THE ORIGINAL SIBOS DAILY 25 YEARS AND COUNTING

Daily News at Sibos

www.bankingtech.com/sibos

Pelican

Sponsored by Pelican

THE INDEPENDENT NEWSPAPER

WEDNESDAY 18 OCTOBER 2017

Web's future "in the balance"

By Neil Ainger

The cross-border, centralised nature of the world wide web is "absolutely in the balance" right now, warned Sir Tim Berners-Lee, its inventor, yesterday.

In his address to the Innotribe conference stream on the past, present and future of the internet, Berners-Lee discussed the balkanisation of the web because of restrictions such as the 'great firewall of China'; corporate appropriation of the technology (such as paywalls); and threats to 'net neutrality' from political populists, social media algorithms and other sources.

The future of innovations such as distributed ledger technology (DLT), which is often described as the 'new web', was also discussed in a wide-ranging speech that touched on open application programming interfaces and banking. This trend, backed by regulations such as the revised EU Payment Services Directive, would mean a consumer is able to access his or her data in one place in the future. "I know some of you are working on it: it'd be good," said Berners-Lee.

He is optimistic that in the long-term, a global, re-centralised internet will emerge, with the desire for easy, global trade as a driver, while not negating the need to fight for security, privacy and democratic and academic freedoms. "When you publish something it should be readable anywhere in the world."

Berners-Lee created the world wide web in 1989 while working at Cern when he realised he could build on the internet file transfer system used by the US military since 1969 with a global Hypertext system (http) that could order it and create "one big book".

The scientist and academic has subsequently worked as a founding director of the World Wide Web Foundation to try to ensure the web is accessible to all and establish it as a global public good and basic right. He is also a director of the World Wide Web Consortium, a global web standards organisation he founded in 1994 to lead the web to its full potential and keep it open. In 2012 he co-founded the Open Data Institute, which advocates for open data in the UK and globally. "The internet and web is a network that reflects humanity," said Berners-Lee. "We can put it to the uses we decide. For instance, political adverts on Facebook can be turned off. It's choice how we use it."

Discussing his early days, Berners-Lee joked that very few understood the web when he wrote the memo for it in 1989, although as a pioneer, "it was a luxury to be able to set standards by myself – something I'm sure the people here understand".

However, early design decisions have an impact later on, he warned, so think about them clearly. He cited email and SMTP as an example where a lack of thought among academics about how commerce would use the protocol led to email spam, "which is still a problem today".

In the early days of development, Berners-Lee's boss called his web concept "vague but exciting". A term that could perhaps be used to describe the DLT arena, which he also discussed. "Blockchain is a way of notarising things," said Berners-Lee. "It could be

Continue to page 2

"CSP isn't rocket science. It is bringing consistency and standards to security"

Jerry Norton, CGI

IN THIS ISSUE

Published by

banking technology

Beware Bigtech Gafa, fintech warned

By Tanya Andreasyan

Bigtech, not fintech, is a threat to banks, Elisabeth Rochman, financial services chief technologist, Hewlett Packard Enterprise, told Sibos delegates yesterday during a panel session on bigtech. "They are big, smart and very hungry companies. And they are investing billions of dollars in R&D."

And yet... surely these bigtech firms – often referred to as Gafa (Google, Apple Facebook and Amazon) – do not want to be regulated like banks, noted Paul Camp, global head of HSBC's financial institutions group.

And if they do take the plunge and decide to venture into banking, there is surely a conflict of interest, Rochman added. "The Gafa firms already know too much about us – would you trust them with your savings or current accounts?" With all that information, including all your financial data, how easy will it be for them to get you to part with your money and shop more, she mused. And all with just a click of a button, and in some cases even before the button is clicked.

Amazon is already developing an anticipatory shipping programme, commented another panel participant, Leonard Hardy, senior vice-president, operations and technology at Northern Trust. Amazon will be shipping products it thinks you are going to buy to a warehouse nearest to you before you actually place an order.

With so much power at their fingertips, Rochman wondered who would be regulating the bigtechs.

The day before at Sibos, delegates heard that the social media and bigtech giants such as Google and Facebook employ armies of data scientists and engineers who are creating the complex algorithms to gather, process and analyse data to a granular level. And they have the financial power to attract the top talent, Vladan Joler, director of Share Foundation, observed.

Our capacity to really understand what's going on inside these companies' "black boxes" is very limited, he said.

Most of us are on some sort of social media these days. It is not obligatory, of course, but it is now almost an integral part of life today. If you are not on Facebook or LinkedIn, it is considered suspicious. When someone applies for a job or goes on a date, their employer or date is very likely to look the person up on social media.

There is no surprise, then, that in terms of population, Facebook is bigger than the US. In 2015, Facebook had 1.6 billion active users, while the US had 323 million citizens.

So what is this country of Facebook? Is it a democracy? Does it have a government and if so, how do we communicate with it?

Since 2004, Facebook had more than one trillion likes. Daily, 350 million photos are uploaded on Facebook; 4.7 billion posts are shared; 1 billion locations tags are made and 10 billion messages are shared.

"Facebook's black box defines new forms of labour, exploitation and generation of enormous amounts of wealth and power – $17.9 billion in 2015 – for the owners of this immaterial invisible factory, creating deep economic gaps between the ones who own and control the means of production and their users who really often live below the poverty line," Joler said.

"Every day more than 1 billion Facebook users – digital workers – spend on average 20-plus minutes on liking, commenting and scrolling through status updates. This is more than 300 million working hours of free digital labour per day."

All this data is put through the Facebook algorithms that try to make sense of who and what you are and then monetise that information. It takes into account your profile (who you are or how you portray yourself/ perceive yourself), your actions (which are a more realistic representation of you) and your device's information (a digital footprint).

Unlike traditional newspapers and magazines, Facebook enables "nano targeting" for advertisers, enabling them to focus on individuals, very small groups of individuals, or groups of like-minded individuals, but at scale.

In comparison, the traditional media can offer advertisers much broader target groups, for example, teenagers or women of a certain age group, or people with a certain income. But Facebook can drill down to very specific behaviours and interests on each individual – and this is a fundamental difference.

The algorithms play around with data and contents, trying to understand the places you visit (home, school, work etc), match keywords, social connections – and build the patterns and routines, and extract the anomalies.

By analysing your spend, where you live, work, shop and socialise, what your hobbies are, what music you listen to etc Facebook can put a price tag on you, Joler said.

Continued from page 1

used to form a new domain name system that isn't subject to cyber-squatting, or to put a public key on it to increase email security. Indeed, it could be used if you no longer trust the web". Again, it is about choice, he said, and decisions need to be made now about "what you are going to build on it".

It is possible, indeed probable, that the same battles that Berners-Lee fought to keep the web open will be replicated in the blockchain world. How many chains will be established, using which consortium's protocols? How much centralisation, interoperability, common standards, security and so forth will there be as DLT usage increases?

All these questions are up for debate, but it is certain that corporates will hive off the technology for their own ends, while hopefully remembering that some commonality must remain to achieve beneficial network effects among multiple parties.

LA Ledger group calls for more participants

By Heather McKenzie

The Liquidity Alliance group of central securities depositories (CSDs) has called for further participants in their distributed ledger technology (DLT)-based LA Ledger prototype for cross-border mobilisation of security collateral. The prototype, currently a proof of concept, aims to provide centralised, faster and more efficient allocation of fragmented securities positions.

"LA Ledger is all about networking," said Sveinung Dyrdal, a director at Norwegian CSD VPS. "We call it a collateral ecosystem with a number of possible connections between the CSDs. Like social media networks, the benefits will increase as more members join the ecosystem, bringing with them clients who can add domestic securities to the collateral pool that can be deployed internationally."

Although LA Ledger is a closed-group DL, it is open to new participants, he added, observing the group is a "friendly initiative" that won't take value from CSDs. To date, the POC has built a strong base for growth and the participants would like to see more potential members.

In joining the group, VPS has done what industry observers believe will be crucial for the survival of smaller CSDs – innovate. "We are a relatively small CSD in a relatively small market and need to be innovative and differentiate ourselves," said Dyrdal. "When we talk to our clients in Norway, particularly the banks, they demand more efficient cross-border collateral mobilisation. They are keen to use Norwegian securities for their international exposures."

The "bottom line" for VPS, he said, was the more efficient cross-border use of collateral. "We want to see a bigger LA Ledger family; we'd like to see the initiative grow".

LA Ledger was launched in January by four CSDs: the Canadian Depository for Securities, Clearstream in Luxembourg, South Africa's Strate and VPS. They are working on the POC with Deutsche Börse. The prototype is based on the Hyperledger Fabric blockchain. Validation by regulatory authorities and market participants is under way.

Brian Gelfand, vice-president at the Canadian depository, said the legal underpinnings of using DLT for collateral mobilisation were "still evolving". The group has taken "a very deep dive into the legal and regulatory aspects of moving collateral across borders on distributed ledgers".

The legal and regulatory aspects were presenting some of the most challenging issues for the group. "This is a very innovative model for moving collateral that has to fit into a legal and regulatory regime that has evolved slowly over very many decades. It is an interesting undertaking for us and regulators are also very engaged with this."

Elsewhere yesterday, Swift announced that it has established ISO 20022-based connectivity to Denmark's CSD, VP Securities. The service will be launched in 2018 and will provide banks with fully standardised communication with VPS.

API strategies have to be holistic to win

By Tanya Andreasyan

If financial institutions want their application programming interface (API) strategies to work, they must take a holistic approach across their organisations, delegates were told yesterday.

While APIs are not really new to any financial services organisation – IT teams have been doing it internally for years – the concept of "plugging APIs with external partners" is a very different proposition, said David Andrzejek, head of vertical solutions for Apigee Google Cloud.

A poll during the session revealed that 55 per cent of the audience had at least some kind of API strategy in place (or are working on creating one). But what are the components to make those strategies successful?

Damian Richardson, head of payments strategy and innovation at NatWest, feels the API journey has no end, as it is always evolving. NatWest is just at the start of it, he said.

It is vital to see "a bigger picture", he added. How does your API strategy fit into a broader value chain that is "much bigger than yourself"? What are your customers trying to accomplish? The outside-in view of a business is very important.

Also, when working with external partners, one has to take into consideration that these partners might also struggle with APIs and understanding them, they might have legacy technology holding them back and a lack of talent.

Saket Sharma, CIO treasury services technology at BNY Mellon, said within an organisation, the alignment across all relevant departments, such as IT, business and management, is vital.

The panel participants agreed that support from the top down is very important, (arguably this is true of any project, not just an API one). And you can't have an IT strategy for APIs without a business strategy, emphasised Sharma.

Andrzejek added: "APIs are not a play thing, they must have business significance". And they are not "a magic answer to everything", so APIs will not deliver value just on their own. It all has to come together – business, data, legacy technology, development and so on.

"A product-centric mindset has replaced the application-centric one," said Sharma. And that means it is all about the customers and their needs and wants.

This, he continued, required a shift in thinking within the organisation, a tighter connection and collaboration between the departments (particularly IT, business, product and compliance) and education. A lot of education.

"The IT department often tends to over-complicate. So they need to simplify APIs for their business colleagues, explain and repeat. If they do this, the business starts asking the right questions, and they can take it from there – and take a more proactive role."

All change in correspondent banking

By Neil Ainger

Swift has launched Correspondent Banking Suite, a solution targeting small to medium sized correspondent banks that are seeking cost-effective access to the Swift network.

Such banks are under pressure to minimise operational costs while keeping their Swift infrastructure current in terms of technology and security. Additionally, regulatory requirements and cyber security challenges make it crucial for banks to have in-depth knowledge of their correspondents.

The Suite gives banks direct, cost-effective access to the Swift network via Alliance Lite2, which is a standardised, cloud-based interface managed and operated by Swift.

Sophie Racquet, head of cloud services at Swift, said different organisations had different connectivity needs. "Small to medium sized banks that engage in correspondent banking face a unique challenge. They must reduce their operational burden without compromising on security while navigating the complexities of dealing with multiple institutions."

On Monday, Sibos delegates heard that correspondent banks must streamline, adopt new technology and change if they are to survive.

"The Tesla car has 18 moving parts, whereas the internal combustion engine has more than 2000," said Nigel Dobson, general manger, wholesale digital transformation at ANZ, as he made an analogy between the automotive industry's migration to electric vehicles and the correspondent banking world.

The threat of non-bank players disintermediating banks, such as has happened with the rise of Alipay and Tencent's WeChat Pay in China, should not be discounted, especially on the consumer side of the business, warned Dobson.

Christian Westerhaus, head of clearing products, Deutsche Bank, GTB cash management, argued for a more "hybrid model" in the future, adding that Swift's global payments innovation (GPI) project "is live now and can already provide benefits".

However, Emma Loftus, head of global payments, FX and channels at JP Morgan, said there was still a need "to get as many banks as possible into the ecosystem" and to make GPI tracking codes as widespread as possible, "although the intention is there."

The transparency benefits of GPI, plus better speed and traceability for cross-border payments, were welcomed by Javier Orejas, banking manager, Emea at the International Air Transport Association, which processes $360 billion on behalf of its 260 members.

Other pain points for corporate treasurers, said Orejas, included cyber security and standards. These need to become more widespread if integrating the benefits of the GPI, instant payment schemes and other banking initiatives around the world into treasuries' enterprise resource planning systems is to be made easier.

"Banks need to match new tech players if they want to survive," concluded Orejas, adding that "corporates' need for faster, quicker, cheaper cross-border payments was plain". Whether the correspondent banking model is the best way of doing this must be up for debate.

Separately, BNY Mellon has published research into the impact of emerging technology on the correspondent banking model. Increased regulation, competition, and the coming age of millennials and their higher levels of technology understanding and expectations are helping to drive innovation and change in the bank payment space that has not been seen for decades, the report found.

The report also found that little more than one-quarter of respondents agreed that blockchain technology would substantially change the global payments experience. Nearly 60 per cent of respondents said it was "too early to tell" if peer to peer system interaction, through the use of APIs, would bring a fundamental shift in the interbank correspondent model.

A quarter of respondents felt compliance screening was the largest impediment to straight-through processing success. Twenty-per cent viewed payment formatting errors as the second greatest impediment.

Enhanced analytics and business intelligence were viewed by respondents as the number one factor in their ability to improve their end clients' payments experience.

Pelican crosses into AI development hub

By Antony Peyton

Pelican, a provider of artificial intelligence (AI) powered payments and financial crime compliance solutions for banks and corporates, has launched the Pelican Innovation Hub.

The hub is not one in the traditional sense of a place for start-ups to turn up wearing jeans and get creative. Pelican's version is a partnership model as it seeks to work with banks. The firm says it will offer the whole package – from proof of concept, prototype development, to final production and service deployment, either on cloud or on premise.

The hub uses the modular PelicanPlatform and incorporates technologies such as AI, machine learning and natural language processing, real-time payments, open APIs, and omni-channel UX.

In addition, banks can partner with the hub through a subscription model on a use-case basis.

Parth Desai, founder and chief executive of Pelican, said the hub could help banks on their "digital journey to innovate and enrich their own service offerings" as it opens them up to its "proven and agile integrated technology platform for banks".

Desai wouldn't name the banks involved with the hub, but said two organisations are working with it and a further three are "engaging" with the company about the hub.

Ultimately the hub is Pelican's way of keeping up with industry demands related to Swift, Sepa and open banking, said Desai, and is aimed at tier two banks that are "seeking to act like bigger banks".

SunTec™

Orchestrating True Customer Value in the Financial World

Delight your customers with SunTec's award winning product suite - **Xelerate®**

Xelerate® provides financial institutions that extra layer of comfort by facilitating customer experience orchestration through product innovation and personalised offers. Using the product, banks can become true owners of the customer value chain, by innovating rapidly on their business models, and expanding their product & service offerings through collaborative partner ecosystems.

- Personalised Offers
- Product & Pricing Innovation
- Partner Ecosystem Management
- Real-time Analytics

Get in touch with SunTec: **contactus@suntecgroup.com**

/SunTecBusinessSolutions /@SunTecGroup | #SunTecViewpoint /SunTec-Business-Solutions /SunTecGroup

Belfast is the top city globally for fintech development projects.

Northern Ireland has an enviable track record of success in financial technology development.

Our advanced infrastructure comes with lower operating costs, and our skilled, abundant workforce comes with a uniquely-driven mindset that achieves real results.

That's why Citi, Cayan, First Derivatives, Visa, CME Group, Tullet Prebon, BNP Paribas and more of the world's top financial services companies are already here.

To find out more, visit Northern Ireland at stand **A06.**

Source:FT fDi Markets, 2003 - 2017

Northern Ireland. Altogether more.

InvestNI.com/Sibos

DTCC assesses fintech impact on stability

By Heather McKenzie

While financial technology startups and established players vie for attention on the exhibition floor at Sibos, the impact of fintech on financial stability is the subject of a new white paper from The Depository Trust & Clearing Corporation (DTCC).

Fintech and Financial Stability – Exploring How Technological Innovations Could Impact the Safety & Security of Global Markets, warns that while fintech adoption benefits the financial services industry in areas such as improving client experience, strengthening critical infrastructure components, creating efficiencies and reducing costs, it could also pose or exacerbate certain risks. These include cyber security threats and third-party risks.

While many fintech offerings are still in their early stages, which makes it difficult to assess their impact on financial stability, DTCC recommends that the rapid growth of fintech adoption requires close monitoring to identify emerging systemic risks on a timely basis. It advises that any impact analysis should be conducted on a case by case basis, given the wide range of underlying applications under consideration for fintech upgrades, each with their own characteristics and specific context.

To guide this analysis, DTCC recommends that potential risks be assessed based on a framework that includes nine main factors for firms to assess when considering the impact of fintech on financial stability. These are:

- Fintechs that provide core banking functions could enhance financial stability through diversification of credit and liquidity risk. However, given the short track-record of these companies, they could also create systemic vulnerabilities
- The unbundling of financial services associated with the rise of fintech has the potential to fragment the creation and delivery of financial services across additional providers and platforms
- The rise of fintech could reduce concentration risk by allowing non-traditional service providers to compete with existing players. Conversely, it could also create new pockets of risk if a small cluster of fintech companies were to become dominant in any given area
- 'Substitutability' is a key concept in assessing systemic risk – financial services that are highly substitutable create less systemic risk than those that are not
- The 'interconnectedness' of financial services providers could have a significant impact on financial stability. It is important to analyse how fintech developments affect financial networks
- Competitive pressures on banks could erode their profitability and may encourage them to pursue riskier strategies. Outright competition between fintech companies and incumbents is less likely to promote financial stability than an environment where parties engage in cooperative arrangements.
- Over-reliance on purely data-driven algorithms could lead to errors that may not have occurred in an environment that requires additional human judgement. In addition to the potential for errors, due to the inherent complexity of decision-making algorithms, their opaque nature could also hide biases that may be hard to identify
- The impact of fintech depends on the extent to which it becomes a mainstream part of the financial ecosystem and how it will ultimately be used for delivering critical financial services
- Policy decisions and regulatory actions will determine to what extent fintech will penetrate and ultimately impact financial stability for years to come

"From its earliest days, financial services has successfully achieved higher levels of efficiency, speed and cost reduction, through the use of technology, but the current fintech revolution may deliver results that far surpass the benefits we've seen in the past," said Andrew Gray, managing director and group chief risk officer at DTCC. "Recent innovations, such as distributed ledgers, cloud computing, artificial intelligence and robotics, have the potential to transform the global marketplace and produce significant changes in everything from market structure to post-trade processing."

As the functional and geographical breadth of fintech grows larger, the discussion needs to evolve to also focus on the potential systemic risks posed by these new technologies and their impact on financial stability – both positive and negative, he added. "For all the investment in fintech and experimentation occurring today, we are still in the early days, making it the opportune time for the industry to thoughtfully consider this question."

DTCC believes fintech is likely to have a greater systemic impact through key transformational mechanisms, such as the disintermediation of incumbents, disaggregation of financial services and decentralisation of networks.

These effects, along with fintech's potential to fundamentally alter competitive forces, market dynamics, financial inclusion, consumer rights and many other areas, could strengthen or weaken overall financial stability. For DTCC, this is a subject of "great concern" given its role as a critical market infrastructure and its mission of protecting the stability and integrity of the global financial system.

The white paper notes that regulators around the world have also taken notice of fintech's growing prominence. A global survey launched by the Financial Stability Board's Fintech Issues Group in February indicated that 20 out of 26 jurisdictions that were surveyed had taken some measures to respond to fintech, with five additional jurisdictions planning to follow suit.

"The importance of the regulatory context in which fintech companies operate cannot be overstated," said Gray. "Policy decisions and regulatory actions will determine to what extent fintech will impact financial stability for years to come."

On Monday at Sibos, Petra Hielkema, division director payments and market infrastructure at De Nederlansche Bank, said regulators were entering "new territory" with fintech. Dialogue between banks and fintechs would help them to navigate the issues.

"All of the new fintech companies and banks are ultimately dealing with the trust of consumers and with financial stability," she said. "We think it is great to see all the innovations and we think they are good. What we strive for as a central bank is efficient, robust, safe and accessible payments. The focus for us as a regulator is safety and robustness. Fintechs coming in is great for technology, but they are dealing with other people's money and that means safety is paramount."

EDITOR
Heather McKenzie

SUB-EDITOR & REPORTER
Paul Skeldon

REPORTERS
Tanya Andreasyan
Antony Peyton
Neil Ainger

SALES MANAGER
Judith McInerney
Judith.McInerney@knect365.com
+44 (0) 203 377 3506

MARKETING MANAGER
Irena Andrisevic
Irena.Andrisevic@KNect365.com
+44 (0) 207 017 5379

DESIGN & PRODUCTION
Kosh Naran

ONLINE
www.bankingtech.com/sibos
@DailyNewsSibos

The *Daily News at Sibos* is an independent publication, wholly owned by KNect365, an Informa business.

PRODUCED & PUBLISHED BY
Banking Technology
Knect365
Maple House
149 Tottenham Court Rd
London W1T 7AD
UK

ISSN 0266-0865

PRINTED BY
Print City, Canada

Daily News at Sibos
Published by
banking technology
KNect 365
an informa business

Volante extends VolPay to Azure

By Heather McKenzie

Volante Technologies has made its entire range of VolPay payments processing products available on Micosoft's Azure cloud platform. Vijay Oddiraju, chief executive, Volante Technologies, said the company wanted to give its customers and prospects as wide a choice as possible in the type of cloud environment on which they could deploy VolPay.

Volante's products are platform agnostic and the company's aim is to enable users to deploy the software on every type of cloud environment. By accessing VolPay on the cloud, users can avoid hosting on-premises or in their data centres. Software and hardware costs are reduced and firms can take advantage of new functionality as it becomes available.

Oddiraju said there was much interest in Azure among Volante's customers and that Microsoft's continuing and substantial investment in its cloud platform made it "definitely a platform we would like to be a part of".

"While technologies such as blockchain and artificial intelligence are the flavour of the month, cloud as an option is gaining traction because it delivers on banks' requirements to reduce costs, improve scalability and benefit from using on-demand products and services," he said.

Three years ago, when Oddiraju talked to banking clients about the cloud, it would be "immediately dismissed" as an

option, he said. This is no longer the case, with tier one banks discussing – and moving to – various cloud deployments including public, private and hybrid.

One of the most important drivers of this change of heart is cost reduction. In a non-cloud deployment, firms must operate their own data centres, maintain hardware and software and ensure their environments are up to date. This is all costly; but it also does not deliver the agility and scalability that banks are seeking.

"Almost all of our tier one customers at the CIO level are discussing cloud strategies – entire or partial – and plan to have some part of their business deployed in a cloud environment very soon," said Oddiraju.

Bian outlines benefits of move to cloud

By Antony Peyton

The Banking Industry Architecture Network (Bian), a not for profit financial technology industry body, has launched the latest release of its service landscape. Termed SL 6.0, the framework is designed to provide a "globally standardised and simplified" banking architecture structure, using a service-based architecture.

Hans Tesselaar, executive director at Bian, said: "The industry often focuses on how developing and opening APIs will empower collaboration between banks and fintech or broader tech enterprises.

"While this is one benefit, on top of this banks will be able to move to the cloud and finally embrace cloud-based solutions that will enable them to operate a leaner tech model. Identifying the standard model for API development, as we have done, is crucial to taking this wave of innovation forward. Without this fundamental planning, banks risk developing APIs that fail to fulfil their full potential."

To explain its intentions further, Bian said traditionally its members have focused on defining the individual business capabilities that make up a bank, grouped into service domains, and subsequently identifying the information dependencies (known as service operations) between these business building blocks.

Tesselaar said the use of APIs can be seen as the "first step to the cloud" for banks and with them they can ultimately reduce infrastructure costs. Swift should be "driving" the adoption of APIs and he expects APIs will be one of the main themes at Sibos.

Alongside continuing to build this out, "specific attention" has been given to building additional architectural layers and providing detail to the model in SL 6.0.

According to Bian's research, a bank is split into three key layers. The infrastructure layer encompasses generic services and functions; the application layer represents the information technology landscape, with all its applications and connections; and the business layer grasps the bank's business direction and the business capabilities.

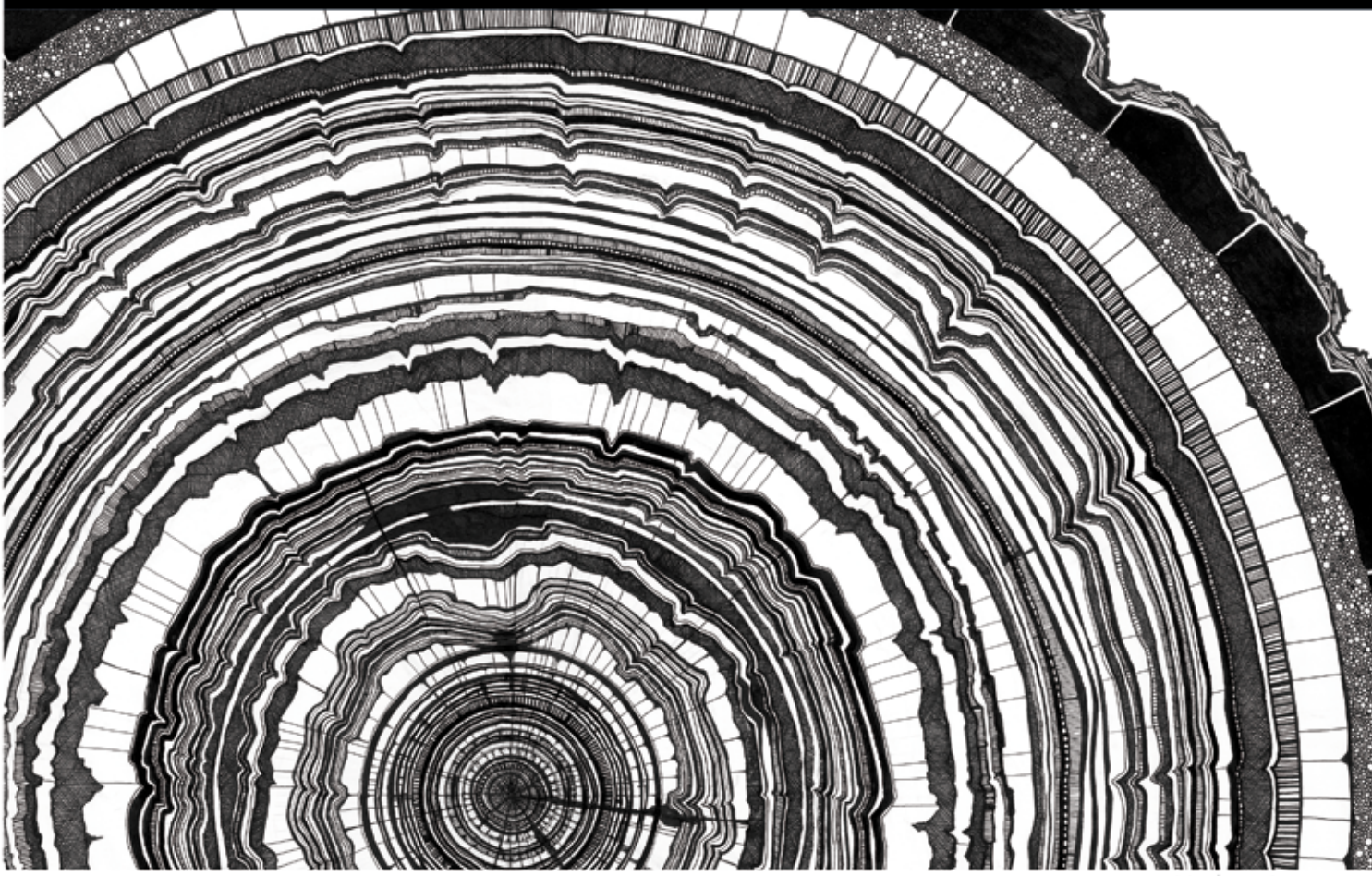
Bian said expanding the framework in this way in the following months will enable consistent interpretation in implementation for banks, enabling them to be "completely vendor agnostic", while also supporting API development and cloud enabling.

With the framework in place, Bian said its next step is to define the individual APIs for banks, with the aim of completing more than 100 definitions by March 2018.

In line with this initiative, Bian added that its members have elected a new board member, Santhosh Pillai, chief architect and data management at Dutch bank ABN Amro.

SmartStream

smartstream-stp.com



art: tonyhong.net

Growing with the business of banking

Like the mighty oak, SmartStream has grown to stand tall in the financial services landscape. Shaped by bold vision, continuous investment in R&D, and by years of experience gained through partnerships with clients, the company is uniquely positioned.

Able to meet an individual financial institution's requirements or to spearhead innovations that benefit the industry as a whole, SmartStream is firmly rooted as the middle and back-office solutions provider.

Whether you are looking to replace legacy systems, build an internal processing utility, utilise the cloud or outsource your entire operation – SmartStream has a comprehensive range of solutions and deployment options to grow with your business.

sibos

Stand H44 / Pre-book your meeting:
smartstream-stp.com/sibos

Old world aces new world

With sizeable market shares, China's mobile payments giants Alipay and WeChat Pay are seeking international expansion. **Zennon Kapron*** looks at what's next for the tech giants

China has gone through a tremendous transformation as 1.3 billion consumers change the way they pay, both online and offline, for anything from taxi rides to e-commerce goods. The tech giants Alipay (part of Ant Financial) and WeChat Pay (Tencent) have made payments mobile and in 2016 processed more than $5 trillion in mobile payments, the largest amount from any country globally. This has had an outsized impact on China's retail consumption. Based on Kapronasia research, in 2010, cash represented 60 per cent of retail consumption, but has decreased to 45 per cent today, and will represent less than 30 per cent in 2020.

Although the tech giants have done a tremendous job shifting consumers over to mobile payments, the Chinese market is changing. Alipay and WeChat Pay have reached a combined 90 per cent share of the mobile payments market in China, leaving very little for competitors, yet are themselves potentially hitting the limits of the market as the growth of overall users of mobile payments is expected to slow in 2017.

As the market shifts from a period of rapid growth to a more tempered expansion, the tech giants are looking for new ways to grow their business and seem to have settled on two main strategies: 'platformisation' and international expansion.

For every app, there is a platform. In the Western markets, users tend to have one app for one function. For example, they might use Facebook Messenger or Whatsapp for chat, Lyft for hailing a taxi ride and Venmo for payments. In China, all that functionality has been combined into the mobile payment wallets. As an example, WeChat started off as a social chat platform, but gradually incorporated payments and now has a variety of other products and services. Without leaving WeChat, you can book flights, invest in wealth management products, hail a taxi or even rent a shared bike. Similarly, Alipay has myriad lifestyle functions within the Alipay Wallet.

Clearly for both players, payments were the basis of what was to be a further digital expansion and offering. By keeping users in-app, the tech giants can drive revenue to other parts of their own business or of their business partners. However, even more important than the cross-selling revenue is the data.

As millions of Chinese use apps like WeChat or Alipay every day, the tech giants are building up an enormous trove of

customer data. If you consider something as simple as hailing a taxi, the transaction can show location information, preferences (luxury or economy ride), as well as provide insight into customer behaviour (ratings).

So far, most of the data is used for simple usage cases. If you order food delivery, the app will suggest new restaurant recommendations based on your previous choices as well as pre-fill the address based on your location, but this is really just the start of what is possible.

Currently, Ant Financial has a credit scoring platform called Sesame Credit that analyses a variety of data-points to come up with a credit score for individuals and merchants. Baidu, China's largest search engine, is focusing on the applications of artificial intelligence within the financial space, including stock picking and portfolio creation. Both are more sophisticated examples of how data can be leveraged to launch new products and services.

Although data privacy is a consideration, China's consumers don't seem to be as concerned. Kapronasia surveyed 1000 Chinese millennials and nearly 50 per cent were happy for the tech giants to use their personal search data to suggest a financial product. There seems to be a general acceptance that data is not particularly private in China anyway and that if data can be leveraged to provide a better product or services, customers are happy with the trade-off.

Beyond creating domestic platforms, Ant Financial and Tencent also have been expanding overseas. In India, Alipay has invested in PayTM and Tencent in Flipkart. Tencent has also pushed into Thailand and Alipay into Hong Kong and the US through its partnership with FirstData and potential acquisition of MoneyGram. The forays overseas have followed a few different strategies.

First, the tech giants have followed Chinese overseas travellers. By expanding into popular Chinese tourist destinations such as the US, Hong Kong and Singapore, the tech giants can provide payment acceptance. This means when Chinese consumers are abroad, they can still use their Chinese mobile wallets to pay. In addition, it allows them to provide additional products and services. Alipay, for example, has partnered with duty-free programs such as Global Blue to allow travellers to receive instant cash-back for their overseas duty-free purchases.

Second, the tech giants have focused on acquisitions and investments in particular ››

Kapronasia surveyed 1000 Chinese millennials and nearly 50 per cent were happy for the tech giants to use their personal search data to suggest a financial product

focus markets where they can partner to achieve better than average returns. Ant Financial, through Alibaba, invested in PayTM, India's largest mobile payment platform. At the time, India's mobile payment market was very nascent and the overall payment system and e-commerce market not as robust as in other markets. By entering the market and combining Alipay's expertise with PayTM, they have had tremendous success in both payments and e-commerce.

Finally, the tech giants are setting up local currency-denominated wallets. Previously, opening a WeChat wallet was only possible for Chinese residents and the wallet would be in Chinese yuan. Today, residents of China, Hong Kong and South Africa can open WeChat wallets in their local currency. Similarly, Alipay is now available in Hong Kong.

This expansion will continue, albeit at a very gradual pace. Setting up a wallet involves a much more complex set of regulations and takes time. In the US alone, payment licences are awarded state by state so starting from scratch can take time. Ant Financial's potential acquisition of MoneyGram is an example of how the company might be able to achieve this much more quickly than by an organic approach.

We should also expect the Chinese tech giants to pursue their platformisation strategy internationally, although this may be a slower burn as platforms involve quite a bit of understanding of customer behaviour. As much as every human eats, we all like to order our food differently and this changes by market. We have seen very few examples so far of tech companies being able to offer the same product and service in every market. Uber is a rare example, but is also struggling.

Clearly the tech giants have changed the way that China spends, the real question will be how they are able to sustain that growth both domestically and internationally in the future. Platforms in China have already shown their value domestically, but new regulations may force standardisation of payments and more restrictions on what they can do.

Internationally, the platforms also have their work cut out for them. Hopefully they have learned from the many foreign tech giants that have tried and failed in China, but expanding internationally will not be easy for either Ant Financial or Tencent. They will face myriad regulations as well as geographic and cultural challenges.

Clearly the tech giants have changed the way that China spends, the real question will be how they are able to sustain that growth both domestically and internationally in the future

Nevertheless, China's tech giants have the drive and funding to continue growing far into the future. There are characteristics that are unique to the Chinese market that may make it difficult to achieve the same level of success overseas, but certainly they provide excellent case studies on what is possible. ***DNS***

Zennon Kapron is founder of Kapronasia, a research and consulting firm focused on financial services in Asia. For more information, visit www.kapronasia.com

Nothing personal

Financial authorities globally are promoting open banking. While it represents a shift in the mindset of traditional banks, **Heather McKenzie** finds they may be up to the challenge

In September, Australia's Macquarie Bank launched a pilot of an open banking platform for customers to transfer data to approved third-party applications. Any third-party provider that meets the bank's open platform standards and security criteria can connect. In launching the pilot, Macquarie attracted plenty of attention as it was seen to be stealing a march on Australia's 'big four' banks.

Macquarie Bank obtained an Australian banking licence in 1985, having operated as a wholly-owned subsidiary of UK merchant bank Hill Samuel since 1969. The bank's retail banking and financial services business recorded net profit of A$513 million in the year to 31 March 2017. It has more than 1 million customers and holds a $A28.7 billion mortgage portfolio – about 2 per cent of the Australian mortgage market. During the year it launched Apple Pay as part of its digital banking program.

The open banking platform features Macquarie devXchange, an open developer portal with a 'sandbox' to help third-party developers to create and test new features in a safe environment. Customers will be given the option to securely connect their personal banking data such as transactions and home loan balances, as well as their business and wealth information, into third-party applications, such as budgeting and accounting solutions, to create personalised banking.

"Open platforms allow for a secure free flow of connectivity," said Wayne Lipschitz, open platforms product owner in Macquarie's banking and financial services group. "The same necessary rules around client data security still apply, but as long as they meet that criteria, any third-party provider can securely connect through an open API."

His colleague, head of personal banking Ben Perham, added: "Our customers have been telling us they want to securely connect their information into their favourite accounting software, budgeting app and other innovative services they're interested in." APIs are being used by leading digital companies such as Amazon and Google to transform consumer experiences, and Macquarie believes it can do the same in financial services.

Macquarie describes open banking as a "mindset shift" away from proprietary control, which was traditionally driven by commercial demands.

As in many other countries, regulators and financial authorities are pushing the concept of open banking in Australia. The country's House of Representatives Standing Committee on Economics issued its second report into the country's four main banks in April 2017. Referring to the proposal contained in the first report to "empower consumers" by forcing deposit product providers to open access to customer and small business

data by July 2018, the second report stated: "All four banks noted general support for data sharing. However, the banks are conflicted on this issue, as the process of opening up data means that an asset which is currently proprietary to the banks will be non-proprietary in the future. For this reason, it is critical that the banks are not allowed to control the process or set the rules by which consumer data is opened. An independent body must lead the change and be responsible for implementation." The committee suggested that the Australian Securities and Investments Commission develop a data sharing framework for Australia's banking sector.

In Europe, the big push towards open banking has come via the European Commission's revised Payment Services Directive (PSD2). "The most impactful element of PSD2 – that banks must open their customers' accounts to third-party payment and information requests – is paving the way for an entirely new end-user experience in digital financial services, one in which the customer will call all the shots," says Maikki Frisk, executive director at Mobey Forum, an independent industry association focused on digital financial services. "It may not happen overnight, but it's coming."

A good way to imagine the post-PSD2 era of open banking, she adds, is to think of it in terms of apps and platforms. This approach brings it all into focus, principally because it has happened before. "The development of this space is starting to look a great deal like the advent of the smartphone."

Frisk points up that before the app and android revolution took hold, a mobile phone's functionality was native to its manufacturer. There was one SMS application, one address book and so on. The arrival of the touch-screen smartphone turned this on its head, making the operating system (OS) into a platform upon which third parties could introduce new apps, widgets and services. "This gave end-users massive choice, very quickly. Users could continue to use the device's native apps, of course, or they could adopt apps and functionalities from elsewhere in their OS ecosystem. The same is about to happen in banking."

Matt Williamson, global head of payments at Finastra, agrees. "Open banking signals the dawn of a new payments era. Banks and payments services providers [PSPs] will have the ability to move between payment markets, building analytics around their client base as »

"The most impactful element of PSD2 – that banks must open their customers' accounts to third-party payment and information requests – is paving the way for an entirely new end-user experience in digital financial services, one in which the customer will call all the shots"

Maikki Frisk, Mobey Forum

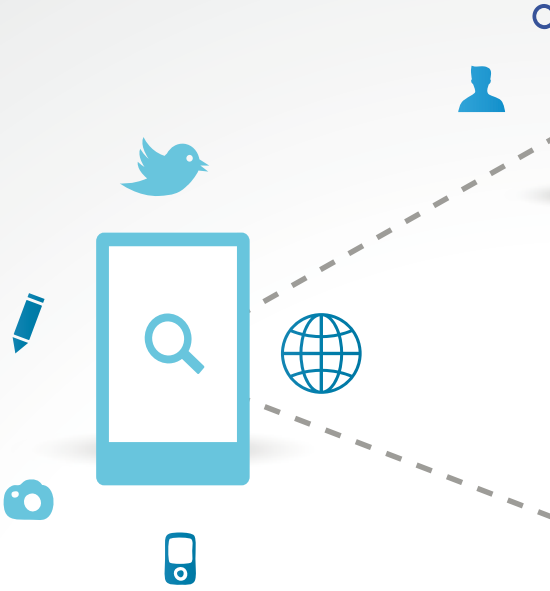
adoption rates increase. These in turn will determine additional value-add and services yet to be considered."

Cross-border PSPs will be able to leverage a better rate for payments based on volumes within the markets. So, if a provider is sending a significant number of payments to one region monthly, they can command a lower fee as a result, he adds.

Tom Durkin, head of digital channels at Bank of America Merrill Lynch global transaction services, says PSD2, the push for APIs and the notion of open banking will possibly deliver a licence for fintechs, vendors and other non-banks to disintermediate banks from their own customer base in terms of maintaining the relationship at the front end. "But banks have customer data on their side," he says. "It is incumbent upon the successful bank to shift its status, in the eyes of its clients, from one of mere assistant to that of valued advisor. A bank should be able to understand more about its clients' financial flows than perhaps even its clients do."

The fintechs focus on payments niches; they will not tackle the entire spectrum of corporate activity, he adds. Forward-thinking banks will not dismiss the fintechs but will instead seek to partner or collaborate with those that have the open banking best solutions. Seeing the competition as a collaborative opportunity could even change the way the traditional partner-bank approach is modelled. Multibank payments will be easier when bilateral agreements are eliminated, and multibank reporting will be timelier when banks can reach directly into partner bank systems.

"With better APIs and improved integration, instead of sending MT 940s over the Swift network, networks could be expanded to deliver considerable



efficiency upsides for all parties. Even Swift has an opportunity to support API progress: its GPI project is all about interaction with Swift.com to pull reference information or connect via an API," says Durkin.

Dr Louise Beaumont, strategic advisor at SapientRazorfish and co-chair of the UK's Open Banking Working Group, says combining data through APIs will allow banks to improve customer experience "hugely" for processes such as account opening, AML checks and product application processes, where personal information can be pre-populated and information verified from official sources.

"We are also likely to see competitors emerge to the standard bank overdraft. Once payments services providers have access to transaction data, they will be able to anticipate when customers are likely to need a short-term line of credit and offer their service as an alternative." Similarly, it is likely that providers will help customers earn a higher return on their money by automatically switching large credit balances from current accounts to interest-bearing accounts. Automated services that help customers manage their money between several accounts is an obvious extension of this idea.

Speaking at the SAP Financial Services Forum in London earlier this year, Kevin Hanley, director of innovation at RBS, said of open banking: "Customers are demanding it, technology is enabling it, and regulators are enforcing it. Financial services will become more collaborative, open, competitive and customer-focused. As a result, we will unbundle and re-bundle our offerings. Production and consumption in financial services are changing."

Hanley said RBS believes future success will be through a combination of its assets and capabilities with those of others. "If we can do that and put customers at the heart of it, we believe that is part of our success. We recognise today that we need to be technically able and culturally willing. Technically means better connected; culturally means in everything we do we have to be a radically different organisation than we have been historically."

Also at the event, Jarkko Turunen, head of open banking at Nordea, said open banking was not solely about technology, but was also about culture. "This means we have to work outside our financial services walls and incorporate different cultures. I see technology as the 'easy' part of open banking."

Hanley agreed: "The winners in the future will be better-connected banks that transform from being traditional providers into end to end services aggregators of other entities' offerings. This will also involve having the courage to leverage the distribution capabilities of others. Financial services in an increasingly networked world will be a much broader proposition."

Finastra's Williamson says until PSD2 comes fully into operation in January 2018, the exact requirements for banks are unknown. "This puts immense pressure on banks who are unable to move as quickly as their PSP counterparts. It also reinforces the importance of collaboration between these parties."

Damian Richardson, head of innovation and strategic initiatives at NatWest, says banks and fintechs have successfully worked with each other for decades. "These symbiotic relationships enable each party to focus on its strengths, such as scale, AML expertise or software engineering. Open banking means the banking and payments ecosystem will evolve to become more collaborative, with all parties adapting and thriving to better serve customers."

However, Mobey Forum's Frisk reckons that large banks stand to gain the most from open banking as it will give them access to the new open data market.

"Here, it's worth asking: who is the end-user likely to trust the most to deliver the next wave of payment and aggregation services – the bank they have trusted for years, or an app developer they have never heard of?" ***DNS***

Reaping the rewards of instant payments takes work

The key benefits of the instant payment systems being rolled out in Australia and in Europe were discussed during yesterday's Instant Payments Over SWIFT session in the SWIFT Auditorium.

Nigel Dobson, General Manager, Wholesale Digital Transformation, ANZ, was joined by Mehdi Manaa, Departmental Manager, European Central Bank (ECB), responsible for the Target Instant Payment Settlement (TIPS) platform, and Hays Littlejohn, CEO of EBA Clearing which is responsible for the RT1 platform.

They identified speed, constant availability and data-rich messaging as the primary advantages of instant payment (IP) backbone infrastructures.

Getting to these benefits, and enjoying the extra identity and liquidity services that open-IP systems can enable if they use ISO 20022 standardised messaging, is not easy, however, warned the moderator Diane Nolan from Accenture. "There is the connectivity challenge for banks and the issue of how best to manage risk controls around fraud, anti-money laundering [AML] and other such activities," she said.

For Elie Lasker, Senior Market Manager at SWIFT, one way to meet the connectivity challenge is to use the SWIFTNet Instant solution, which can act as a messaging bridge to the new IP systems being rolled out around the world. "Unlike FileAct or FIN messaging, it can operate 24x7 and act as a connectivity gateway," he said.

"SWIFT's journey in this area began in 2015 when we won a bid to build the New Payments Platform (NPP) in Australia, which will be live imminently," continued Lasker. "Our three SWIFT design principles were followed to ease the challenges facing banks and prioritise efficiency."

These principles are:

- Enable infrastructure re-use, where possible.
- Multi-CSM connectivity – the new SWIFTNet Instant solution conforms to this design requirement.
- Future proof the system.

"Future-proofing was the last, but not least requirement for the NPP. It is also something we follow for all new systems," said Lasker, as he explained how this approach means the SWIFTNet Instant solution will connect to the ECB's TIPS platform. It will also connect to EBA Clearing's RT1 platform, which is designed for the single euro payments area instant credit transfer (SCT^{Inst}) that is about to go live next month.

According to EBA's Littlejohn, the pan-European RT1 will be able to process 50 million transactions per day. "It will go live next month with 25 banks," he said. "This time next year 100-plus banks will be live. Banks don't have to use it, the scheme is optional but many are realising it's in their interests."

"Some of the friction that exists in the global value chain at the moment could be reduced by interoperable ISO 20022-enabled IP systems"

The TIPS platform will go live in November 2018, said Manaa, who explained that the ECB is talking to a "contact group" of banks and other interested participants to design the build out. "There will also be a TIPSApp challenge on 6 February next year where banks and alternative payment services providers (PSPs) are invited to share their connectivity pilots and service ideas."

ANZ's Dobson was also excited by the "ability to invite non-banks and financial technology players in to do innovations on the service layer".

"Some of the friction that exists in the global value chain at the moment could be reduced by interoperable ISO 20022-enabled IP systems," he added.

The future is bright therefore, but getting there and overcoming the connectivity and integration obstacles at banks, will be a challenge.

Back to basics

Ensuring security on Swift's network doesn't have to be rocket science. Getting the basics right will help individual institutions and Swift's community, writes **Heather McKenzie**

Amid the hype and disinformation about cyber attacks and who perpetrates them, it is often easy to forget that prevention isn't rocket science. While those launching such attacks are increasingly well-organised groups that act like corporates, they often take advantage of lax security – the equivalent of leaving a window open, or the keys in a car's ignition. The May ransomware attack on the UK's National Health Service, for example, was made possible because the service – subject to swingeing government cuts – was using unsupported XP operating systems.

The attempts to hack into Swift's network last year were largely made via central banks or other banks in emerging economies. Attackers started by exploiting security weaknesses within institutions' local environments to steal valid operator credentials to their local payment infrastructure. They then inputted seemingly legitimate payment instructions with those valid credentials and hid the evidence of fraud.

Following these attacks, Swift launched the Customer Security Programme (CSP) to support users in their fight against cyber attacks. While Swift members are responsible for protecting their own environments, CSP is designed to raise standards among Swift members. It focuses on three aspects: an institution itself, the institution's counterparties, and the community.

Swift points out that securing a bank's local environment is the most important action to take. Securing the physical set-up of the local Swift-related infrastructure and putting in place the right people, policies and practices, are critical to avoiding cyber-related fraud. This can be as simple as ensuring that the Swift terminal is in a secured environment and accessible only to those who are authorised to use it.

From January 2018, Swift members will be required to meet mandatory rules within CSP, including inspections from internal or external auditors conducted with samples of customers to check quality. The detailed compliance status of each customer will be made available to their counterparties (for example via the KYC Registry), providing transparency and allowing other users on the network to apply risk-based decision-making regarding their counterparty relationships.

Swift has introduced new security features to its products to make those requirements easier to meet. For example, two-factor authentication has been introduced for Alliance Access customers that do not yet have the facility.

For counterparties, Swift operates the Relationship Management Application, which enables members to control access and check that they are doing business with their trusted counterparties. Swift is also facilitating discussions with banks to develop a common understanding between sending and receiving parties of the warning signs that should lead to payments being investigated, and of how suspicious payments should be stopped.

Finally, Swift is also encouraging members to share information about attacks. The cooperative's Customer Security Intelligence team can help limit the community impact by sharing anonymous information on indicators of compromise and by detailing the *modus operandi* ››

FinTech CONNECT Live!

6-7 DECEMBER 2017 | EXCEL LONDON, UK

THE UK'S LARGEST MEETING PLACE FOR THE FINTECH COMMUNITY

#FTCLIVE17

ATTEND
Over 120 sessions & 8 Workshops covering Fintech/Payments/ Insurance and Cloud

HEAR
From over 250 excelling global Fintech leaders and founders

MEET
With over 3000 potential partners, customers, investors & advisors

BENEFIT
From on site advisory clinics run by senior market experts

WATCH
An array of product demos from start-ups and large tech companies

INTERACT
With over 200 partners and exhibitors showcasing the latest industry solutions.

+ 3000 ATTENDEES

+ 50 COUNTRIES REPRESENTED

+ 200 EXHIBITORS & PARTNERS

+ 250 SPEAKERS

BE THERE! VISIT WWW.FINTECHCONNECTLIVE.COM

Supported By:

Department for International Trade

Cymru Wales

Host Publication:

THE FINTECH TIMES

used in known attacks. This information is disseminated through Swift's Security Notification Service to which all members can subscribe.

"With CSP, Swift is attempting to raise the bar on security," says Jerry Norton, head of strategy for CGI's UK financial services business. "It provides a set of controls to which Swift members have to adhere, whether they are banks, corporates, bureaus etc. Some members will be very well-versed in these controls, but others possibly not."

A chain is only as strong as its weakest link, which makes Swift's CSP a "necessary step" in addressing cyber crime, says Phillipe Lepoutre, deputy head of global transaction and payment services at Société Générale. "As a global network, Swift allows exchanges between different types of banks – from the very largest multinational institutions through to very small banks. The perception is that perhaps some of the smaller banks have not taken cyber security as seriously as they should, which has created weak points in the Swift network. The fraud attacks on the network were a wakeup call for many Swift members. That is why the CSP is very timely and the whole Swift community should engage with it." CSP will create transparency between members on the Swift network and will be a strong incentive for all banks to show they are not lagging when it comes to cyber security, he adds.

Initially the CSP assessments are based on self-evaluation, but that may evolve over time to assessments conducted by a third-party. The card industry's Payment Card Industry Data Security Standard (PCI DSS) is a good indicator of how CSP may evolve, says Lepoutre. Most of the card industry players have engaged with PCI DSS, which provides a strong and demanding standard for card security. It is becoming very necessary for the Swift community to engage in a similar type of project, he says.

To a certain extent, self-certification protects Swift from taking on the responsibility of certifying the security of all its members. It is up to each Swift member bank to assess its counterparty's security and make a risk-based decision on whether it is prepared to do business with that member bank.

"CSP isn't rocket science," says Norton. "It is bringing consistency and standards to security." For example, in addition to ensuring Swift access is isolated from non-authorised users, firms are also urged to have robust password policies. For example, passwords should be longer than four characters and be regularly changed.

"There is an issue that while some larger institutions may have policies and procedures, not everyone enforces them. Smaller institutions may not have such policies at all and CSP is a way of helping those that don't know where to start," he adds.

Any security policy must start at the top, in the boardroom, says Norton. Moreover, the policy must be enforced. Cyber security is not a back-end IT problem, but is all about best practice and how risk is managed. Cyber attacks are a business risk and therefore should be put on a register of risks by the institution's risk committee.

Leigh Mahoney, head of wholesale digital transformation at ANZ, says good cyber security successfully considers both people ››

"CSP isn't rocket science. It is bringing consistency and standards to security"

Jerry Norton, CGI

"It used to be thought of as foolish if you spoke out about these issues; now it is foolish if you don't"

Stephen Scharf, DTCC

and technology. "The focus is often on having the latest, best in class technology, but cyber attacks more often occur because someone, somewhere, did something they shouldn't have. It is important to consider this 'people' element, the user experience and the culture of an organisation where the technology is deployed from the outset."

Stephen Scharf, chief security officer, DTCC, says mitigating cyber risk requires a joint effort as it is an industry-wide challenge. "We don't believe any firm can be 100 per cent successful fighting cyber attacks on their own. In the securities industry, we have learned that we are better protected if we work together, rather than in isolation."

Whereas in the past security was a private issue and few people spoke about their challenges, this trend has completely reversed, says Scharf. "It used to be thought of as foolish if you spoke out about problems; now it is foolish if you don't."

Industry groups, based on collaborative sharing of information about security, can help. For example, the Financial Services Information Sharing and Analysis Centre (FS-ISAC) is a collaborative effort between banks and utilities. It was launched in the US in 1999, after a Presidential Directive (later updated in 2003) mandated that public and private sectors share information about physical and cyber security threats and vulnerabilities to help protect US critical infrastructure.

More recently, FS-ISAC established Sheltered Harbor, a "forward looking attempt to prevent future risks", says Scharf. An industry-led organisation, it enables financial institutions to securely store and rapidly reconstitute account information, making it available to customers, whether through a service provider or another financial institution, if an institution appears unable to recover from a cyber incident in a timely fashion. Consumer data stored in a Sheltered Harbor specified data vault is kept private by each institution, is encrypted and protected from change. The model is a distributed one, with no central repository of information. The concept for Sheltered Harbor arose during a series of successful cyber security simulation exercises between public and private sectors.

It is "inevitable" that the cyber control environment of a bank's clients will become a larger and more integral part of their know your customer framework, says Mark McNulty, head of global clearing and FI payments at Citi treasury and trade solutions. "The increase in cyber attacks on banks, that have often resulted in the successful transfer of money, highlights the need for counterparty cyber risk assessments to grow in sophistication."

While he welcomes the development of Swift's customer security controls and the upcoming transparency that Swift counterparties will have on each other's attestation against those mandatory controls, more industry work is needed, he says. "The industry must create a common interpretive framework for counterparty risk with the information on Swift mandatory controls being a critical, but not the sole, input."

The common framework is required to ensure that assessments can happen in the most efficient way possible and banks can focus on acting on the output.

Scharf emphasises that the way to strengthen cyber security lies in "getting the basics right". This includes adhering to core principles of updating software patches, identifying vulnerabilities and ensuring ID management is robust. "The core, fundamental tenets of a security program are very important. Often these are tried and true approaches; firms should understand that innovation and security can work together. Building in these basic tenets of security from the start of any product design will ensure that new products can be very secure."

Lepoutre points up that knowing how to fight a fraud or cyber attack that has not yet happened is challenging. Banks must bring together specialists in payments, Swift, data science and technology to work together and detect the possible ways a fraud might be attempted through Swift. "A deep understanding of the flow that comes through the Swift pipes every day will help in pinpointing suspicious transactions. In retail payments, the large volumes mean that machine learning systems can self-learn more easily based on the track-record of frauds; this is not the case with Swift payments."

Ideally, says Lepoutre, internal defences at banks should be combined with defences inside Swift itself. Within a global network like Swift it is often easier to detect fraudulent transactions than it is within a single bank. "Such an approach could involve Swift managing a set of generic rules, which are based on members' experiences. This combination of security at individual financial institutions and at Swift would provide the most secure approach. This will take time to build, but is in the direction the industry should head." ***DNS***

Instant Payments in Europe: a recipe for success

Isabelle Olivier, **head of Securities Initiatives and Payment Market infastructures, EMEA, SWIFT**

There is intense interest in instant payments (IP) throughout Europe. Domestic schemes are already live in the UK, Denmark, Poland and Sweden. The success of these schemes shows what's possible but also teaches many lessons.

Perhaps the most valuable lesson is the need for banks to strike a delicate balance between an IP solution that is cost effective but also meets evolving customer needs. Establishing a compelling business case is critical but challenging.

In practice a successful IP solution is about much more than payments – it is a strategic platform for the development of value-added overlay services. Until now, there has been no mandate to adopt IP and schemes have evolved along national lines, each with its own rules, message formats and currency. But the move to pan-European IP requires a standardised approach.

At a pan-European level, SEPA Instant Credit Transfer (SCT^{Inst}) offers a real-time scheme for euro transactions based on the SCT scheme and the ISO 20022 messaging format. While this is a good start, the practicalities of instant payments are formidable: the investment required is substantial and there are many pitfalls for the unwary. So what are the key ingredients of a recipe for success?

Ensure maximum reach. On top of being easy and convenient to use, a successful IP solution must be ubiquitous. Achieving this is a strategic challenge for the entire European (and global) industry. SCT^{Inst} has the potential to reach 500 million users but IP must attain a 'network effect' to drive uptake. The lack of true interoperability between European IP platforms represents an obstacle for payment service providers that may have to access multiple IP platforms in order to reach enough banking counterparts across Europe and beyond.

Develop value added products and services. While the deployment of pan-European IP is a major challenge, it also brings opportunities for banks to review what they do and how they do it. But developments are moving fast and there are plenty of new players with an eye on the payments prize, so the industry will need to be innovative and develop appealing products and services in collaboration with the right partners. This will be key to driving IP uptake and building competitive advantage.


Isabelle Olivier, SWIFT

"The industry will need to be innovative and develop appealing products and services in collaboration with the right partners"

Implement agile integration solutions. Payments touch nearly every bank system and IP requires 24/7 operations and immediate responses, so a successful implementation will demand major changes in banks' systems and operations. Experience shows that around 90% of costs incurred in the move to IP relate to systems integration. Banks will be looking for a financial messaging platform that sits between their systems and the various domestic and cross-border IP platforms on one end, and acquisition and reporting solutions towards the other. It will also have to offer the necessary agility for banks to evolve their offer and retain relevance in this fast moving ecosystem.

Guarantee security and resiliency. The move to instant requires the orchestration of multiple layers of technology over disparate geographies. Banks will need to maintain an uncompromising approach to security to reduce exposure to cyber threats, fraud and system outages.

Contain costs. As banks build their IP business case, controlling costs is crucial. Re-using existing infrastructures will help to keep unnecessary investment to a minimum and mitigate project risk. And by leveraging existing connections, the transition to IP can be achieved more quickly and smoothly. In the same way, solutions that offer access to multiple IP systems will help to solve the ubiquity challenge while minimising spend.

The transformation of the payments landscape to the instant world is inevitable and desirable. It comes with many challenges for the industry, but also represents a unique opportunity for banks to re-invent themselves, building upon their strengths and capturing the unexplored benefits of new technologies. Selecting the right partners, providers and solutions will be key for the success of banks' IP implementation projects and for their digital transformation in the coming decade.

Your ultimate guide to Sibos 2017

Disruption idea 1: The supersonic escalator

Disruption idea 2: Seeing VR Sibos... at Sibos

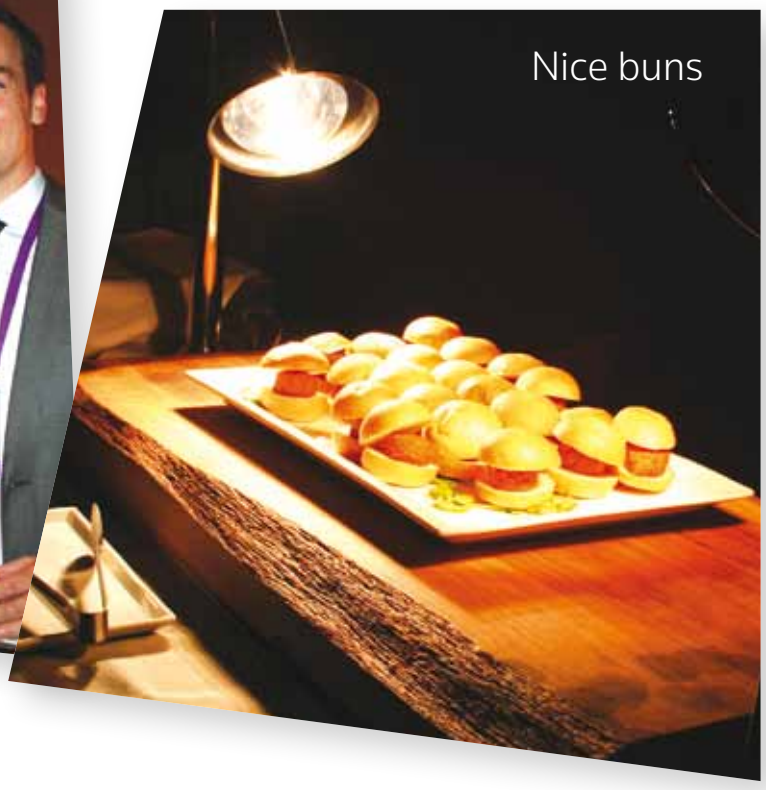
Disruption idea 3: The non-returning boomerang

Disruption idea 4: Organise your own event

Your ultimate guide to Sibos 2017

Why are you coming in through the window? The party is for everyone

Come on Steven, chest out, mouth closed



banking technology

The definitive source of news & analysis of the global fintech sector

Monthly page views:
218,000+

Customer database:
53,000+

Newsletter subscribers:
28,000+

Magazine distribution:

print and online

banking technology

ADVERTISE WITH US

Twitter @BankingTechno:

29,000+ followers

LinkedIn Group:

1,800+ members

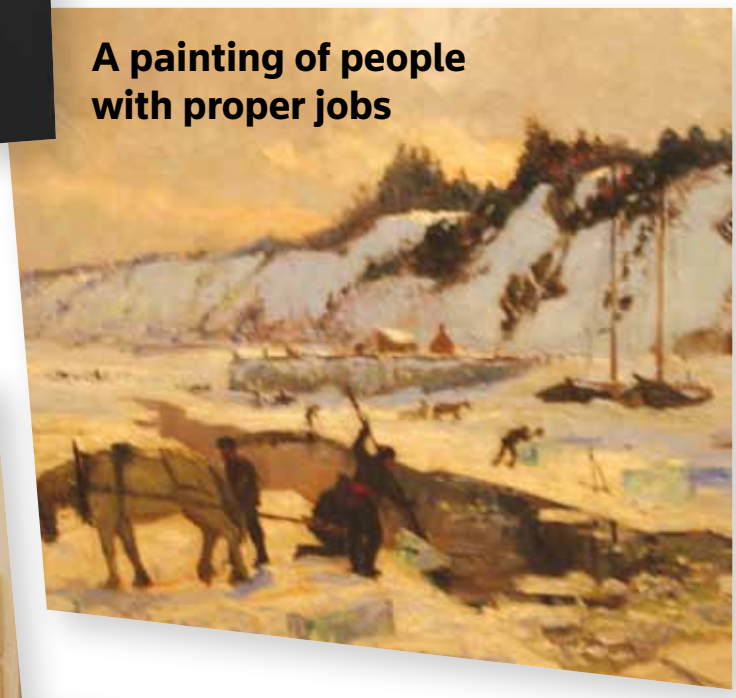
Onalytica's
Top 100 Fintech Influencer and Brand

www.bankingtech.com

*Contact **Judith McInerney***
Tel: +44 203 377 3506 | Email: judith.mcinerney@knect365.com

Your ultimate guide to Sibos 2017

Meat and greet



A painting of people with proper jobs

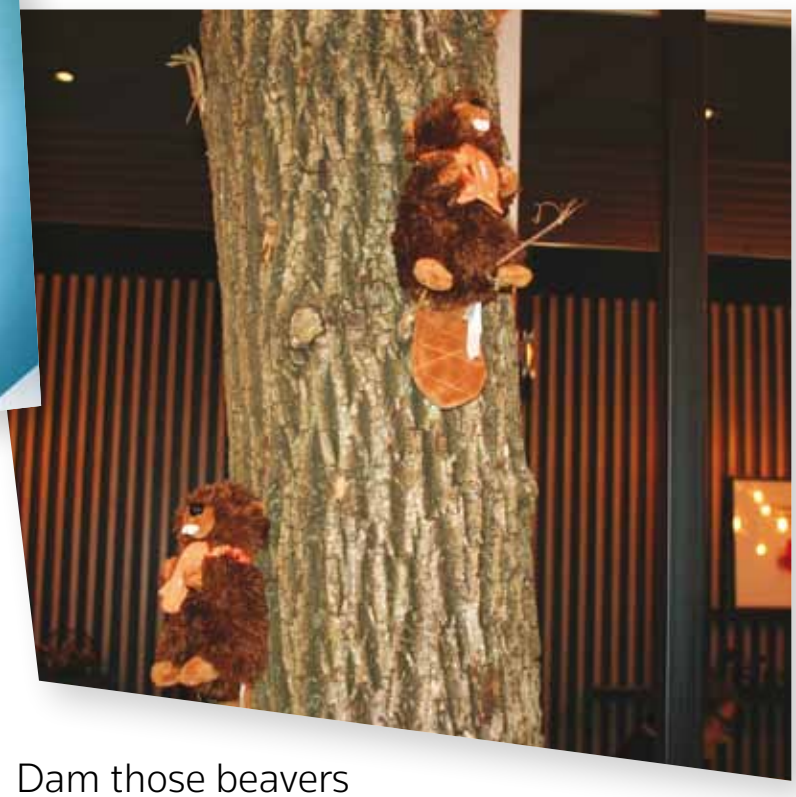
Where's the carrot?

The unsmiling carapace of the corpse of the capitalist dream... or "Mike" to his friends

Always wise to have rent-a-crowd on standby

Worst 'you are here' map ever

That certainly is a small world



Dam those beavers

Your ultimate guide to Sibos 2017

Going home happy: an armful of beavers

You can never be too sure if your competitors are listening in or not

The 'basic stand package' comes with only two vowels

These chatbots get ever more human

See us at Sibos
Stand G44

Value.

From our headline.
To your bottom-line.

Saving you money. Or making you money. Either way, you win.

This is the way we look at how we bring you value.

Through creating Advanced Services that let you reduce your cost base. Significantly. And sustainably.

Through compliance services that reduce your exposure. But not your visibility.

And through services that improve efficiencies and margins for you. All of which go straight to your bottom-line.

Solutions for the future. Now.

SIX Securities Services

To find out more about our Advanced Services, call +41 58 399 6639.

Pelican

Introducing the Pelican Innovation Hub

Partnering to build your digital future, today.

The Pelican Innovation Hub is a partnership model that gives banks a rapid and cost-effective means to explore new product opportunities, from proof of concept, prototype development, to final production and service deployment.

Leveraging Pelican's extensive heritage in AI disciplines, alongside over two decades of expertise in payments and banking, the Innovation Hub provides a highly functional and proven digital banking development environment.

Talk to Pelican today on Stand H52 to find out more, or visit www.pelican.ai

Pelican 15-Minute Insight & Innovation Sessions - Stand #H52

	10.00	11.00	14.00	15.00
Wednesday 18 October	Innovation Hub Solutions	The AI Advantage	Payment Fraud	Integrated Financial Crime Compliance
Thursday 19 October	Payment Fraud	The Real-Time Challenge	STP Revenue Opportunities	API and Open Banking

www.pelican.ai