insurance and Occupational Pensions Authority and the European Securities and Markets Authority, "Opinion on the use of innovative solutions by credit and financial institutions in the customer due diligence process", may discourage banks from deploying such innovation, Ms Jee believes. This is because these regulators say that banks have to approve any upgrade to the AI software rather than just accept the upgrades. As the systems are in constant use—and AI is permanently being improved—the process would be unwieldy as well as costly.

The banks generally do not have sufficient in-house AI expertise to develop such products. For them, it is easier if the burden of proof that the software works is with the provider, not the bank itself.

"The whole point is you stay ahead of the game. The only thing the bank needs to worry about is whether performance has been degraded. Of course, the software providers are going to improve it, and they are going to fix bugs," Ms Jee says.

CONCLUSION: PLAY TO YOUR ADVANTAGES

There is no question in the minds of retail bankers that the digital revolution is the defining trend of the current era. Changing customer behaviour and technology have eclipsed regulation to become the most significant factors shaping their industry.

Perhaps this acknowledgment reflects a growing confidence by the banks. Respondents to the current survey are much less frightened by peer-to-peer lenders and non-financials or even robo-advisers and automated wealth management than they were in previous years.

GAFA may pose more of a present threat to the established retail banking order. Amazon is in discussions with JPMorgan Chase to offer current-account services to its American shoppers. It already has some experience in providing financial services, having lent over US\$3bn since 2011 to small businesses via its Marketplace platform.

But banks still enjoy some advantages over GAFA: an established banking customer base, for example, and long-held reputations in the financial services space. Most crucially, their customers trust them with their most significant financial assets. Recent scrutiny of the digital giants' use of private data and their impact on society may increase this advantage.

For most retail banks, the transformation required to capitalise on these attributes has barely begun. They can be forgiven for their caution: there is no sense in breaching their customers' trust in the rush to release a popular new app.

Indeed, outside of China and app-heavy Asian markets there is some wisdom in watching the fintechs as they upgrade from simple transactions and prepaid cards to more complex current-account, investment and lending products. Learning from their inevitable missteps could be good for banks' profits and their reputation.

That shouldn't be an excuse for inaction. The trust customers have in their bank will mean little if it cannot provide the services that accommodate their lifestyles.

Being steadfast in the protection of what makes them strong, and ruthless in their willingness to change everything else, is the order of the day for retail banks.

While every effort has been taken to verify the accuracy of this information, The Economist Intelligence Unit Ltd. cannot accept any responsibility or liability for reliance by any person on this report or any of the information, opinions or conclusions set out in this report. The findings and views expressed in the report do not necessarily reflect the views of the sponsor.

LONDON
20 Cabot Square
London
E14 4QW
United Kingdom
Tel: (44.20) 7576 8000
Fax: (44.20) 7576 8500
Email: london@eiu.com

NEW YORK
750 Third Avenue
5th Floor
New York, NY 10017
United States
Tel: (1.212) 554 0600
Fax: (1.212) 586 1181/2
Email: americas@eiu.com

HONG KONG
1301 Cityplaza Four
12 Taikoo Wan Road
Taikoo Shing
Hong Kong
Tel: (852) 2585 3888
Fax: (852) 2802 7638
Email: asia@eiu.com

GENEVA
Rue de l'Athénée 32
1206 Geneva
Switzerland
Tel: (41) 22 566 2470
Fax: (41) 22 346 93 47
Email: geneva@eiu.com

DUBAI
Office 1301a
Aurora Tower
Dubai Media City
Dubai
Tel: (971) 4 433 4202
Fax: (971) 4 438 0224
Email: dubai@eiu.com