EMERGING PAYMENTS ASSOCIATION

VOICES OF THE EPA

THE FUTURE OF PAYMENTS REGULATION

VOICES OF THE EPA

Sponsored by

moorwand

MARCH 2020

Emerging Payments Association
The News Building,
3 London Bridge Street,
SE1 9SG, UK
Tel: +44 (0) 20 7378 9890
Web: emergingpayments.org
Email: info@emergingpayments.org
@EPAssoc
Emerging Payments Association

CONTENTS

FOREWORD

ALISON DONNELLY
DIRECTOR
FSCOM, LEADER OF EPA'S PROJECT REGULATOR

The Emerging Payments Association's Project Regulator brings our members together to consider regulatory issues, provide feedback to the regulators and influence change.

While the second Payment Services Directive (PSD2) is still in the final throes of implementation, it's clear to us that now is the right time to begin considering the changes that could, and should, be made to continue to improve and enhance our payment services market.

Overall, we are satisfied that bringing payments into regulation more than ten years ago created opportunities for emerging payment businesses. This was the objective that the European Commission set for the first Payment Services Directive (PSD1), which was eventually agreed in 2007 and implemented in 2009. The theory was that to drive greater competition in the payments market the same consumer protection standards had to be applied to all payment service providers. It was believed that the market was skewed in favour of banks because consumers valued the regulatory status of banks; obliging all payment service providers to comply with the same basic standards and protections would level the playing field. We can see from the growth, diversity and innovation evident among our membership that it has been successful.

PSD2 was agreed in 2015 and should have been fully implemented in the second half of 2019 but, for reasons explained below, deadlines have been extended. It has turned on its head the accepted definition of a regulated payment service by bringing into the fold players who don't touch the funds and those who don't even initiate payments. The impacts of these changes are yet to be fully seen but already we have fine-tuning changes to propose.

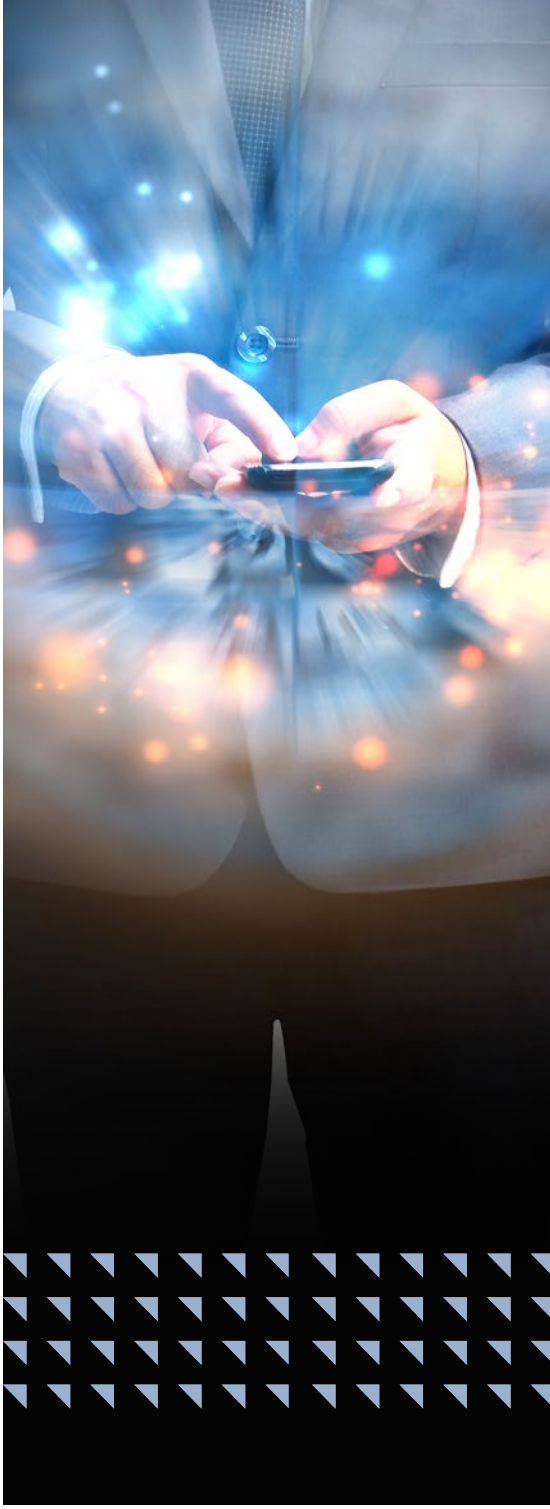
I would like to thank the contributors to this e-book, all of whom are members of Project Regulator and have taken time to put forward their own, personal view as to what they would like changed by the next iteration of the directive. This collection of individual articles will hopefully be the start of a conversation and we are keen to continue to challenge and debate the issues raised here and in other fora because the bearing of regulation, in terms of the shaping of the market, consumers' expectations and the cost of compliance, cannot and should not be underestimated. It's important to get it right.

The collection is referred to as 'the voices of the EPA' precisely because it marks the start of a discussion that Project Regulator intends to lead and facilitate as we continue to take stock of the regulatory changes, including those brought about by Brexit, over the months ahead.

I would also like to thank the EPA team for facilitating the work of Project Regulator and the delivery of this collection, particularly Tom Brewin and Tony Craddock for the wise counsel and editing support. ■

MESSAGE FROM OUR BENEFACTOR

VICKI GLADSTONE
COO
MOORWAND



It comes as a great honour for Moorwand to sponsor the Emerging Payments Association's 2020 Voice of Payments whitepaper.

As confusion grows around what is and is not possible within the increasingly complex world of payments legislation, Moorwand was passionate to become an EPA Benefactor of Project Regulator to encourage clear and open communication within the industry. Since coming on board last March, we have continued to push the agenda that members' views about the future of regulation in the payments sector must be heard throughout Europe and beyond.

The genesis of this paper was the frustration members felt with the constant evolution of payments regulation with many unintended consequences for our industry peers, and this guide aims to address these issues with practical feedback ahead of the next round of EU regulation.

Despite the pace of change, Moorwand sees payment regulation as the backbone of its success. Working with our Programme Managers we are able to see how the fast-moving world of payment technology and innovation can be implemented and work efficiently and effectively to unlock value. Moorwand wants its Programme Managers to feel in safe hands so that they can focus on product delivery to their end customers, whilst ensuring compliance throughout. Getting the regulation right is key to this.

Our great contributors consist of not only legal professionals but also leaders of businesses in the forefront of innovation in payments. It wouldn't have been possible without the depth of knowledge from great industry minds such as Alison Donnelly (fscom and the European Women in Payments Network), Myles Stephenson (Modulr), Mike Chambers (ex-CEO of BACS) and Fabien Ignaccolo (Okay), as well as leading payments lawyers, Chris Hill (Kemp Little) and Giedre Mitkute (Locke Lord). These individuals are using their voices to help facilitate the changes needed within our industry. ■

"The genesis of this paper was the frustration members felt with the constant evolution of payments regulation with many unintended consequences for our industry peers, and this guide aims to address these issues with practical feedback ahead of the next round of EU regulation."

SHOULD THE UK ADOPT A PSD3 OR CHART ITS OWN COURSE?

MYLES STEPHENSON
CEO
MODULR

Why would there be a third Payments Services Directive (PSD3)?

Before considering the merits of a further iteration of the Payment Services Directives, it is worth reflecting on the objectives of PSD2. Its primary focus was to drive greater competition in the payments market in part through the introduction of new services. Aligned to this is a strong focus on increasing consumer rights & protection alongside the development of stronger security and by association confidence in payments.

Its effectiveness is difficult to gauge, primarily due to the relative immaturity and newness of PSD2 and the fact certain elements are yet to be implemented. However, even considering this, some key elements (such as enabling access to accounts/payment initiation) are yet to see meaningful traction in customer-facing propositions. This is also the case in the UK market, where Open Banking has in effect been driving the implementation of the Third-Party Provider (TPP) elements of PSD2 into the market and driving consistency around standards to achieve this.

Critically, the timing of considering any future development opportunities should reflect the experiences of PSD2. This becomes even more critical on the basis that a key motivation would be to build on the original objectives and tackling those shortcomings as opposed to dealing with new topics.

What might a PSD3 include?

With this in mind, what could a future phase look like? As mentioned above, the natural starting point is to assume the objectives of PSD3 remain consistent with PSD2 and therefore understanding reasons for a lack of success in driving change becomes key. One natural reaction to any failings would be to consider whether requirements or technical specifications should be defined in greater detail to tackle the potential for the market not fully embracing opportunities due to a lack of confidence or understanding.

Driving greater and more detailed specification would certainly be a consideration, but one balanced with the role the regulators see themselves fulfilling. They have, until now, worked to the principle that this level of definition can be counterproductive and not part of their scope. It's unlikely that this position will change, not least

"Critically, the timing of considering any future development opportunities should reflect the experiences of PSD2."

because Regulators are lawmakers and supervisors, not technologists.

A PSD3 could bring a wider range of accounts into scope of the regulations. To help drive the innovation agenda further and faster, PSD3 could also include provisions to drive the implementation of pan-European instant payments, essentially forcing the roll out of SEPA Instant. This of course depends on the timeframe of any new regulations vs the speed of rollout driven naturally by market demand in the meantime.

Should the UK adopt PSD3?

The final question is whether the UK's interest would be best served continuing to develop the payments regulations at a country or regional level. Whilst being mindful of the political situation, and, although fluid, becoming slightly clearer, it is also helpful to consider the role the Financial Conduct Authority (FCA) has played in the European and global regulatory environment to date. The FCA is very much seen as an innovator and leader at a global level and at the forefront of regulatory development in financial services and enablement of markets.

Based on this, the question then becomes not whether the UK should adopt PSD3, but rather, if the UK should drive PSD3. Clearly, in a post-Brexit world, the opportunity to do this directly will be limited, but the UK could feasibly implement its next set of Payment Services Regulations aligned to the current PSD2 objectives. The UK's focus would then be to drive changes further in the likely direction of any PSD3, keeping the market moving forward and driving further benefit. This might set out the stall for a broader PSD3 for Europe to adopt or build on in the future.

At this time though, the risks of developing a UK specific approach would be bold and introduce the potential risk of divergence during a period of increased complexity and some uncertainty. As a result, it would make more sense for the FCA to ensure consistency with the regulations set out by our European neighbours in a post-Brexit UK. The principles of PSD2 are hard to disagree with, and the same is likely to be true of any PSD3, so there's perhaps no ideological reason not to. Leaders may also take a view that financial services firms have already had a significant amount to deal with in setting up parallel operations across Europe to maintain European market access post-Brexit and may not think it wise to increase the burden of operating in the UK and serving the UK market by driving regulatory divergence. It's not in anyone's interest to force firms to the point of choosing between the UK and the EEA by making the two markets so different from one another that it is too complicated to serve both. It's also important not to dismiss this as an anti-Brexit mindset; it's not done the Singapore Financial Services and FinTech scene any harm that the Monetary Authority of Singapore has worked to align itself closely with European regulatory framework, and not just in payments, making it a natural landing pad for European businesses looking to extend eastwards. ■

PULLING THE PLUG ON E-MONEY

GIEDRE MITKUTE
ASSOCIATE
LOCKE LORD LLP

Since its inception, e-money has been a delivery vehicle for innovative payment solutions, providing viable alternatives to more traditional financial and payments products and increasing competition in the marketplace.

The relevance of e-money based solutions in the future is very much dependent on the evolution of the regulatory framework to cater for developments in this sector and the broad range of products or services to which it may apply. In fact, a wholesale update to the regulatory framework may mean it is time to pull the plug on the concept of e-money, at least as we know it today.

The evolution of e-money

To make sense of what the future of e-money may look like, it is important to appreciate how far it has come. In the EU, the legal concept of e-money emerged from the first Electronic Money Directive (EMD1) in 2000. This was followed by the second Electronic Money Directive (EMD2) in 2009, aimed at solving some of EMD1's shortcomings by introducing a clear and technology-neutral definition of e-money, removing barriers to market entry for e-money issuers and, to ensure a level playing field, aligning the regulatory

requirements to those applicable to other payment service providers under the first Payment Services Directive issued in 2007, which was replaced with the second Payment Services Directive (PSD2) in 2015. EMD2 has been in place for over ten years and PSD2 has been in place for four years; both directives could, in the context of an ever-evolving payments landscape, benefit from appropriate revision.

E-money products and services continue to evolve. It started with prepaid products such as Mondex, with monetary value stored on the chip of a card (practically unheard of these days). Its earliest application was as a form of stored value facility for making payments, typically of a limited amount and for a limited period, such as a multi-store prepaid gift card or voucher. Today e-money is used for a broad range of card and account products, providing solutions for rewards and incentives, budgeting, travel, insurance pay-outs, business expenses, and corporate settlement and reconciliation just to name a few. E-money payments typically involve using a business's own network or a scheme-branded (Visa/Mastercard) prepaid card. However, these are no longer the only routes through which payment transactions are made. With the e-money issuers' ability to access other payment schemes for making credit transfers, standing orders and direct debits, either as a direct member or through a sponsoring member bank, these so-called "bank account lite" products have become commonplace. One of the more recent trends is the use of stablecoins, i.e. cryptoassets which, when backed by one or more fiat currencies and can be used for payments, closely resemble e-money.

In this ever-changing e-money and payment services landscape, regulators across the EU are grappling with the distinctions between a payment account, an e-money account and a bank account- and the appropriate legal framework that should apply to each one. A clear and consistent regulatory framework for these products is key to ensuring that e-money delivers on lawmakers' promises to promote innovation and competition. So, what would the logical next steps be for e-money in the future?

"Today e-money is used for a broad range of card and account products, providing solutions for rewards and incentives, budgeting, travel, insurance pay-outs, business expenses, and corporate settlement and reconciliation just to name a few."

Merging payments and e-money

There has been a divergence in the approach of EU regulators in the treatment of e-money and payment service providers across the EU. Providers of similar, if not identical, products may be required to be authorised as a payment institution (PI) or an electronic money institution (EMI), depending on the local regulatory interpretation in the EU country in which it seeks to be authorised. Brexit has served to highlight this divergence, as authorised EMIs and PIs seek second licenses in the UK or elsewhere in the European Economic Area (EEA) in order to continue providing services in those markets.

The issuance of e-money invariably involves the provision of payment services to enable the holder to use e-money to make payments. But does holding customer funds for the provision of payment services amount to issuance of e-money, which would then require authorisation as an EMI, rather than a PI? This situation is less clear and is often the subject of confusion and divergence across EU member states. An obvious solution to this problem is to merge the regulatory frameworks for e-money (EMD2) and payment services (PSD2) to ensure a more coherent and consistent approach. This idea is not especially controversial and was supported by a number of EU Member States' regulators, according to the European Commission's January 2018 report on the conformity of the transposition of the EMD2 (a report which was published over five years late). While the opportunity to implement such an overhaul was missed with PSD2, we may have better luck when it is refreshed in the future in the form of, say, the third Payment Services (and, perhaps, e-money?) Directive (PSD3).

What should PSD3 deliver?

Firstly, the e-money definition is crying out for a refresh to reflect the way e-money is used in practice. E-money is saddled with awkward terminology, such as a right to redemption which is just a type of transaction (repayment of the remaining balance to the e-money holder). The common denominator between customer funds held as e-money by EMIs and funds held for the purpose of providing payment services by PIs is that there is a monetary value on a payment account used for making payment transactions.[1] The scope of PSD3 should cover holding such value as a regulated activity, such that it can be undertaken by entities authorised under PSD3. Taking this approach, the concept of e-money could be disposed of altogether as superfluous, being already covered by the concept of funds held on a payment account, and there would be no need for a separate EMI license.

Currently, different capital requirements apply to EMIs and PIs, and with respect to PIs, the amount of capital required differing depending on the particular activity carried out. Combining e-money and payment services under a single PSD3 licensing regime would not remove the prudential (capital) requirements, but the amount required could be calculated in a different way. It could, for example, take into account the length of time the monetary value is stored and the payment services are provided. Adjusting PSD2's current tiered minimum capital approach to consider the length of time the monetary value is held, ensures that authorised entities are capitalised in line with the risks associated with their activities.

Finally, holding monetary value on a payment account by institutions authorised under PSD3 must be differentiated from accepting deposits (funds held in a bank account) which only credit institutions can do. The ability to hold customer funds without authorisation as a credit institution is crucial to maintaining competitiveness in the payment services market.

The unstable stablecoin question

One of the more recent developments in the e-money landscape is the emergence of stablecoins, i.e. cryptoassets backed by one or more fiat currencies or assets or specific algorithms to stabilise their volatility. The UK's Financial Conduct Authority (FCA) has said that assets/tokens which are pegged to a fiat currency and used for the payment of goods or services on a network could fall within the definition of e-money. Without a coherent regulatory framework, opinions on when stablecoins fall within regulated e-money/payment services are likely to diverge between EU member state regulators, creating an opportunity for regulatory arbitrage. To deliver on the PSD2/EMD2 promise of technological neutrality, and to achieve a level playing field for all payment service providers, stablecoins that are pegged to fiat currencies and are used for payments should be subject to the same prudential and conduct regime that applies to e-money/payment services. One way to achieve this would be by express inclusion of such cryptoassets within the scope of PSD3. ■

[1] *With the exception of money remittance, which is a payment service that does not, by definition, involve the creation of a payment account.*

SAFEGUARDING THE CUSTOMERS' MONEY

ALISON DONNELLY
DIRECTOR
FSCOM

Crown Currency Exchange, a business based in Cornwall that sold currency mainly to consumers for holiday spending but was also a small payment institution, collapsed on 4 October 2010 owing £22 million to more than 12,000 customers.

In the days and weeks that followed there were, naturally, many angry questions put to the government and the regulator, the Financial Services Authority (FSA), by those who lost money and their representatives as to why this was able to happen.

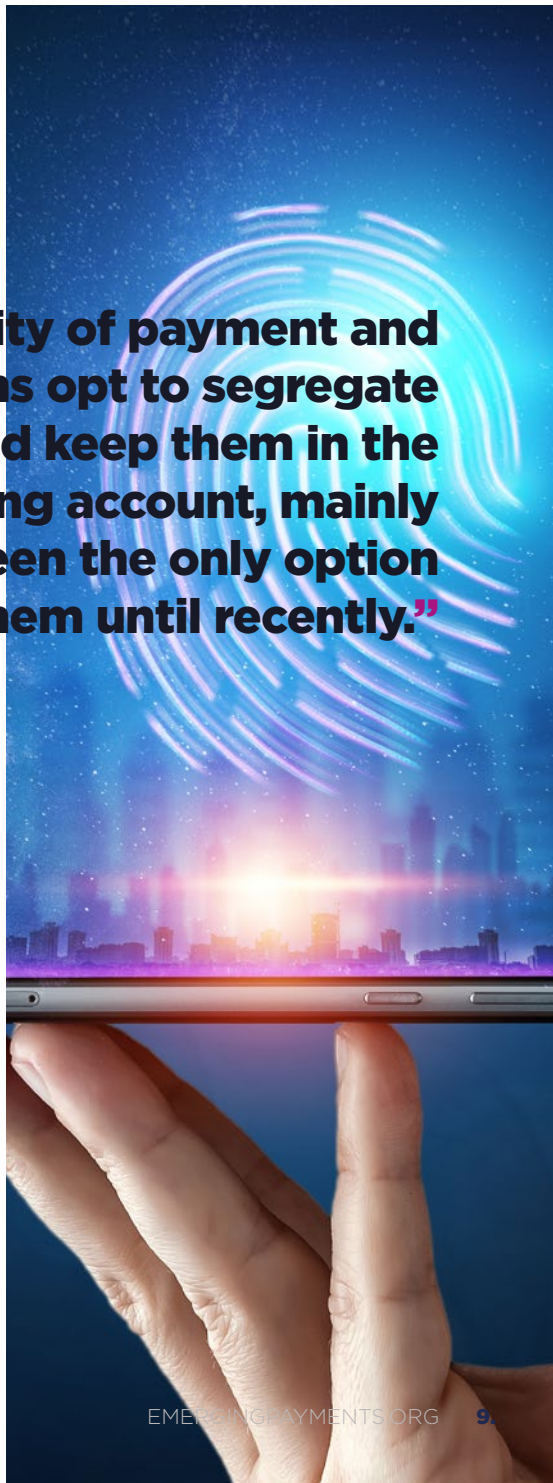
One of the many questions posed was why, when consumers could clearly see the FSA's logo on the business's website, was their money not covered by the compensation scheme.

In the UK, if your UK-authorised bank or building society goes bust, you can apply to the Financial Services Compensation Scheme (FSCS) for reimbursement up to £85,000, or £170,000 if the money was held in a joint account (balances up to £1 million are also covered in certain cases where the funds are held in the account temporarily, for example because of the sale of a home). This compensation scheme also kicks in if a credit union, mortgage adviser, investment firm, pension provider, insurance company or debt management company fails, but not if a payment institution or an e-money institution collapse.[2]

When a payment or e-money institution collapses

If that happens, you have to rely on the payment institution or e-money institution having 'safeguarded' the funds it holds for you. The safeguarding provisions are stipulated by the second Payments Services Directive (PSD2) and the second Electronic Money Directive (EMD2), implemented through the Payment Services Regulations 2017 (PSRs) and the Electronic Money Regulations 2011 (EMRs) and interpreted by the regulator, the Financial Conduct Authority (FCA), in their approach document. They require authorised payment institutions, authorised e-money institutions and registered small e-money institutions to either hold funds received from customers for payment services or e-money separately from all other funds and place them in a special account held with an European Economic Area (EEA)-authorised bank or to cover the funds with an insurance or guarantee policy.

"The vast majority of payment and e-money institutions opt to segregate their funds and keep them in the special safeguarding account, mainly because this has been the only option available to them until recently."



The vast majority of payment and e-money institutions opt to segregate their funds and keep them in the special safeguarding account, mainly because this has been the only option available to them until recently.[3]

The legislative requirements for this safeguarding method are straightforward but, as is often the case, the devil is in the detail of the interpretation. As I have set out in detail previously,[4] and has been illustrated by the FCA's report of its thematic review of safeguarding,[5] the implementation of the safeguarding rules into the real life scenarios of the various business models, is very difficult and many firms are struggling to meet the FCA's expectations.

The difficulty with interpreting the rules

In some business models it's difficult to agree when funds should be safeguarded. For others, difficulties arise in immediately stripping profit and fees from the funds as they arrive from payment service users throughout the day, 24/7. And what surprises those new to safeguarding the most is that the FCA says that over-safeguarding (putting too much money into the special safeguarding account) is as bad as under-safeguarding because a judge may decide, in the event of the insolvency, that the funds in the account actually belong to the company, even though they are clearly marked and documented as being held for the benefit of its payment service users!

To further illustrate my point, consider an example. The legislation is clear when the safeguarding obligation begins (on receipt of the funds) but doesn't clearly specify when the obligation ends. The FCA's approach document states that it remains in place until the funds are 'paid out' to the payee or the payee's payment service provider (PSP).

'Paid out' isn't defined but we're going to assume it means when the instruction is given for the funds to be taken from the payment or e-money institution's account for sending to the payee, rather than when the payee actually receives the funds into their account (though this has been the subject of much discussion already with conflicting guidance coming from the FCA).

The difficulty arises when the payment or e-money institution wants to use a correspondent to hold or move the funds for them because it is cheaper and quicker.

> “However, the FCA’s findings in respect of how poorly safeguarding is implemented at present demonstrates there is no easy answer to this essential objective of consumer protection.”

If the correspondent is not a bank or is outside of the EEA, the payment or e-money institution cannot safeguard with the correspondent (because it is not a credit institution in the EEA). Instead, it will have to either hold matching funds in their EEA-authorised safeguarding account or cover it with insurance/a guarantee, both of which come with increased cost.

There are three solutions to this problem.

- One is to allow non-bank PSPs to be able to safeguard for the underlying payment service user without entering into the contract.
- The second is that payment and e-money institutions should be allowed to safeguard with credit institutions anywhere in the world[6], providing the institutions meet specific criteria. This is, in fact, what will be the case for UK payment and e-money institutions when the implementation period comes to an end following Brexit.
- The third is to allow the customers of payment and e-money institutions the benefit of coverage by the FSCS. This brings me back to the reason I mentioned Crown Currency Exchange. As a payments policy specialist in the FSA at the time, I was involved in working with HM Treasury to consider the options. The extension of FSCS coverage was considered and dismissed, as it had been when we implemented the second E-money Directive the year before, for being expensive and operationally complex.

No easy answer to protecting consumers’ money

However, the FCA’s findings in respect of how poorly safeguarding is implemented at present demonstrates there is no easy answer to this essential objective of consumer protection. This raises the importance of formalising the protection scheme so that protection is no longer left to chance but is guaranteed. The overwhelming problem with the method currently used by most payment and e-money institutions is that it relies on the safeguarding procedure being correct and properly followed on the day the payment or e-money institution calls in the administrator. Let’s face it, running the safeguarding procedure on that day is unlikely to be the top priority. ■

[2] For example, see https://www.fscs.org.uk/news/firm-news/premier-fx-limited-customers/ for a statement from FSCS regarding Premier FX, an authorised payment institution, also with permission for money remittance only, that went into administration in August 2018.
[3] While there are very few EEA-authorised credit institutions that serve the payment and e-money institution sector with accounts, there is even fewer providers of insurance/guarantee policies. The difficulty in securing safeguarding accounts is a significant and well documented problem.
[4] https://blog.fscom.co.uk/payment-services-making-safeguarding-work
[5] https://blog.fscom.co.uk/dear-ceo-safeguarding-attestation-required-by-31-july-2019
[6] Under the directives, safeguarding accounts can only be held with EEA-authorised banks.

UNLOCKING STRONG CUSTOMER AUTHENTICATION (SCA)

FABIEN IGNACCOLO
CEO
OKAY

While the first Payment Services Directive (PSD1) brought payments into the scope of regulation for the first time throughout most of Europe, the second Payment Services Directive (PSD2) will be known as the real game-changer; the one that created the market for new players to infiltrate the systems of the traditional providers to give customers a different way to access services and get more from their own data.

I'll explain the nature of the new players below, but my interest lies in the second significant change introduced by PSD2, which was brought in to counterbalance this new openness: Strong Customer Authentication (SCA).

Under the new rules, payment service users must use two of three factors to authenticate themselves when accessing data and giving payment instructions. The three factors are possession, knowledge and inherence; in other words:

- something you have (like a mobile device);
- something you know (like a password); and
- something you are (like your fingerprint)

Put like this, it's not overly complicated and we, as consumers, are used to verifying certain transactions with two factors. However, its transition into day-to-day reality has not been easy. There has been a contentious

debate in the card sector because increasing friction in the card payment experience is likely to lead to abandoned sales, which impacts merchants who have no control, under these rules, as to whether SCA should be applied. As a result, stakeholders have been reluctant to develop the necessary software and hardware changes, to the extent that the European Banking Authority (EBA) agreed to extend the implementation deadline.

No-one can deny the rationale behind PSD2 was good. It aimed to spur innovation in the financial services industry in Europe, whilst advancing the fight against cybercrime, especially for 'card not present' purchases in a booming e-commerce market. Yet, even at this early stage, we can see that vital changes must be made to improve SCA for all involved. I believe that in 'unlocking' SCA in the card not present payment scenario we could simplify the process and provide a great business opportunity to a wider market.

"PSD2 brought payment initiation service providers (PISPs) and account information service provider (AISPs) into the scope of regulation."

Rebalancing SCA for merchants

Prior to the SCA requirement under PSD2, merchants had a certain level of discretion as to whether they would require further authentication from customers before accepting their payment and handing over the goods. This proved useful, for instance, where merchants pride themselves on the ease and speed with which they enable consumers to make purchases. The cost to the merchant for this benefit is the risk they take if something goes wrong with the transaction. Under PSD2, the merchant no longer has any control over whether SCA is applied or not. SCA doesn't always have to be applied; there are nine exemptions listed in the legislation, but it is up to the customer's card issuer to decide whether an exemption can and should be applied.

Looking ahead, I believe PSD3 should unlock SCA by rebalancing the control between merchants/acquirers and issuers and allowing the well-established chargeback system to play its role in keeping merchants and their acquirers honest in their responsibility to fight fraudulent payments. A good example of how this could work in practice is for merchants with recurring customers who have created an account; SCA could be applied once, perhaps to register, but not to every subsequent transaction.

Rebalancing SCA for the new payment service providers

As I mentioned above, PSD2 brought payment initiation service providers (PISPs) and account information service provider (AISPs) into the scope of regulation. Payment initiation and account information services have not been the norm in the UK and while some 50 new players have become authorised in the UK as PISPs, and 150 have registered as AISPs, consumers' use of, and familiarity with, their services remains low so far.

The European Commission sees PISPs as a viable alternative to card usage in e-commerce. A large merchant could become a PISP and offer customers the opportunity to pay directly from their bank account rather than use their card. From a customer's perspective, however, paying from their account could be just as much of a headache as paying by card, since responsibility for the authentication lies with the payment account provider, known as the account servicing payment service provider (ASPSP). Therefore, the customer has to use the PISP's app to initiate a purchase, then use another banking app from the ASPSP to complete the authentication. This is not particularly "frictionless", and is frankly quite worrying from a user journey perspective. Instead, allowing the PISP to take responsibility for the SCA challenge would be helpful.

The need for an SCA authority

If merchants or PISPs were given the option to perform the SCA challenge themselves, how could an ASPSP trust the challenge? One would need an independent authority that could set the SCA standards, audit the SCA process and deliver compliance, in much the same way as the Payment Card Industry Data Security Standard (PCI DSS) currently does.

On the one hand, and since trust is paramount here, mechanisms would have to be invented to create such trust throughout the process. On the other, existing systems could be leveraged, such as eIDAS - Electronic Identification, Authentication, and Trust Services - an EU regulation on electronic identification and trust services for electronic transactions in the European Single Market. Card issuers or ASPSPs could then whitelist merchants and PISPs that are accredited or implement further controls if accumulated payments reach a certain threshold. This would be a new service, as well as a way of sharing the responsibility again when it comes to fraud and chargebacks.

All this seems rather complex to put in place for a few PISPs, but I believe this would be a crucial first step. Unlocking SCA would present an enormous opportunity as it could be sold as a new service outside the financial world and could help build a Digital Single Market.

Turning SCA into an opportunity: The long-term

Yes, ASPSPs could sell this new service outside the financial sector.

The final missing piece would be for banks and SCA providers to offer a digital identity. Many European countries – such as the UK or France – have initiated government-run ID programmes, although the market adoption of these is still very low. The Nordics, on the other hand, have succeeded with similar initiatives around BankID-like projects. When governments in the Nordics saw customers trusting banks not only with their money, but also their digital identity, they saw this as an opportunity to leap into the digital arena. BankIDs – or the equivalent – are owned by the banks of each country in the Nordics (Norway, Denmark, Sweden and Finland), but the use has extended to government services and others that require ID authentication. In Sweden, more than half the use of BankID is from outside the financial sector.

Such a combination between SCA and digital identity would be very useful when a merchant needs to know who they are selling to. For instance, this service could be used to check that a person is above the legal age to access a service, it could automate the process of buying or renting an apartment and could even secure access to your company email. In the financial industry, it could be used to manage insurance agreements, communicate with the government, onboard new customers (KYC) for your service and would make it easier for challenger banks to open new accounts.

Business to business (B2B) would be another major beneficiary of this new service. There are many ways to defraud a company. One common method is by changing the contact information regarding an invoice. An invoice from a vendor is intercepted by a fraudster, who changes the beneficiary account number and then forwards the invoice to the correct recipient. Using an SCA challenge would prevent this.

So, although SCA is seen by the financial services industry as a hurdle and an extra cost, if handled properly in PSD3, it could accelerate innovation in the financial industry and other sectors, creating new businesses and new opportunities. The first responsibility of the EBA should be to lay the foundation for an unlocked SCA in a future PSD3, allowing SCA to develop outside the EBA and the financial sector to become the cornerstone of the Digital Single Market. ■

CHANGING THE FOCUS OF OPEN BANKING RISK FOR DATA

CHRIS HILL
COMMERCIAL TECHNOLOGY PARTNER
KEMP LITTLE LLP

One of the major talking points surrounding PSD2 was the introduction of two entirely new categories of payment service: payment initiation services and Account Information Services (AIS).

These were introduced largely to regulate services that were already being provided, particularly in continental Europe, without any regulatory oversight. However, the introduction of not only these new types of regulated service providers, commonly referred to as third party providers (TPPs), but also the regulatory structures through which banks and other account providers are obliged to provide consent-driven account access to such TPPs, opens up enormous potential for new innovation. This is particularly the case for account information services, where there is a myriad of possibilities for the usage of transaction data to create services that benefit consumers and small and medium-sized enterprises (SMEs) and assist in the growth of the economy overall.

Huge progress has been made in open banking in the UK, especially through the Open Banking programme driven by the Competition and Markets Authority (CMA) and the Open Banking Implementation Entity (OBIE). However, in relation to AIS there are a few points of difficulty caused by the structure of its definition and subsequent interpretation by regulators, which threaten to slow innovation significantly without any tangible benefit to customers.

"In order to get to a point where you can display consolidated information in an online service, one first must extract the data from the payment accounts."

"Huge progress has been made in open banking in the UK, especially through the Open Banking programme driven by the Competition and Markets Authority (CMA) and the Open Banking Implementation Entity (OBIE)."

Extraction vs. display

The first point of difficulty revolves around the difference between (a) the access point to the payment accounts needed to extract data, and (b) the way in which that data is then used and distributed. The definition of the regulated activity of AIS is essentially purposive: the activity is providing an online service which provides customers with 'consolidated' information "on" one or more payment accounts held with another payment service provider. In other words, the regulated activity is the display of the "consolidated information". When the definition was originally put together, it was looking mostly backwards at existing account aggregation services, where screen scraping (the use of a customer's login details to access accounts on their behalf) was being used to extract the data, and that data was then being used by the same entity to display aggregated information across multiple accounts.

The need to regulate such an intrusion into a customer's financial information makes complete sense, but the definition of the regulated activity ignores the fact that there are not one but two separate elements within any such service. In order to get to a point where you can display consolidated information in an online service, one first must extract the data from the payment accounts.

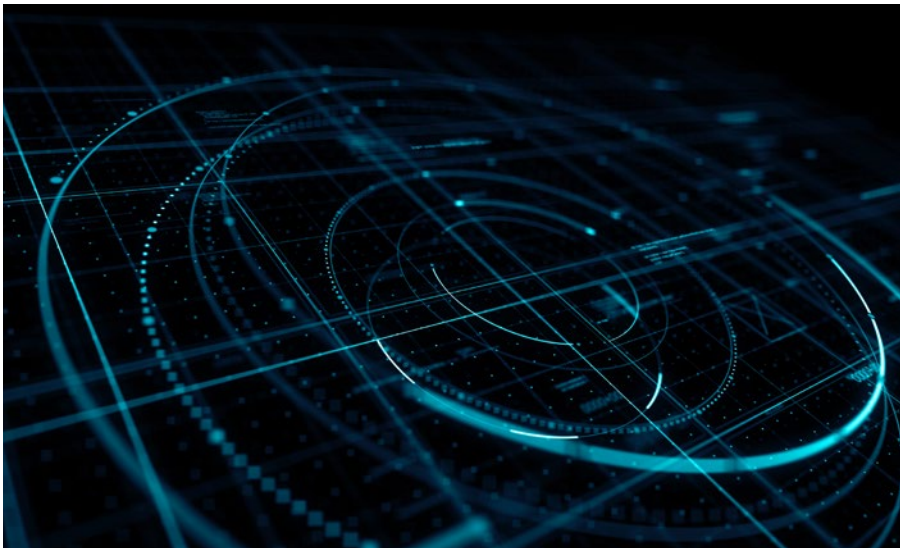
The difficulty arises because the extraction of data does not necessarily involve the provision of an online service displaying consolidated information, and the display does not necessarily involve extraction. It is perfectly possible for the two functions to be split, whereby one entity extracts data (but does not provide an online portal displaying it) and another entity then takes that data from the first company and does provide the online service to customers.

The splitting of these two functions is beneficial to the industry: it allows those who are skilled at building systems which connect to banking application programming interfaces (APIs) to focus on the efficient extraction of the data from the payment accounts, whilst those with the different skill set of data manipulation and display can focus on doing that. The fact that the definition of AIS lumps both functions together, and technically only regulates one of them, creates something of a Catch 22 situation for the "extractor" companies that want to provide the extraction element of this process but not the display: in order to extract the data they need to be registered as an Account Information Service Provider (AISP) in order to gain the access credentials that the banks demand, even if they have no desire to display it themselves; but in order to attain the AISP registration they have to meet the requirements of the AIS definition – which are all about display.

On the flip side, companies that are displaying data but have no desire to access the payment accounts directly are also given the keys to the accounts in the form of the AISP registration, which entitles them to demand account access from a bank even if they have no intention of doing this themselves. By way of analogy, this is a little like saying that anyone who wants to ride in the back of a car taking in the passing landscape, has to have a full driving licence and will be given their own set of car keys, even though you only need one driver sitting in the front. This can result in a conceptual contortion, with extractor companies having to create a display element in order to get their registration and car keys; while companies that are displaying data that has already been extracted by a regulated AISP need to have a driving licence to do so, even though they are bound by contract to use the data only as required by the customer.

The market has created some useful workarounds to these issues, whereby extractors classify themselves as technical service providers and issue access tokens (the keys) to the banks in the name of the registered AISPs who are just providing display. But this is surely an unsatisfactory situation, whereby the entity which is actually entering the bank's data vaults does not have to be regulated, but the company which simply takes that data and displays it to the customer does. If the purpose of introducing this new regulated service was to ensure that access to customers' financial information was handled more safely, this is arguably an odd way to approach it. The current definition also creates situations where a company can become registered as an AISP for providing one service which extracts and displays account information, but can then use those same access keys to extract data and use it in other services which, because they don't involve display of the data, are not technically regulated within the scope of AIS at all.

I think there are two possible routes through which a third Payment Services Directive (PSD3) could address these issues. The first route is to regulate access to accounts on the one hand, and display of financial information on the other, as two separate activities. The second



is to regulate only the access to accounts, on the basis that it would be up to the extractor company to control, by contract, the use of the data by any further recipient. This would ensure that usage of that information was carried out only in accordance with the wishes of the customer. There are arguments for and against each approach, which hang mostly on the viability of determining a workable regulatory perimeter based on the type of data being displayed.

"Consolidated information" and the regulatory perimeter

This leads to the second difficulty posed by the AIS definition, which is that it all revolves around the concept of "consolidated information on one or more payment accounts", but there is no useful guidance on what "consolidated information" actually means. In many instances this makes it almost impossible for those looking to provide data-related services to know whether their services will fall within or outside the regulatory perimeter.

Again, whilst the definition was probably created with a particular set of existing account aggregation services in mind, where it is obvious that the information displayed is still sensitive, it does not deal at all well with the almost infinite gradations of derivation that data can undergo.

Take an example: if Company A is taking transaction data and displaying that raw data, clearly that falls within the definition of "consolidated information on one or more payment accounts". If Company A then passes that transaction data to Company B, and Company B mixes it with location data to produce a new set of data showing the location where the customer spends most money, the position is less clear, and therefore Company B may be uncertain as to whether or not it needs to be regulated. If Company B then gives that data to Company C, and Company C mixes that data with merchant data so that it can display loyalty offers a customer is entitled to, it is even less clear. From a realistic point of view, it seems odd that the treatment of that last set of data could potentially be subject to a regulatory licence, even though the information being displayed is so very far removed from the original transaction data, and probably reveals little to nothing about the financial position of the customer.

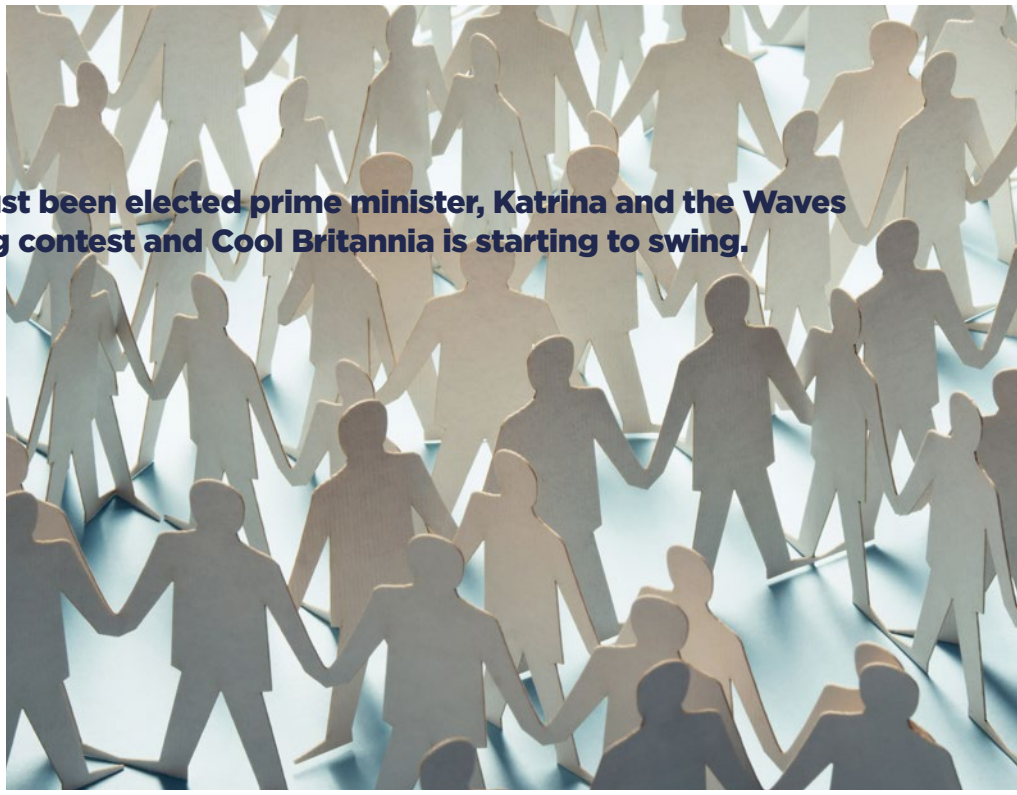
There is a useful parallel here in market data licensing, where data sets, which are licensed out for often significant amounts of money and are heavily guarded by contract are often permitted to be used to derive new data. The standard position is that if the original data set has been derived to a point where the original data cannot reasonably be reverse engineered from it, it is out of scope of the control of the licensor. Therefore the display elements of AIS should be regulated in a similar way, such that the display of consolidated information should not be regulated under PSD3 if it is not reasonably possible to (i) derive the original transaction data from it or (ii) to discern the customer's financial status or wellbeing from it. This is not to say that the use of derived data should not be controlled at all, as other bodies of law such as General Data Protection Regulation (GDPR), contract, intellectual property and confidentiality can be used to regulate that usage – but rather that the purview of a financial regulator should be limited to that which demonstrably pertains to a customer's finances.

Conclusion

The creation of AIS and the related structures mandating banks' provision of access to accounts has already brought real benefits to many companies and their customers. It is in no way surprising that innovators have – as is always the case – created services which legislators could not have been expected to legislate for. In the case of AIS in particular, in order to foster certainty around a sensible regulatory perimeter for those looking to innovate, and to achieve the safety levels which will facilitate the adoption of new services, it is necessary to revisit the definition of the regulated activity so that its constituent parts are each addressed in a way which is proportionate to the risks they pose. ■

EDUCATION: THE 'SECRET SAUCE' FOR THE SUCCESSFUL IMPLEMENTATION OF PAYMENTS REGULATION

MIKE CHAMBERS
DIRECTOR
EAZY COLLECT



It's 1997 and Tony Blair has just been elected prime minister, Katrina and the Waves have won the Eurovision song contest and Cool Britannia is starting to swing.

The new prime minster quickly set out his priorities for office and 'education, education, education' is placed at the very top of the political agenda. Whilst one may argue that such a reality has never truly matched this rhetoric change; the importance of effective, accessible and inclusive education cannot be underestimated. But what part should education play in payments and what has education got to do with the future of payments regulation? I would argue that payment providers ignore embedding end user education into their regulatory change programmes at their peril.

Put simply, customer education refers to the set of activities or processes a business puts in place to equip customers with the knowledge and skills needed to make the most out of its product or services. As an industry we should ensure that education is more than just a regulatory or compliance response. A positive consumer-focused education programme will increase trust, build confidence and generate loyalty. Conversely, a poorly designed consumer education programme will lead to complaints, disenfranchisement and a prize for the provider's competitors. In the UK, we have the benefit of two significant payment related initiatives that prove the case for the role of clear and impactful consumer-focused education when successfully delivering significant change.

- Valentine's Day in 2006 saw the successful introduction of chip and PIN in the UK. Described by the UK Cards Association (now part of UK Finance) as the largest change to the way we pay since decimalisation in 1971. The multimedia campaign 'Safety in Numbers' was created by Saatchi and Saatchi and played a significant role in the awareness, consumer adoption and continued smooth operation of card-based transactions. The 'Safety in Numbers' campaign cemented the successful introduction of chip and PIN across the UK.

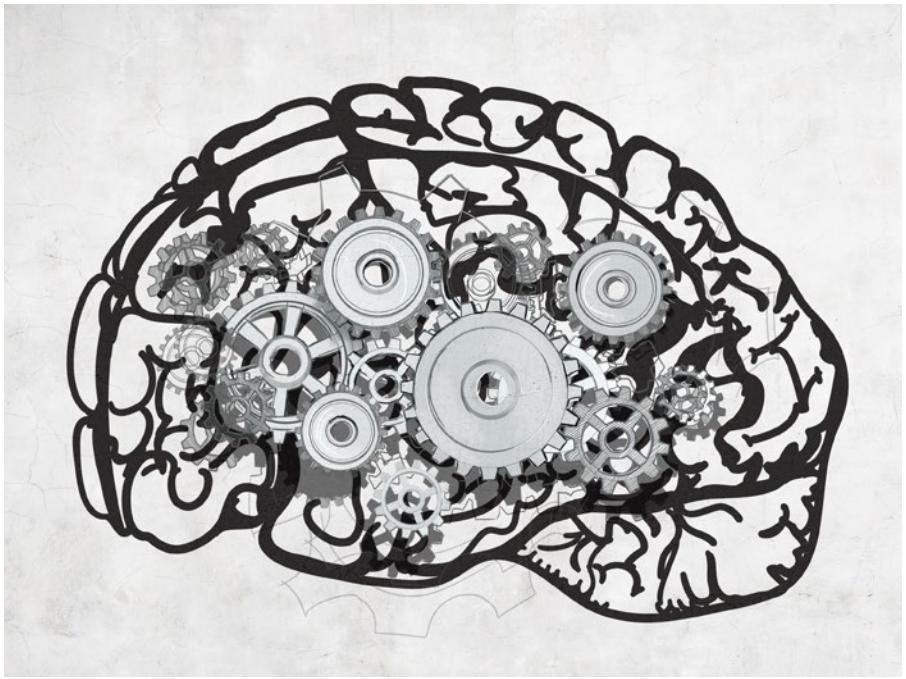
- From its launch in 2013, Bacs Payment Schemes Limited (now part of Pay.UK) recognised the importance of communicating with consumers to promote a smooth, simple, reliable and stress-free current account switch experience. A clear communication programme focussing on awareness, confidence and trust that led to over six million individuals, small businesses and charities choosing to make a significant financial decision.

Having led transformational change in payments both at a large bank and as a Payment System Operator of a systemically important payment system, my experience is that we must not assume that everything is straight forward from an end user perspective, we must explore potential unintended consequences before it is too late and we must never assume that the customer won't be interested. Instead, there are many facets to these considerations and the mantra of 'education, education, education' should feature centre stage.

In fact, the current roll out of Strong Customer Authentication (SCA) is providing a real time case study on the importance of end user communication. Receiving a 'payment declined' message at a Point of Sale (POS) device is not helpful and fails to communicate to the person purchasing their morning latte that SCA means that the contactless payment needs to be verified via CHIP and PIN this time. Equally the Barista needs to understand that a SCA check is being undertaken rather than believing the customer has drained their bank account dry.

From a fraud prevention perspective, SCA should be a step forwards but without an end user understanding of the reasons for a PIN check this could lead to people abandoning their use of contactless payments - beware of unintended consequences.

There are some great examples of payment providers implementing regulatory change supported by strong educational initiatives. For instance, electronic billboards in the windows of Royal Bank of Scotland (RBS) stating that all banks will be checking contactless payments more often (so be ready with your PIN!). These campaigns are accompanied by the hashtag '#ItsReallyMe', a fantastic example of an education imperative being soundly executed. There are clear examples that challenger banks too have also risen to the SCA education challenge. Monzo's use of creative in-app and watch notifications pre-warn that, rather than one's next transaction being contactless, they will need to verify the next transaction with a PIN.



My premise is that if we propose that the primary directive of schooling is to make students happy, confident, secure and valued then, as the payments landscape enters a period of transformational change, we should apply this principle to payments. The regulatory pathway beyond the second Payment Services Directive (PSD2) should make consumers' relationship with their banking partner a happy, confident, secure, inclusive, accessible and valued one. End user education should feature as an integral requirement of both the regulation itself and its implementation.

Whilst my argument is for appropriate end user education requirements to be built into the regulation, there is a danger of the extremes of a diktat at one end of the spectrum and the potential weakness of 'best practices' at the other. Regulation should include a specific requirement for appropriate principles-based education to support the regulatory outcomes of change. Each institution would then be accountable for delivering against the principles defined within the regulation.

Having suggested that payment providers ignore embedding end user education into their regulatory change programmes at their peril, perhaps we ought to be bold and adopt the principle of delivering effective end user education for the soon to be launched Request to Pay (RTP) and Confirmation of Payee (CoP) initiatives?

If the 'secret sauce' of successfully implementing payments regulation is education, then the principle of 'education, education, education' moves beyond compliance for compliance sake, reinforces our desire to 'Treat Customers Fairly' and should be a central tenet of our principles of business. ■

Emerging Payments Association

The News Building,
3 London Bridge Street,
SE1 9SG, UK

Tel: +44 (0) 20 7378 9890

Web: emergingpayments.org

Email: info@emergingpayments.org

@EPAssoc

Emerging Payments Association

About the EPA

The Emerging Payments Association (EPA), established in 2008, connects the payments ecosystem, encourages innovation and drives profitable business growth for payment companies. Its goals are to strengthen and expand the payments industry to benefit all stakeholders.

It achieves this by delivering a comprehensive programme of activities for members with help from an Independent Advisory Board, which addresses key issues impacting the industry.

These activities include:

- A programme of 70 events annually
- Annual Black-Tie award ceremony
- Leading industry change projects
- Lobbying activities
- Training and development
- Research, reports and white papers

The EPA has over 150 members and is growing at 30% annually. Its members come from across the payments value chain; including payment schemes, banks and issuers, merchant acquirers, PSPs, merchants and more. These companies have come together, from across the UK and internationally, to join our association, collaborate, and speak with a unified voice.

Emerging Payments Association
The News Building,
3 London Bridge Street,
SE1 9SG, UK
Tel: +44 (0) 20 7378 9890
Web: emergingpayments.org
Email: info@emergingpayments.org
@EPAssoc
Emerging Payments Association