ROUNDTABLE

What's ahead in 2018: thoughts from the *Payments & FinTech Lawyer* Editorial Board

To mark the first edition of the publication of 2018 and with the implementation of PSD2 and the GDPR to take place this coming January and May respectively, we asked members of the Editorial Board to reflect on 2017 and comment on what's ahead in the payments and FinTech space.

Fiona Ghosh, Partner at Addleshaw Goddard

Looking backing back in 2017, the one major issue which has dominated the worlds of payments and FinTech, both in terms of regulatory headache and from an operational perspective, has been the thorny and multi layered issue of customer consent - for authorisation of processing of personal data, for executing a payment transaction and in allowing third party access to payment accounts.

The obvious place to see this in action is the milestone of the General Data Protection Regulation ('GDPR'). However, concepts of consent have also revealed themselves as embedded into other areas of law such as the revised Payment Services Directive ('PSD2') and, more operationally, within the onset of Open Banking in the UK.

As a firm, we have been heavily involved in the matrix of all three areas (the GDPR, PSD2 and Open Banking combined), advising our clients as to how to navigate through the maze of customer consent, fair processing and achieving the innovation dictated by PSD2 and Open Banking. It's not an easy nor a comfortable place to be, especially considering that all three should be up and running by early to mid-2018.

Looking forward, there is no doubt that the next year will see the GDPR have a huge impact on both customer rights and the obligations on controllers to roll out fresh fair processing notices. However, I expect that we will also see data processors flexing their muscles. Data processors too now carry legal duties under the GDPR. They will thus expect controllers to take on more contractual risk and responsibility, especially in the way in which those controllers process the personal data which is subcontracted out to processors. There is definitely going to be quite a bit of data protection 'hot potato-ing' when the GDPR finally bites in May 2018.

David G.W. Birch, Member of the *Payments & FinTech Lawyer* Editorial Board

I can't stress enough just how big a deal the UK's transition to Open Banking is. *Wired* had a great article about this (written by Rowland Manthorpe[1]) in October. Having talked to some of the key players and examined some of the key concepts, he drew an important conclusion[2], which is that Open Banking is not "just a technical fix, or even a solution specific to banking, but a new way of dealing with the twenty-first century's most sought-after resource, personal data."

What this says to me is that banks are about to be transformed from places that store digital monies (which they really don't anyway, since the proportion of household wealth held in the form of demand deposits has already fallen to minuscule levels) to places that store digital identities. Identity is, if you will, the new money! It's not a new idea. Back in 2014, the *Financial Times* was reporting that[3] "Britain's high street banks believe their future role will be as repositories of more than just money: they want to be the safe place where customers store their digital identities." This makes complete sense as a strategy and as a European Banking Association ('EBA') white paper of the time put it, "banks are well positioned[4]" to be a crucial, supporting, positive part of their customers' online lives.

Well, we're going to start finding out if this is true in January, because I can't help but feel that the major beneficiaries of the regulators' pressure to open up the banks will not be nimble startups or new 'challenger' banks but big, rich organisations who already have the customer relationships. I agree with Erik Tak, Head of ING's Payment Centre, who said at Trustech in Cannes that the people who will benefit most from this opening up of retail banking will not be FinTechs but Google, Apple, Facebook, Amazon and their ilk.

This has implications. Manthorpe speculated that Open Banking may expose some institutions to change and to competition from these internet giants that they simply cannot respond to. He even goes as far as to suggest that banks may well fail because of it! This is not wholly implausible because if customers access financial services through those platforms then there will be pressures for consolidation in volume-based retail banking pipes and not all banks will be able to achieve the operational efficiencies. If you think Open Banking is just some technical stuff about APIs and authentication, you could not be more wrong.

Angus McFadyen, Partner at Pinsent Masons

The heavyweight infrastructure underlying our transactions is often left well alone. That is changing.

The UK's cheque image clearing system went live in November 2017 and is ramping up to take over from the far less automated paper transport, sort and present approach. Established technology is being deployed to revolutionise processes, improve the clearing cycle for customers, and achieve maximum automation.

As cheque imaging ramps up through 2018, resilience, security and fraud will be key risks. They always are, particularly when new transaction handling processes are introduced. Across the industry, significant investment has been made to manage them. This will continue through 2018-19 with the renewal of the UK's Faster Payments

continued

Service infrastructure, which transacted £126 billion in December 2017 alone.

The same resilience, security and fraud risks are present - in different guises - with the adoption of PSD2-supported payment initiation. We'll see these services in our homes as we move through 2018 and major online retailers pick them up (following the footsteps of iDEAL in the Netherlands).

Finally, we must mention the regulators. They have been pushing hard on these risks, becoming less tolerant of legacy system issues - in 2017, amidst a number of bank system outages, the FCA identified resilience as a matter that'll be of continuing focus year on year, with firms being required to publish outage statistics.

The principle of transparency is being taken further in 2018 around security incidents - three regulations (PSD2, the GDPR and the NIS Directive) are to come in and oblige some institutions to notify regulators and customers of security incidents - up until now, there have been no firm rules requiring this. A big question remains - with greater transparency, leading to more incidents in the news, will the industry sow greater concern, or a malaise, with customers?

Dr Michael Salmony, Executive Adviser at equensWorldline SE

We have all seen the massive cyber breaches and the rampant identity fraud of the last years. We all experience daily the horror of having to deal with countless user IDs and passwords and filling in endless forms on the internet. The time is ripe to set up modern identity solutions that are Secure, Simple-to-use, Private and Pervasive: 'SSPP Authentication.' Current EU initiatives are focussing on government-issued identities and how to make them interoperate across Europe (eIDAS) but we now need to think beyond this. Instead of the current isolated silos from government and industry, we need a federated system where multiple identity providers (government, commercial entities, social media, mobile operators, banks etc) verify the rights of access which can then be used by multiple replying parties (government services, online platforms, the Internet of Things ('Iot')...). That leads to a four corner model that we know from banking and payments and shows that SSPP Authentication is a real opportunity for banks. It is firstly a strategic opportunity for banks to win back the position as the customer's main trusted partner against the onslaught of social media platforms now offering very non-private online 'identity' services. It is secondly also a commercial opportunity for banks: the Nordics have shown that it is good business for banks to provide reliable identity - and the margins are much better than for payments and the volumes are much bigger too (you log on/identify yourself many more times per day, than you pay per day).

Of course one must also employ modern technology - not 1970's-style user ID/password, or rigid two factor - going forward. There are many mature SSPP solutions available, from biometrics to modern 'data'/'user'-based identity. The latter uses information about a person's habits, location, devices, social media profiles etc with smart analytics to give seamless recognition (which the customer likes), massive fraud reduction (which the banks like) and much reduced transaction abandonment (which merchants like). Many mature solutions are now available and used by thousands of businesses. In future such services will also be provided by forward thinking banks under Open Banking, since these smart banks are offering commercial bank-verified age-ID API, bank-verified shipping address ID, etc since they have to open up with PSD2 APIs anyway[5].

Finally it is worth noting that we actually should not be talking about 'identity' (formally a term used to identify a natural or legal person). Nowadays one must also identify/authenticate programs (apps), devices (IoT) and more. It's no longer only about people and companies. Indeed very rarely is the real name/identity required - pseudonymity is the way forward, also in terms of improving privacy. The cigarette vending machine needs to verify that the customer is over 18; it is none of its business what the customer's name and passport number are. Authentication by pseudonym/alias reveals only the attributes that are necessary. This data minimisation is a requirement of the GDPR and hence it is high time we moved away from revealing the whole identity.

We must also abandon the thinking (e.g. in eIDAS) of a linear scale of trust (low/mid/high) - instead we must authenticate attributes (is she over 18, is he allowed to enter here, is that really the company's address, is it allowed to see my balance...) which cannot be placed on a linear scale.

Thus Secure, Simple-to-use, Private and Pervasive authentication is the future - and banks can and should play a key role in this space to protect us from crime and fraud and to make our online lives easier and truly enable the online and offline economy.

Michelle Cohen, Member at Ifrah Law

Cryptocurrencies became a 2017 phenomenon. People who, a couple of years ago, may have thought a 'bitcoin' was something you used to play games at Dave & Buster's suddenly sought to be part of the next Initial Coin Offering ('ICO'). The interest around cryptocurrencies and their ICOs will continue into 2018. Along with the popularity comes interest from regulators in the US. In July 2017, the Securities and Exchange Commission's ('SEC') Office of Investor Education and Advocacy expressed its view that ICOs may be subject to federal securities laws and SEC regulation: "Depending on the facts and circumstances of each individual ICO, the virtual coins or tokens that are offered or sold may be securities. If they are securities, the offer and sale of these virtual coins or tokens in an ICO are subject to the federal securities laws."

On 4 December 2017, the SEC's new 'Cyber Unit' shut down an ICO by PlexCorps and its founder, Dominic Lacroix. Mr Lacroix recently received a prison sentence in Quebec for continuing to solicit the sale of PlexCoins, in violation of a previous order by the Financial Markets Administrative Tribunal of Quebec. PlexCorps had already raised $15 million from thousands of investors, promoting to investors that they could see a return of over 1000% within just 30 days.

Image: MirageC / Moment / Getty Images

On 11 December 2017, SEC Chairman Clayton issued a Statement providing his guidance on ICOs. While he recognises ICOs as encouraging innovation, he also asserted that they may be regulated as securities: "I believe that initial coin offerings - whether they represent offerings of securities or not - can be effective ways for entrepreneurs and others to raise funding, including for innovative projects. However, any such activity that involves an offering of securities must be accompanied by the important disclosures, processes and other investor protections that our securities laws require. A change in the structure of a securities offering does not change the fundamental point that when a security is being offered, our securities laws must be followed."

The same day, the SEC issued a cease and desist order to Munchee Inc., a restaurant app developer that had promoted an ICO for 'MUN tokens.' The agency focused on the fact that Munchee's investors would anticipate that profits would be derived from the significant entrepreneurial and managerial efforts of others (Munchee and its associates). This is a key element of the SEC's analysis - i.e., whether the future efforts of the issuer and any promise to establish a trading system for the token are expected to increase the token's value.

We anticipate the SEC will continue to carefully review ICOs, focusing on promotional materials and offerors' representations. While each situation is different, the SEC's guidance thus far indicates that it will be aggressive in taking action where it believes the cryptocurrency offering is a securities offering.

1. http://www.wired.co.uk/profile/rowland-manthorpe
2. http://www.wired.co.uk/article/open-banking-psd2-regulation-banking
3. https://www.ft.com/content/9c1e4b06-328b-11e4-93c6-00144feabdc0
4. https://www.innopay.com/content/digital-identity-how-banks-can-position-themselves-their-customer-s-online-lives
5. See M. Salmony 'Access to accounts: Why banks should embrace an open future' in Journal of Payments Strategy & Systems, vol. 8 no. 2, pp 157-171, May 2014.

NEWS ANALYSIS

EBA finalises guidance for firms outsourcing to cloud

The European Banking Authority ('EBA') issued on 20 December 2017 its final report on 'Recommendations on outsourcing to cloud service providers' ('Recommendations'), guidance which looks to provide financial institutions ('FIs') with further clarity on supervisory expectations across Europe for firms adopting cloud computing. The Recommendations follow a consultation on the subject published in May 2017, and also build on the 2006 outsourcing guidance from the Committee of European Banking Supervisors, which will in time be updated and should be read in concert with the Recommendations. UK firms will be aware that guidance on outsourcing to the cloud was issued by the Financial Conduct Authority ('FCA') in July 2016.

"The Recommendations are, for the most part, principles-based and as such are written at a high level," explains Tim Wright, Partner at Pillsbury LLP. "This is consistent with the approach taken in the UK and in a number of other EU Member States. Whilst at the consultation stage, some of the respondents argued for a more detailed, prescriptive approach, the EBA's stance enables each firm to take into account its own policies and procedures, IT infrastructure and organisational design, as well as industry best practices, when selecting and contracting for cloud computing and other cloud services. Where the guidelines are specific and detailed, the requirements generally follow industry practice such as the requirement for a right to terminate where planned changes to subcontracted services would have an adverse effect on the risk assessment of the outsourced services."

The Recommendations cover five major areas, including data and systems security, supply chain oversight ('chain outsourcing') and access and audit rights. The Recommendations seek to identify and manage risks for firms in relation to the cloud while also clarifying applicable regulatory requirements for firms who may wish to adopt cloud services; the EBA also seeks to foster supervisory convergence in terms of the expectations and processes applicable to the cloud.

Section 4.1 of the Recommendations contains a discussion of how FIs looking to outsource to the cloud should perform an assessment on which of their activities should be considered as 'material' before commencing outsourcing. Firms should consider, *inter alia*, the criticality and risk profile of the activities to potentially be outsourced, and what the impact of disruption to such activities could be for revenue. "Only material cloud outsourcings will need to be notified," said Wright. "Previously some EU supervisors required notification of non-material cloud outsourcings and some didn't. This may help to speed up the sales and contracting processes where a cloud outsourcing is non-material."

"The materiality risk assessment, and hence notification to the competent authority where an outsourcing is determined to be material, should be undertaken prior to the outsourcing taking place," continues Wright. "The firm also needs to maintain a register of all cloud outsourcings, material and non-material. Information from the register, together with a copy of the cloud outsourcing agreement, should be made available to the regulatory authority on request."

The Recommendations will become applicable on 1 July 2018.