



This is a high-level industry news and business intelligence update bulletin. For further information on any of the items contained within the bulletin or to discuss the potential impact of these items on your business, please contact Savantor on info@savantor.com.

Savantor Limited
68 Lombard St
London EC3V 9LJ
Tel: +44 20 7868 1734
email: info@savantor.com
www.savantor.com

Items in this issue:

Savantor's View	1	China's central bank to release its own digital currency... 3
Technological change and payments	1	FCA delays introduction of Strong Customer Authentication rules
Products and Initiatives	2	UK PSR confirms Confirmation of Payee deadline
New York MTA 'tap and pay' success	2	BoA terminates First Data partnership
MasterCard acquires Nets account-to-account payments business	2	Capital One data breach exposes 100 million
Facebook prepares Indian launch for WhatsApp Pay	2	Link data highlights decline in cash usage
ING tests mobile phones POS software	2	Mobile Money
Swift connects with Singapore's Fast to cut cross-border payment times	3	Starling sets target of 2020 to break even
Market News	3	Data protection agencies raise Libra concerns
Huge biometric security breach exposed	3	Monzo customers asked to change PINs after discovery of storage bug

Savantor's View

Technological change and payments

UK Finance has recently issued their UK Payment Markets 2019 report, which provides a detailed analysis of the use of all types of payments in the UK during 2018, as well as forecasts of payment trends in the UK for the next 10 years.

One of the most striking aspects of the trends highlighted is the increase in speed of technological change and significant innovation in payment methods evolution. In particular, the advent of smartphones together with online banking, mobile banking and contactless payments have greatly influenced our behaviour in making payments.

This speed of change does not come without casualties – only this week the ECB warned that “accidents” are likely to happen as the big banks try to mimic the success of digital challengers, leading to an increase in the risk of being hacked as they attempt to offer similar features to the new players.

Barely a week goes past without news of another large hacking incident coming to light and the banking industry is no exception – with arguably more potential vulnerability to data misuse because of the content of the data held.

Not so long ago challenger banks were perceived to be more vulnerable because of their newness and lack of establishment. However, as banking apps are increasing significantly in popularity with the rise in smartphone popularity, these newer banks are currently winning the popularity race with their mobile banking apps.

In a recent poll of bank apps undertaken by MoneySavingExpert of over 5,000 consumers, the apps of challenger banks Monzo and Starling won easily in terms of being rated by the quality of their features and their ease of use. 78% and 70% of users respectively regarded their apps as having lots of features and excellent usability, whereas of the traditional banks, Barclays came top with 57%.

Apps have to some extent become a de facto guide for many aspects of life, with many aimed at self-help or self-education in a variety of topics. Amongst the myriad available to consumers today, there are a number aimed at helping youngsters to manage their money responsibly and learn how to control their finances – surely something that must be viewed in a positive light when many struggle with personal finance management.

The pace of evolution in technology and its integration into our day-to-day lives is a fact that cannot be escaped; the impact of these changes on today's payments landscape is equally as fast-paced and behaviour-influencing.

Whilst Savantor Limited ("Savantor") has used reasonable efforts to obtain information from sources which it believes to be reliable it does not make any representations or give any warranties or guarantees that the information provided or any opinions expressed herein are accurate, reliable or complete and none should be relied upon as statements of fact. In no event, including (without limitation) negligence, and in no circumstances will Savantor be liable for any loss or damage of any kind whatsoever, including (without limitation) any direct, special indirect or consequential damages, caused by the use of or reliance upon information provided or opinions expressed herein.

Products and Initiatives

New York MTA 'tap and pay' success

New York's Metropolitan Transport Authority has hailed the success of tap and pay fares for subway and bus journeys, recording a much higher take-up among passengers than initially anticipated.

Dubbed Omny, the new fare payment option allows passengers to use their debit and credit cards and mobile wallets to pay for their ride. It was launched as a limited public pilot at the end of May at 16 subway stations and on all Staten Island buses.

Within the first three days, subways and bus customers used Omny more than 18,000 times, far exceeding original estimates of 7,000 taps in the first week. Nearly three months later, average usage rates are three to four times greater than expected, topping 22,000 per weekday and leading to the million-tap milestone just 69 days after the public launch.

Also unexpected was the surprisingly high number of Omny customers using smartphones for payment, with 80% using it through digital wallets compared to 20% tapping their contactless cards. (Source date: 15 August 2019)

MasterCard acquires Nets account-to-account payments business

MasterCard has acquired the account-to-account payment business of Nordic platform Nets for €2.85 billion. The acquisition comprises the clearing and instant payment services, and e-billing software of Nets' Corporate Services business.

The deal places MasterCard at the forefront of the move to real-time payments and acts as bulwark against the incursion of account-to-account payments into the credit card business, complementing last year's acquisition of Vocalink. It follows a recent agreement struck between MasterCard and the Nordic bank-backed P27 coalition to provide the underlying infrastructure for its real-time, cross-border payment project.

The acquisition provides more depth to the MasterCard Send and Transfast technologies that deliver cross-border payments to bank accounts, mobile wallets and cards. The deal also complements the technical assets and partners recently added to MasterCard's bill payment capabilities through the acquisition of Transactis.

The operations sold to MasterCard represent the majority of Nets' Corporate Services division and comprise the clearing and instant payment services and e-billing businesses, including Betalingsservice in Denmark and AvtaleGiro/eFaktura in Norway. The transaction is anticipated to close in the first half of 2020. (Source date: 6 August 2019)

Facebook prepares Indian launch for WhatsApp Pay

WhatsApp is set to launch its P2P payments system later this year, beginning in India, before rolling out to its 1.5 billion users globally.

The Facebook-owned messaging system has been testing the system in India for the past year, where the app has 400 million users.

The idea behind WhatsApp Pay is to make transferring cash as easy as sending a message.

The move deepens Facebook's interest in the payments industry, coming in the wake of the announcement of the social media giant's planned cryptocurrency Libra. (Source date: 26 July 2019)

ING tests mobile phones POS software

Dutch bank ING has piloted a software-based 'tap on phone' app, which transforms mobile devices into point-of-sale terminals. The app, which poses a threat to the dongle-dependent mPOS technology of firms like Square as it requires no additional hardware plug ins to accept payments, is currently undergoing testing with 200 small businesses in Istanbul.

Transaction data passed over the app is encrypted and stored in the cloud, which users can access to track inventory and check daily transactions in real-time.

Working with MasterCard, ING is the first European bank to pilot the service in a commercial setting.

According to MasterCard, there are 1.5 million small-medium enterprises and millions of other micro businesses owners such as taxi drivers, florists and electricians who can increase their sales and lower costs by adopting digital payments. (Source date: 23 July 2019)

Swift connects with Singapore's Fast to cut cross-border payment times

Banking co-operative Swift is boasting of the success of its integration with Singapore's domestic instant payment service, cutting the time taken to process inbound cross-border message transfers to as little as 13 seconds.

The trial run, which connected Swift gpi Instant into Singapore's Fast and Secure Transfers network (Fast), involved 17 banks across seven countries.

In total, 11 banks initiated cross-border payments into Singapore, and six banks in Singapore processed the payments domestically via the Fast system. Payments between all continents settled with 25 seconds, says Swift, the fastest in just 13 seconds.

Swift says additional tests are planned in other markets with instant payment systems, ahead of the planned global launch of gpi Instant later this year.

The company believes that the roll out of the service will steer banks away from alternative networks, such as Ripple and IBM's World Wire, as demand for real-time payments escalates beyond domestic markets into the cross-border realm. (Source date: 18 July 2019)

Market News

Huge biometric security breach exposed

Privacy researchers at vpnmentor have uncovered a huge data breach in security platform Biostar 2, a centralised biometric access control system used by UK police forces and major banks. Biostar 2 uses facial recognition and fingerprinting technology to control access to secure areas of facilities, manage user permissions, integrate with 3rd party security apps, and record activity logs.

Vpnmentor says it was able to access over 27.8 million records, a total of 23 gigabytes of data, on a publicly accessible database. The data leaked includes detailed personal information of employees and unencrypted usernames and passwords as well as access to over 1 million fingerprint records, as well as facial recognition information.

Researchers at vpnmentor say the breach would enable hackers to gain complete access to admin accounts on Biostar 2, enabling them to change user accounts and create their own accounts. Furthermore, hackers can change the fingerprints of existing accounts to their own and hijack a user account to access restricted areas undetected.

The researchers apparently made multiple unsuccessful attempts to contact Suprema, the developer of Biostar 2, before taking the paper to the Guardian newspaper late last week. The vulnerability was closed within a few days. (Source date: 14 August 2019)

China's central bank to release its own digital currency

The People's Bank of China is "almost ready" to launch its own digital currency, according to a senior official.

The impending launch comes after five years of work. The People's Bank set up a research team to investigate a digital currency back in 2014.

Details of the project are scant, but the currency will rely on a two-tier system meaning that both the central bank and commercial financial institutions can issue it. Blockchain technology will be used but not exclusively.

In addition to speeding up the transition away from cash, the digital currency is designed to give China's authorities more control over the financial system, says Bloomberg. (Source date: 14 August 2019)

FCA delays introduction of Strong Customer Authentication rules

The UK's Financial Conduct Authority (FCA) has confirmed an 18-month delay to the introduction of Secure Customer Authentication (SCA) rules for e-commerce transactions.

From September, the SCA regulation under PSD2 is supposed to mean that European shoppers will have to authenticate online payments over EUR30 with two of the following: something they know (like a password), are (fingerprint/face ID), or have (phone).

However, accepting the complexity of the requirements, a lack of preparedness and the potential for a significant impact on consumers, the European Banking Authority in June paved the way for some firms, on an "exceptional basis", to get an extension if cleared by national authorities.

The UK's FCA indicated that it would give the industry extra time and has now confirmed an 18-month implementation plan for card issuers, payments firms and online retailers. This is in line with recommendations from UK Finance and European trade association EPSM. The Central Bank of Ireland is also delaying the roll out of SCA rules. (Source date: 13 August 2019)

UK PSR confirms Confirmation of Payee deadline

Following a slow roll out of 'Confirmation of Payee' (CoP) technology, the UK Payment Systems Regulator has ordered Lloyds, RBS Natwest, Barclays, HSBC, Nationwide and Santander to ensure implementation by 31 March 2020.

CoP technology is devised to safeguard banking customers against Authorised Push Payment (APP) scams - the type of deception that costs UK consumers £345m in 2018, of which only £83m was recovered. The mechanism operates by checking that the account name entered by a payer matches the account paid, alerting the individual if there is any discrepancy.

The PSR is demanding that by 31 December 2019 each of the six banks has the capability to notify the sending bank that a payment is unmatched, requiring inter-communication between Lloyds, RBS Natwest, Barclays, HSBC, Nationwide and Santander.

By March, the banks will have an obligation to send confirmation of payee requests and notify the payer of the outcome, whether matched or mis-matched. (Source date: 2 August 2019)

BoA terminates First Data partnership

Bank of America is to terminate its merchant services partnership with First Data when the ten-year contract expires in June 2020. The news came within hours of Fiserv acquiring control of First Data, causing share prices to drop.

BofA says it expects to incur an impairment charge of about \$1.7 billion to \$2.1 billion in Q3 2019 due to the termination of the partnership, which started in 2009. Under the terms, First Data will continue to provide uninterrupted services to the BofA merchant base until 2023.

A spokesperson for BoA commented that the company is "looking forward to investing in our merchant solution and delivering the capabilities our clients need to thrive in an ever-changing payments environment." (Source date: 31st July 2019)

Capital One data breach exposes 100 million

Capital One has revealed that 100 million credit card applications had been accessed, resulting in thousands of Social Security and bank account numbers being left at risk.

Dubbed one of the largest data breaches to hit a financial services firm, the Capital One hack is expected to cost the company between \$100 million and \$150 million.

Apparently although some Social Security numbers had been tokenised or encrypted, information such as names, addresses, dates of birth and credit history had not. The data at risk includes "likely tens of millions of applications and approximately 77,000 bank account numbers." However, the company has reiterated that no credit card numbers or log-in credentials were compromised, nor were most of the Social Security numbers on the applications.

An individual who formerly worked for Amazon Web Services, which hosted the Capital One database that was breached, has since been arrested. (Source date: 30th July 2019)

Link data highlights decline in cash usage

New data from the UK's Link ATM network shows an ongoing decline in the use of cash machines for withdrawing money and checking balances, as contactless cards and mobile banking services take hold.

In the first four months of 2019 compared with the same period of 2018 there was an 8.7% decline in Link cash withdrawals in London. The data highlights regional disparities in the trend, with the North East showing the smallest drop at -3.7%.

The numbers are in line with a recent UK Payment Markets report by UK Finance that predicts a fall in cash usage from 28% of consumer payments in 2018 to only 9% by 2028.

According to Link, looking forward the rate of decline in Link transactions appears to be accelerating, and is currently expected to be at least between 9% and 10% for 2019 as a whole when compared with 2018. (Source date: 24 July 2019)

Mobile Money

Starling sets target of 2020 to break even

Starling Bank is set to break even in the UK by 2020, as the challenger forecasts that it will hit one million accounts before the end of 2019.

The bank has doubled customer numbers in the past eight months, reaching 775,000 accounts in total: 695,000 retail current accounts, 59,000 business accounts for small and medium-sized enterprises (SMEs) and a further 22,000 retail euro accounts.

Total deposits have exceeded £600 million and are expected to top £1 billion by the end of the year, as more users entrust Starling with their salaries.

The company, which is aiming for further growth via European expansion and through a big push into the business banking market, has grown its workforce by 170% over the past twelve month. The bank plans to add 400 staff over the course of the next year, bringing total employee numbers to over 1000. (Source date: 5 August 2020)

Data protection agencies raise Libra concerns

The UK's data protection watchdog has joined with other privacy regulators around the world in calling for more openness about Facebook's proposed Libra digital currency and infrastructure.

A statement to Facebook and 28 other companies behind the project asks them to provide details of how customers' personal data will be processed in line with data protection laws. It asks for assurances that only the minimum required data will be collected, that the service will be transparent, and requests details of how data will be shared between Libra Network members.

The statement is signed by a cross section of authorities representing millions of people in Europe, the Americas, Africa and Australasia, including the UK's Information Commissioner, counterparts in Australia, the USA, Canada, Burkina Faso and Albania, as well as the EU's European Data Protection Supervisor. (Source date: 5 August 2020)

Monzo customers asked to change PINs after discovery of storage bug

Monzo has asked up to half a million customers to change their PINs after discovering a bug that rendered them accessible to engineers working on the bank's systems.

The security oversight saw customer PINs inadvertently stored in two distinct files in the company's architecture, one of which was open to engineers as part of their job.

The challenger has spent the weekend deleting the files that were stored incorrectly and releasing updates to the Monzo app. The issue affected a fifth of the bank's 2.5 million customers. (Source date: 5 August 2020)